Solving the Estonian ID Card Crisis: the Legal Issues

Arnis Parsovs
STACC OÜ, Estonia
University of Tartu, Estonia
arnis.parsovs@ut.ee

ABSTRACT

In 2017, Estonia experienced a cyber crisis caused by a vulnerability found in the smart card chips produced by Infineon Technologies AG. Since the affected chip was used in the electronic identity card (ID card) issued by the State to more than half of the Estonian population, the vulnerability posed a risk to the resilience of Estonian e-state and thus quickly escalated into a manageable crisis. This work studies to what extent, in such a national emergency, the involved parties were able to precisely follow the applicable laws and regulations in the field. We enlist the cases where the requirements were not fully followed, either due to the lack of technical preparedness, suboptimal decisions made under heavy time pressure, or the critical nature of the situation.

Keywords

Cyber Resilience, Electronic Identity, Cyber Legislation, eIDAS.

INTRODUCTION

At the end of August 2017, Estonian authorities became aware of a critical security vulnerability affecting the smart card chips produced by Infineon Technologies AG. The affected chip was used in more than 750 000[1] identity documents (hereinafter – ID cards) issued by the Estonian State (ERR News 2017b). The chip was used to store the cryptographic keys enabling Estonian ID card holders to access e-services, give legally binding digital signatures and even cast an i-vote in national elections.

The flaw in the non-standard RSA key generation algorithm used by the chip provided a way to compromise the affected key using the computation power estimated to cost around $40 000 (Nemec et al. 2017). While no keys were compromised at that time, it was clear that it was only a matter of time before the flaw was exploited. These findings started the so-called Estonian ID card crisis, where the authorities had to focus on minimizing the security risks to the affected ID card holders, but at the same time ensuring continuous functioning of the e-state.

The ID card crisis was solved in a couple of months. The authorities announced the technical solution on 2017-10-25, when cardholders were provided with an option to patch their ID cards, either by visiting customer service points of the document issuer or by using software provided by the State to update the ID card remotely over the Internet. The security risk was largely mitigated on 2017-11-03, when the certificates containing the vulnerable keys were suspended. Cardholders were able to update (including remotely) their ID cards until 2018-03-31. On 2018-04-01, the certificates of the non-updated ID cards were revoked and the government considered the ID card crisis to be fully solved[2].

In this work, we study to what extent, in such a national emergency[3], the involved parties were able to precisely follow the applicable laws and regulations in the field. We describe a list of cases where the requirements were not fully followed, either due to the lack of technical preparedness, suboptimal decisions made under heavy time pressure, or the critical nature of the situation. The aim of this work is not to provide a definite legal interpretation, but rather to point out the legal and technical issues that emerged while resolving the crisis. We start by introducing the legal framework, the involved parties, and the specific issues being analyzed in the following sections of this paper.

[1] This covers more than half of the 1.316 million Estonian population.
[2] For a more detailed chronology of the Estonian ID card crisis and the analysis of the measures taken, see (Parsovs 2020).
[3] We note that while to some extent the situation was handled as an emergency, a state of emergency was not officially declared.

Legal framework and the involved parties

The Estonian State issues several types of credit card sized identity documents that contain a smart card chip that provides cryptographic functionality. These are the *identity card*, the *digital identity card*, the *residence permit card*, the *e-resident's digital identity card* and the *diplomatic identity card*. We use the common term "ID card" to denote all of these types of identity documents.

Each Estonian ID card contains two cryptographic keys with the corresponding certificates: an authentication certificate for digital identification in e-services and a digital signature certificate for giving qualified electronic signatures.

On the European Union level, qualified electronic signatures and other trust services are regulated by Regulation (EU) No. 910/2014 (The European Parliament and the Council of the European Union 2014) (hereinafter – eIDAS). The aspects not regulated by eIDAS are regulated in the Estonian national law – Electronic Identification and Trust Services for Electronic Transactions Act (Riigi Teataja 2016) (hereinafter – EITSETA).

The process of ID card manufacturing and issuance is presented in Figure 1. The ID cards are issued by the Police and Border Guard Board (Politsei- ja Piirivalveamet – PPA) as a public service. The aspects related to the ID card issuance are regulated by the Identity Documents Act (Riigi Teataja 1999) (hereinafter – IDA). For the ID card production, personalization and certificate issuance, PPA had a contract with the card manufacturer Gemalto (formerly Trüb Baltic AS). For issuance of the ID card certificates, Gemalto had a subcontract with Estonian Certificate Authority (CA) SK ID Solutions AS, which is a qualified trust service provider under eIDAS (hereinafter – the TSP). In the context of trust services, PPA is a registration authority (RA) of the TSP, whose duty is to perform the initial identification of the certificate holders.

To receive the ID card, the cardholder must accept the "Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia" (SK ID Solutions AS 2018b) (hereinafter – Terms and Conditions) agreement. The Terms and Conditions agreement is a legally binding contract between the cardholder and the TSP. It includes references to certificate policies, the Certification Practice Statement (SK ID Solutions AS 2018c), SK Trust Services Practice Statement and other statements of the TSP, which are considered to be a part of the contract. These policy documents and statements of the TSP are also considered to be legally binding towards any relying party that relies on the trust services provided by the TSP.

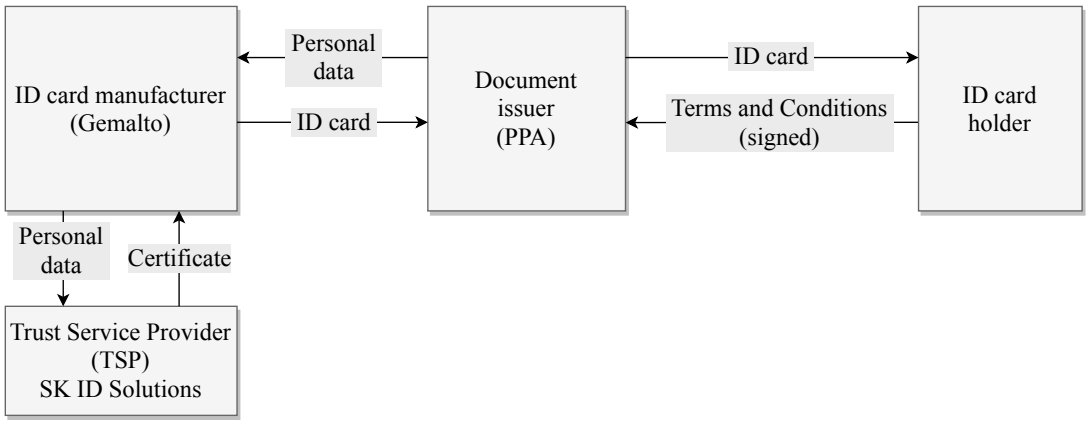


Figure 1. ID card manufacturing and issuance process

In the ID card crisis, the Estonian Information System Authority (Riigi Infosüsteemi Amet – RIA) played a key role in coordinating the crisis management. Among other tasks, RIA is responsible for the coordination and development of electronic identity and cyber security. The other relevant legal concepts and parties will be later introduced in the discussion of that particular issue.

RESTRICTING ACCESS TO THE PUBLIC CERTIFICATE DIRECTORY

On 2017-09-05, a press conference was held where the prime minister of Estonia together with other State officials informed the public of the ID card security risk. It was announced that, as a mitigation measure, the TSP had closed down the public directory containing the ID card certificates. As it was explained by the director general of RIA: "We closed the ID card public key database because without the public key being known it is not possible to use this security risk to attack the card." (Estonian Information System Authority 2017).

We note that the directory service is a trust service provided by the TSP. This service is used to obtain public keys of the ID card holders for the encryption use case. According to the TSP's Trust Services Practice Statement (clause 2.3.1 in (SK ID Solutions AS 2018c)), the service is accessible in a public data communications network 24 hours a day, contains valid certificates and is provided to any party to make inqueries about the certificates and their validity. The legal grounds for the directory service are also present in clause 9^4 (6) of IDA, which states that the certificates are publicly verifiable through the personal identification code of the cardholder.

According to the TSP, the directory service was closed based on the order given by PPA, which was substantiated by the ID card manufacturing contract concluded between PPA, Gemalto and the TSP. By ordering the closure of the directory service, PPA effectively forced the TSP to break its contractual obligations towards the relying parties. Later, on 2017-11-20, with the permission of PPA the directory service was reopened.

In practice, the service was technically still operating, but the ID card certificates were returned only to authorized contractual parties of the TSP. For IP addresses not explicitly authorized, the service returned incorrect data (i.e., empty response) as though the ID card certificates were not valid. In the whole restriction period there was no announcement made by the TSP to inform the relying parties of the non-compliant operation of the trust service. According to the TSP, the decision was made to protect cardholders and was approved by the TSP's auditor – the certification body TÜV Informationstechnik GmbH (hereinafter – TÜViT).

Restricting access to this information, which by law is public information, requires a legal basis. Clause 4 (1) 10) of the State of Emergency Act (Riigi Teataja 2015b) provides a possibility to restrict the right to freely access information disseminated for public use. This, however, requires the declaration of a state of emergency, which was not done. The law gives PPA and the TSP the right to suspend or revoke the certificates in case of suspicion that a private key can be used without the consent of the cardholder. We note that the legal framework and the public key infrastructure (PKI) does not foresee any other security measure than the invalidation of the compromised certificates. It was clear that the State could not afford to invalidate the certificates, as it would have immediately made the affected ID cards electronically unusable, endangering the healthy functioning of the e-state.

In practice, the restriction enforced by the directory service possibly had a very limited effect in mitigating the risk. This measure might have dissuaded only disorganized attackers, as certificates are attached to each digital transaction and have otherwise been accumulated by quite a few entities. A party seriously interested in obtaining a certificate could have used their legal rights to obtain the certificate from the TSP using an official information request. The decisive decision to close the directory service, however, might have achieved a public relations objective – showing that the parties were mitigating the risk.

TIMING OF THE VULNERABLE CERTIFICATE INVALIDATION

Two months after the beginning of the ID card crisis, on the night of 2017-11-02, after five hours of Cabinet meeting, the Estonian government decided to support the decision of the director general of PPA to suspend the vulnerable ID card certificates starting from 2017-11-03 (ERR News 2017a).

The decision of PPA director general referred to the risk analysis made by RIA on 2017-11-02, according to which an overwhelming risk had arisen that the private keys could be used without cardholders' consent (Director General of the Police and Border Guard Board 2017). According to the public announcement, the risk of exploiting the flaw increased to a critical level after the researchers, who found the flaw, published their research on 2017-10-30 in full (ERR News 2017a).

The fact that this decision had to be supported by the Estonian government shows the political nature of the decision. The escalation of this decision to the political level suggests that the legal norms regulating these issues were not followed. Indeed, it was already clear from the initial information given by the researchers that the affected ID card platform did not meet the security requirements of eIDAS (see Section "Qualified signature creation device status"). The situation was similar to the compromise of Dutch CA DigiNotar, after which the Dutch government decided to keep the compromised certificates valid for an additional two weeks (Arnbak and Eijk 2012). In a closed ecosystem the State can have its own safety standards. This, however, is not so in the case of the EU digital single market, where the supervisory bodies of all member states are expected to apply common security requirements to all qualified trust service providers and qualified trust services.

Compelling the TSP to not invalidate the certificates

According to clause 17 (1) of EITSETA, the TSP has the right to suspend the certificates in case a suspicion arises that the cardholder's private key can be used without his consent. According to the CA standards (Section 6.3.9 in (European Telecommunications Standards Institute 2018)) the revocation of compromised certificates is not

just a right but the obligation of the CA. In the outbreak of the ID card crisis, the government lawyers analyzed the possibility of using the Emergency Act (Riigi Teataja 2018) to compel the TSP to not revoke the vulnerable certificates before the government made a decision to revoke (see Section 7.1 in (Laanest and Kask 2017)). Since, by law, the TSP is considered to be a vital service provider, the State can exercise its rights provided by the Emergency Act, forcing the TSP to continue providing services of general interest despite the plans of the vital service provider to discontinue them. However, we note that this legal interpretation seems to be quite problematic, because by invalidating the affected certificates the TSP is not discontinuing the provision of trust services. Quite the opposite – the provisioning of trust services requires the TSP to assure that any untrustworthy certificates are invalidated.

In this particular case, the TSP and their auditor TÜViT agreed to follow the plan of the authorities. The problem, however, is that in general, the authorities who usurped the exclusive rights to decide on this matter, do not carry the financial risks resulting from the decision to not revoke certificates that should be revoked.

PROBLEMS APPLYING THE SUSPENSION MECHANISM

In the context of certificate validity, the only difference between suspension and revocation is the ability to restore the validity of a temporarily suspended certificate. Since there were no plans to restore the validity of the affected certificates, the question arises as to why the certificates were first suspended and only then revoked. According to the explanation provided by the authorities, the certificates were suspended to allow the affected cardholders to remotely renew their ID cards after the certificate suspension. The legal requirements do not allow remote renewing of invalid certificates, therefore it was intended that in the remote renewal process the validity of suspended certificates would be shortly restored, thereby making the solution legally compliant. This, however, was not done in practice, and if done, would only have been a fiction (see Section "Remote renewal of suspended certificates").

The decision of the authorities to apply a suspension mechanism instead of revoking the certificates created legal issues which could have been avoided. These issues are discussed below.

Covering already suspended certificates

The law does not foresee the suspension of already suspended certificates, therefore PPA's decision could not be applied to those certificates that were already suspended based on the request of certificate holders. According to clause 18 (3) of EITSETA, the suspension can be terminated only by the party who requested the suspension. This led to a situation where the certificate holders, who had suspended the validity of their certificates before the PPA decision was enforced, were able to terminate the suspension later, thereby avoiding the consequences of the decision, which was to restrict the use of the vulnerable ID cards.

Such a situation was prevented, in practice, by forcing the cardholders who applied for certificate validity restoration to renew their ID cards, thereby revoking their vulnerable suspended certificates and obtaining new certificates. While from the cardholders' perspective the end result was the same (i.e., the ID card with valid certificates), from the legal point of view, the certificate holders were denied their right to restore the validity of their suspended certificates. Such a problem would not have arisen if the certificates were instead revoked, since revocation can also be applied to suspended certificates.

Handling the cases of lost ID cards

In the event a cardholder loses his ID card, he is expected to call the TSP helpline and request a certificate validity suspension, thereby eliminating the risk of abuse. If the card is later found, the cardholder can restore certificate validity. In case the card is not found, the cardholder can apply for a new ID card revoking the lost card.

In the event the ID card with the PPA-suspended certificates was lost, the cardholders could not request a temporary suspension of their certificates, as they were already suspended by PPA. In practice, if the cardholders called to request a certificate suspension, the certificates were revoked. The practice of certificate revocation based on a request received over the phone was not in compliance with the legal requirements. In particular, clause 19 (1) of EITSETA requires the TSP to revoke a certificate based on an application, and the Certification Practice Statement (Section 4.9.3 in (SK ID Solutions AS 2018a)) requires the subscriber to submit a signed application for revocation.

In this case, the TSP made the decision to revoke the PPA-suspended certificates to eliminate the risk that someone could remotely renew the cardholder's lost ID card and then abuse it to the full extent. In addition, there was also a theoretical risk that the authority, on whose request the certificates were suspended, later restores certificate validity, thereby opening the lost ID card for abuse. Only the cardholders who were aware of such risks were likely to approach the TSP with the request to invalidate the PPA-suspended certificates of their lost ID cards.

This case has highlighted the flaw in the current legal suspension mechanism for cases when the certificates are suspended by some party other than the cardholder.

REMOTE RENEWAL OF SUSPENDED CERTIFICATES

The technical solution for the remote renewal of ID card certificates renewal[4] was already introduced in 2016 to replace the certificates with incorrectly encoded public keys (ERR News 2015). The availability of the solution played a crucial role in solving the ID card crisis. Hundreds of thousands of ID card holders could update their flawed ID cards over the Internet without overwhelming PPA customer service points. The problem, however, was that the remote update solution was not designed to securely update ID cards with invalid certificates.

According to the TSP, the legal basis for remote certificate renewal is eIDAS article 24 (d), which provides an option for a qualified TSP to verify the identity of the person to whom the qualified certificate is issued "by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.". According to clause 18^1 (2) of IDA, "the digital verification of the identity of the holder of a document is carried out through the certificate enabling digital identification". This can be interpreted in a way that the authentication with the ID card's authentication certificate is recognized in Estonia to provide equivalent assurance in terms of reliability to physical presence[5]. The TSP follows this reasoning and in the Certification Practice Statement (Section 3.3.1.1 in (SK ID Solutions AS 2018a)) states that the renewal request must be authenticated based on a valid authentication certificate of the document that needs to be renewed.

While the legal framework requires a renewal request to be authenticated using a valid authentication certificate, the remote certificate renewal service was also provided after 2017-11-03, when the certificates of the vulnerable ID cards were suspended. According to the TSP, the legal requirement could have been formally satisfied by restoring the validity of the suspended certificates right before the renewal. Since such a short-term restoration of the validity would have no practical effect, this step was skipped in practice. The implemented solution was approved by the TSP's auditor TÜViT.

We note that if the validity of the certificate had indeed been temporarily restored, the restoration of the validity would have required a separate decision by the entity who requested the suspension of the certificates. Such a decision would require that the legal basis for the initial certificate suspension (i.e. the suspicion that the private key can be used without the consent of the certificate holder) would cease to exist, which was not the case.

Regardless of the legal basis, the decision to restore the validity would have been effectively based on the actions performed with the suspended certificate, which is against the principle that the actions performed with a suspended or revoked certificate should have no legal effect. This principle is based on the presumption that in the period when the certificate is not valid, the card and PIN codes (private key activation data) may not be in the sole control of the cardholder. The authorities made a non-standard assumption that if cardholders lost control of their ID cards, they would turn to PPA requesting the revocation of their PPA-suspended certificates, thereby eliminating the risk of someone performing remote certificate renewal. Only the cardholders who were aware of such a risk may have applied for the revocation of their lost ID cards.

A technologically and legally sound solution would have required the renewal requests to be authenticated using some other valid electronic identity document or electronic identification means (e.g., Mobile-ID) satisfying the requirements of eIDAS article 24. However, at that time, a significant portion of affected cardholders did not have access to an independent secondary authentication tool, therefore the use of such a solution would have been limited.

REVOCATION OF THE VULNERABLE ID CARD CERTIFICATES

On 2018-03-16, the director general of PPA signed the decision to revoke the certificates of the non-updated ID cards starting from 2018-03-31 23:59. The decision refered to the initial risk analysis performed by RIA on 2017-11-02, and the letter received from RIA on 2018-03-13, stating that there was no basis to change the initial risk assessment. The PPA concluded that since the certificate owners did not find the need to renew their certificates over the 5-month period, their interests will not be restricted by revoking their certificates. (Director General of the Police and Border Guard Board 2018)

We note that 2018-04-01 was already mentioned in the initial announcement of suspension as the date of revocation (ERR News 2017a). While there may be a public impression that the revocation was required due to some security concerns, the choice of 2018-04-01 was purely a political decision to have some end-date for the ID card crisis, and also to provide a reason as to why the renewal service for the affected ID cards was being discontinued.

The cardholders who did not renew their ID cards and thus were left with a dysfunctional ID card were not eligible to compensation, because according to clause 4^1 of IDA, the State fee is not paid for the ID card, but for the

[4]For a detailed analysis of the technical solution and its applications, see (Parsovs 2020).

[5]Such an equivalence, however, has not been assured by the conformity assessment body.

review of the application for the issuance of the ID card. We note that in the previous large scale ID card security incident in 2011, the flawed ID cards could be renewed in PPA customer service points even after the certificate revocation (Police and Border Guard Board 2013).

EFFECTIVE TIME OF CERTIFICATE INVALIDATION

To ensure legal certainty, it is of crucial importance to establish the precise time when the validity of the certificate changed. For instance, digital signatures created after the certificate was invalidated will not have the legal effect of a qualified electronic signature (see article 32(1)(b) of eIDAS). The requirement for time precision in establishing the effective time when the certificate changed its status is not provided in the law. However, the technical standards of certificates and certificate validity services define one second granularity for timestamps of a certificate validity period (Boeyen et al. 2008). We encountered serious problems in establishing the effective time when the validity status changed for the vulnerable certificates. Over time, the TSP's validity services reported an inconsistent certificate validity status for the affected certificates (see Figure 2). We discuss these problems in detail below.

Effective time of suspension

The enforcement of PPA's decision to suspend the affected certificates starting from 2017-11-03 faced serious difficulties. The technical capabilities of the TSP did not allow for the suspension of such a large amount of certificates to be registered quickly – a week was required to complete the operation. As a temporary solution, the validity services were manually modified to return an immediate negative validity status for the affected certificates until the suspensions were fully registered in the certificate database kept by the TSP.

We looked at the validity status of our vulnerable digital signature certificate[6] in the Certificate Revocation List (hereinafter – CRL) published by the TSP. The first CRL that listed the serial number was issued at 2017-11-03 23:05:54 (`thisUpdate` field) with the `revocationDate` field set to the future – 2017-11-03 23:59:59, and the `reasonCode` field set to `unspecified`. However, starting with the CRL issued at 2017-11-10 04:25:07, the `revocationDate` field was changed to 2017-11-*10* 00:03:38 and the `reasonCode` field was changed to `certificateHold`. Apparently, 2017-11-10 was the date when the suspension operation completed and the standard validity services of the TSP resumed their normal operation.

The CRL technical standard (Boeyen et al. 2008) implies that the revocation status `certificateHold` should be used when the certificate validity is on hold (i.e., the validity is suspended). However, in the CRLs we see that before 2017-11-10, the CRLs used a technical reason code denoting revocation, and only after 2017-11-10 used a reason code denoting certificate suspension. This technical discrepancy most likely did not cause any problems in practice, because to the best of our knowledge, the relying parties do not differentiate between the legal types of revocation (whether it is temporary suspension or permanent revocation). Another side-effect of the temporary solution was that the unique numbering of the CRLs became disrupted, resulting in different CRLs being issued with the same `CRLNumber`.

According to the TSP, the legally binding certificate suspension time is the one that is shown on the TSP's web service `https://minutoimingud.sk.ee/`. There the suspension time for our certificate is set to 2017-11-10 00:03:40, which is two seconds after the `revocationDate` shown in the CRLs issued after 2017-11-10. If the suspension time of our certificate is indeed 2017-11-10 00:03:40, then by returning a negative certificate validity status from 2017-11-03 23:59:59, the TSP effectively restricted our use of the trust service without legal basis. If the suspension date is the one specified in the initial CRLs (i.e., 2017-11-03 23:59:59), the TSP failed to fulfill the legal requirement to correctly indicate the suspension period.

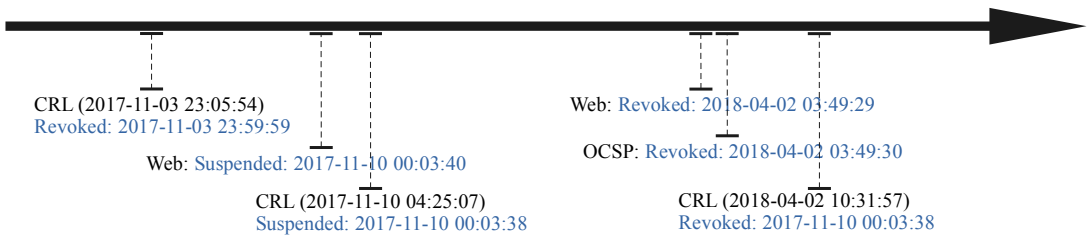


Figure 2. Timeline of certificate validity status changes as reported by the TSP's validity services

[6]The certificate with serial number 862527105210340231301506071770806272 73 issued under the intermediate CA "ESTEID-SK 2011".

The current situation, where there are several interpretations of the effective time of suspension, fails to provide legal certainty for the parties involved in the ecosystem. The case also clearly shows that the technical capabilities of a TSP must ensure immediate certificate status change for all non-revoked unexpired certificates issued by the TSP.

Effective time of revocation

As it was not security critical to quickly revoke already suspended certificates, the TSP did not use temporary validity services to indicate revocation, but rather relied on the standard procedure for registering certificate validity status change.

In the CRLs issued by the TSP, we see that the `reasonCode` of our suspended certificate changed to `unspecified` in the CRL first published at 2018-04-02 10:31:57. The `revocationDate` field, however, stayed the same showing the backdated revocation date of 2017-11-10 00:03:38. In the Online Certificate Status Protocol (hereinafter – OCSP) (Santesson et al. 2013) response produced on 2018-04-09, we see the `revocationTime` field set to 2018-04-02 03:49:30. While the `revocationDate` field of the CRLs contain an incorrect value, to the best of our knowledge, the relying parties do not rely on the date specified therein. The revocation date shown in the web service of the TSP is 2018-04-02 03:49:29, which is one second off the `revocationTime` returned by the OCSP validity service.

Article 24 (3) of eIDAS states that "If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.". Therefore according to eIDAS, the effective time of the revocation is the time of publication. Here, publication can be interpreted as the time when the TSP started to distribute the revocation status via the validity services of the TSP. Therefore, the effective time of the revocation should be 2018-04-02 03:49:30, when the OCSP service started to respond with the revoked status (according to the TSP's web service, the registration of the revocation happened one second before).

Contrary to eIDAS, clause 20 (4) of EITSETA states that "The validity of a certificate ends upon entry of the data on revocation of the certificate in the certificate database kept by a trust service provider". We conclude that EITSETA is not eIDAS compliant in this matter and the provisions of eIDAS should take precedence.

As we see, the information provided by the TSP validity services is not consistent. This is in conflict with the technical requirements (Section 6.3.10 in (European Telecommunications Standards Institute 2018)) according to which the TSP is audited. While the PPA decision required the revocation of the affected certificates on 2018-03-31 23:59, our certificate was revoked 27 hours later, exceeding the 24 hour requirement of eIDAS.

CERTIFICATE STATUS CHANGE NOTIFICATIONS TO CARDHOLDERS

According to clauses 17 (4), 18 (4) and 20 (5) of EITSETA, the TSP is required to notify the certificate holder promptly of the suspension, restoration and revocation of the certificate. The Terms and Conditions of the TSP (clause 6.2.7 in (SK ID Solutions AS 2018b)) sets an obligation for the TSP to "inform the owner by using @eesti.ee e-mail address that their certificate has been suspended, suspension is terminated or certificate is revoked". Figure 3 shows an example of an e-mail notification that is usually sent by the TSP to inform the cardholder of the changes in the certificate validity status. In the case of certificate revocation, the IDA clause 9[6] (3) also requires the issuer of the document (PPA in this case) to "immediately notify the holder of the document of the revocation of the certificate".

We found that the cardholders affected by the flaw were not informed in a proper manner that their certificate validity status had changed. The shortcomings of the received notifications are analyzed below.

Subject: AS Sertifitseerimiskeskuse teade
From: abi@id.ee
Date: 2013-04-03 10:53
To: john.doe@eesti.ee

Lgp. JOHN DOE.

Teie ID-kaart nr. E0044843 sertifikaat numbriga 4C7F6AD9 peatati 03-04-2013 10:50.
Sertifikaat on peatatud ja kasutada ei saa. Sertifikaadi peatatuse lõpetamise või
uue dokumendi tellimise info www.politsei.ee. Lisainfo 1777.

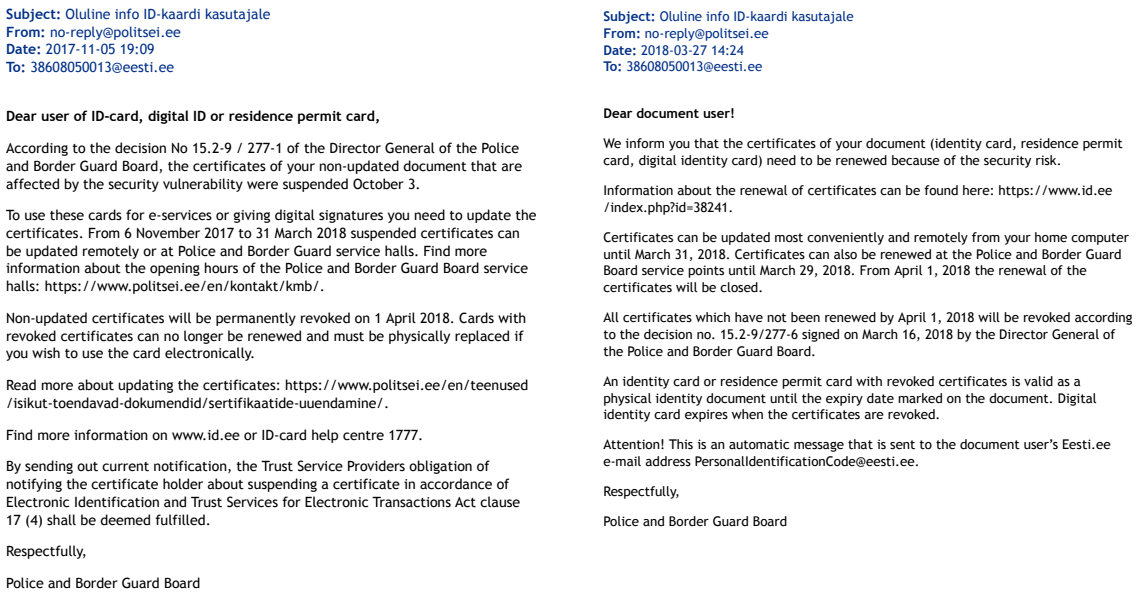
AS Sertifitseerimiskeskus

Figure 3. An example of TSP's certificate suspension notification (in Estonian)

Certificate suspension notification

On 2017-11-05, we received an e-mail notification from PPA (Police and Border Guard Board 2017), which stated that "[...] the certificates of your non-updated document that are affected by the security vulnerability were suspended October 3"[7] (see Figure 4a). The notification also included a paragraph stating that by sending out the notification, the TSP's obligation set out in the clause 17 (4) of EITSETA shall be deemed fulfilled. According to the TSP, the task of notifying was delegated to PPA, which is the registration authority of the TSP.

As we see, the notification fails to identify the cardholder, the ID card whose certificates were suspended, and the effective date and time of the suspension. According to PPA, the first notifications included also the document number, which was later removed, because wrong document numbers were sent out. Many people contacted PPA because they received notification e-mails even though they had already updated their ID card or had an ID card which was not affected by the flaw. It turned out that the notifications regarding ID cards issued to underage persons were sent to their parents, but, as the notifications were not personalized, it created confusion (Postimees 2017).



Subject: Oluline info ID-kaardi kasutajale
From: no-reply@politsei.ee
Date: 2017-11-05 19:09
To: 38608050013@eesti.ee

Dear user of ID-card, digital ID or residence permit card,

According to the decision No 15.2-9 / 277-1 of the Director General of the Police and Border Guard Board, the certificates of your non-updated document that are affected by the security vulnerability were suspended October 3.

To use these cards for e-services or giving digital signatures you need to update the certificates. From 6 November 2017 to 31 March 2018 suspended certificates can be updated remotely or at Police and Border Guard service halls. Find more information about the opening hours of the Police and Border Guard Board service halls: https://www.politsei.ee/en/kontakt/kmb/.

Non-updated certificates will be permanently revoked on 1 April 2018. Cards with revoked certificates can no longer be renewed and must be physically replaced if you wish to use the card electronically.

Read more about updating the certificates: https://www.politsei.ee/en/teenused/isikut-toendavad-dokumendid/sertifikaatide-uuendamine/.

Find more information on www.id.ee or ID-card help centre 1777.

By sending out current notification, the Trust Service Providers obligation of notifying the certificate holder about suspending a certificate in accordance of Electronic Identification and Trust Services for Electronic Transactions Act clause 17 (4) shall be deemed fulfilled.

Respectfully,

Police and Border Guard Board

(a) Suspension notification (2017-11-05)

Subject: Oluline info ID-kaardi kasutajale
From: no-reply@politsei.ee
Date: 2018-03-27 14:24
To: 38608050013@eesti.ee

Dear document user!

We inform you that the certificates of your document (identity card, residence permit card, digital identity card) need to be renewed because of the security risk.

Information about the renewal of certificates can be found here: https://www.id.ee/index.php?id=38241.

Certificates can be updated most conveniently and remotely from your home computer until March 31, 2018. Certificates can also be renewed at the Police and Border Guard Board service points until March 29, 2018. From April 1, 2018 the renewal of the certificates will be closed.

All certificates which have not been renewed by April 1, 2018 will be revoked according to the decision no. 15.2-9/277-6 signed on March 16, 2018 by the Director General of the Police and Border Guard Board.

An identity card or residence permit card with revoked certificates is valid as a physical identity document until the expiry date marked on the document. Digital identity card expires when the certificates are revoked.

Attention! This is an automatic message that is sent to the document user's Eesti.ee e-mail address PersonalIdentificationCode@eesti.ee.

Respectfully,

Police and Border Guard Board

(b) Revocation notification (2018-03-27)

Figure 4. PPA notifications to cardholder's @eesti.ee e-mail address

Certificate revocation notification

On 2018-03-27, we received a non-personalized e-mail notification from PPA (Police and Border Guard Board 2018), which stated that "[...] certificates of your document need to be renewed because of the security risk" and that "[...] all certificates which have not been renewed by April 1, 2018 will be revoked [...]" (see Figure 4b).

Since this e-mail was sent before the revocation took place and it mentions some conditions that have to be satisfied for the revocation to take place, this e-mail, in our opinion, cannot be considered as the notification required by IDA clause 9^6 (3), which shall be carried out immediately after the revocation.

According to PPA, all public activities related to the ID card flaw are considered to fall under the notification specified in IDA clause 9^6 (3). Unfortunately, these public activities did not achieve the lawmaker's aim to undoubtedly inform the cardholder about their certificate validity change and the effective time of that change.

The TSP did not send the revocation notifications. According to the TSP, there was an agreement that PPA's notification will include a statement that the obligation of TSP set out in the clause 20 (5) of EITSETA shall be deemed fulfilled, but for some reason PPA failed to include such clause in their notification.

Notification in the renewal process

Contrary to the obligation set out in the Terms and Conditions of the TSP, the TSP did not send an e-mail notification in cases where the vulnerable certificates were revoked as a result of renewing the ID card. According to the TSP, the e-mail notifications in these cases were not sent as such notifications would have confused the cardholders.

[7]There is a typo in the English version – Estonian and Russian versions have "starting from November 3".

PPA also did not fulfill their obligation to notify the cardholder of the certificate revocation in the case of remote certificate renewal. We note that since TSP is already obliged to notify the cardholder of the certificate revocation, the need for such an obligation from the document issuer is questionable.

QUALIFIED SIGNATURE CREATION DEVICE STATUS

One of the requirements for an electronic signature to have the equivalent legal effect of a handwritten signature is that it has to be created by a qualified electronic signature creation device (hereinafter - QSCD). Annex II of eIDAS specifies the security requirements for QSCDs, and eIDAS article 30 requires QSCDs to pass a certification process. The Commission Implementing Decision (EU) 2016/650 (European Commission 2016) specifies Common Criteria evaluation standards and Protection Profiles according to which the QSCDs must be certified.

In the event the affected ID card platform lost its QSCD status, the TSP would be required to revoke the digital signature certificates, as they would contain a QSCD claim that does not hold anymore. It was already clear that the affected ID card platform did not satisfy the QSCD requirements when the Estonian authorities became aware about the flaw on 2017-08-30. Ironically, due to a loophole in eIDAS, there was no authority that could have revoked the QSCD status of the affected ID card platform.

The affected ID card platform obtained the QSCD status not through the certification set out in eIDAS article 30, but through the transitional measures specified in eIDAS article 51. Article 51 states that signature creation devices, which were recognized as secure-signature-creation devices (hereinafter – SSCDs) under eSignature Directive 1999/93/EC (The European Parliament and the Council of the European Union 2000) (hereinafter – Directive), under eIDAS are deemed to be QSCDs. Under the Directive, the Estonian Ministry of Economic Affairs and Communications (Majandus- ja Kommunikatsiooniministeerium – MKM) acted as a conformity assessment body, assessing a SSCD's conformance based on its internal procedure (see Section 6 in (Laanest and Kask 2017)). After the Directive was repealed on 2016-07-01, the MKM lost its authority to assess SSCD conformity and hence also the authority to declare the signature creation device as non-conformant.

Currently, the legal regulation is also not much better for these QSCDs that have obtained QSCD status through the certification process set out in article 30 of eIDAS. eIDAS does not require regular reassessment of a signature creation device's compliance to the security requirements. Since the decision of QSCD conformance must be based on a Common Criteria certification process which must be initiated and sponsored by the vendor, the removal of the QSCD status, even in the event of obvious non-compliance, may lack legal basis, unless the vendor of the product is cooperating. We have found that even today Common Criteria security certificates of some of the chip products affected by the flaw have not been updated and are still considered valid (Parsovs 2020). This shows that eIDAS lacks effective means to maintain the trustworthiness of the signature creation devices after their QSCD status has been granted.

Another legal issue related to the QSCD status of the Estonian ID card arose due to the modifications made to the affected ID card platform. Starting from 2017-10-25, the smart card chip applet was modified, replacing the vulnerable RSA algorithm with the elliptic curve algorithm supported by the chip. The changes, however, were made without reassessing the device's conformance. We note that the chip applet implements logical protection of private keys and hence is subject to security assessment (see Decision 2003/511/EC (European Commission 2003) and recital 56 of eIDAS). This means that after any changes are made to the chip applet, the SSCD conformity of the modified ID card platform has to be reassessed.

After the Directive was repealed, the MKM lost its authority to assess signature creation device conformity to SSCD requirements, therefore the modified platform had to be certified according to the requirements of eIDAS article 30. It was clear that under the given time constraints it was not possible to certify a smart card applet that had never been formally certified before. According to the government lawyers (see Section 6 in (Laanest and Kask 2017)), since the changes made to the applet were minimal, it was decided that going through the time-consuming certification as required by eIDAS was not needed.

LIABILITY OF ID CARD PRIVATE KEY SECURITY

In the press conference on 2017-09-05, a journalist asked the prime minister whether the State was ready to compensate for losses in the event the security risk materialized. The prime minister answered: "[...] I do not know what your case is, but basically the State naturally has to be fully responsible of our ID and e-solutions. Yes, the State is responsible in any case." (time 06:32 in (ERR News 2017c)). From the prime minister's answer it is not clear whether he was referring only to moral responsibility or also to legal liability.

The legal analysis by the government lawyers touched the question of the State's liability, but did not provide a positive answer (see Section 8.2 in (Laanest and Kask 2017)). According to clause 7 (1) of the State Liability Act (hereinafter – SLA) (Riigi Teataja 2015a), a person whose rights are violated by the unlawful activities of a public authority may claim compensation for damage. Furthermore, according to clause 12 (1) of SLA, a public authority that fails to issue an administrative act or take a measure in due time is required to compensate for damage.

In this particular case, the claimant would have to substantiate that the vulnerability in the private keys was the result of some unlawful activity of PPA. Alternatively, the claim could be based on the failure of the authorities to revoke the affected certificates in due time, after the authorities became aware of the flaw. In this context it is important to note that clause 19 (3) of EITSETA sets an obligation for the cardholder to request revocation of his certificate if there is suspicion that his private key can be used without his consent. The cardholders' failure to revoke their certificates on 2017-09-05, after the prime minister informed the public of the vulnerability, hlin our opinion, could already be interpreted as negligence, making the cardholders liable for any fraud conducted with their identities after that date.

According to Annex II of eIDAS, generating electronic signature creation data (private key) on behalf of the signatory may only be done by a qualified TSP. It is unlikely that the State would be willing to take over the liability of the TSP, especially since the operation and liability of the TSP is explicitly regulated by law. In addition, by accepting the ID card with the Terms and Conditions, the cardholder enters into the contract with the TSP and not the State.

It is important to note that in the Terms and Conditions of the TSP (SK ID Solutions AS 2018b), the TSP takes no liability for key generation. In clause 8.1 the TSP states that "the Subscriber is solely responsible for the maintenance of his/her Private Key" and clause 8.7.1 states that the TSP is not liable for "the secrecy of the Private Keys of the Subscribers".

Since neither party is willing to take liability for the security of the generated keys, the end result may be that the ID card is provided to the cardholder "as is", leaving the cardholder to bear the losses resulting from fraud. The Terms and Conditions, which shifts all the liability to the cardholder, however, may turn out to be non-enforceable. Unless the person agrees to the Terms and Conditions, the ID card is not issued (ID Help Centre 2019). Since the ID card is a mandatory identity document for all Estonian residents aged 15 and above, the cardholder's free will, when entering into the contract, is questionable.

As of this date there has been no significant damage caused by the ID card security issues, therefore liability questions for now have remained purely hypothetical. This, however, does not contribute to the legal certainty of the eID field and may lead to a situation where the party taking the risks is not the party that bears the cost of these risks.

CONCLUSIONS AND RECOMMENDATIONS

The ID card crisis has shown that in a crisis situation where the continuity of the e-state is at stake, the fulfillment of all applicable legal requirements can become quite a challenge. The legal non-compliances observed in this work can be grouped by three main causes – the lack of technical preparedness, suboptimal decisions made under heavy time pressure, and the critical nature of the situation.

The TSP's failure to quickly invalidate a large number of certificates and correctly indicate their status, and the TSP's and PPA's failure to accurately notify the affected cardholders, can be explained by the *lack of technical preparedness* and incomplete crisis management planning.

The legal issues resulting from the decision to restrict the access to the public certificate directory and the decision to suspend (and not revoke) the affected certificates, can be explained by the heavy time pressure under which these *suboptimal decisions* were made.

Some of the failures to meet the legal requirements, in particular, the hesitation to revoke the vulnerable certificates, the remote renewal of suspended certificates, and the use of the modified ID card platform whose compliance to QSCD requirements had not been assessed, we can consider to be rooted in the *critical nature of the situation*. The root cause of the crisis was the fact that the failure in a single ID card platform supplied by a single TSP put the reputation and functioning of the entire e-state at risk.

To reduce the risk of a similar incident in the future escalating into crisis, the State should seek to equip its residents with a secondary electronic identity tool that would rely on a different technological platform (preferably also a different public-key cryptography algorithm) and a different TSP. This, in case of a similar event, would allow sustaining legally compliant continuity of the e-state, and potentially also a safe remote renewal of the affected electronic identity tool.

In the list below we provide more specific recommendations based on the findings of this work.

1. This work has highlighted the problems in the current regulation of certificate validity suspension, in particular, when the suspension is requested by a party other than the certificate holder. A potential solution would be to amend EITSETA granting certificate suspension rights only to the certificate holder. However, since the use of a suspension mechanism leads to other legal issues[8], we recommend to completely deprecate the suspension mechanism, provided that cardholders are able to replace the revoked certificates with the same ease as the validity restoration of suspended certificates.

2. The current QSCD assessment mechanism, as provided by eIDAS, does not ensure that the product's compliance to the security requirements is maintained after the QSCD status has been granted to the product. The legislation should establish a continuous management process for the security of QSCDs over its lifecycle as suggested by ANSSI (Romain Santini, ANSSI 2019). At the same time the certification mechanism should provide flexibility when a security flaw found in the product has to be quickly mitigated, as nicely demonstrated by the ingenious Estonian ID card remote update solution.

3. In this work we have pointed out several technical and legal non-compliances of the TSP and its validity services (e.g., CRL, OCSP and the web service of the TSP displays inconsistent revocation time for the revoked certificates). While the described non-compliances may look insignificant, it is not uncommon to see a combination of such separately unimportant issues lead to serious security risks. We advice the TSP and its auditors to not underestimate such issues.

4. Clause 20 (4) of EITSETA states that validity of a certificate ends upon entry of revocation in the certificate database kept by a TSP, while eIDAS in article 24 (3) sets the effective time of revocation to be immediately upon its publication. We recommend to amend clause 20 (4) of EITSETA to be in line with eIDAS.

5. The document issuer's obligation specified in IDA clause 9[6] to notify the cardholder of certificate revocation, overlaps with the obligation of the TSP specified in EITSETA clause 20 (5). It should be reviewed whether such an overlapping obligation is needed.

6. Last but not least, to ensure legal certainty for the participants of the ecosystem, we recommend the legal framework to be updated, providing clear answers to the liability questions discussed in this work.

Acknowledgements. We are thankful to the employees of RIA (Margus Arm, Kristiina Laanest), PPA (Kaija Kirch) and the TSP (Kalev Pihl, Tanel Kuusk) for their open communication and the information provided for this study. We also thank Anto Veldre for the discussions and his feedback on the draft. This research has been supported by the European Regional Development Fund through the Estonian Centre of Excellence in ICT Research under grant number EU48684 and by the European Social Fund through the IT Academy programme.

REFERENCES

Arnbak, A. and Eijk, N. van (Aug. 2012). *Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain*. URL: https://dx.doi.org/10.2139/ssrn.2031409.

Boeyen, S., Santesson, S., Polk, T., Housley, R., Farrell, S., and Cooper, D. (May 2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. RFC 5280 (Proposed Standard). Internet Engineering Task Force. URL: http://tools.ietf.org/html/rfc5280.

Director General of the Police and Border Guard Board (Nov. 2017). *Decision No 15.2-9/277-1 (in Estonian)*. URL: https://cybersec.ee/storage/20171102_PPA_decision_ROCA_suspension.bdoc.

Director General of the Police and Border Guard Board (Mar. 2018). *Decision No 15.2-9/277-6 (in Estonian)*. URL: https://cybersec.ee/storage/20180316_PPA_decision_ROCA_revocation.bdoc.

ERR News (Sept. 2015). *250,000 Estonian ID cards could be faulty*. URL: https://news.err.ee/116849/250-000-estonian-id-cards-could-be-faulty.

ERR News (Nov. 2017a). *Government to suspend ID card certificates with security risk at midnight*. URL: https://news.err.ee/640385/government-to-suspend-id-card-certificates-with-security-risk-at-midnight.

[8]The suspension mechanism prevents to determine whether the digital signature was given at the time when the certificate was valid (Mets and Parsovs 2019).

ERR News (Sept. 2017b). *Potential security risk could affect 750,000 Estonian ID cards*. URL: https://news.err.ee/616732/potential-security-risk-could-affect-750-000-estonian-id-cards.

ERR News (Sept. 2017c). *The agencies are hoping to eliminate the security risk of ID cards in two months (in Estonian)*. URL: https://www.err.ee/616731/ametid-loodavad-id-kaardi-turvariski-likvideerida-kahe-kuuga.

Estonian Information System Authority (Sept. 2017). *Security Vulnerability Detected in the Estonian ID Card Chip (in Estonian)*. URL: https://www.ria.ee/ee/id-kaardi-kiibis-avastati-turvarisk.html.

European Commission (2003). *2003/511/EC: Commission Decision of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council*. URL: https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=celex:32003D0511.

European Commission (2016). *Comission Implementing Decision (EU) 2016/650*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.109.01.0040.01.ENG.

European Telecommunications Standards Institute (Feb. 2018). *ETSI EN 319 411-1 V1.2.1 (2018-02) Electronic Signatures and Infrastructures (ESI); Policy and securityrequirements for Trust Service Providers issuing certificates; Part 1: General Requirements;* URL: https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.02.01_30/en_31941101v010201v.pdf.

ID Help Centre (June 2019). *Terms and Conditions for Use of Certificates*. URL: https://www.id.ee/index.php?id=30479.

Laanest, K. and Kask, L. (Oct. 2017). *Legal Issues of ID Card Security Risk (unofficial translation)*. URL: https://cybersec.ee/storage/RIA_MKM_idcard_risklegal.pdf.

Mets, T. and Parsovs, A. (2019). "Time of signing in the Estonian digital signature scheme". In: *Digital Evidence and Electronic Signature Law Review* 16, pp. 40–50. URL: https://journals.sas.ac.uk/deeslr/article/view/5076.

Nemec, M., Sys, M., Svenda, P., Klinec, D., and Matyas, V. (2017). "The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17. Dallas, Texas, USA: ACM, pp. 1631–1648. URL: http://doi.acm.org/10.1145/3133956.3133969.

Parsovs, A. (2020). "Estonian Electronic Identity Card and its Security Challenges". PhD thesis (to be completed). University of Tartu.

Police and Border Guard Board (May 2013). *FAQ: Renewing ID-Cards issued in 2011*. URL: https://www.id.ee/index.php?id=36348.

Police and Border Guard Board (Nov. 2017). *Email notification from no-reply@politsei.ee: Important information for ID card user*. URL: https://cybersec.ee/storage/20171105_PPA_post-suspension.eml.

Police and Border Guard Board (Mar. 2018). *Email notification from no-reply@politsei.ee: Important information for ID card user*. URL: https://cybersec.ee/storage/20180327_PPA_pre-revocation.eml.

Postimees (Nov. 2017). *Simply and clearly: why certificate update notification was sent also for ID cards issued before autumn 2014 (in Estonian)*. URL: https://tehnika.postimees.ee/4301359/lihtsalt-ja-selgelt-miks-saavad-sertifikaatide-uuendamise-teateid-ka-enne-2014-aasta-sugist-id-kaardi-saanud.

Riigi Teataja (1999). *Identity Documents Act – RT I, 21.04.2018, 5. English translation*. URL: https://www.riigiteataja.ee/en/eli/521062017003.

Riigi Teataja (2015a). *State Liability Act – RT I, 17.12.2015, 76. English translation*. URL: https://www.riigiteataja.ee/en/eli/507062016001.

Riigi Teataja (2015b). *State of Emergency Act – RT I, 12.03.2015, 12. English translation*. URL: https://www.riigiteataja.ee/en/eli/529012016004.

Riigi Teataja (2016). *Electronic Identification and Trust Services for Electronic Transactions Act – RT I, 25.10.2016, 1. English translation*. URL: https://www.riigiteataja.ee/en/eli/527102016001.

Riigi Teataja (2018). *Emergency Act – RT I, 22.05.2018, 5. English translation*. URL: https://www.riigiteataja.ee/en/eli/525062018014.

Romain Santini, ANSSI (Jan. 2019). *Standardisation supporting sectorial certification – The eIDAS stories*. URL: https://www.enisa.europa.eu/events/cybersecurity_standardisation/presentations/3a%5C%20Santini.pdf.

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C. (June 2013). *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. RFC 6960 (Proposed Standard). Internet Engineering Task Force. URL: https://tools.ietf.org/html/rfc6960.

SK ID Solutions AS (Apr. 2018a). *ESTEID-SK Certification Practice Statement, Version 4.0*. URL: https://sk.ee/upload/files/SK-CPS-ESTEID-EN-v4_0_20180401.pdf.

SK ID Solutions AS (July 2018b). *Terms and Conditions for Use of Certificates of Personal Identification Documents of the Republic of Estonia*. URL: https://sk.ee/upload/files/SK-TCU-ESTEID-EN-20180701.pdf.

SK ID Solutions AS (June 2018c). *Trust Services Practice Statement, Version 5.0*. URL: https://sk.ee/upload/files/SK-PS-EN-v5_0_20180625.pdf.

The European Parliament and the Council of the European Union (2000). *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31999L0093.

The European Parliament and the Council of the European Union (2014). *Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.