

LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

LATVIJAS REPUBLIKAS ELEKTRONISKO DOKUMENTU LIKUMA
REALIZĀCIJAS RISKU APSKATS

MAĢISTRA DARBS

Autors: **Edgars Siliņš**

Stud. apl. Nr. ES09014

Darba vadītājs: Dr. math. Māris Alberts

RĪGA 2013

ANOTĀCIJA

Šajā darbā tiek identificēti un autora kompetences ietvaros aprakstīti kriptoloģiskie, tehnoloģiskie, juridiskie, uzraudzības, iekšējo un ārējo uzbrukumu, sociālie (cilvēku izlūkošana, manipulēšana, interešu konfliktu utt.) riski saistībā ar Elektronisko dokumentu likuma realizāciju Latvijas Republikā. Darbā ir aplūkots Elektronisko dokumentu likuma realizācijas process un realizācijas atbilstība Eiropas Savienības un Latvijas Republikas likumdošanai un informācijas tehnoloģiju labajai praksei, un secināts, ka desmit gadu laikā kopš Elektronisko dokumentu likuma apstiprināšanas, Latvijā nav ieviesti kvalitatīvi sertifikācijas pakalpojumi. Autors savas kompetences ietvaros sniedz rekomendācijas darbā identificēto risku iespējamai novēršanai. Darba mērķis ir pārliecināt Latvijas valdību par nepieciešamību izveidot profesionālu Latvijas nacionālās datu drošības skolu paātrinātā tempā, lai varētu realizēt topošās Eiropas Savienības Regulas par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū prasības Latvijas Republikā.

Atslēgvārdi: Elektroniskais paraksts, riski, datu drošība, kriptoloģija, Latvija, risinājumi.

ANNOTATION

In this master's thesis „Risk review of the Electronic documents law realization in the Republic of Latvia” author reviews the cryptological, technological, juridical, supervisorial, inner and outer attack, social (human intelligence, manipulation, conflict of interests etc.) risks of the Electronic documents law realisation in the Republic of Latvia. In this thesis a review of Electronic documents law realisation process and its accordance to the information technologies best practices and the legislation of European Union and Latvia are made. A conclusion is made that during ten years since the coming into force of the Electronic documents law there are no qualitative certification services in Latvia. Author within his competence gives possible solutions for the identified risks. The goal of this thesis is to convince the Latvian government of creating a national data security school as soon as possible in order for Latvia to be able to implement the upcoming regulation of the European Parliament and the council on electronic identification and trust services for electronic transactions in the internal market.

Keywords: Electronic signature, risks, data security, solutions, cryptology, Latvia.

AUTOREFERĀTS

Šajā darbā autors ir apzinājis Elektronisko dokumentu likuma realizācijas procesu Latvijas Republikā un identificējis sertifikācijas pakalpojumu kriptoloģiskos, tehnoloģiskos, juridiskos, uzraudzības, iekšējo un ārējo uzbrukumu, sociālos (cilvēku izlūkošana, manipulēšana, interešu konfliktu utt.) riskus.

Savas kompetences ietvaros autors apraksta iespējamus risinājumus kriptoloģisko, tehnoloģisko, juridisko, uzraudzības, iekšējo un ārējo uzbrukumu, un sociālo risku novēršanai vai ierobežošanai.

Juridisko risku jomā autors ir veicis Latvijas Elektronisko dokumentu likuma salīdzinājumu ar Igaunijas Digitālā paraksta likumu, kā arī identificējis klientu elektroniskā paraksta lietošanas riskus un sniedzis rekomendācijas to iespējamai novēršanai.

SATURA RĀDĪTĀJS

APZĪMĒJUMU SARAKSTS	8
IEVADS	10
1 ELEKTRONISKAIS PARAKSTS.....	12
2 EIROPAS SAVIENĪBAS LIKUMDOŠANA.....	14
3 ELEKTRONISKAIS PARAKSTS LATVIJĀ	17
3.1 Latvijas Elektronisko dokumentu likuma salīdzinājums ar Igaunijas Digitālā paraksta likumu.....	23
4 ELEKTRONISKĀ PARAKSTA IESPĒJAMIE RISKI.....	27
4.1 Auditora neatkarības un kvalitātes riski.....	27
4.2 Virtuālā elektroniskā paraksta portāla izmantotā SSL sertifikāta riski.....	29
4.2.1 SSL sertifikāta apskats	31
4.2.2 SSL sertifikāta drošības pārbaude	32
4.2.2.1 „BEAST” uzbrukuma ievainojamība	37
4.2.2.2 „CRIME” uzbrukuma ievainojamība	38
4.2.2.3 SSL 2.0 protokola atbalsts.....	39
4.2.2.4 Zemas šifrēšanas kodu komplektu atbalsts	39
4.2.2.5 RC4 protokola atbalsts	40
4.3 Uzraudzības iestādes pienākumu izpildes kvalitāte.....	41
4.3.1 Uzraudzības iestādes publicētās informācijas aktualitāte.....	44
4.3.2 Virtuālā paraksta atbilstība Elektronisko dokumentu likumam	45
4.4 Sertifikācijas pakalpojumu pieejamība un uzticamība	47
4.5 Iespējamie riski saistībā ar izstrādātājiem	53
4.5.1 Virtuālā elektroniskā paraksta pin koda drošība.....	56
4.5.2 Trešo pušu izstrādātāju risinājumi un to uzticamība	62
4.6 Latvijas elektroniskā paraksta viedkaršu riski, ņemot vērā Igaunijas elektroniskās identifikācijas kartes sekmīgu uzlaušanu	64
4.7 Citi riski	65
4.7.1 RSA algoritma specifiskie riski.....	65

4.7.1.1	Pieaugošs šifrēšanas atslēgas garums.....	67
4.7.1.2	Ilgtermiņa elektroniski parakstītu dokumentu glabāšana.....	68
4.7.1.3	Izvēlēta šifrēta teksta uzbrukumu riski.....	70
4.7.1.4	Kopēja moduļa uzbrukums.....	72
4.7.2	Izmantoto jaucējfunkciju veidošanas tehnoloģiju riski	73
4.7.3	Elektroniski dokumenti ar mainīgu un/vai slēptu saturu	75
4.7.4	Informācijas pārtveršana un noklausīšanās	77
4.7.5	Cilvēku izlūkošanas un iekšējo uzbrukumu riski	81
4.7.6	Likumdošanas riski.....	87
4.7.6.1	Dokumenta parakstītāja atbildības	88
4.7.6.2	Sertifikāta anulēšanas vai tā darbības pagaidu apturēšanas riski	89
4.7.6.3	Riski saistībā ar laika zīmogu.....	92
4.7.6.4	Nepārdomātu likuma grozījumu riski	94
4.7.6.5	Pakalpojumu sniedzēja definīcijas un prasību riski	95
4.7.6.6	Paraksta radīšanas datu definīcijas risks	96
REZULTĀTI UN SECINĀJUMI.....		98
IZMANTOTĀ LITERATŪRA UN AVOTI.....		100
PIELIKUMI.....		118
1.	pielikums. Portāla Eparaksts.lv SSL sertifikāts 1 [145]	118
2.	pielikums. Portāla eparaksts.lv SSL Sertifikāts nr.2 [165].....	120
3.	pielikums. SSL pārbaūžu kopsavilkuma tabula.....	124
4.	pielikums. KPMG Vērtējums par USPS atbilstību 2005. Gada 12. Jūlija Ministru kabineta noteikumiem Nr.514 [41,54]	125
5.	pielikums. Open ID tīmekļa vietnes informācija (www.open-id.lv)	128
6.	pielikums. EUSO izstrādātāja tīmekļa vietne (www.euso.lv)	130
7.	pielikums. Jāņa Boktas un Ilmāra Poikāna saruna par <i>PIN</i> drošību(<i>twitter.com</i>)	131
8.	pielikums. Java eDoc bibliotēku licences līguma teksts.....	132
9.	pielikums. Mozilla Firefox interneta pārlūkā saglabāto paroli atklāšana	134

10. pielikums. Sertifikācijas pakalpojumu sniedzēja tehniskas problēmas.	135
11. pielikums. Arnis Paršovs Datu Valsts inspekcijai par Latvijas pasta neiekļaušanu uzticamu sertifikācijas pakalpojumu sniedzēju reģistrā. [45]	138
12. pielikums. Datu Valsts inspekcijas atbilde Arnim Paršovam par VAS „Latvijas Pasts” statusu [45]	139
13. pielikums. Datu Valsts inspekcijas atbilde Arnim Paršovam [45]	140
14. pielikums. Arņa Paršova iesniegums Datu valsts inspekcijai 08.01.2013 [45]	142
15. pielikums. VAS „Latvijas Valsts radio un televīzijas centrs” atbilde Arnim Paršovam par auditiem. [54]	143
16. pielikums. Arņa Paršova vēstule VAS „Latvijas Valsts radio un televīzijas centrs” par auditiem. [54]	144
17. pielikums. „Qualyslabs SSL server rating guide” [189]	145
18. pielikums. „SSL threat model”	154
19. pielikums. Droša Elektroniskā paraksta nesēju veidi. (https://www.eparaksts.lv/lv/palidziba/eparaksta-neseju-veidi/)	156

APZĪMĒJUMU SARAKSTS

AES – *Advanced Encryption Standard* (uzlabots datu bloka simetriskās šifrēšanas standarts)

AES- GCM – *Advanced Encryption Standard Galois/Counter Mode* (vairāku šifrētu datu bloku virknēšanas metode, izmantojot Galuā laukus un AES)

AS - Akciju sabiedrība

CA – *Certification authority* (Sertificēšanas iestāde)

CBC - *Cipher-block chaining* (vairāku šifrētu datu bloku virknēšanas metode)

DSA – *Digital Signature Algorithm* (Digitālā paraksta algoritms)

DSS – *Digital Signature Standard* (Digitālā paraksta standarts)

ECDSA – *Elliptic Curve Digital Signature Algorithm* (Eliptisko līkņu digitālā paraksta algoritms)

eDOC - Elektroniskā dokumenta formāts (Latvijā)

Elektroniskais paraksts - ir dati elektroniskā formā, kas pievienoti vai loģiski saistīti ar citiem elektroniskiem datiem un ko izmanto par autentificēšanas metodi [12]

HSM – *Hardware security module* (aparatūras drošības modulis)

IP – *Internet protocol* (interneta protokols)

Laika zīmogs - ir elektroniski parakstīts apstiprinājums tam, ka elektroniskais dokuments ir parakstīts ar elektronisko parakstu noteiktā laika brīdī [12]

MAC - *Media access control* (fiziskās piekļuves vadība)

MD4 – *Message-Digest Algorithm* (Raivesta jaucējkode algoritms 4)

MD5 – *Message-Digest Algorithm* (Raivesta jaucējkode algoritms 5, labo MD4 nepilnības)

MiTM – *Man-in-the-middle* („Cilvēks pa vidu” uzbrukums)

NIST - National Institute for Standards and Technology (ASV Nacionālais standartu un tehnoloģijas institūts)

OAEP - *Optimal asymmetric encryption padding* (asimetriskās šifrēšanas optimāla papildināšanas shēma)

PIN – *Personal identification number* (personas identifikācijas numurs)

PKCS#11 - *Public-Key Cryptography Standard* (asimetriskās šifrēšanas standarts šifrēšanas marķiera saskarnei)

PKCS#1v1.5 – *Public-Key Cryptography Standard* (asimetriskās šifrēšanas standarti RSA šifrēšanai)

RC4 – *Rivest Cipher 4* (Raivesta ceturtais paaudzes datu bloka simetriskās šifrēšanas algoritms)

RSA – (*Rivest-Shamir-Adleman*) asimetrisks šifrēšanas algoritms

SHA-0 – *Secure Hash Algorithm* (NIST jaucējkode funkcija)

SHA-1 - *Secure Hash Algorithm* (NIST pirmās paaudzes jaucējkode funkcija, kas labo kļūdas un nepilnības sākotnējā SHA-0 specifikācijā)

SHA-2- *Secure Hash Algorithm* (NIST otrās paaudzes jaucējkode funkcija)

SHA-3- *Secure Hash Algorithm* (NIST trešās paaudzes jaucējkode funkcija)

SIA - sabiedrība ar ierobežotu atbildību

SSL - *Secure Socket Layer* (drošligzdu slānis)

TLS – *Transport Layer Security* (transporta slāņa protokols, kas nodrošina sakaru konfidencialitāti, pārraidīto datu integritāti u.c. starp diviem tīkla savienojuma punktiem)

URL – *Uniform resource locator* (vienotais resursu vietvārdis)

UTC - *Coordinated Universal Time* (koordinētais universālais laiks, ko koordinē Starptautiskais Mēru un svaru birojs Francijā)

VAS - valsts akciju sabiedrība

IEVADS

1999. gada 13. decembrī tiek parakstīta Eiropas Parlamenta un padomes Direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu. 2003. gada 1. maijā stājas spēkā Latvijas Elektronisko dokumentu likums. Kopš šī likuma pieņemšanas ir pagājuši desmit pilni gadi, bet sertifikācijas pakalpojumi Latvijā vēl joprojām netiek plaši lietoti, un to realizācija ir nekvalitatīva (skatīt darba tekstu). Galvenais un faktiski vienīgais tā iemesls ir tas, ka Latvijā nav profesionāla nacionāla datu drošības skola. Šīs direktīvas realizācijas neveiksme ir likumsakarīga. Sagaidāms, ka 2013. gada beigās stāsies spēkā Eiropas Savienības parlamenta un padomes Regula par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū.

Darba mērķis ir pārliecināt Latvijas valdību par nepieciešamību izveidot profesionālu Latvijas nacionālās datu drošības skolu paātrinātā tempā, lai Latvija varētu realizēt topošās Eiropas Savienības Regulas par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū prasības.

Datu drošības praksē pastāv ķēdes vājākā posma princips. Drošu sistēmu izveide nav iedomājama bez kriptogrāfijas. Pat vājš kriptogrāfijas algoritms var būt par vienu no datu drošības sistēmas ķēdes stiprākajiem posmiem. Kriptogrāfijas algoritma realizācija darbojas konkrētā aparatūras un programmatūras vidē. Drošas sistēmas izveides autoriem bez kriptogrāfijas zināšanām ir izcili jāpārzina gan aparatūras, gan standartprogrammatūras, operētājsistēmas, datu pārraides protokolu, cilvēcisko faktoru riski, likumdošana un citas sistēmas vidi veidojošās komponentes. Darba autoram nav zināms neviens speciālists vai speciālistu kolektīvs Latvijā, kam būtu drošu sistēmu izveidei pietiekamā kompetence. Profesionāla kriptologa iesaiste ir nepieciešams nosacījums. Diemžēl autoram Latvijā nav zināms arī neviens profesionāls kriptologs. Informācijas tehnoloģiju jomas darbinieku nekritiska paļāvība uz kriptogrāfijas algoritmu vispēcību, ignorējot vides riskus, ir raksturīga parādība Latvijā, arī Latvijas Elektronisko dokumentu likuma realizācijas procesā.

Otrs princips ir neērtais uzbrucējs. Nekad nevar paredzēt, kas un kad uzbruks, kādi ir viņa mērķi, kādi resursi un zināšanas ir viņa rīcībā. Ķēdes vājākais posms katram uzbrucējam var būt individuāls.

Šī darba uzdevums ir identificēt un apskatīt Latvijas Elektronisko dokumentu likuma realizācijas riskus un darba autora kompetences ietvaros sniegt iespējamus risinājumus to novēršanai.

Darbā izmantotā metodika:

- Likumdošanas un tiesību aktu izpēte un analīze;
- Teorētiskās literatūras izpēte;
- Ekspertu intervijas;
- Publikāciju masu informācijas līdzekļos un specializētos izdevumos izpēte
- Publicētu starptautisko profesionāļu zinātniskie darbi un pētījumi kriptanalīzes un kriptoloģijas jomā;
- Pētījuma darba autora uzkrātā informācija, zināšanas un pieredze;
- Autora speciāla risinājumu izpēte un analīze;
- Publiski pieejamu drošības testu rīku izmantošana konkrētu sistēmu drošības līmeņa pārbaudei;
- Pasaules pieredzes izmantošana, apgūšana un izmantošana;
- Datu savākšana un analīze;
- Informācijas analīze;

Darbs ir iedalīts četrās nodaļās, kur pirmajās trīs nodaļās tiek apskatīts elektroniskais paraksts, Elektronisko dokumenta likuma realizācija un realizācijas process, tiek apskatīta sertifikācijas pakalpojumiem saistošās Eiropas Savienības likumdošanas attīstība, tiek salīdzināts Latvijas Elektronisko dokumentu likums ar Igaunijas Digitālā paraksta likumu. Darba ceturtajā nodaļā tiek aplūkoti elektroniskā paraksta iespējamie riski. Ceturtā nodaļa ir sadalīta septiņās apakšnodaļās. Tiek aplūkoti riski saistībā ar uzticama sertifikācijas pakalpojuma sniedzēja pārbaūžu veikšanas praksi, uzraudzības organizācijas darbību, virtuālā elektroniskā paraksta portālu, sertifikācijas pakalpojumu pieejamību un uzticamību, iekšējiem, ārējiem trešo pušu izstrādātājiem, izmantotajām tehnoloģijām, iekšējiem un ārējiem uzbrukumu, cilvēku izlūkošanu, kriptogrāfiju un spēkā esošo likumdošanu. Aplūkotajiem riskiem darba autors savas kompetences ietvaros sniedz ierosinājumus to iespējamai risināšanai.

1 ELEKTRONISKAIS PARAKSTS

Eiropas Parlamenta un padomes Direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu 2. panta 1. punktā elektroniskais paraksts tiek definēts: „1) *elektroniskais paraksts* ir dati elektroniskā formā, kas pievienoti vai loģiski saistīti ar citiem elektroniskiem datiem un ko izmanto par autentificēšanas metodi” [12]

Latvijas Republikas Elektronisko dokumentu likuma 1. panta 4. punktā elektroniskais paraksts tiek definēts šādi: ”4) *elektroniskais paraksts* — elektroniski dati, kas pievienoti elektroniskajam dokumentam vai loģiski saistīti ar šo dokumentu, nodrošina elektroniskā dokumenta autentiskumu un apstiprina parakstītāja identitāti” [14]

Lai elektronisko parakstu varētu radīt ir nepieciešami tā radīšanas dati.

Eiropas Parlamenta un padomes Direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu 2. panta 4. punktā elektroniskā paraksta radīšanas dati tiek definēti: „4) *paraksta radīšanas dati* ir unikāli dati, piemēram, kodi vai privātas šifrēšanas atslēgas, ko parakstītājs izmanto elektroniska paraksta radīšanai;” [12]

Latvijas Republikas Elektronisko dokumentu likuma 1. panta 6. punktā elektroniskā paraksta radīšanas dati tiek definēti šādi: ”6) *elektroniskā paraksta radīšanas dati* — tikai vienreiz radīti dati, kurus parakstītājs izmanto, lai radītu elektronisko parakstu;” [14]

Elektroniskā paraksta izpratnē tā radīšanas dati ir privātā šifrēšanas atslēga.

Darba autors uzskata, ka paraksta pārbaudīšanas datu definīcija Elektronisko dokumentu likumā ir ļoti riskanta, jo nenosaka paraksta radīšanas datu unikalitāti. Detalizētāk šis risks tiek apskatīts darba 4.7.6.6 nodaļā.

Eiropas Parlamenta un padomes Direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu 2. panta 7. punktā elektroniskā paraksta pārbaudīšanas dati tiek definēti: ”7) *paraksta pārbaudes dati* ir dati, piemēram, kodi vai publiskas šifrēšanas atslēgas, ko izmanto elektroniska paraksta pārbaudei;” [12]

Latvijas Republikas Elektronisko dokumentu likuma 1. panta 5. punktā elektroniskā paraksta pārbaudīšanas dati tiek definēti šādi: ”5) *elektroniskā paraksta pārbaudes dati* — dati, kurus izmanto, lai pārbaudītu elektronisko parakstu;” [14]

Elektroniskā paraksta izpratnē tā pārbaudes dati ir publiskā šifrēšanas atslēga.

Elektronisko parakstu var realizēt, izmantojot dažādus risinājumus, tai skaitā šifrēšanas algoritmus. Latvijā elektroniskais paraksts tiek realizēts ar RSA šifrēšanas algoritmu, vienkārši nošifrējot parakstāmā dokumenta jaucējfunkcijas vērtību (darba rakstīšanas laikā Latvijas Republikas Elektronisko dokumentu likuma realizācijā tiek izmantota SHA-1 jaucējkode funkcija). [16] Elektroniskais paraksts tiek veidots parakstītājam noteiktu informāciju

nošifrējot ar savu privāto atslēgu. Šīs informācijas saņēmējs to var atšifrēt ar parakstītāja publisko atslēgu, kas viņam ir zināma. Atšķirībā no Latvijas, Amerikas Savienotajās Valstīs no 1994. gada valdības vajadzībām tiek izmantots *DSA* (digitālā paraksta algoritms), kura pamatā ir *ElGamala* konstrukcija un kuru izmanto tikai elektroniskā paraksta radīšanai. [163] *DSA* algoritmā tiek izmantota dokumenta jaučējfunkcijas vērtība, bet tā netiek vienkārši šifrēta kā *RSA* gadījumā. [163] Pastiprinātas drošības vajadzībām ieteicams izmantot *DSA* algoritma eliptisko līkņu variantu *ECDSA*(eliptisko līkņu digitālā paraksta algoritms). [163] *DSA* algoritma gadījumā paraksta pārbaude tiek balstīta uz citiem principiem nekā tas ir *RSA* gadījumā. [163]

Eiropas Parlamenta un padomes Direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu 2. panta 2. punkta c apakšpunkts un Latvijas Republikas Elektronisko dokumentu likuma 1. panta 2. punkta c apakšpunkts nosaka prasību, ka uzlabota/droša elektroniskā paraksta radīšanas datus var kontrolēt tikai parakstītājs. [12,14] Latvijas drošs virtuālais elektroniskais paraksts neatbilst šīm prasībām un šis Latvijas Republikas Elektronisko dokumentu likuma realizācijas risks plašāk tiek apskatīts šī darba 4.3.2 nodaļā.

2 EIROPAS SAVIENĪBAS LIKUMDOŠANA

1997. gada 16. aprīlī Eiropas Komisija iesniedz Eiropas Parlamentam, Padomei, Ekonomikas un sociālo lietu komitejai un Reģionu komitejai ziņojumu par Eiropas elektroniskās tirdzniecības iniciatīvu. [12]

1997. gada 8. oktobrī Eiropas Komisija iesniedz Eiropas Parlamentam, Padomei, Ekonomikas un sociālo lietu komitejai un Reģionu komitejai ziņojumu par drošības un uzticības nodrošināšanu elektroniskajā saziņā. [12]

1998. gada 13. maijā Eiropas Savienības parlamentam un padomei tiek iesniegts likumdošanas projekts *COM(1998)0297*. [178] Tā pēdējā versija tiek parlamentā parakstīta 1999. gada 13. decembrī. [160]

2000. gada 19. janvārī iepriekš minētais un apstiprinātais likumdošanas projekts tiek publicēts Eiropas Savienības oficiālajā vēstnesī kā Direktīva 1999/93/EK par Kopienas elektronisko parakstu sistēmu. [160,12] Tā ir juridiski saistoša visām Eiropas Savienības dalībvalstīm attiecībā uz tajā noteikto sasniedzamo rezultātu un mērķi. [57]

Šīs direktīvas pamata mērķis ir izveidot kopienas regulējumu elektroniskā paraksta ieviešanai un izmantošanai, veicināt tehnoloģiju attīstību, brīvā tirgus konkurenci, sakārtotību un informācijas tehnoloģiju pakalpojumu starptautisku sadarbību. [8, 113, 12] .

2012. gada 4. jūnijā tiek publicēts priekšlikums Eiropas Savienības parlamenta un padomes Regulai par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū *COM/2012/0238*. [180]

Tiesiskā regulējuma priekšlikuma pamatojumā tiek norādītas Eiropas digitalizācijas programmas atklātās problēmas Direktīvas 1999/93/EK ieviešanā un spēkā esošajā regulējumā. [113, 84] Tiek atzīts tas, ka nav izdevies direktīvu īstenot pietiekamā apmērā. [179, 156] Šīs problēmas tiek uzskaitītas: *"Tika konstatētas četras problēmas: direktīvas atšķirīgā īstenošana valsts līmenī, ko radīja atšķirīgā interpretācija dalībvalstīs, de facto izņēmumu piemērošana lietojumiem publiskajā sektorā, novecojuši standarti un neskaidras uzraudzības saistības, kas radīja pārrobežu sadarbības problēmas, sadrumstalotību Eiropas Savienībā un iekšējā tirgus izkropļojumus."*

Tiek norādītas divas problēmas un šķēršļi veiksmīgai elektroniskās identifikācijas un autentifikācijas, elektronisko parakstu un saistīto papildus uzticamības pakalpojumu ieviešanai un izmantošanai Eiropas Savienībā: [179]

1. tirgus sadrumstalotība,
2. nepietiekama uzticamība un palāvība.

Par pirmo problēmu Eiropas Komisijas regulas priekšlikuma ietekmes novērtējuma kopsavilkumā par tiek rakstīts: „(..) eID jomā sadarbības problēmas radīja atšķirīgie personas identifikācijas tehniskie risinājumi atsevišķās dalībvalstīs, tiesiskās noteiktības trūkums un nepietiekama eID pārrobežu izmantošana, kā arī neskaidri sadalīta atbildība par identifikācijas datu pareizību.

Attiecībā uz saistītajiem uzticamības pakalpojumiem ES tiesiskā regulējuma trūkuma dēļ atsevišķās dalībvalstīs tika pieņemti valsts tiesību akti, kuri reglamentēja dažus no šiem pakalpojumiem, un pakalpojumu sniedzēji, kuri vēlējās piedāvāt savus pakalpojumus vairākās dalībvalstīs, saskārās ar augstām izmaksām. Abos gadījumos iekšējā tirgū tika radīti šķēršļi un sadrumstalotība.” [179]

Par otro problēmu Eiropas Komisijas regulas priekšlikuma ietekmes novērtējuma kopsavilkumā tiek rakstīts: „*Uzticēšanās trūkums un nepietiekama paļāvība uz elektroniskajām sistēmām, piedāvātajiem rīkiem un tiesisko noteiktību var radīt iespaidu, ka šajā jomā ir mazāk tiesisko garantiju nekā fiziskajā pasaulē.*

E-parakstu jomā valsts līmeņa uzraudzības prasības kvalitatīvi atšķiras atkarībā no konkrētās dalībvalsts, un tādēļ pusēm, kuras izmanto e-parakstu, ir grūtāk izvērtēt, kā pakalpojumu sniedzējs tiek uzraudzīts.

Savukārt eID un saistīto uzticamības pakalpojumu jomā dažādie valsts tiesību akti neļauj lietotājiem, tiešsaistē veicot pārrobežu darījumus, justies droši.” [179]

Eiropas Komisijas regulas priekšlikuma ietekmes novērtējuma kopsavilkumā tiek nosaukti četri galvenie iemesli iepriekš minētajām problēmām: [179]

1. Nepietiekami plaša piemērošanas joma pašreizējā tiesiskajā regulējumā, [179]
2. Nepietiekama koordinācija elektronisko parakstu un elektroniskās identifikācijas risinājumu izstrādē, [179]
3. Pārredzamības trūkums attiecībā uz drošības nodrošinājumu, [179]
4. Nepietiekama informētība / lietotāju piesaistīšana. [179]

Šīs problēmas piedāvā risināt ar Eiropas Savienības regulas izdošanu. Regula, atšķirībā no spēkā esošās direktīvas, pēc savas definīcijas ir juridiski saistoša visās tās daļās un tieši piemērojama bez dalībvalstu individuālām interpretācijām vai adaptācijām. Tā ir adresēta visām Eiropas Savienības dalībvalstīm, juridiskām un fiziskām personām. [57]

Regulas priekšlikumā COM(2012)238 tās mērķis ir izteikts šādi: „*Mērķis ir uzlabot spēkā esošos tiesību aktus, piemērošanas jomā ietverot arī paziņoto elektroniskās identifikācijas shēmu un ar tām saistīto citu nozīmīgu elektronisko uzticamības pakalpojumu savstarpēju atzīšanu un akceptēšanu ES līmenī”.* [180] Tajā tiek definēti uzticamības pakalpojumi, un tiek noteiktas vienotas prasības un uzraudzības kārtība katram no tiem, un citi aspekti, kas sekmēs

izvirzīto mērķu sasniegšanu. [180] Attiecībā uz tehnoloģijām, regula tiek veidota neitrāla.[180] Saskaņā ar priekšlikumu uzticamības pakalpojumi nozīmē: „*visi elektroniskie pakalpojumi, kas ietver elektronisko parakstu, elektronisko zīmogu, elektronisko laika zīmogu, elektronisko dokumentu, elektronisko piegādes pakalpojumu, tīmekļa vietņu autentifikācijas un elektronisko sertifikātu (tostarp elektroniskā paraksta un elektroniskā zīmoga sertifikātu) radīšanu, pārbaudi, validāciju, apstrādi un saglabāšanu;*” [180]

Ar šīs regulas stāšanās spēkā tiek paredzēts sasniegt šādus mērķus: [180]

- Nodrošināt digitālā vienotā tirgus izveidi; [180]
- Sekmēt galveno pārrobežu sabiedrisko pakalpojumu attīstību; [180]
- Veicināt un stiprināt konkurenci vienotajā tirgū; [180]
- Sekmēt lietotājiem (iedzīvotājiem un uzņēmumiem) ērti izmantojamas tehnoloģijas. [180]

2013. gada 4. aprīlī tiek sagatavots nozīmētās Rūpniecības, pētniecības un enerģētikas komitejas sagatavots ziņojama projekts *PE507.971* par priekšlikumu Eiropas Parlamenta un Padomes regulai par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū. [158] Tajā tiek atzinīgi novērtēti jau padarītais darbs, tiek izteikti precizējoši grozījumi un ierosinājumi, kas priekšlikuma pamata būtību nemaina, bet to papildina un konkretizē. [158]

Darba rakstīšanas brīdī tiek prognozēts, ka 2013. gada septembrī atbildīgā komiteja veic balsojumu par izvirzīto priekšlikumu, un tā paša gada decembrī priekšlikums tiek izskatīts plenārsēdē.

3 ELEKTRONISKAIS PARAKSTS LATVIJĀ

Tā kā elektroniskā paraksta pats pamats ir elektroniski dokumenti, tad pirmie aizmetņi elektroniskā paraksta ieviešanai Latvijā radās ar tā laika Ministru prezidenta Andra Bērziņa 2000. gada 4. janvārī izdoto rīkojumu Nr.1 „Par darba grupu elektronisko dokumentu ieviešanai”. Tas savu spēku saglabāja līdz 2000. gada 21. jūlijam, kad Ministru prezidents izdeva rīkojumu Nr. 278 „Par darba grupu ar elektronisko dokumentu ieviešanu saistīto jautājumu risināšanai”. Šis rīkojums sevī iekļāva izmaiņas atbildīgo darba grupas personu sarakstā. [38, 37, 50] Pa starpu tam Ministru kabinets 2000.gada 13.jūnijā apstiprināja koncepciju par elektronisko dokumentu juridisko statusu Latvijā, kuras realizēšanai bija nepieciešams Elektronisko dokumentu likums. [14]

2002.gada 6.februārī stājās spēkā Ministru kabineta noteikumi Nr.141 „Informācijas sistēmās esošo dokumentēto datu un elektronisko dokumentu arhivēšanas noteikumi”, kas bija saistoši valsts un pašvaldību iestādēm, kur bija noteikti izmantojamie failu formāti datu ilgstošai vai patstāvīgai glabāšanai.[31, 50] Elektronisko dokumentu glabāšana šo noteikumu divdesmitā punkta kārtībā ir noteikta magnētiskajās lentēs vai ierakstāmajos kompaktdiskos.[31, 50]

2002. gada 31. oktobrī Saeimā tiek pieņemts Elektronisko dokumentu likums, un tas stājās spēkā 2003. gada 1. janvārī. Šī likuma 19. panta pirmajā daļā tiek noteikts: *”Datu valsts inspekcija ir uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzības iestāde”*. Praktiski ieviests šis likums uzreiz netiek, jo tajā laikā vēl tiek meklēta institūcija, kas uzņemtos uzticama sertifikācijas pakalpojumu sniedzēja statusu. [14, 50] Pēc diviem likuma grozījumiem 2004. gadā Ministru kabinets 2005. gada 3. maijā apstiprina elektroniskā paraksta ieviešanas grafiku.[72, 50] Tā paša gada 19. aprīlī, pēc Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta informatīvā ziņojuma „Par elektroniskā paraksta ieviešanas gaitu” izskatīšanas un pieņemšanas zināšanai, Ministru kabinets uzdod Īpašu uzdevuma ministra elektroniskās pārvaldes lietās sekretariātam sadarbībā ar Satiksmes, Finanšu, Iekšlietu un Tieslietu ministrijām izstrādāt koncepcijas projektu par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā.[50, 63, 111] Šīs Ministru kabineta sēdes protokola divdesmit devītā paragrāfa trešajā punktā tiek noteikts: *”3. Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariātam uzsākt konsultācijas ar SIA (sabiedrība ar ierobežotu atbildību) „Lattelekom” un VAS (valsts akciju sabiedrība) „Latvijas Pasts”, kā arī citiem interesentiem par droša elektroniskā paraksta ieviešanas iespējamiem risinājumiem Latvijā (..)”* [50, 63, 91] Secīgi

2005. gada 14. jūnijā Ministru kabinetā tiek apstiprināts un pieņemts zināšanai Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta ziņojums "Par vienošanos droša elektroniskā paraksta ieviešanai Latvijā". [101, 79, 78, 62] Ziņojuma otrajā nodaļā tiek teikts: „Konsultāciju laikā starp ĪUMEPLS, VAS „Latvijas Pasts” un SIA „Lattelekom” (puses), puses nonāca pie slēdziena, ka droša elektroniskā paraksta ieviešanas optimāls risinājums ir Latvijas valsts, VAS „Latvijas Pasts” un SIA „Lattelekom” sadarbība droša elektroniskā paraksta ieviešanas pasākumu grafikā apstiprināto pasākumu realizēšanai. Puses vienojās par nepieciešamību minētās sadarbības pamatprincipus nostiprināt trīspusējā sadarbības līgumā starp Latvijas valsti, VAS „Latvijas Pasts” un SIA „Lattelekom””. Minētais trīspusējais līgums tiek parakstīts 2005. gada 15. jūnijā. [50, 124, 62] Viens no līguma pamata mērķiem ir, visām trīs pusēm sadarbojoties, izveidot droša elektroniskā paraksta izmantošanai nepieciešamo infrastruktūru un gan attīstīt elektronisko pakalpojumus, gan veicināt to izmantošanu Latvijā. [62, 125]

Tikmēr notiek darbs pie elektronisko dokumentu apstrādi reglamentējošiem noteikumiem un 2005. gada 2. jūlijā stājas spēkā Ministru kabineta noteikumi Nr.473 „Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām”. [50, 13] Tie galvenokārt ir tieši saistoši valsts un pašvaldību iestādēm un arī gan fiziskām, gan juridiskām personām, kas veido saziņu ar iepriekš minētajām iestādēm. Šie noteikumi nosaka arī to, ka elektronisko dokumentu apritei var izmantot elektronisko pastu, iestāžu pārziņā esošās speciālās tiešsaistes formas un 3,5” formāta disketes. [50,13] Tie ietver arī norādījumus iekļaut elektroniskajos dokumentos drošu elektronisko parakstu un laika zīmogu. [13]

2005. gada 18. oktobrī Ministru kabineta sēdē tiek apstiprināts koncepcijas projekts par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijā, un 2005. gada 7. novembrī stājas spēkā Ministru kabineta rīkojums Nr. 714 „Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā”. [50, 7, 73, 90] Tiek nolemts kā elektroniskā paraksta nesēju izvēlēties nevis USB marķierierīci, bet viedkarti, jo tad gūto pieredzi varēs veiksmīgi izmantot elektroniskā paraksta iestrādāšanai personas apliecību kartēs (tagad elektroniskās identifikācijas kartes). [7]

2005. gada 19. augustā tiek izsludināts atklāts iepirkuma konkurss „Par uzticama sertifikācijas pakalpojumu sniedzēja informatīvās sistēmas piegādi un uzstādīšanu droša elektroniskā paraksta ieviešanai Latvijas Republikā”. Tajā uzvaru gūst SIA „Microsoft

Latvia”, un 2005. gada 20. decembrī tiek parakstīts iepirkuma līgums starp VAS ”Latvijas Pasts” un uzvarētāju par Uzticama sertifikācijas pakalpojumu sniedzēja nepieciešamo informācijas sistēmu un programmnodrošinājuma piegādi un uzstādīšanu droša elektroniskā paraksta ieviešanas vajadzībām.[69,50,65,88,103,74]

2006. gada 24. aprīlī Ministru kabineta sēdē tiek apstiprināti un tā paša gada 21. jūlijā stājas spēkā Grozījumi elektronisko dokumentu likumā, kas paredz iekļaut papildus tiesību normas, regulējumus un likuma punktu konkretizējumus, kas izriet no Eiropas Parlamenta un Padomes 1999.gada 13.decembra direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu.[50,20,100]

2006. gadā tiek veiksmīgi pabeigts VAS „Latvijas Pasts” sertifikācijas pakalpojumu sistēmu audits un 2006. gada 4. oktobrī tiek saņemta Datu valsts inspekcijas akreditācija un VAS „Latvijas Pasts” kļūst par vienīgo uzticamu sertifikācijas pakalpojumu sniedzēju Latvijā.[50,75] Tajā pašā mēnesī tā laika Ministru prezidents Aigars Kalvītis paraksta pirmo dokumentu ar elektronisko parakstu. Tiek parakstīts valdības gada piecdesmitais sēdes protokols. VAS „Latvijas Pasts” tā laika ģenerāldirektors Gints Škodovs pasniedz Ministru prezidentam pirmo elektroniskā paraksta viedkarti.[62,73]

2007. gada 27. februāra Ministru kabineta sēdē tiek apstiprināts Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta iesniegtais likumprojekts par grozījumiem Elektronisko dokumentu likumā.[97,106] 2007. gada 24. maijā minētie grozījumi stājas spēkā, kas sevī ietver izmaiņas esošos likuma punktos, to precizējumus, papildinājumus ar mērķi samazināt tehniskus un organizatoriskus šķēršļus elektroniskā paraksta ieviešanai un lietošanai.[106,6,20]

Sākot ar 2007. gada 23. aprīli Sekretariāts sarakstei ar valsts iestādēm sāk izmantot dokumentus, kas ir parakstīti ar drošu elektronisko parakstu.[65,81]

2007. gada 31. maijā Valsts sekretāru sanāsmē tiek izsludināts Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta veidotais koncepcijas projekts „Par droša elektroniskā paraksta finansēšanu atsevišķās iedzīvotāju mērķa grupās”, kur tika atbalstīts lēmums finansēt elektroniskā paraksta iegādi ārstiem, skolotājiem un bibliotekāriem piecdesmit procentu apmērā no valsts budžeta līdzekļiem.[50,85,86] Šis koncepcijas projekts 2007. gada 13. decembra Valsts sekretāru sanāsmē tiek atsaukts.[122]

2007. gada 13. novembrī Ministru kabineta sēdē tiek apstiprināti un tā paša gada 16. novembrī stājas spēkā Ministru kabineta noteikumi Nr.760 „Grozījumi Ministru kabineta 2005.gada 28.jūnija noteikumos Nr.473 "Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm

iestādēm un fiziskajām un juridiskajām personām”[50,122,22,112]. Noteikumu projekts precizē elektroniskā dokumenta noformēšanas prasības, izmantojamās datņu formātus, elektroniskā pasta sūtījumam pievienoto datņu pieļaujamo lielumu un papildina elektronisko dokumentu apriti nodrošinošo datu nesēju sarakstu.[22,108,112]

2008. gada 1. aprīlī Ministru kabineta sēdē tiek pieņemti zināšanai Satiksmes ministrijas informatīvie ziņojumi „Par valsts akciju sabiedrības "Latvijas Pasts" problēmām, kas saistītas ar pasta pamatpakalpojumu nodrošināšanu Latvijas teritorijā” un „Par valsts akciju sabiedrības "Latvijas Pasts" preses izdevumu piegādes pakalpojumu sniegšanas lauku apvidos radīto zaudējumu kompensēšanu”.[92,89] Tiek atbalstīts Satiksmes ministrijas izvirzītais priekšlikums par to, ka VAS "Latvijas Pasts" neturpinās sertifikācijas pakalpojumu sniegšanu, un tiek uzdots Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariātam sagatavot un līdz 2008. gada 6. jūnijam iesniegt koncepcijas projektu par sertifikācijas pakalpojumu turpmāko attīstību.[92,89]

2008. gada 28. maijā ārkārtas Ministru kabineta sēdē tiek pieņemts zināšanai Satiksmes ministrijas sagatavotais informatīvais ziņojums „Priekšlikumi par valsts akciju sabiedrības "Latvijas Pasts" turpmāko rīcību saistībā ar sertifikācijas pakalpojumu nodošanu citai institūcijai” un apstiprināts priekšlikums atsavināt sertifikācijas pakalpojumus no valsts akciju sabiedrības „Latvijas Pasts” un tos nodot valsts akciju sabiedrībai „Latvijas Valsts radio un televīzijas centrs”. [73,62,93]

2008. gada 14. jūlijā Ministru kabineta sēdē tiek pieņemts zināšanai Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta sagatavotais informatīvais ziņojums „Par koncepcijas "Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā" īstenošanas gaitu”, kurā kā problēmas droša elektroniskā paraksta ieviešanā tiek minētas: iestāžu darbinieku neinformētība par iespējām saņemt elektronisko parakstu, iestāžu darbinieku mazā aktivitāte sagatavoto viedkaršu izņemšanā un iestāžu darbinieku mazā aktivitāte personīgo viedkaršu izgatavošanas pieteikumu iesniegšanā.[70,110]

2008. gada 17. septembrī tiek parakstīts līgums starp VAS „Latvijas Valsts radio un televīzijas centrs” un VAS „Latvijas Pasts” par sertifikācijas pakalpojumu pārņemšanu.[73]

2009. gada 10. martā Ministru kabineta sēdē tiek pieņemts zināšanai Īpašu uzdevumu ministra elektroniskās pārvaldes lietās sekretariāta sagatavotais informatīvais ziņojums „Par valsts un pašvaldību iestāžu (to skaitā arī iestāžu struktūrvienību) gatavību ar 2010.gada 1.janvāri pāriet uz dokumentu apriti starp iestādēm, izmantojot elektroniski parakstītus dokumentus”, un tiek uzdots atbildīgajām iestādēm sagatavot rīcības plānu valsts pārvaldes iestāžu teritoriālo struktūrvienību un novada domju pārejai uz elektroniski parakstītu

dokumentu apriti, veikt interneta ātruma pieslēguma analīzi, paātrināt elektroniskā dokumenta parakstīšanas procedūras. [68,71,98]

2009. gada 31. maijā tiek pabeigts sertifikācijas pakalpojumu sistēmu un procedūru audits un VAS „Latvijas Valsts radio un televīzijas centrs” iegūst uzticama sertifikācijas pakalpojumu sniedzēja statusu, un pārņem šo funkciju no VAS „Latvijas Pasts”. [73]

2010. gada 10. februārī stājas spēkā Ministru kabineta rīkojums Nr.62 „Par Elektronisko identifikācijas karšu koncepciju”, kur tiek noteikts, ka elektroniskā identifikācijas karte ir elektroniskā paraksta radīšanas (lietošanas) līdzekļu nesējs. [76,99]

2011. gada 1. februārī tiek ieviests virtuālais elektroniskais paraksts. [107,115]

2011. gada 22. februārī Ministru kabineta sēdē tiek pieņemts zināšanai Satiksmes ministrijas sagatavotais informatīvais ziņojums „Par eParaksta praktiskās ieviešanas reālo situāciju un problēmām tā ieviešanā”, kur tiek norādīts uz šādām problēmām elektroniskā paraksta plašai lietošanai valsts sektorā: [62,73]

- Nav iespējams iesniegt valsts vai pašvaldību iestādei pilnu elektronisko dokumentu paketi [62,73]
- Vairākos likumos un Ministru kabineta noteikumos ir noteikts, ka dokumenti jāiesniedz vai nu papīra veidā vai klātesot pašam iesniedzējam. [62,73]
- Valsts un pašvaldību iestāžu ierēdņi bieži tulko normatīvos aktus sašaurināti, jo pietrūkst zināšanu darbam ar elektroniskajiem dokumentiem. [62,73]
- Neskaidrības par un ap elektronisko dokumentu nodošanu Valsts arhīvam. [62,73]

Ministru kabineta sēdē tiek dots uzdevums Satiksmes ministrijai sagatavot un nedēļas laikā iesniegt rīkojuma projektu par darba grupas izveidošanu ar mērķi izvērtēt veidus, kā nodrošināt elektroniskā paraksta plašāku lietošanu un sagatavot attiecīgus priekšlikumus. [96]

2011. gada 8. martā Satiksmes ministrija iesniedz un Ministru kabineta sēdē tiek pieņemts rīkojuma projekts „Par darba grupu elektroniskā paraksta plašākas lietošanas nodrošināšanai” [38]

2011. gada 17. martā stājas spēkā Ministru kabineta rīkojums Nr.114 „Par darba grupu elektroniskā paraksta plašākas lietošanas nodrošināšanai”. Darba grupā ir pārstāvji no Valsts kancelejas, Pilsonības un migrācijas lietu pārvaldes, Valsts ieņēmumu dienesta, VAS "Latvijas Valsts radio un televīzijas centrs", Satiksmes ministrijas, Veselības ministrijas, Tieslietu ministrijas, Vides aizsardzības un reģionālās attīstības ministrijas, Valsts kases un Iekšlietu ministrijas. Darba grupas vadītājs ir tā laika Satiksmes ministrijas valsts sekretārs Anrijs Matīss. [38]

2011. gada 7. jūnijā Ministru kabineta sēdē tiek apstiprināts Satiksmes ministrijas izstrādāts rīkojuma projekts „Grozījumi Elektronisko identifikācijas karšu koncepcijā”, kas

paredz koncepcijā veikt izmaiņas, nosakot VAS „Latvijas Valsts radio un televīzijas centrs” par elektroniskās identifikācijas karšu sertifikācijas pakalpojumu sniedzēja funkciju veicēju. [102,115,22] Šie grozījumi stājas spēkā 2011. gada 16. augustā ar Ministru kabineta rīkojumu Nr. 377. [22]

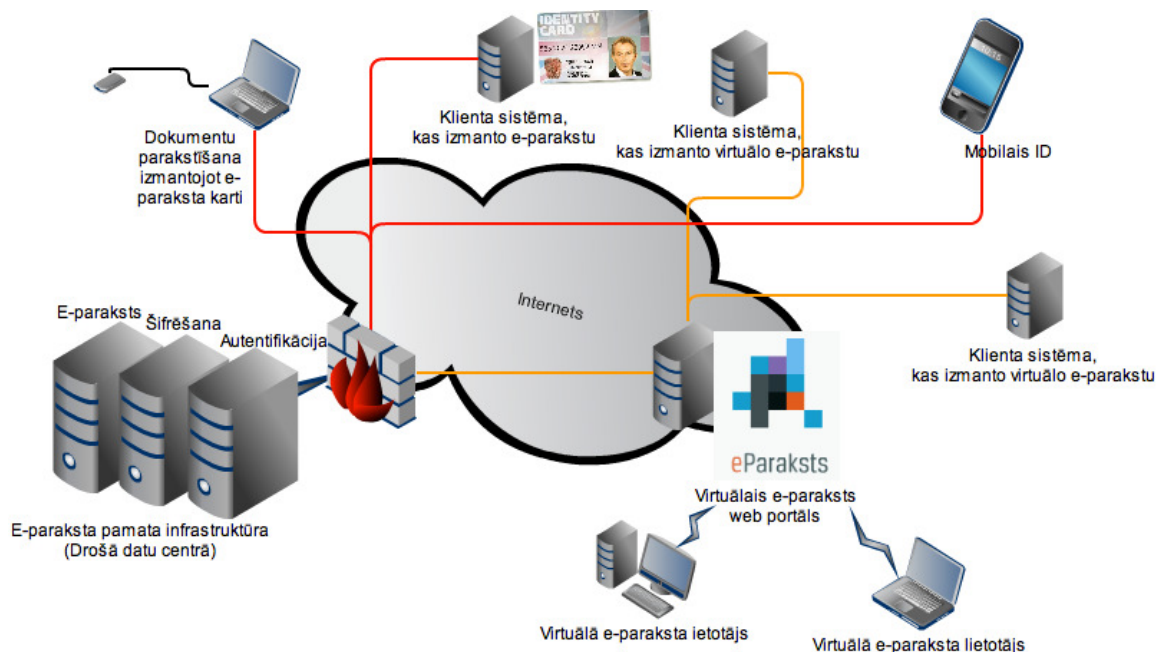
2011. gada 20. decembrī Ministru kabineta sēdē tiek pieņemts zināšanai Satiksmes ministrijas informatīvais ziņojums „Par priekšlikumiem elektroniskā paraksta plašākas lietošanas nodrošināšanai”, kas satur aprakstu par būtiskākajiem politikas plānošanas dokumentos ietvertajiem pasākumiem, kas nodrošinātu elektroniskā paraksta plašāku lietošanu. [76,66] Ziņojumā minētie priekšlikumi tiek atbalstīti un atbildīgajām institūcijām uzdoti attiecīgi uzdevumi to realizēšanai.[66]

2012. gada 1. aprīlī Latvijā sāk izsniegt elektroniskās identifikācijas kartes.[56]

2012. gada 23. oktobrī Ministru kabineta sēdē tiek izskatīts un apstiprināts Satiksmes ministrijas sagatavots likumprojekts „Grozījumi Elektronisko dokumentu likumā”, kas paredz izmaiņas Elektronisko dokumentu likumā ar mērķi paplašināt un atvieglot elektroniskā paraksta lietošanu. Darba rakstīšanas laikā likuma grozījumi Saeimā vēl nav pieņemti. [104,94,18]

2012. gada 11. decembrī Ministru kabineta sēdē tiek pieņemts zināšanai Satiksmes ministrijas informatīvais ziņojums „Par priekšlikumiem elektroniskā paraksta plašākas lietošanas nodrošināšanai”. [95,77,68] Ņemot vērā ziņojumā minētos priekšlikumus, tiek uzdots atbildīgajām iestādēm sagatavot saistošo normatīvo aktu labojumus, lai nodrošinātu plašāku un aktīvāku elektroniskā paraksta lietošanu starp valsts institūcijām un valstij piederošajām kapitālsabiedrībām. Tiek uzdots Satiksmes ministrijai sagatavot informatīvo ziņojumu par valsts kapitālsabiedrību iespējām un praksi izmantot drošu elektronisko parakstu elektroniskās saziņas procesā ar fiziskām un juridiskām personām, kā arī par iedzīvotāju informēšanu par dokumentu elektroniskās aprites iespējām.[95,77]

Maģistra darba rakstīšanas laikā esošā VAS „Latvijas Valsts radio un televīzijas centrs” sertifikācijas pakalpojumu arhitektūra redzama attēlā 3.1



3.1 att. eParaksta sistēmas arhitektūra [73,62]

Droša elektroniskā paraksta nesēju veidu pārskats ir pieejams pielikumā Nr. 19.

3.1 LATVIJAS ELEKTRONISKO DOKUMENTU LIKUMA SALĪDZINĀJUMS AR IGAUNIJAS DIGITĀLĀ PARAKSTA LIKUMU

Maģistra darba autors šajā nodaļā iekļaus tikai tās lietas, ko uzskata par būtiskākajām atšķirībām starp Latvijas Elektronisko dokumentu un Igaunijas Digitālā paraksta likumu, neapskatot visas tās lietas, kas ir identiskas, vienādas vai līdzīgas.

Latvijas Elektronisko dokumentu likumā tiek runāts tikai par sertifikācijas pakalpojumu sniegšanu, kur sertifikācijas pakalpojumos ir iekļauti arī laika zīmoga pakalpojuma sniegšana. [14] Vienīgā pakalpojumu atdalīšana ir tajā, vai sertifikācijas pakalpojumu sniedzējs ir uzskatāms par uzticamu vai nav (8. panta trešā daļa). [14] Igaunijas digitālā paraksta likumā tiek izdalīti atsevišķi laika zīmoga pakalpojuma sniedzēji (atrunāts Igaunijas Digitālā paraksta likuma 23. – 28. pants) un sertifikācijas pakalpojumu sniedzēji (atrunāts Igaunijas Digitālā paraksta likuma 17. – 22. pants). [43]

Latvijas Elektronisko dokumentu likuma 8. panta pirmā daļa nosaka: „*Sertifikācijas pakalpojumu sniedzējs ir fiziskā vai juridiskā persona, kas sniedz sertifikācijas pakalpojumu bez speciālas atļaujas saņemšanas*”. [14] Tātad sertifikācijas pakalpojumu sniedzējs Latvijā var būt jebkura fiziska vai juridiska persona. Šie pakalpojumu sniedzēji Latvijā tiek dalīti

divās grupās – uzticami un pārējie. [14] Igaunijas Digitālā paraksta likumā ir plašāks definējums tam, kas var būt sertifikācijas pakalpojumu sniedzējs. Tas nosaka, ka gan laika zīmoga pakalpojumu sniedzējs (25. pants), gan sertifikācijas pakalpojumu sniedzējs (18. pants) var būt tikai: [43]

- Sabiedrība ar ierobežotu atbildību, [43]
- privāta akciju sabiedrība, kuru akciju kapitāls pārsniedz 400 000 kronas jeb apmēram 18 180 Ls, [43]
- publiska persona, ja tas ir noteikts publiskās personas regulējošajā likumā, [42]
- valsts aģentūras, ko noteikusi valsts valdība. [43]

Igaunijas Digitālā paraksta likums nosaka arī to, ka sertifikācijas un laika zīmoga pakalpojumu sniedzējiem nedrīkst būt nodokļu parādu vai jebkādu citu parādu, kas varētu apdraudēt likumā noteikto pakalpojuma sniegšanas prasību izpildi (Igaunijas Digitālā paraksta likuma 19.panta trešā daļa).[43] Latvijas Elektronisko dokumentu likums, savukārt, pieļauj jebkādas esošas parādu saistības sertifikācijas pakalpojumu sniedzējiem un uzticamiem sertifikācijas pakalpojumu sniedzējiem, ja tiek pildīta 9. panta 3. punkta prasība: *”uzturēt pietiekamus finansiālos resursus, lai izpildītu šā likuma un uz tā pamata izdoto normatīvo aktu prasības, un apdrošina savu profesionālās darbības civiltiesisko atbildību šā likuma 14. pantā noteiktajā apjomā un kārtībā.”* [14]

Tātad, Igaunijā ir stingrākas prasības pret sertifikācijas pakalpojumu sniedzējiem, tie nevar būt fiziskas personas, un tiem ir nepieciešams būt bez nodokļu parādiem un tādiem parādiem, kas var apdraudēt pakalpojumu sniegšanu.

Abos likumos ir atšķirība arī attiecībā uz pakalpojumu sniegšanas uzraudzību un kontroli. Latvijā kā uzraudzības iestāde ir nozīmēta Datu valsts inspekcija (Elektronisko dokumentu likuma 19. panta pirmā daļa). [14] Igaunijas Digitālā paraksta likums nosaka, ka atbildīgā par pakalpojuma kontroli, likuma izpildi un uzraudzību ir Igaunijas Ekonomikas un komunikācijas lietu ministrija (41. panta pirmā daļa), bet tā institūcija, kas ir atbildīga par personas datu aizsardzību (Latvijā Datu valsts inspekcija), ir atbildīga par sertifikācijas pakalpojumu sniedzēju reģistra uzturēšanas likumiskumu un personu datu aizsardzību, un to procedūru ievērošanu, kas noteiktas Igaunijas personu datu aizsardzības likumā un publiskās informācijas likumā (41. panta trešā daļa). [43]

Igaunijas Digitālā paraksta likuma 24. panta otrajā daļā tiek reglamentēta rīcība, ja dažādu laika zīmogu pakalpojumu sniedzēju izdotiem laika zīmogiem nevar precīzi noteikt to uzlikšanas laiku un secību uz viena dokumenta. [43] Tādā gadījumā tiek uzskatīts, ka visi laika zīmogi ir uzlikti vienlaicīgi.[43] Latvijas Elektronisko dokumentu likumā tādas procedūras neatrunā, bet 23.panta 20. punktā norāda, ka uzticamam sertifikācijas

pakalpojumu sniedzējam ir pienākums: *"nodrošināt, lai laika zīmogs norādītu starptautiski koordinēto precīzu laiku;"*. [14] Latvijas Elektronisko dokumentu likuma 9.panta 9. punktā norāda, ka laika zīmogam ir jānodrošina, lai datums un laiks būtu neapšaubāms. [14] Darba autors uzskata, ka šādas prasības nav pietiekošas, lai atrisinātu dažus no riskiem, kas var rasties šādas likumdošanas rezultātā. Daži no iespējamajiem riskiem tiks apskatīti šī darba 4.7.6.3 nodaļā.

Maģistra darba autors uzskata, ka viena no būtiskākajām atšķirībām starp Latvijas un Igaunijas sertifikācijas pakalpojumus regulējošo likumdošanu ir saistīta ar parakstītāja atbildību. Latvijas Elektronisko dokumentu likuma 25. panta pirmās daļas 4. punkts nosaka, ka parakstītājam ir pienākums: *"nodrošināt, lai elektroniskā paraksta radīšanas dati netiktu izmantoti bez parakstītāja ziņas"*. [14] Bet tā paša panta otrā daļa nosaka: *"Parakstītājs ir atbildīgs par zaudējumiem, kas nodarīti personai, kura saprātīgi paļāvusies uz kvalificētu sertifikātu, ka:*

- 1) Parakstītājs sniedz uzticamam sertifikācijas pakalpojumu sniedzējam nepatiesu informāciju;*
- 2) Parakstītājs pienācīgi nerūpējas par elektroniskā paraksta radīšanas datu aizsardzību pret neatļautu izmantošanu;*
- 3) Ir bijis pamats uzskatīt, ka elektroniskā paraksta radīšanas dati izmantoti bez parakstītāja ziņas, bet parakstītājs nav pieprasījis, lai uzticams sertifikācijas pakalpojumu sniedzējs anulē kvalificētu sertifikātu vai aptur tā darbību"* [14]

Tātad Latvijā pats parakstītājs ir atbildīgs par elektroniskā paraksta lietošanu neatkarīgi no tā, vai tas ir bijis izmantots ar vai bez viņa ziņas, un neatkarīgi no tā, vai ir iespējams pierādīt tiesā, ka pats parakstītājs nav varējis būt tas, kurš ir konkrētajā laikā un dienā radījis attiecīgo parakstu. Kā arī pat, ja tiek pierādīts, ka sertifikāta īpašnieks dokumentu nav parakstījis, tā parakstam tik un tā ir tāds pats juridiskais spēks kā ar roku parakstītam dokumentam.

Savukārt, Igaunijas Digitālā paraksta likuma 3. pantā atrunā, ka digitālajam parakstam nav tāds pats juridisks spēks kā ar roku rakstītam, ja to nosaka likums vai, ja var pierādīt, ka konkrētā sertifikāta privātā atslēga tika izmantota bez tā īpašnieka ziņas. Ja tiek pierādīts, ka privāto atslēgu ir izmantojusi persona, kas nav sertifikāta īpašnieks un kā cēlonis tam ir sertifikāta īpašnieka liela nolaidība vai speciāls nolūks, viņam(īpašniekam) ir jākompensē visi radušies zaudējumi. [43]

Gan Latvijas Elektronisko dokumentu likums, gan Igaunijas Digitālā paraksta likums nosaka sertifikāta īpašnieka atbildību par zaudējumiem, kas radušies gadījumā, ja paraksts ir izveidots bez sertifikāta īpašnieka ziņas vai viņa lielas nolaidības dēļ. [14,43] Bet lielākā

atšķirība ir tāda, ka šāds kļūdainš paraksts Latvijā būs ar juridisku spēku, bet Igaunijā tas savu juridisko spēku būs zaudējis.[14,43] Tas paver iespējas dažādiem riskiem, no kuriem uzskatāmākie tiek aplūkoti šī darba 4.7.6 nodaļā.

4 ELEKTRONISKĀ PARAKSTA IESPĒJAMIE RISKI

Šajā maģistra darba nodaļā tiek aplūkoti dažādu jomu riski saistībā ar Elektronisko dokumentu likuma realizāciju Latvijas Republikā.

4.1 AUDITORA NEATKARĪBAS UN KVALITĀTES RISKI

Latvijas Republikas Elektronisko dokumentu likums un Ministru kabineta noteikumi Nr.358 „Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi” nosaka nepieciešamību un kārtību, kādā tiek veikta uzticama sertifikācijas pakalpojumu sniedzēja pārbaude un akreditācija, lai uzticama sertifikācijas pakalpojumu sniedzēja statuss tiktu iegūts, saglabāts vai anulēts. [35,14]

Pielikumā Nr.15 esošajā VAS „Latvijas Valsts radio un televīzijas centrs” atbildē uz Arņa Paršova iesniegumu par sertifikācijas pakalpojumu auditiem (Pielikums Nr. 16) ir lasāms, ka visas uzticama sertifikācijas pakalpojumu sniedzēja ikgadējās pārbaudes ir veikusi viena un tā pati auditorkompānija SIA „KPMG Baltics”. [54] Arī 2012. gada pārbaudi veica šis uzņēmums(Pielikums Nr.4).

Darba autors vērš uzmanību tam, ka ne vienmēr veiksmīgs pārbaudes atzinums garantē drošu un uzticamu pakalpojumu sniegšanu. 2012. gada decembra beigās izskanēja sertifikācijas iestādes *TurkTrust* incidents, kur tika izsniegti vairāki krāpnieciski sertifikāti. [139,196,148] Saskaņā ar *TurkTrust* sniegto informāciju, incidenta cēlonis radās jau 2011. gada augustā.[139,196,148] No incidenta cēloņa rašanās līdz incidenta atklāšanai *TurkTrust* bija veiksmīgi nokārtojis divus *KPMG* auditorkompānijas *ETSI TS 102 042* standarta atbilstības auditus, vienu 2011. gada novembrī, otru 2012. gada novembrī. [139,196,148] Incidenta cēlonis radās sistēmas iekšēju testēšanas darbību rezultātā. [139,196,148] Darba autors uzskata, ka paļauties tikai uz ikgadēju pārbaudes ziņojumu nevar un ir nepieciešams veikt papildus ārpus kārtas pārbaudes pakalpojumu sniedzējiem.

Darba autors vērš uzmanību tam, ka to ekspertu, kurš veiks pārbaudi uzticamam sertifikācijas pakalpojumu sniedzējam pašreizējā Latvijas Elektronisko dokumentu likuma realizācijā izvēlas pats uzticamais sertifikācijas pakalpojumu sniedzējs, piemērojot Publisko iepirkumu likuma izņēmumu saskaņā ar tā 3. panta ceturto daļu (Pielikums Nr.15). [54]

Darba autors uzskata, ka tik ilga sadarbība ar tikai vienu konkrētu ekspertu kļūst par pamatojumu pārbaužu kvalitātes un neatkarības apšaubīšanai. Viens no piemēriem, kādas var būt sekas tam, ka ar konkrētu klientu strādā viens un tas pats auditors, ir 2013. gada aprīlī izskanējušajā *KPMG* un *Skechers* incidentā, kad tika atklāts, ka viens no *KPMG* partneriem tirgojies ar konfidenciālu klienta informāciju. [168]

Šāda stabila sadarbība ar vienu konkrētu auditoru tādā nopietnā jautājumā kā uzticama sertifikācijas pakalpojumu sniedzēja akreditācijas saglabāšana vai anulēšana ļauj abām iesaistītajām pusēm veikt savstarpējas vienošanās ar mērķi, lai uzticama sertifikācijas pakalpojumu statuss tā turētājam tiktu saglabāts un auditorkompānijai būtu garantēti ienākumi arī nākošajā gadā no līdzīgas pārbaudes veikšanas. Respektīvi, nākošā gada auditors kļūst neoficiāli zināms jau iepriekšējā audita veikšanas laikā. Piemēram, top spēkā noruna, ka auditors sniedz pozitīvu pārbaudes atzinumu, ja uzticams pakalpojumu sniedzējs apņemas nodrošināt to, ka arī nākošā gada auditu veiks šis pats eksperts. Darba autors pieļauj, ka auditorkompānija ir ieinteresēta veidot sadarbību ar klientu tādu, lai viņš arī nākošā gada audita veikšanai izvēlētos tieši viņa sniegtos pakalpojumus. Nav izslēgta iespēja, ka pārbaudes pakalpojuma ņēmējs VAS „Latvijas Valsts radio un televīzijas centrs” un pārbaudes pakalpojuma sniedzējs SIA „*KPMG Baltics*”, neilgi pirms ikgadējā audita oficiāli vai neoficiāli veic pirmsauditu, kur, tādā veidā, mēģinot nodrošināt pēc iespējas pozitīvāku audita atzinumu, laicīgi tiek sertifikācijas pakalpojumu sniedzējam atrastas esošās neatbilstības pret saistošajām Ministru kabineta noteikumos noteiktajām prasībām. Tad auditors dod sertifikācijas pakalpojumu sniedzējam pietiekoši daudz laika, lai tās kļūdas pirms īstā audita novērstu. Ar šādu pretimnākšanu, piemēram, auditors var paaugstināt savu iespējamību tapt izvēlētam par pārbaudes veicēju arī nākošā gada auditā.

Darba autors uzskata, ka tā ir nepareiza prakse, ka sertifikācijas pakalpojumu pārbaudes veicēju izvēlas pats sertifikācijas pakalpojumu sniedzējs bez jebkādiem speciāliem kontroles mehānismiem vai nosacījumiem. Tāpēc darba autora viedoklis un ierosinājums, kā uzlabot gan auditu veikšanas neatkarību, gan uzticamību ir noteikt kā obligātu ekspertu rotāciju ar nosacījumu, ja uzraudzības iestādes apstiprinātajā ekspertu sarakstā ir vairāk kā viena fiziska vai juridiska persona. Ar šo regulējumu, piemēram, tiktu ierobežotas iespējas pārbaudes veicējam ar sertifikācijas pakalpojumu sniedzēju slēgt neoficiālas vienošanās vai norunas, kas varētu apdraudēt sertifikācijas pakalpojumu drošību. Apziņa, ka nākošo pārbaudi veiks cits eksperts, radīs pārbaudes veicējiem lielāku motivāciju savu pienākumu veikt pēc iespējas kvalitatīvāk un pilnīgāk. Tas ir tāpēc, ka var tikt apšaubīta iepriekšējā eksperta kompetence, ja nākošais eksperts atklāj tādas neatbilstības normatīvajiem aktiem un drošības prasībām, ko varēja atklāt jau iepriekšējais eksperts. Negatīva pārbaudes vērtējuma gadījumā var tikt

apšaubīta arī iepriekšējo pārbaužu kvalitāte, kas pārējiem iesaistītajiem ekspertiem var radīt zaudējumus nesošus faktorus, piemēram, sliktu slavu, kas pasaules mēroga auditorkompānijai var būt ļoti nozīmīga.

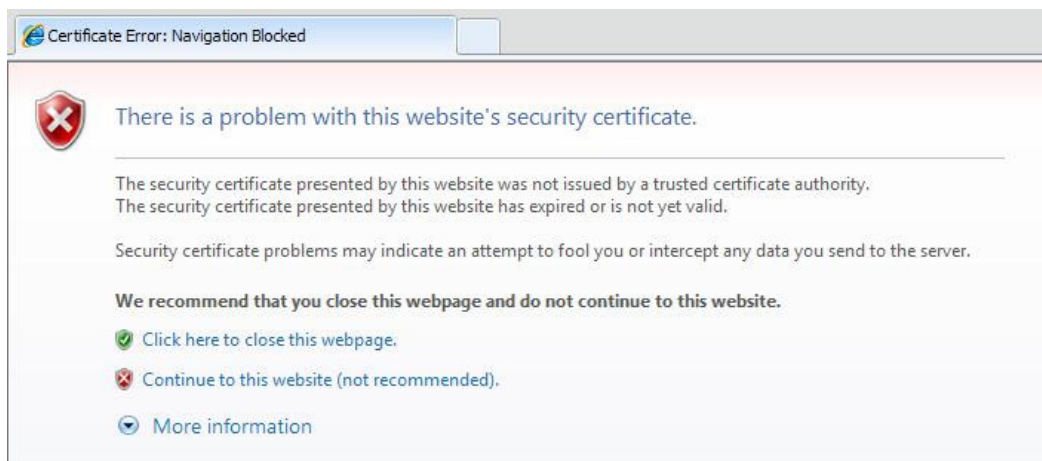
Darba autors vērs uzmanību tam, ka ilggadējam uzticama sertifikācijas pakalpojumu sniedzēja atbilstības pārbaužu (auditu) veicējam SIA „KPMG Baltics” tika atteikta dalība Valsts ieņēmumu dienesta organizētajā iepirkumu procedūrā „VID informācijas sistēmu drošības un veiktspējas novērtēšana”. [61]

4.2 VIRTUĀLĀ ELEKTRONISKĀ PARAKSTA PORTĀLA IZMANTOTĀ SSL CERTIFIKĀTA RISKI

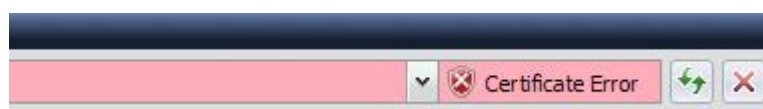
Virtuālā elektroniskā paraksta portālam *www.eparaksts.lv* ir paaugstinātas prasības pret drošību (darbs ar lietotāja datiem, dažāda veida autentificēšanās), tam ir nepieciešams izmantot arī drošus un šifrētus savienojumus datu pārraidei. To parasti panāk ar *SSL*(drošīgzdu slānis) sertifikātu izmantošanu, kas nodrošina apstrādāto un pārsūtīto datu šifrēšanu un aizsardzību pret to zagšanu, aizvietošanu vai citām kaitnieciskām darbībām.

Pazīstamākie *SSL* sertifikāta iegūšanas veidi:

- **Pašparakstīts** – sertifikātu ir radījis un tā uzticamību nodrošina un garantē pats sertifikāta izdevējs un radītājs. Ne visi sertifikātu izdevēji ir uzticami un pasaulē atzīti. Ja, piemēram, students sava praktiskā darba ietvarā izdod savu *SSL* sertifikātu, tad šis sertifikāts citām sistēmām var likties neuzticams, jo par konkrēto izdevēju nav atrodami dati uzticamu drošības sertifikātu izdevēju sarakstos. Ja sertifikāts tiek izmantots tīmekļa lapai, tad populārākajās interneta pārlūkprogrammās būs redzams brīdinājuma ziņojums par sertifikāta neuzticamību kā tas ir redzams attēlos 4.1 un 4.2



4.1 att. neuzticam savienojuma ziņojums Nr.1



4.2 att. neuzticama savienojuma ziņojums Nr.2

Lai paša izdots sertifikāts kļūtu pasaulē atzīts un uzticams, ir jāizpilda ļoti daudz prasību un kritēriju saistībā ar drošības procedūrām, tehniskās infrastruktūras drošību u.c. aspektiem, kas sekmē to, ka konkrētajam izdevējam var uzticēties.

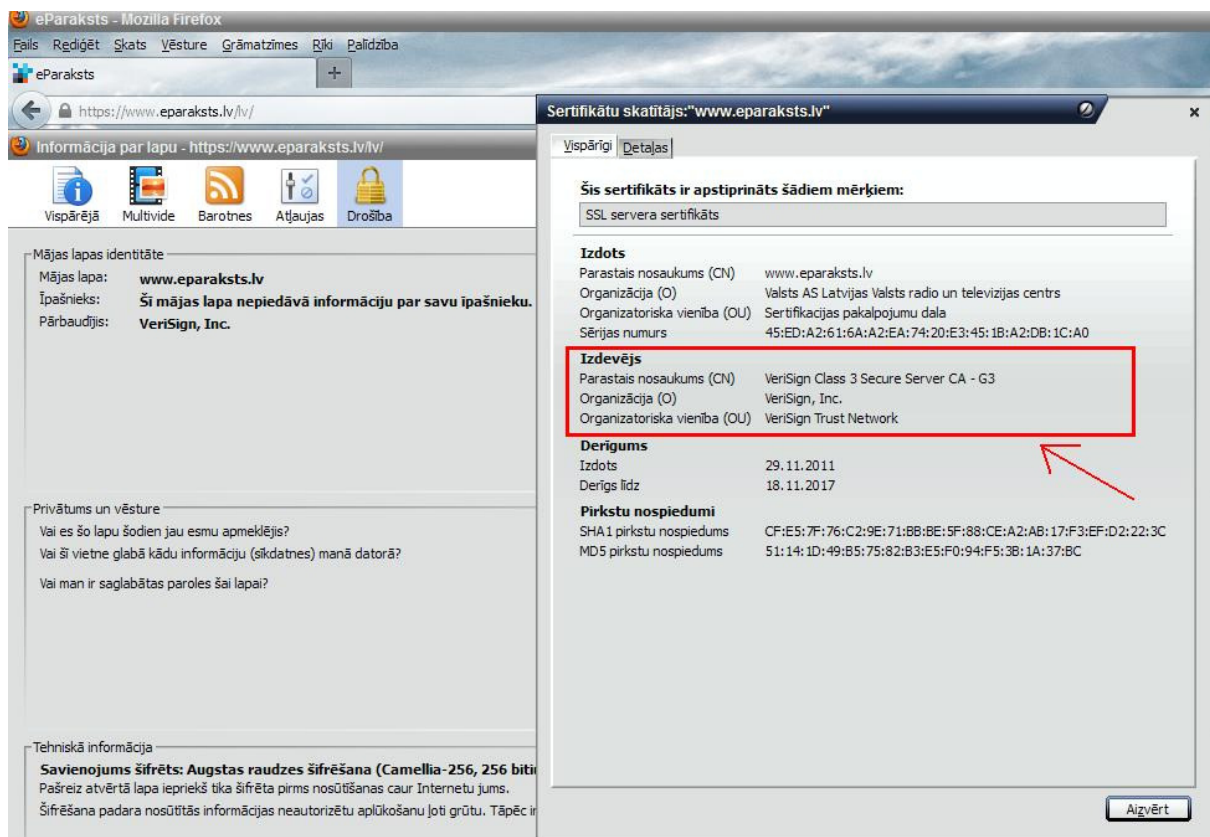
- **Nopirkts** – pasaulē ir ļoti daudz sertificēšanas pakalpojumu sniedzēju, kam kā viens no populārākajiem pakalpojumiem ir tieši *SSL* sertifikātu izdošana. Viens no pazīstamākajiem tāda veida pakalpojumu sniedzējiem ir *VeriSign*, kas tagad ir uzņēmuma *Symantec* sastāvā kopš 2010. gada augusta. [191]
Šāda veida sertifikātu ieguvums ir tāds, ka pasaules informācijas sistēmās tie jau tiek atzīti kā uzticami un droši kā tas ir redzams attēlā 4.3.



4.3 att. Uzticams savienojums

4.2.1 SSL CERTIFIKĀTA APSKATS

Aplūkojot portāla *www.eparaksts.lv* izmantoto *SSL* sertifikātu, var redzēt, ka sertifikāts nav paša uzticama sertifikācijas pakalpojumu sniedzēja izdots. Sertifikāts ir iegādāts no pasaulē pazīstama drošības un autentifikācijas pakalpojumu sniedzēja *VeriSign*. [197] Tas redzams attēlā nr.4.4



4.4. att. Informācija par SSL sertifikātu

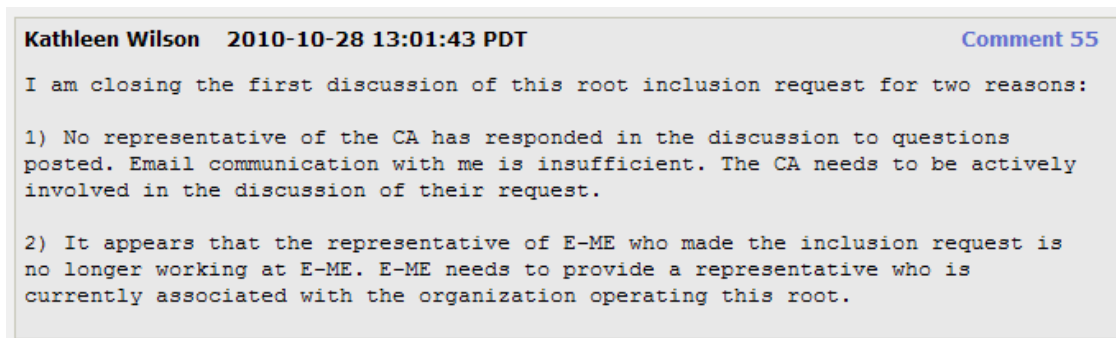
Detalizēta sertifikāta informācija atrodama pielikumā Nr. 1. un Nr. 2. Tātad Latvijā uzticama sertifikācijas pakalpojumu sniedzēja statusa turētājs VAS „Latvijas Valsts radio un televīzijas centrs” neizmanto sevis izdotu drošības sertifikātu.

Tam var būt dažādi iemesli, bet var izšķirt divus attiecībā no uzticības skatu punkta:

- 1) VAS „Latvijas Valsts radio un televīzijas centrs” neuzticas pats sevis izdotiem sertifikātiem,
- 2) Citas institūcijas neuzticas VAS „Latvijas Valsts radio un televīzijas centrs” izdotam SSL sertifikātam.

Otrais iemesls ir visticamākais, jo 2009. gada 9. septembrī VAS „Latvijas Valsts radio un televīzijas centrs” ir iesniedzis pieprasījumu iekļaut institūcijas izsniegtos sertifikātus

uzticamo sarakstā *Mozilla* korporācijai, kas uztur un attīsta *Mozilla Firefox* interneta pārlūku. [176,146,135,136,54] Iesniegtais pieprasījums šī darba rakstīšanas brīdī vēl nav apstiprināts. [176,146,135,136,54] Kopš pieprasījuma veikšanas saskaņā ar *Mozilla* korporācijas procedūru, kas nosaka sertificēšanas iestādes iekļaušanas *Mozilla Firefox* tīmekļa pārlūkprogrammas uzticamo saknes sertifikātu sarakstā, pirmā publiskā diskusija tika slēgta ar pamatojumu, kas redzams attēlā 4.5. [176,146,135,136,54]



4.5. att. Mozilla pārstāves atbilde par publiskās diskusijas slēgšanu

Pamatojuma būtība ir sertificēšanas iestādes neaktivitāte un neatbildēšana uz uzdotajiem jautājumiem. [176,146,135,136,54] Otra publiskā diskusija tika uzsākta 2012. gada 17. janvārī un tika noslēgta ar trīs nepieciešamām darbībām, kas jāveic elektroniskā paraksta pakalpojuma sniedzējam. [176,146,135,136,54] Vairākas no noteiktajām darbībām tika realizētas, bet pieteikuma pēdējā aktivitāte ir 2012. gada 6. jūlijā, kur uzticama sertifikācijas pakalpojumu sniedzēja pārstāvji informē, ka tiek veikti sistēmas uzlabojumi un vēlāk tiks sniegta papildus informācija. [176,146,135,136,54]

VAS „Latvijas Valsts radio un televīzijas centrs” saknes sertifikāts pašlaik ir iekļauts *Microsoft* saknes sertifikātu programmas dalībnieku sarakstā un tiek atpazīts kā uzticams tikai *Internet Explorer* interneta pārlūkprogrammā. [146,203]

VeriSign pakalpojumus saviem *SSL* sertifikātiem izmanto arī vairākas bankas Latvijā: AS (akciju sabiedrība) „SEB banka”, AS „UniCredit Bank”, AS „Expobank”, VAS "Latvijas Hipotēku un zemes banka", AS „Rigensis Bank”, AS "Latvijas Biznesa banka", AS "GE Money Bank", AS „ABLV Bank”, AS "Baltic International Bank", AS „Swedbank”. [52] [58]

4.2.2 SSL SERTIFIKĀTA DROŠĪBAS PĀRBAUDE

Attīstoties tehnoloģijām, tās kļūst arī daudz pieejamākas. Ir pieejami daudzi tiešsaistē pieejamu rīki, ar kuru palīdzību var tikt pārbaudīts jebkurš izmantotais *SSL* sertifikāts. Daži rīki veic arī padziļinātu *SSL* sertifikāta uzstādīšanas drošības analīzi. Šī darba ietvarā darba

autors vairākus no šiem rīkiem izmantoja, lai pārbaudītu virtuālā elektroniskā paraksta portālā *www.eparaksts.lv* izmantotā SSL sertifikāta drošību un uzticamību. SSL sertifikātu draudu un risku karte ir aplūkojama pielikumā Nr. 18.

Izmantotie tiešsaistes pārbaudes rīki:

- „COMODO SSL Analyzer” - <https://sslanalyzer.comodoca.com/>
- „The H Security SSL certificate test” - <http://www.h-online.com/nettools/tools/chksslkey>
- „GOGETSSL SSL installation checker” - <http://www.gogetssl.com/check-ssl-installation/>
- „Networking4all site check tool” - <http://www.networking4all.com/en/support/tools/site+check/>
- „Secure128 SSL certificate installation checker” - <http://www.secure128.com/resource/ssl-certificate-installation-checker.aspx>
- „VeriSign(Symantec) SSL certificate checker” - <https://ssl-tools.verisign.com/#certChecker>
- „Wormly SSL test” - https://www.wormly.com/test_ssl/
- „Digicert SSL certificate tester” - <http://www.digicert.com/help/>
- „BlueSSL Online server SSL test” - <https://www.bluessl.com/en/ssltest>
- „SSLShopper SSL checker” - <http://www.sslshopper.com/ssl-checker.html>
- „GlobalSign SSL configuration checker” - https://sslcheck.globalsign.com/en_US/sslcheck?host=www.eparaksts.lv
- „Qualys SSL Labs SSL server test” - <https://www.ssllabs.com/ssltest/index.html>

Izmantoto pārbaudes rīku pārbaūžu rezultātu kopsavilkuma tabula atrodama pielikumā Nr. 3

No izmantotajiem rīkiem visplašāko un detalizētāko analīzi veica „Qualys SSL Labs SSL server test” rīks. Tā analīzes metodoloģijas apraksts atrodams šī darba Pielikumā Nr. 17.

Portāla *www.eparaksts.lv* izmantotā SSL sertifikāta pārbaudes rezultātā tika atklātas vairākas ievainojamības un atvērtība dažādiem drošības riskiem.[118] Nopietnākie no atklātajiem riskiem ir:

- „BEAST” uzbrukuma ievainojamība [118]
- „CRIME” uzbrukuma ievainojamība[118]
- SSL 2.0 protokola atbalsts[118]
- Zemas šifrēšanas kodu komplektu atbalsts[118]
- RC4 protokola atbalsts[118]

Detalizētāks katra riska un ievainojamības apraksts tiks sniegts šīs nodaļas apakšnodaļās. Pārējie *SSL* sertifikāta pārbaudes rīki pārsvarā veica virspusēju sertifikāta uzticamības pārbaudi, līdz ar to arī testi tika nokārtoti veiksmīgi, pamatojoties uz to, ka sertifikāta pamata informācija bija atbilstoša un tā izdevējs ir uzticams.

Darba autors uzskata, ka drošības prasībām virtuālā elektroniskā paraksta interneta portālā ir jābūt tikpat augstām vai pat vēl lielākām nekā tās ir interneta bankām. Lietotāja autentifikācijai virtuālā elektroniskā paraksta portāls izmanto banku autentifikāciju, kur tiek izmantots attiecīgās bankas *SSL* sertifikāts, nodrošinot paaugstinātas drošības savienojumu. Pēc lietotāja autentificēšanas bankas *SSL* sertifikāta lietošana tiek pārtraukta un turpinās eparaksts.lv *SSL* sertifikāta izmantošana.

Virtuālā elektroniskā paraksta portāls tāpat kā *SEB* un *Swedbank* interneta bankas savienojumu nodrošināšanai izmanto *VeriSign* izdotus *SSL* sertifikātus, tāpēc darba autors veica uzstādīto *SSL* sertifikātu salīdzinājumu, tajā iekļaujot arī piezīmju veikšanas tiešsaistes rīku *Evernote*. Salīdzinājums ir redzams tabulā 4.1.

„Qualys sslabs” testa rezultātu salīdzinājums

	<i>eParaksts</i> (eparaksts.lv)	<i>Evernote</i> (evernote.com)	<i>SEB banka</i> (ibanka.seb.lv)	<i>Swedbank</i> (swedbank.lv)
Sertifikāta izdevējs	VeriSign Class 3 Secure Server CA - G3	VeriSign Class 3 Secure Server CA - G3	VeriSign Class 3 Extended Validation SSL SGC CA	VeriSign Class 3 Extended Validation SSL SGC CA
Testa vērtējums	F	A	B	A
Sertifikāta derīguma termiņš nav beidzies	<i>Passed</i>	<i>Passed</i>	<i>Passed</i>	<i>Passed</i>
Sertificēšanas organizācija ir uzticama	<i>Passed</i>	<i>Passed</i>	<i>Passed</i>	<i>Passed</i>
„BEAST” uzbrukuma ievainojamība	<i>Failed</i>	<i>Passed</i>	<i>Failed</i>	<i>Passed</i>
„CRIME” uzbrukuma ievainojamība	<i>Failed</i>	<i>Passed</i>	<i>Passed</i>	<i>Passed</i>
SSLv2 Protokola atbalsts	<i>Failed</i>	<i>Passed</i>	<i>Passed</i>	<i>Passed</i>
Zemas šifrēšanas kodu atbalsts	<i>Alarm</i>	<i>Passed</i>	<i>Passed</i>	<i>Passed</i>
RC4 protokola atbalsts	<i>Alarm</i>	<i>Alarm</i>	<i>Passed</i>	<i>Alarm</i>
Testa rezultāta URL	https://www.ssllabs.com/ssltest/analyze.html?d=www.eparaksts.lv	https://www.ssllabs.com/ssltest/analyze.html?d=evernote.com&s=204.154.94.73	https://www.ssllabs.com/ssltest/analyze.html?d=ibanka.seb.lv	https://www.ssllabs.com/ssltest/analyze.html?d=https%3A%2F%2Fwww.swedbank.lv%2F

Testa kopējo vērtējumu izsaka vērtībās A, B, C, D, E un F, kur „A” ir augstākā atzīme, bet „F” ir zemākā. [189] Tabulas 4.1 šūnās atzīme „*Failed*” nozīmē, ka tests ir neveiksmīgs un risks vai ievainojamība ir atklāta, „*Passed*” nozīmē, ka tests ir veiksmīgs un konkrētais risks vai ievainojamība nav atklāta. [189]

Virtuālā elektroniskā paraksta portāls *www.eparaksts.lv* un tiešsaistes piezīmju veikšanas rīks *Evernote* izmanto „*VeriSign Class 3 Secure Server CA - G3*” klases sertifikātu, bet abas aplūkotās interneta bankas izmanto „*VeriSign Class 3 Extended Validation SSL SGC CA*” klases SSL šifrēšanas sertifikātus. Tabulā 4.1 ir redzams, ja abām interneta bankām kopējā vērtējuma rezultāts ir līdzīgs (vērtējumi A un B), tad elektroniskajam paraksta un *Evernote* atšķirība ir ļoti būtiska (vērtējumi A un F). Šāds SSL sertifikāta drošības tests rada iespaidu ne tikai par to, cik kvalitatīvi un kompetenti tas ir tehniskajā risinājumā uzstādīts, bet no tā var spriest arī par pašu vidi, kurā SSL sertifikāts tiek izmantots. Var spriest arī par to, kāds konkrētajā vidē ir organizatorisko pasākumu kopums, kā tiek uzturēta tehniskā saimniecība u.c. pakalpojuma sniegšanas aspekti.

Tā kā vairākas ievainojamības un drošības riski tika atklāti neatkarīgi no izsniegtā sertifikāta klases, tas pierāda, ka svarīgāk par pašu sertifikāta klasi ir tieši informācijas sistēmas realizācija veids un uzstādījumi, ar kādiem konkrētais SSL sertifikāts ir uzstādīts uz serveriem. Ņemot vērā atklātās ievainojamības, portāla *eparaksts.lv* gadījumā SSL sertifikāta instalācija ir veikta ļoti nekvalitatīvi.

Ja atklātās ievainojamības darba rakstīšanas laikā netiek uzskatītas par praktiski ekspluatējamām, tas neatbrīvo uzticamu sertifikācijas pakalpojuma sniedzēju no to novēršanas atbildības. [45] Pastāv fakts, ka ievainojamība ir. Darba autors uzskata, ja ir atklāta ievainojamība, kas ilgu laiku netiek novērsta, tad tiek apšaubīts pakalpojumu sniegšanas un paša pakalpojuma uzticamības faktors.

Jebkurai ievainojamība jebkurā brīdī var tikt radīts uzlabots vai pilnveidots jau esošs mūķis, kas to padara praktiski ekspluatējamu. Labākajā gadījumā mūķa izstrādātāji un uzlaboto uzlaušanas algoritmu autori laicīgi informē sabiedrību par sava darba rezultātiem un iespējamiem aizsardzības veidiem. Vēl labākā gadījumā autori pirms publicēt sava darba rezultātu plašākai sabiedrībai, informē individuāli atbildīgās un ieinteresētās organizācijas, izstrādātājus un pakalpojumu piegādātājus, lai tie var laicīgi sagatavot ielāpus savām sistēmām.

Sliktākajā gadījumā ievainojamību padara praktiski ekspluatējamu un mūķi izstrādā cilvēks, kas sava darba rezultātu izmanto nevis plašas sabiedrības, bet gan savu personīgu vai ieinteresētu kaitniecisku grupu interesēs.

4.2.2.1 „BEAST” UZBRUKUMA IEVAINOJAMĪBA

Viens no portāla *eparaksts.lv* SSL sertifikāta analīzes rezultātā atrastajiem drošības riskiem ir ievainojamība pret „BEAST” uzbrukumu. „BEAST” ir abreviatūra no „*Browser Exploit Against SSL/TLS*” jeb „Pārlūka Mūķis Pret SSL/TLS”. [188,194,164]

Par šo ievainojamību pirmās ziņas parādījās jau 2001. gadā, un tika izskatīta rakstos 2005. un 2006. gadā, bet tā tika atzītā par nepraktisku un atrisināma, ieliekot šifrētu bloku virknēšanas papildinājumu(*CBC padding*) kriptogrāfiskā risinājuma inicializācijas vektorā tukšus datu fragmentus. [188,194,164, 141] Tas tika jau izdarīts *TLS 1.1* versijā, kas vēl mūsdienās nav plaši lietota. [188,194,164] Vairākās tīmekļa vietnēs un serveros vēl tiek izmantots *TLS 1.0* versija, kur šī ievainojamība vēl ir aktuāla.[193,169,188]

2011. gadā šī ievainojamība tika aktualizēta, kad tās uzbrukuma veikšanai izmantotie algoritmi un metodes tika uzlabotas, kas padarīja to ātrāk veicamu un praktiski pielietojamāku. [188,194,164] Tā balstās uz iepriekš zināmu šifrētu bloku virknēšanas (*CBC*) ievainojamību, kas ļauj veikt *MiTM*(„*Man in the middle*” jeb „*cilvēks pa vidu*”) uzbrukumus *SSL* protokolam, lai slepeni atšifrētu un atgūtu autentifikācijas marķierus. [143,188] Tas nodrošina uzbrucējam piekļuvi datiem, kas tiek pārsūtīti starp tīmekļa serveri un pārlūkprogrammu. [143,188]

Mūķa darbību demonstrējošs video ir atrodams tīmekļa vietnē *Youtube* - <http://youtu.be/BTqAIDVUvrU> (skatīts 2013. gada 24. maijā) [188,194,164] Tajā tiek parādīts, kā, izmantojot šo ievainojamību un mūķi, tiek, ar sīkfaila atšifrēšanu, pārtverta interneta norēķinu portāla *PayPal* lietotāja savienojuma sesija. Sīkfaila atšifrēšanai esot bijušas vajadzīgas ne vairāk kā divas minūtes.[143,144]

Pirms raksta publicēšanas mūķa autori par ievainojamību un sava darba rezultātu informēja tīmekļa pārlūkprogrammu un *SSL* tehnoloģiju piegādātājus, lai tie var laicīgi sākt izstrādāt ielāpus saviem risinājumiem. [188,194,164] Visi reaģēja un sāka strādāt pie ievainojamības novēršanas ļoti ātri. [188,194,164] Piemēram, *Mozilla* uzreiz savā incidentu pietikumu sistēmā reģistrēja kļūdu nr. 665814, kas kļuva par diskusiju vietni visiem, kas strādāja pie ievainojamības risinājuma. [188,194,164, 147] Tas, ka tika radīti vairāki ielāpi populārākajos interneta pārlūkos nenožīmē, ka problēma ir atrisināta. [143]

Šī ievainojamība ir reģistrēta ar „*CVE-2011-3389*” identifikācijas numuru Amerikas Savienoto Valstu Nacionālā standartu un tehnoloģiju institūta nacionālajā ievainojamību datu bāzē.[199]

Atvērtā koda ievainojamību datu bāzē (*OSVDB*) šai ievainojamībai ir piešķirts identifikācijas numurs 74829. [138,199] Abās vietnēs šīs ievainojamības ietekme tiek norādīta

kā „informācijas izpaušana” un „konfidencialitātes zaudēšana”[138,199] Tā kā šī ievainojamība tika atklāta arī *eParaksts.lv* portālam, šīs ietekmes un riski ir aktuāli arī darbā aplūkotajam pakalpojumam. [138,199] Viens no biežāk minētajiem šīs ievainojamības novēršanas risinājumiem ir prioritizēt un ieslēgt *RC4* šifru komplektu, kas neizmanto šifrēto bloku virknēšanas(*CBC*) algoritmu. [187, 151]

Par to, vai šī ievainojamība kādā no interneta vietnēm ir novērsta var pārlicināties jebkurš datora lietotājs, izmantojot tiešsaistē pieejamus *SSL* sertifikāta pārbaudes rīkus. Darba autors tam mērķim iesaka izmantot „*Quallys SSL Labs*” pārbaudes rīku, kas ir atrodams saitē <https://www.ssllabs.com/ssltest/>

4.2.2.2 „CRIME” UZBRUKUMA IEVAINOJAMĪBA

Virtuālā elektroniskā paraksta portālam *eParaksts.lv* tika atklāta arī „*CRIME*” uzbrukuma ievainojamība. Šī uzbrukuma pamatā ir nešifrēta teksta kompresija pirms tas tiek pārraidīts.

Pirmo reizi par šāda uzbrukuma iespējamību tika runāts jau 2002. gadā, bet tajā laikā tas tika uzskatīts par teorētisku un praktiski nepielietojamu. [156,127] 2012. gada septembrī tika prezentēts jau praktisks un realizējams uzbrukuma risinājums.[5]

Lai uzbrucējs varētu veikt veiksmīgu uzbrukumu prezentētajā risinājumā, viņam ir jābūt iespējai noklausīties tīklā pārraidītos datus, uzbrukuma upurim ir jāapmeklē uzbrucēja kompromitēta interneta adrese. [156,127] Gan upura interneta pārlūkam, gan serverim, kam upuris slēdzas klāt savu ikdienas darbību veikšanai, ir nepieciešams, lai būtu ieslēgta *SSL/TLS* kompresija. [156,127] Kompromitētā adrese ielādē upura interneta pārlūkā „*CRIME*” uzbrukuma rīku *JavaScript* formātā. [127] Pēc tam uzbrucēja rīks sāk minēt sīkfailu vērtības, kā blakus kanāla informāciju, izmantojot pārraidīto datu garumu, kas ir atkarīgs no izmantotās kompresijas. [156,127]

Risinājums ir atslēgt *SSL/TLS* kompresijas izmantošanu. Droša elektroniskā paraksta portāla *www.eParaksts.lv* serveru uzstādījumos *SSL/TLS* kompresija šī darba rakstīšanas laikā vēl ir ieslēgta. Ja arī plašāk izmantotajos interneta pārlūkos ar atjauninājumiem šī ievainojamība ir novērsta, vissvarīgāk ir novērst to arī servera pusē.

Par to, vai šī ievainojamība kādā no interneta vietnēm ir novērsta var pārlicināties jebkurš datora lietotājs, izmantojot tiešsaistē pieejamus *SSL* sertifikāta pārbaudes rīkus. Darba autors tam mērķim iesaka izmantot „*Quallys SSL Labs*” pārbaudes rīku, kas ir atrodams saitē <https://www.ssllabs.com/ssltest/>

4.2.2.3 SSL 2.0 PROTOKOLA ATBALSTS

SSL protokola otrā versija (SSL 2.0) tiek uzskatīta par nedrošu, jo tajā ir atklātas šādas ievainojamības un drošības riski: [137,142]

- Protokols izmanto nedrošus ziņojumu autentifikācijas kodus, samazinot to izmēru līdz četrdesmit bitu izmēram, [137,142]
- Nedrošu ziņojumu autentifikācijas kodu izmantošana, [137,142]
- Ziņojumu autentifikācijas kodu veidošanā, tiek izmantota šifrētu bloku virknēšanas metodes, bet procesā papildinājuma garuma lauks netiek atbilstoši apstrādāts, tādā veidā radot uzbrucējam iespēju dzēst ziņojuma beigu baitu informāciju, [137,142]
- Ziņojumu autentifikācijas kodu konstrukcijās tiek izmantots nedroši šifrēšanas algoritmi, [137,142]
- Ievainojamība pret šifru komplekta atrites uzbrukumu, kur ļaundaris var upuru sesijai noteikt izmantot vājākas šifrēšanas nekā upuri to vēlētos, [137,142]
- Ievainojamība pret *MITM* uzbrukumiem, [137,142]
- Šifrētu tīmekļa pieprasījumu plūsmas analīze var atklāt lejupielādētās lapas, datus, apmeklētos tīmekļa serverus u.c. informāciju. [137,142]
- Ievainojamība pret Bellovina izgriešanas un ielīmēšanas (*cut-and-paste*) uzbrukumu, [133,137,142]
- Bellovina īsā bloka uzbrukuma ievainojamība. [133,137,142]

Šāda nedrošu protokolu izmantošana paver interneta vietni vairākām ievainojamībām, ko prasmīgs uzbrucējs var izmantot kaitniecisku darbību veikšanai. [137,142]

Risinājums ir atslēgt SSL 2.0 protokola versijas savietojamību un izmantot SSL 3.0 versiju. [137,142]

Par to, vai šī ievainojamība kādā no interneta vietnēm ir novērsta var pārliccināties jebkurš datora lietotājs, izmantojot tiešsaistē pieejamus SSL sertifikāta pārbaudes rīkus. Darba autors tam mērķim iesaka izmantot *Quallys SSL Labs* pārbaudes rīku, kas ir atrodams saitē <https://www.ssllabs.com/ssltest/>

4.2.2.4 ZEMAS ŠIFRĒŠANAS KODU KOMPLEKTU ATBALSTS

Testos tika atklāts, ka virtuālā elektroniskā paraksta portāla www.eparaksts.lv atbalsta savienojumus, kas tiek šifrēti ar četrdesmit bitu atslēgas garumu. Tas ir pārraidīto datu

drošības risks, jo darba rakstīšanas brīdī tehnoloģijas un kriptanalīze ir attīstījusies līdz līmenim, kad šifrus, kas veidoti ar četrdesmit bitu garuma atslēgām atšifrēt vairs nav sarežģīti. [161,150] Ja lietotājs izveido šādu nedroši šifrētu savienojumu un veic dokumentu parakstīšanas darbības, tad uzbrucējam ir iespēja atšifrēt šo savienojumu un, piemēram, pārtvert lietotāja ievadīto *PIN* kodu ar, ko tiek veidots drošs elektroniskais paraksts. [161,150] Šī darba 5.5.1 nodaļā ir apskatīts *PIN* drošības risks, kas darba autoram rada pamatotas šaubas par to, ka *PIN* kods pats par sevi papildus šifrēts netiek.

Risinājums šim riskam ir nokonfigurēt portālu uzturošos serverus tā, lai ar tiem nebūtu iespējams izveidot šifrētus savienojumus ar četrdesmit vai piecdesmit sešu bitu garuma atslēgām.

Par to, vai šī ievainojamība kādā no interneta vietnēm ir novērsta var pārliccināties jebkurš datora lietotājs, izmantojot tiešsaistē pieejamus SSL sertifikāta pārbaudes rīkus. Darba autors tam mērķim iesaka izmantot „*Qualys SSL Labs*” pārbaudes rīku, kas ir atrodams saitē <https://www.ssllabs.com/ssltest/>

4.2.2.5 RC4 PROTOKOLA ATBALSTS

Portālam *www.eparaksts.lv* tika arī atklāta straumes šifra *RC4* nodrošināšana. Līdz ar kriptanalīzes un divdesmitā gadsimta beigu matemātikas attīstību, arī šim šifram tiek atklāti jauni uzbrukumu veidi. 2013. gada 13. martā tika publicēta informācija par veidu, kā uzbrucējs, zinot *RC4* algoritma viena baita nobīdes var, izmantojot statistikas analīzi, veikt veiksmīgus nešifrēta teksta atgūšanas uzbrukumus. [175,200] Šāda uzbrukuma veikšanai ir nepieciešams pietiekoši liels viena un tā paša teksta šifrētu rezultātu apjoms, kas ģenerēts ar dažādām atslēgām. Darba rakstīšanas brīdī šis uzbrukums vēl tiek uzskatīts par praktiski nepielietojamu un drīzāk teorētisku uzbrukumu. [175,200] Ņemot vērā vēsturisko pieredzi kriptanalītikā, kad iepriekš atzīts nepraktisks uzbrukums tiek uzlabots, padarot to praktiski pielietojamu, darba autors uzskata, ka nepaies ilgs laiks, kad arī šis uzbrukums tiks pilnveidots līdz praktiskai pielietojamībai. [175,200]

Tā kā *RC4* šifrēšanas algoritma izmantošana ir viens no „*BEAST*” uzbrukuma ievainojamības risinājumiem, bet pats ir ievainojams, risinājums, kā tikt galā ar abiem diviem ir izmantot *AES-GCM* (Galuā lauku uzlabots šifrēšanas standarts) šifrēšanas komplektu, kas ir pieejams *TLS 1.2*. (transporta slāņa drošība).[169,181] Bet tam pašlaik ir savietojamības un sadarbības problēmas ar esošajām informācijas sistēmām, kur šie tehnoloģiskie risinājumi vēl netiek atbalstīti. Lai uz to pārietu, nepieciešama tā integrācija visās sistēmās, kur pašlaik izmanto *RC4*. *AES-GCM* balstās uz Galuā lauku matemātiku, apvieno gan autentifikācijas,

gan šifrēšanas funkcijas, un to rekomendē izmantot Amerikas Savienoto Valstu Nacionālas Standartu un Tehnoloģiju institūts. [129,131]

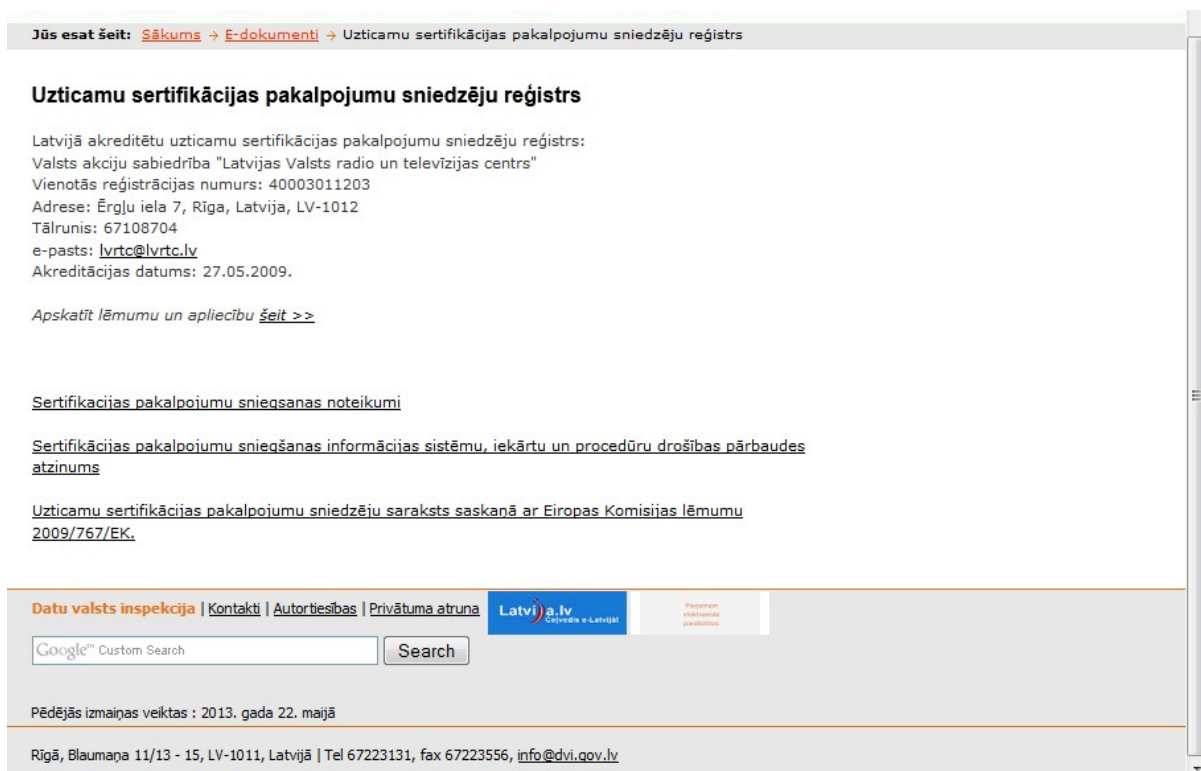
Par to, vai šī ievainojamība kādā no interneta vietnēm ir novērsta var pārliecināties jebkurš datora lietotājs, izmantojot tiešsaistē pieejamus *SSL* sertifikāta pārbaudes rīkus. Darba autors tam mērķim iesaka izmantot „*Quallys SSL Labs*” pārbaudes rīku, kas ir atrodams saitē <https://www.ssllabs.com/ssltest/>

4.3 UZRAUDZĪBAS IESTĀDES PIENĀKUMU IZPILDES KVALITĀTE

Latvijas Republikā Elektronisko dokumentu likums nosaka Datu valsts inspekcijai pienākumus veikt un uzraudzīt uzticamu sertifikācijas pakalpojumu sniedzēju darbību.[14] Elektronisko dokumentu likuma 19. panta otrā daļa nosaka: „*Uzraudzības iestāde regulāri uzrauga uzticamu sertifikācijas pakalpojumu sniedzēju darbības atbilstību šā likuma un citu normatīvo aktu prasībām.*”[14]

Tā paša likuma 19. panta pirmās daļas 5. punktā tiek noteikta prasība uzraudzības iestādei uzturēt tiešsaistē pieejamu uzticamu sertifikācijas pakalpojumu sniedzēju reģistru.[14] Likuma 20. panta otrās daļa nosaka informāciju, kurai ir jābūt šajā reģistrā pieejamai.[14] Šīs daļas 7. punkts nosaka: „*7) informācija par uzraudzības iestādes aizrādījumiem, brīdinājumiem vai akreditācijas anulēšanu.*” [14]

Attēlā 4.6 redzams, ka šī darba rakstīšanas brīdī Datu valsts inspekcija vēl nav iekļāvusi informāciju par VAS „Latvijas Pasts” uzticama sertifikācijas statusa akreditācijas anulēšanu.



4.6 att. Uzticamu sertifikācijas pakalpojumu sniedzēju reģistrs

2013. gada 15. februārī uzraudzības iestāde sniedz rakstisku atbildi (Pielikums Nr. 12.) uz Arņa Paršova 2013. gada 15. janvārī nosūtītu iesniegumu (Pielikums Nr. 11) par uzticamu sertifikācijas pakalpojumu sniedzēju VAS „Latvijas Pasts”. [54,14] Atbildē Datu valsts inspekcija raksta: „ (...) *informācija par uzticama sertifikācijas pakalpojuma sniedzēja VAS „Latvijas Pasts” anulēšanu ir izņemta no uzticamu sertifikācijas pakalpojumu reģistra, jo sākot ar 2011. gada 1. jūniju tika gandrīz pilnībā likvidēta VAS „Latvijas Pasts” sertifikācijas institūcijas un ar to saistītā servisu infrastruktūra (..)*”[54,14]

Tātad Datu valsts inspekcija neievēro Elektronisko dokumentu likuma 20. panta otrās daļas 7. punktā noteiktās prasības. [54,14] Lai tās tiktu ievērotas, uzticamu sertifikācijas pakalpojumu sniedzēju reģistrā būtu jābūt ievietotai informācijai par to, ka VAS „Latvijas Pasts” noteiktā laika periodā bija ieguvis uzticama sertifikācijas pakalpojumu sniedzēja statusu, bet pašlaik tā akreditācija ir anulēta(attēls 4.6.). [54,14]

Darba rakstīšanas laikā pēdējais publiski pieejamais uzticama sertifikācijas pakalpojumu sniedzēja pārbaudes atzinums ir SIA „KPMG Baltics” vērtējums par uzticama pakalpojumu sniedzēja atbilstību 2005. gada 12. jūlija Ministru kabineta noteikumiem Nr.514. 2012. gada 24. aprīlī. (Pielikums Nr.4.). [36] Cita starpā šajā vērtējumā tiek rakstīts: *”Darbības nepārtrauktības plāns, iespējams, ir neaktuāls, jo satur neaktuālas atsauces uz citām procedūrām, novecojušu informāciju par iesaistītajiem darbiniekiem, nesatur atsauces*

uz esošajiem plāniem. Šis atklājums tika konstatēts arī iepriekšējā akreditācijas auditā; šī ir neatbilstība LVS ISO/IEC 17799 sadaļai 14.1.5.”. [54] Tas nozīmē, ka šī pati neatbilstība tika atklāta jau 2011. gada ikgadējā auditā un viena gada laikā nav tikusi novērsta. [54] Darba autors vērs uzmanību tam, ka esošā uzticamu sertifikācijas pakalpojumu uzraudzības procedūra nav pietiekoša, ja ir iespējama situācija, ka pārbaudē atklāta neatbilstība kādam no standartam netiek novērsta pat divpadsmit mēnešu laikā. Būtu nepieciešams uzlabot likumdošanu un uzraudzība iestādes pienākumu regulējumu. Piemēram, noteikt papildus esošajiem uzraudzības iestādes pienākumiem obligāti dot norādījumus uzticamam sertifikācijas pakalpojumu sniedzējam novērst neatbilstības kādam no standartiem.

Esošajā redakcijā Elektronisko dokumentu likuma 21. panta pirmā daļa nosaka: *”Uzraudzības iestādei ir tiesības dot norādījumus uzticamam sertifikācijas pakalpojumu sniedzējam, lai novērstu neatbilstību šim likumam, citiem normatīvajiem aktiem, uzticamu sertifikācijas pakalpojumu sniedzēju reģistrā iekļautajiem sertifikācijas pakalpojumu sniegšanas noteikumiem vai sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības aprakstam.”*. [54,14] Acīmredzot, pēc 2011. gada audita Datu valsts inspekcija šīs tiesības nav izmantojusi. Tā rezultātā audits atkārtoti atklāj uzticama sertifikācijas pakalpojumu sniedzēja darbības neatbilstību normatīvajos aktos noteikta standarta sadaļai. [54,14]

Atbildot 2013. gada 13. februārī uz Arņa Paršova 2013. gada 8. janvāra iesniegumu (Pielikums Nr.14), Datu valsts inspekcija cita starpā informē: *„2. Datu valsts inspekcija saskaņā ar Elektronisko dokumentu likuma 21. panta pirmo daļu kā uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzības iestāde ir devusi norādījumus VAS „Latvijas Valsts radio un televīzijas centrs” novērst audita laikā konstatētās nepilnības”* (Pielikums Nr. 13). [54,14]

Darba autors secina, ka Datu valsts inspekcija nepilda kvalitatīvi savas kā uzraudzības iestādes funkcijas. Ir nepieciešamas vai nu darbinieku apmācības, atbildīgo darbinieku maiņa vai uzraudzības iestādes funkcijas izpildītāja maiņa kā tāda. Darba autors uzskata, ka vai nu ir jāveic pasākumi Datu valsts inspekcijas kompetences un motivācijas celšanai vai uzraudzības iestādes funkcijas ir jānodod citai institūcijai, kas ar uzraudzības iestādes funkcijām tiktu galā labāk un kvalitatīvāk.

Lai pēc iespējas uzlabotu sertifikācijas pakalpojumu lietošanu Datu valsts inspekcijai kā personu datu aizsardzības funkciju izpildītājam būtu nepieciešams publicēt iespējamās sertifikācijas pakalpojumu nevērīgas lietošanas riskus. Būtu nepieciešams norādīt vadlīnijas, norādījumus un rekomendācijas veidiem, kā visdrošāk var lietot sertifikācijas pakalpojumus. Šos norādījumus būtu nepieciešams publicēt elektroniskā paraksta sadaļā savā tīmekļa vietnē.

4.3.1 UZRAUDZĪBAS IESTĀDES PUBLICĒTĀS INFORMĀCIJAS

AKTUALITĀTE

Kopš Latvijas Republikas Elektronisko dokumentu likuma apstiprināšanas 2002. gada 31. oktobrī, un tā stāšanās spēkā 2003. gada 1. janvārī tas ir mainīts septiņas reizes kā tas ir redzams tabulā 4.2. [14]

4.2 tabula

Grozījumi Elektronisko dokumentu likumā [28,29,30,24,25,26,27,14]

Nr.p.k.	Likuma grozījums pieņemts	Stājas spēkā	Piezīme	Publikācija „Latvijas Vēstnesis”	Statuss
1.	06.05.2004	27.05.2004	Saeimas pieņemts un Valsts prezidenta izsludināts likums	13.05.2004., Nr.75 (3023)	Spēkā esošs
2.	17.08.2004	20.08.2004	Ministru kabineta noteikumi Nr.711	19.08.2004., Nr.131 (3079)	Nav spēkā esošs
3.	28.10.2004.	24.11.2004	Saeimas pieņemts un Valsts prezidenta izsludināts likums	10.11.2004., Nr.178 (3126)	Spēkā esošs
4.	25.04.2006.	04.05.2006.	Ministru kabineta noteikumi Nr.340	03.05.2006., Nr.69 (3437)	Nav spēkā esošs
5.	22.06.2006.	21.07.2006.	Saeimas pieņemts un Valsts prezidenta izsludināts likums	07.07.2006., Nr.107 (3475)	Spēkā esošs
6.	24.05.2007.	26.06.2007.	Saeimas pieņemts un Valsts prezidenta izsludināts likums	12.06.2007., Nr.93 (3669)	Spēkā esošs
7.	24.09.2009.	22.10.2009.	Saeimas pieņemts un Valsts prezidenta izsludināts likums.	08.10.2009., Nr.160 (4146)	Spēkā esošs

Uzraudzības iestādes tīmekļa lapas „e-paraksts” nodaļas sadaļā „likumdošana” vēl joprojām ir aplūkojama tikai šī likuma pirmā versija bez informācijas par tā grozījumiem. [53,15] Darba autoram rodas iespaids, ka šī sadaļa pēdējo reizi ir atjaunota tikai pirms septiņiem gadiem – 2006. gadā.

Darba autors uzskata, ka ar aktuālas informācijas neuzturēšanu tiek maldināti valsts iedzīvotāji, kuri apmeklē Datu valsts inspekcijas tīmekļa vietni ar cerību tur atrast aktuālo informāciju par viņus interesējošiem jautājumiem. Tai skaitā arī elektroniskā paraksta likumdošanu. Šādā situācijā, kad ir publicēta likuma neaktuāla versija, rodas risks, ka valsts iedzīvotāji nav pietiekoši informēti par jaunāko likumdošanu no uzraudzības iestādes puses, un viņi var veikt darbības, kas var tikt uzskatītas ārpus likuma saskaņā ar veiktiem grozījumiem, ko Datu valsts inspekcija nav publicējusi. Tādā veidā iedzīvotājiem var rasties zaudējumi saistībā ar elektroniskā paraksta lietošanu un izmantošanu savā ikdienā.

Risinājums būtu ievietot tīmekļa lapā aktuālākas likumu versijas vai arī norādīt saiti uz likumu *www.likumi.lv* vietnē, kur vienmēr ir pieejama tiesību akta jaunākā versija un izmaiņu vēsture. Būtu jāpārskata visas sadaļas un jāpārbauda, lai tur būtu pieejama jaunākā un aktuālākā informācija.

Darba autors pieļauj, ka šāda informācijas atjaunošanas un uzturēšanas kultūra un regularitāte liecina par uzraudzības iestādes darba iespējamo kvalitātes līmeni arī citos uzticama sertifikācijas pakalpojumu sniedzēja uzraudzības aspektos.

4.3.2 VIRTUĀLĀ PARAKSTA ATBILSTĪBA ELEKTRONISKO DOKUMENTU LIKUMAM

Latvijas Republikas Elektronisko dokumentu likumā viena no droša elektroniskā paraksta prasībām ir noteikta 1. panta otrā punkta c apakšpunktā: *”c) tas ir radīts ar drošiem elektroniskā paraksta radīšanas līdzekļiem, kurus var kontrolēt tikai parakstītājs”*. [14] Viens no uzticama sertifikācijas pakalpojumu sniedzēja pienākumiem tiek noteikts iepriekš minētā likuma 23. panta 19. punktā: *”neglabāt un nekopēt droša elektroniskā paraksta radīšanas datus”* [14]

Elektroniskajam parakstam tā visizplatītākajā formātā radīšanas līdzekļi tiek glabāti uz viedkartes tās mikroshēmā. Pati viedkarte ir tās lietotāja uzraudzībā un pilnīgā kontrolē. Tātad Elektronisko dokumentu likuma 1. panta otrā punkta c apakšpunkta prasība tiek realizēta un pildīta. [14,16]

Uzticamam sertifikācijas pakalpojumu sniedzējam klienta viedkarte ar paraksta radīšanas datiem nav sasniedzama, jo tā fiziski atrodas pie tās īpašnieka. Tā kā uzticama

sertifikācijas pakalpojumu sniedzēja tehnoloģiskie risinājumi tiek pārbaudīti, tad var pieļaut, ka Elektronisko dokumentu likuma 23. panta 19. punktā noteiktais pienākums tiek pildīts. [14,16]

Virtuālajam elektroniskajam parakstam tā radīšanas dati tiek glabāti pie uzticama sertifikācijas pakalpojumu sniedzēja *HSM* (aparātūras drošības modulis) iekārtā. [14,16,54] Šī iekārta atrodas datu centrā ar augstu drošības kontroli, lai nepieļautu nesankcionētu piekļuvi sertifikācijas pakalpojumu infrastruktūrai. Parakstīšanas datu īpašnieks sava elektroniskā paraksta radīšanas datiem fiziski klāt piekļūt nevar, tie atrodas viņam nezināmā atrašanās vietā un vienīgais veids, kā paraksta īpašnieks var piekļūt klāt tā radīšanas datiem ir, izmantojot viņam zināmu PIN kodu. [14,16]

PIN koda drošības riski virtuālā elektroniskā paraksta risinājumā ir apskatīti šī darba 4.5.1 nodaļā.

Virtuālā elektroniskā paraksta īpašnieka paraksta radīšanas līdzekļi tiek glabāti iekārtā, kas ir uzticama sertifikācijas pakalpojumu īpašums. Šī iekārta tiek glabāta telpās, kur fiziska piekļuve ir ļauta tikai uzticama sertifikācijas pakalpojumu sniedzēja darbiniekiem. Tas nozīmē, ka kontrole pār droša elektroniskā paraksta radīšanas datiem ir gan tā īpašniekam, izmantojot PIN kodu, gan uzticamam sertifikācijas pakalpojumu sniedzējam, izmantojot fizisku piekļuvi iekārtai. Līdz ar to tiek pārkāpta Elektronisko dokumentu likuma 1. panta otrā punkta c apakšpunkta prasība. [14,16,54]

Tā kā iekārta, kurā tiek glabāti droša elektroniskā paraksta radīšanas dati, fiziski atrodas uzticama sertifikācijas pakalpojumu sniedzēja pārziņā, ir uzskatāms, ka netiek ievērots Elektronisko dokumentu likuma 23. panta 19. punktā norādītais uzticama sertifikācijas pakalpojumu sniedzēja pienākums. [14]

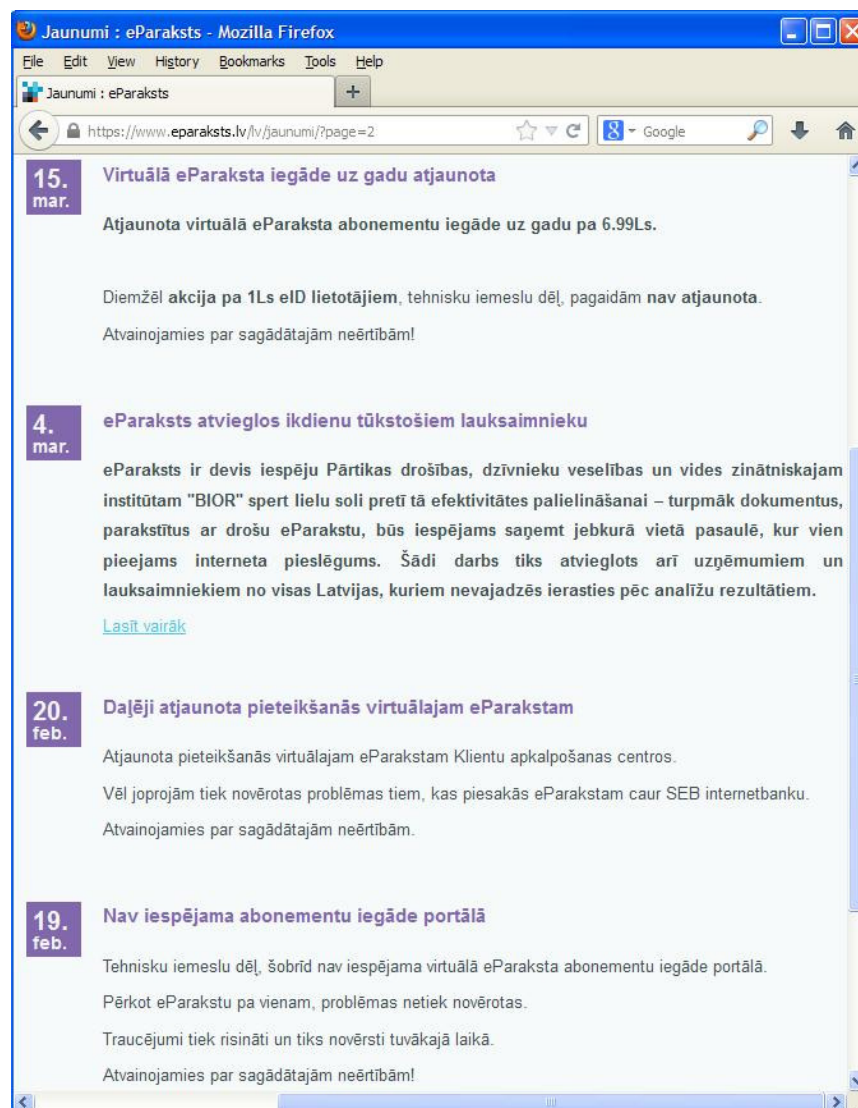
Tāpēc virtuālā elektroniskā paraksta risinājums ir pretrunā Elektronisko dokumentu likumam un šī konkrētā pakalpojuma sniegšana būtu jāpārtrauc. [14,54] It kā tikai paraksta īpašniekam zināma PIN koda piekļuve paraksta radīšanas līdzekļiem noteikti nav pamatojums iepriekš minētā likuma 1. panta otrā punkta c apakšpunkta ievērošanai, jo gadījumā, ja uzticama sertifikācijas pakalpojumu sniedzēja darbinieks, piemēram, nejauši atslēgs *HSM* iekārtai elektrisko strāvu droša elektroniskā paraksta īpašnieks, pat gribēdams, ar savu PIN kodu nevarēs saviem paraksta radīšanas datiem piekļūt un tos kontrolēt. Tādā brīdī pilna kontrole pār šiem datiem ir konkrētajam darbiniekam, kurš šos datus, iedarbojoties uz *HSM* iekārtu, var brīvi pārvietot vai pat iznīcināt.

4.4 SERTIFIKĀCIJAS PAKALPOJUMU PIEEJAMĪBA UN UZTICAMĪBA

Sertifikācijas pakalpojumi ir ļoti nozīmīgi valstiskā mērogā. Piemēram, elektronisko parakstu iedzīvotāji lieto gan biznesa darījumiem, gan personīgām vajadzībām. Tā kā Latvijas Republikā pašlaik ir tikai viens uzticama sertifikācijas pakalpojuma sniedzēja statusu ieguvis uzņēmums, ir ļoti svarīgi, lai tā sniegtie pakalpojumi vienmēr būtu pieejami un kvalitatīvi. Pretējā gadījumā Latvijā sniegto sertifikācijas pakalpojumu klientiem var rasties lieli zaudējumi.

Latvijas elektroniskā paraksta portālā *www.eparaksts.lv* ir pieejama sadaļa „Forums”, kur lietotāji var publiski uzdot jautājumus, veidot diskusijas un arī ziņot par problēmām. Tāpat portālā ir arī sadaļa „Jaunami”, kur tiek ziņots par aktuālākajām lietām sertifikācijas pakalpojumu nodrošināšanā.

Attēlā 4.7. ir redzami četri secīgi uzticama sertifikācijas pakalpojumu sniedzēja ziņojumi.



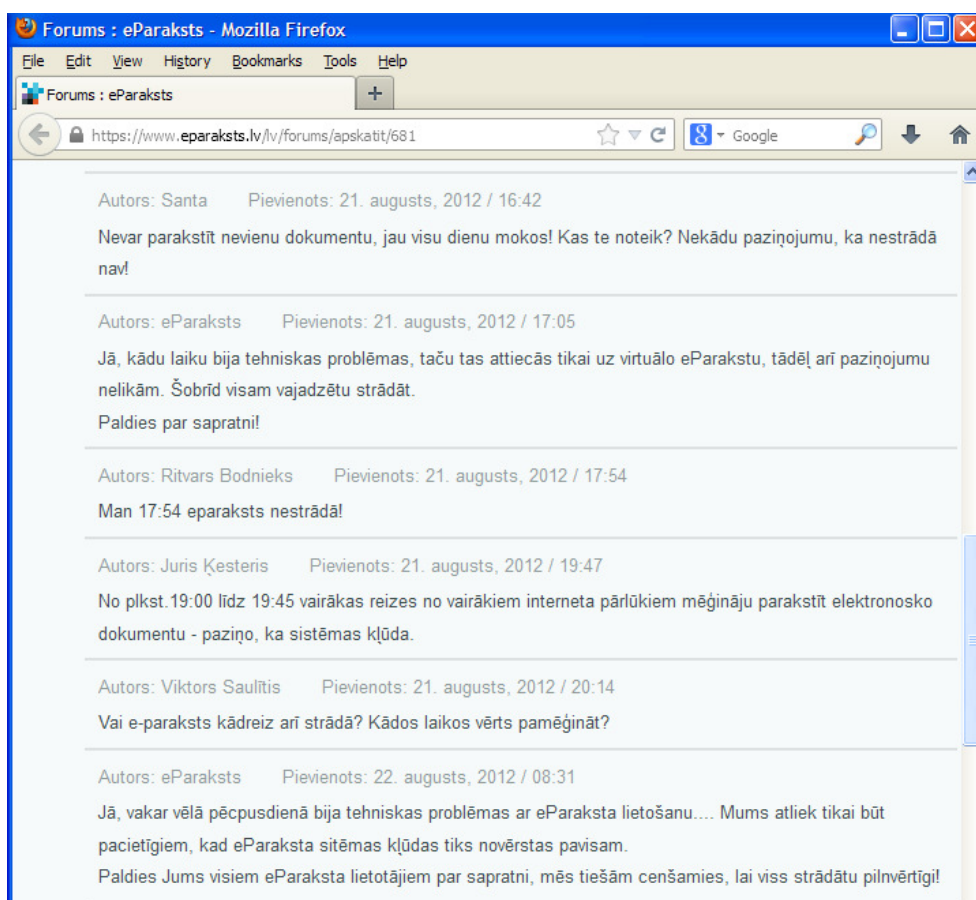
4.7 att. Elektroniskā paraksta portāla jaunumu sadaļa

Trīs no šiem ziņojumiem tiek pabeigti ar vārdiem: *"Atvainojamies par sagādātājām neērtībām!"*. 2013. gada 19. februāra, 20. februāra un 15. marta ziņojumos (Attēls 4.7) lietotāji tiek informēti par tehniskām problēmām, kuru dēļ nav pieejama daļa uzticamu sertifikācijas pakalpojumu funkcionalitāte.

Šie ir oficiāli paziņojumi jaunumu sadaļā, bet ne par visām tehniskajām pakalpojuma problēmām lietotāji tiek uzskatāmi informēti.

Ja tiek aplūkota foruma sadaļa tad ir atrodami daudzi klientu sistēmas kļūdu pieteikumi, kas rodas pakalpojuma darbības pārtraukumu rezultātā. Par šādiem pārtraukumiem vienīgā publiski pieejamā informācija bieži vien ir tikai foruma sadaļas ierakstā. Piemēram, 2012. gada augustā lietotājs reģistrēja elektroniskā paraksta pakalpojuma sniedzējam problēmu parakstīt dokumentu ar vārdiem: *"Nevar parakstīt nevienu dokumentu, jau visu dienu mokus!"*

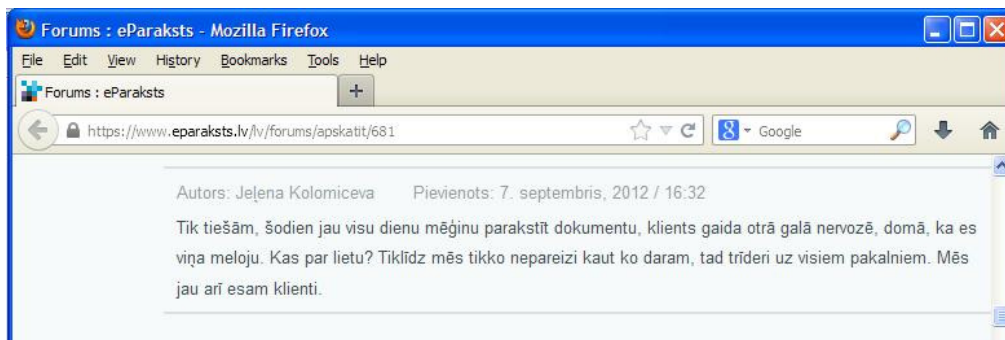
Kas te notiek? Nekādu paziņojumu, ka nestrādā nav!”. Šis pieteikums un elektroniskā paraksta pakalpojuma sniedzēja atbildes redzamas attēlā 4.8



4.8 att. Klientu sūdzības *www.eparaksts.lv* portālā Nr.1

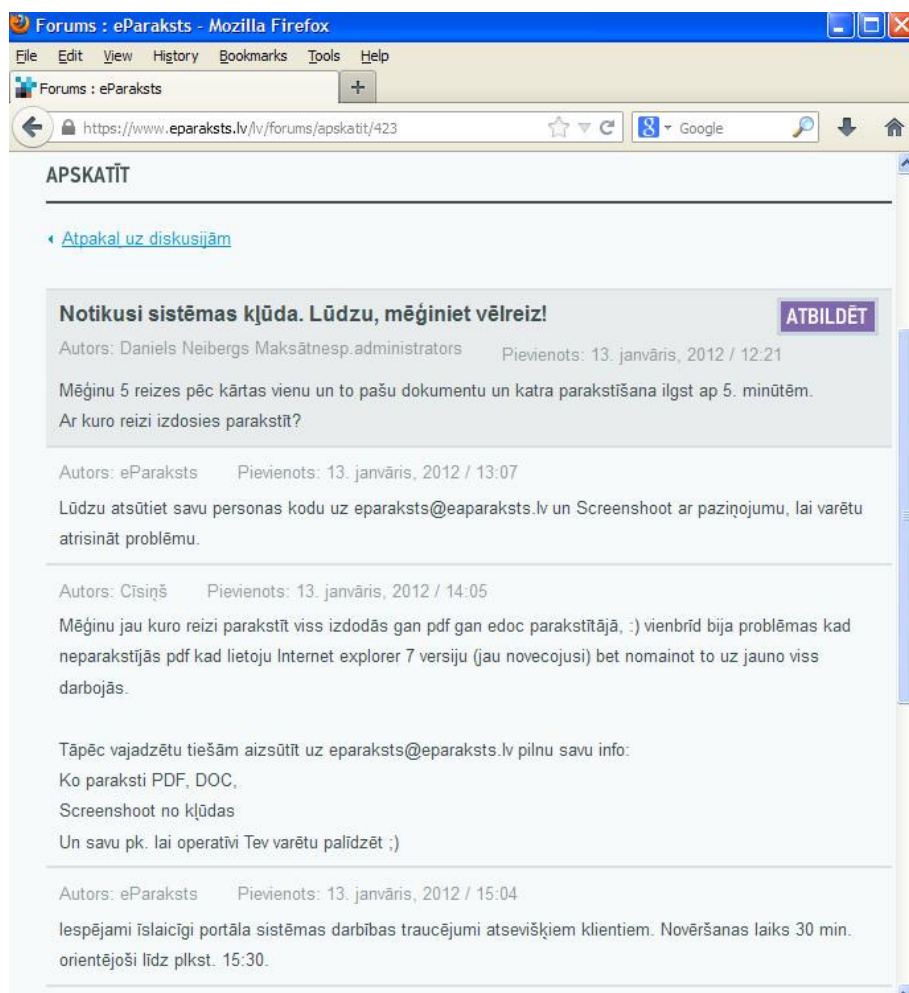
Uzticamā pakalpojumu sniedzēja pārstāvis atbild apstiprinoši, ka tajā dienā ar virtuālo elektronisko parakstu ir bijušas problēmas, bet paziņojums par to nav likts. Attēla 4.8. sarunā ir redzams, ka problēmas ar pakalpojuma izmantošanu tajā dienā ir vairākiem lietotājiem un pēc sākotnējo tehnisko problēmu novēršanas tās pašas dienas vakarā tās rodas atkārtoti, kas arī šoreiz tieši skar tā lietotāju. Viens no klientiem jautā: *”Vai e-paraksts kādreiz strādā? Kādos laikos var mēģināt?”*. Atbildi viņš saņem nākošās dienas rītā, ar apstiprinošu atbildi, ka iepriekšējās dienas pēcpusdienā bija tehniskas problēmas.

Tehniskas problēmas, kad sertifikācijas pakalpojumi vai kāda to daļa nav pieejama Latvijas uzticamam sertifikācijas pakalpojumu sniedzējam rodas pat vairākas reizes gadā. Tas rada klientiem zaudējumus un sarežģījumus savas uzņēmējdarbības kvalitatīvā nodrošināšanā kā tas ir redzams attēlā 4.9.



4.9. att. Klientu sūdzības *www.eparaksts.lv* portālā Nr.2. [60]

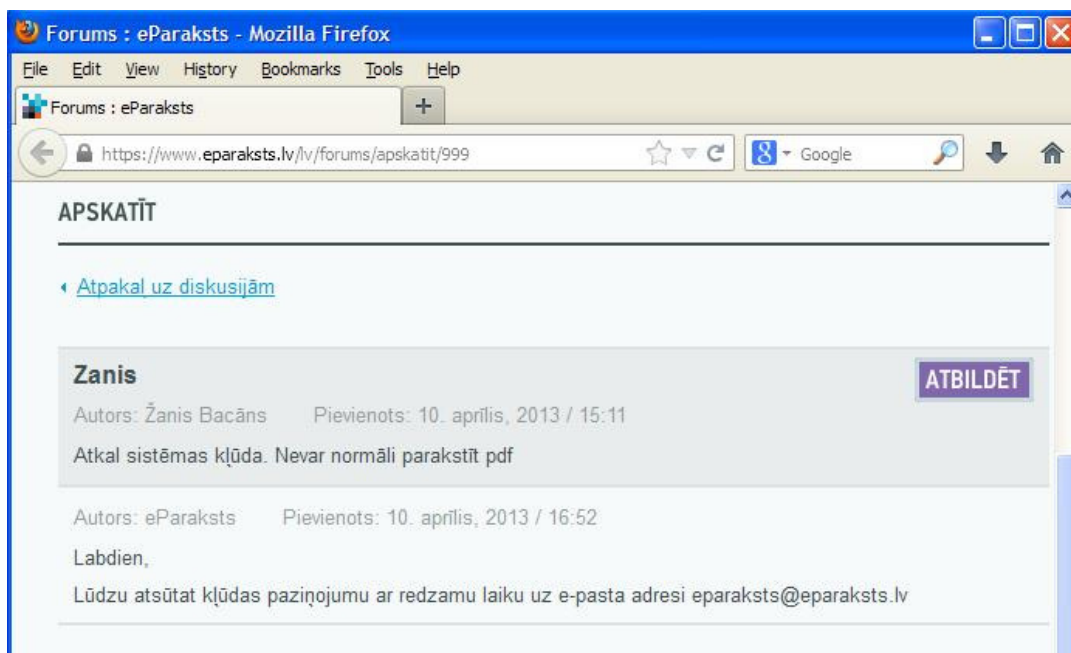
Dažreiz pirms uzticams sertifikācijas pakalpojumu sniedzējs paziņo, ka tā sniegtā pakalpojuma atteice ir radusies tehnisku problēmu dēļ, klientam tiek palūgts atsūtīt sistēmas kļūdas paziņojuma ekrānuzņēmumu un viņa kontaktinformāciju uz pakalpojuma sniedzēja elektroniskā pasta adresi. Tāds piemērs ir redzams attēlā 4.10.



4.10. att. Tehniskas problēmas *www.eparaksts.lv* portālā

Attēlā 4.10 ziņoto tehnisko problēmu novēršanas laiks ir minēts trīsdesmit minūtes. Nav izslēgts variants, ka uzticams sertifikācijas pakalpojumu sniedzējs klientam uz viņa sūdzību

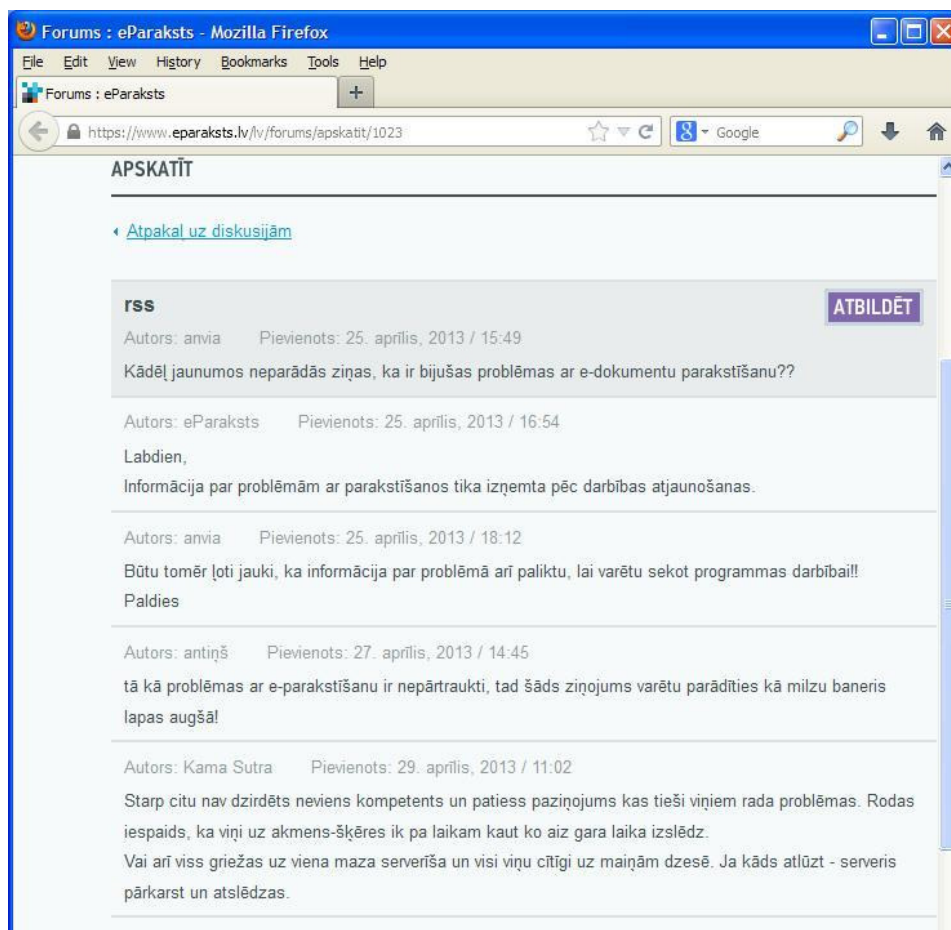
atbild ar lūgumu atsūtīt kļūdas paziņojuma ekrānuzņēmumu speciāli ar mērķi, tikmēr, kamēr klients sagatavo un atsūta elektroniskā pasta vēstuli ar kļūdas detalizētu aprakstu, pakalpojuma sniedzēja tehniskie speciālisti varētu paspēt problēmas salabot. Tādā gadījumā klients redz, ka sertifikācijas pakalpojums atkal tiek nodrošināts, bet pats pakalpojumu sniedzējs var neizziņot publiski faktu par savu informācijas sistēmu tehniskām problēmām. Šādas iespējams scenārijs ir redzams attēlā 4.11



4.11. att. Klientu sūdzības Nr.3 [59]

Vairāki citi tehnisku problēmu ziņojumi un lietotāju pieteikumi redzami pielikumā Nr.10.

Attēlā 4.12 uzticams sertifikācijas pakalpojumu informē klientus par to, ka paziņojumi par sertifikācijas pakalpojuma atteices problēmām tiek dzēsti.



4.12. att. *www.eparaksts.lv* foruma jautājumi Nr. 1

Darba autors uzskata, ka uzticamam pakalpojumu sniedzējam ir nepieciešams ziņot uzreiz par jebkādam tehniskām problēmām, ja tādas ir radušās. Tam ir jābūt godīgam un atklātam pret savu klientu. Pretējā gadījumā tiek maldināti lietotāji un zūd viņu uzticamība pakalpojuma drošumam. Kā arī ir grūtāk atsekot pakalpojuma stabilitātei.

Darba autors novēro manāmas problēmas uzticamam sertifikācijas pakalpojumu sniedzējam ar sertifikācijas pakalpojumu stabilu un kvalitatīvu nodrošināšanu, jo priekš tehniskā risinājuma ar lielu valstisku nozīmi, neplānotas tehniskas problēmas tam rodas pārāk bieži.

Risinājums, kā varētu uzlabot pakalpojuma stabilitāti, būtu veikt esošā risinājuma tehnisku pārbaudi, pieaicinot speciālistus no valstīm, kur ir lielāka un veiksmīgāka pieredze sertifikācijas pakalpojumu sniegšanā, piemēram, Vācijas Informācijas drošības aģentūras tehniskos speciālistus un konsultantus. Pārbaudes laikā būtu nepieciešams piesaistīt arī maksimāli kompetentu un daudzskaitlīgu Latvijas akadēmisko personālu.

4.5 IESPĒJAMIE RISKI SAISTĪBĀ AR IZSTRĀDĀTĀJIEM

Ieviešot valstī sertifikācijas pakalpojumus un tādus pakalpojumus, kam ir augstas prasības pret to izpildes drošību, pastāv vairāki scenāriji, kā to paveikt:

1. Iegādāties gatavu risinājumu,
2. Izstrādāt risinājumu pašiem,
3. Nolīgt citu uzņēmumu kā ārpakalpojumu, kas izstrādā tehnoloģijas un risinājumus, kas nodrošina pakalpojumu,
4. Iepriekš minēto scenāriju dažādas kombinācijas.

Pirmais scenārijs nozīmē izvēlēties un iegādāties pasaulē pārbaudītu un uzticama tehnoloģiju uzņēmuma izstrādātu risinājumu. Izvēlē noteikti būtu jāvērtē risinājuma noturība pret dažādiem kibernetiskajiem uzbrukumiem, cik no tiem ir bijuši veiksmīgi, kā izstrādātājs tos ir risinājis, kāda izstrādātājam ir pieredze drošības risinājumu jomā, kādus drošības sistēmu un procedūru auditors tas ir nokārtojis, cik profesionālu kriptologu strādā izstrādātāja komandā, kādi sadarbības partneri strādājuši pie risinājuma izveidošanas u.c. svarīgi faktori.

Ļoti svarīgi ir, lai pie risinājuma būtu strādājis, vai to būtu pārbaudījis vismaz augstas klases profesionāls kriptologs, jo viņš sevī apvieno gan kriptogrāfa, gan kriptanalītiķa kompetences. Izmantojot kriptogrāfa prasmes, kriptologs ir spējīgs izstrādāt drošu risinājumu, ņemot vērā drošības risinājumu ieviešanas biežāk pieļautās kļūdas un lielākos riskus. Tāpat viņš var no tāda paša skatu punkta izvērtēt esošu risinājumu, vai tas ir uzražots kvalitatīvi, izmantojot drošas tehnoloģijas. Savukārt, kriptologs, izmantojot kriptanalītiķa kompetences ir spējīgs paredzēt iespējamus riskus un potenciāli ekspluatējamus un apejamus drošības risinājuma aspektus. Kriptologam jāpārzina arī cilvēku izlūkošanas, iekšējo uzbrukumu, likumdošanas riski un incidenti. Līdz ar to kriptologs labi orientējas drošības jautājumos no detalizēta aparatūras līmeņa līdz pat programmatūras līmenim. Bet arī viens augstas klases kriptologs nevar zināt visu. Tāpēc ir ļoti vēlama vismaz divu kriptologu dalība risinājuma izstrādē vai ieviešanā.

Otrs scenārijs ir izveidot profesionālu komandu pašiem un izstrādāt drošības un sertifikācijas pakalpojumu risinājumu no jauna. Šajā scenārijā obligāti ir jāņem vērā pasaules pieredze un labā prakse attiecībā uz drošības risinājumos izmantotajiem standartiem, prasībām un riskiem. Arī šeit ir ļoti svarīgi vismaz viena profesionāla kriptologa dalība un pārdomāta risinājuma ieviešana un izstrāde.

Trešais scenārijs ir, saglabājot daļu pakalpojuma sniegšanas funkciju, nodot risinājuma izstrādi ārpakalpojuma sniedzējam. Piemēram, pakalpojuma pamata uzturēšanu un mārketingu uzņemas pats pakalpojuma sniedzējs, bet jaunas izstrādes un risinājuma ieviešana

tiek nodota citam uzņēmumam, noslēdzot ar to sadarbības un konfidencialitātes līgumus. Šajā scenārijā arī ir ļoti svarīgi, lai vismaz vienā no iesaistītajām pusēm būtu kāds profesionāls kriptologs. Visu iesaistīto pušu komandām jābūt ļoti profesionālām, lai pasūtītāji spētu sagatavot kvalitatīvus un augstas klases risinājumu aprakstus un atbilstošo pasūtījuma dokumentāciju, bet izstrādātājs būtu spējīgs kvalitatīvi izpildīt, izstrādāt un notestēt savus risinājumus pirms nodot pasūtītājam.

Ceturtais scenārijs ir iespējama kombinācija no iepriekš aprakstītajiem. Piemēram, pakalpojuma sniedzējs daļu risinājuma izstrādā un rada pats, daļu iepērk jau gatavu, daļu pasūta izstrādāt un uzturēt ārpuskalpojumam. Šādā gadījumā ir uzmanīgi jāvērtē un jāpārbauda gan sadarbības partneru uzticamība, gan arī pašu risinājuma drošība un iespējamie riski.

Latvijas Republikā, ieviešot elektroniskā paraksta risinājumu, tika izvēlēts ceturtais scenārijs. Sākumā savstarpēji risinājuma izstrādē un radīšanā sadarbojās *Lattelecom*, VAS "Latvijas Pasts", SIA „*Microsoft Latvia*”, SIA „*Lattelekom*” kā pamata pakalpojuma ieviesēji un uzturētāji. [124] Dažādu papildus sadarbības nodrošināšanu risinājumu izstrādē tika uzticēta SIA "EUSO". Šīs kompānijas produktu sarakstā ietilpst uz *Java* tehnoloģijām balstīta sīklīdētne „*SignAnywhere Free*”, *Microsoft.NET* ietvara klašu bibliotēkas „*EDocLibraries.NET*” un „*EDOC Java bibliotēkas*” priekš citiem izstrādātājiem, lai viņi savos risinājumos varētu iestrādāt Latvijas elektroniskā dokumenta formāta veidošanas un pārbaudes funkcionalitāti. [55] (Pielikums Nr. 6) Līdz ar sertifikācijas pakalpojumu nodošanu VAS „Latvijas Valsts radio un televīzijas centrs” tiek samazināta sadarbība ar SIA „*Lattelekom*” un SIA „*Microsoft Latvia*”, un virtuālā un elektroniskā paraksta radīšanai kā galvenais ārējais izstrādātājs sertifikācijas pakalpojumiem kļūst SIA „*Open ID*”. SIA „*Lattelekom*” (darba rakstīšanas brīdī SIA „*Lattelecom*”) tika dibināts 1994. gadā, SIA „*Microsoft Latvia*” tika dibināts 1999. gadā, SIA „*EUSO*” tika dibināts 2000. gadā, kas visiem uzņēmumiem dod vismaz veiksmīgu desmit gadu darbību, ieviešot un izstrādājot dažādus risinājumus. [87,110,117] Savukārt, „*Open ID*” tika dibināts 2010. gadā un kā vienīgais izstrādātāja projekts ir norādīts drošs virtuālais elektroniskais paraksts (Pielikums Nr.5.). Tas nozīmē, ka jaunizveidotam uzņēmumam bez iepriekšējas pieredzes drošības risinājumu ieviešanā tiek pasūtīts izstrādāt vēl nebijušu un jaunu sertifikācijas pakalpojuma formātu, kam ir ļoti lielas prasības attiecībā pret konkrētā risinājuma drošību un kvalitāti.

Darba autors uzskata, ka tas ir ļoti liels risks saistībā ar elektroniskā paraksta ieviešanu Latvijā, ka nepieredzējušam izstrādātājam tiek uzdots izveidot augstas drošības pakāpes risinājumu. Tā kā šī maģistra darba rakstīšanas laikā saskaņā ar darba autoram pieejamo informāciju Latvijā nav ne profesionālu kriptologu, ne kriptogrāfijas vai kriptanalītikas skolu, pastāv liels risks, ka esošo sertifikācijas pakalpojumu izstrādē kriptologa klātbūtne nav

bijusi. Programmatūras izstrādes drošības risinājumu projektos ļoti svarīgi ir, lai tiktu izmantotas tikai pārbaudītas un drošas programmēšanai nepieciešamās bibliotēkas. It īpaši tas attiecas uz tām, kas nodrošina kriptogrāfijas algoritmu funkcijas. Ja drošības risinājuma izstrādātājs nav pieredzējis konkrētajā jomā, un klāt nav kompetentu kolēģu, tad ir viegli risinājumā ieviest drošības caurumus vai nenovērst vispār zināmas ievainojamības.

Lai pēc iespējas samazinātu šādu ārējo izstrādātāju un ārpakalpojumu sniedzēju riskus, ja tie strādā pie tādiem drošības sertifikācijas pakalpojumu risinājumiem kā virtuālais elektroniskais paraksts, ir būtiski veikt drošības procedūru un sistēmu auditu ne tikai uzticamiem pakalpojumu sniedzēja statusa ieguvušajām organizācijām, bet arī tām juridiskām vai fiziskajām personām, ar ko sertifikācijas pakalpojumu sniegšanas ietvaros ir noslēgti konfidencialitātes un sadarbības līgumi. Ja arī uzticams pakalpojuma sniedzējs drošības auditu ir izturējis, tad nav garantija, ka ārpakalpojumu sniedzējiem iekšienē arī ir līdzīga drošības pakāpe attiecībā pret klientu informācijas glabāšanu, apstrādi, darbinieku apmācībām drošības jomā u.c. jautājumiem, kas var ietekmēt pakalpojuma drošību un uzticamību. Ir nepieciešams, piemēram, pārbaudīt, vai noslēgtais starporganizāciju konfidencialitātes līgums atbilst informācijas drošības un neizpaušanas pasaules labākās prakses vadlīnijām, vai abas līguma puses slēdz iekšējos konfidencialitātes līgumus ar saviem darbiniekiem, kādus informācijas drošības pasākumus un procedūras veic ārpakalpojuma sniedzējs iekšienē, vai darbiniekiem tiek veiktas apmācības cilvēku izlūkošanas uzbrukumu risku novēršanai, kādas kvalitātes šīs apmācības ir un citus uzņēmuma darbības aspektus, kas garantētu uzticamību ne tikai oficiālā pakalpojuma sniedzēja, bet arī ārpakalpojumu sniedzēju pusē, kas palīdz piegādāt sertifikācijas pakalpojumus klientiem.

Šāds scenārijs, kad pie pakalpojuma ieviešanas strādā ierobežots iesaistīto juridisko un fizisko personu loks, kāds ir izmantots Latvijā, nav augstu kvalitāti nodrošināt spējīgs. Tas ir tāpēc, ka salīdzinoši šaurs iesaistīto personu loks nozīmē ierobežotu izmantoto zināšanu klāstu ar ierobežotu specialitāšu un kompetenču apjomu.

Darba autors uzskata, lai tiktu radīts pēc iespējas drošāks risinājums un visas potenciālās ievainojamības un riski novērsti, veidojot risinājumu ir jādarbojas plaši starptautiskā līmenī un jāveic publiskā apspriešana, jāpieaicina kompetentas fiziskās un juridiskās personas ar kā minimums piecu gadu praktisku pieredzi līdzīgu risinājumu vai līdzīgas drošības pakāpes risinājumu ieviešanā. Darba autors uzskata, ka Latvijas apstākļos, kādi ir šī darba rakstīšanas laikā, nav citas iespējas kā maksimāli kompetenta un daudzskaitlīga akadēmiskā personāla piesaistīšana uzticamu sertifikācijas pakalpojumu risinājumu izstrādē. Publiskās apspriešanas labo praksi parāda Amerikas Savienoto Valstu Nacionālā tehnoloģiju un standartu institūta procedūra, kādā tika izvēlēts jaunā šifrēšanas

standarta *AES*(uzlabots šifrēšanas standarts) (publiskais konkurss 1997.g. – 2000.g.) un jaunās jaučējfunkcijas standarta *SHA-3* (publiskais konkurss 2007.g. – 2012.g.) risinājums.[173,154] Tika veidots publiskais konkurss, kur visi iesniegtie risinājumi tika nodoti publiskai apspriešanai. Tas ir labs scenārijs, kas garantē pēc iespējas lielāku tehniskā risinājuma drošību un laicīgu risku novēršanu, jo risinājuma izveidē un analīzē tiek iesaistīti pēc iespējas vairāk speciālisti ar dažādām kompetencēm un praktisku pieredzi drošības risinājumu jomā. [173,154] Pastāv risks, ka kāds var sevis ieraudzītos riskus un ievainojamības noklusēt, bet salīdzinoši ar iespējami novērstajām problēmām, šis scenārijs ir uzskatāms par vienīgo. Darba autors vērš uzmanību tam, ka šāda publiskā apspriede nav ideju izvērtēšana, bet gan risinājuma apspriede un izvērtēšana tā sīkākajos aspektos. Konkurss ar publisko apspriedi nav ātrs process. Tas var ilgt pat līdz pieciem gadiem, bet vismaz tad ir pēc iespējas lielāka garantija, ka risinājums ir tiešām kvalitatīvs un ilgtspējīgs. Latvijas sertifikācijas pakalpojumu risinājuma izstrādes publiskā apspriede neskartu tikai pamata algoritmus, bet būtu obligāti jāapriež visu elektronisko dokumentu pielietošanas un to realizācijas shēmu. Darba autors prognozē, ka šādai apspriedei varētu pietikt ar vienu līdz diviem gadiem, kur tiktu iesaistīts arī akadēmiskais personāls, iespējami daudzi profesionāļi no pasaules, kas būtu aicināti ar personīgiem uzaicinājumiem. Darba autors uzskata, ka obligāti būtu nepieciešams piesaistīt Arni Paršovu un Madaru Virzu, kuriem ir ļoti liels potenciāls jautājumos, kas saistīti ar potenciālas Latvijas nacionālās datu drošības skolas izveidi, bez kuras kvalitatīvi sertifikācijas un drošības pakalpojumi Latvijā ir maz iespējami.

Vairāki kriptogrāfiski un tehniskā risinājuma riski, kas jāņem vērā, ieviešot elektroniskā paraksta risinājumus ir apskatīti šīs darba 4.7.1 un 4.7.4 nodaļās.

4.5.1 VIRTUĀLĀ ELEKTRONISKĀ PARAKSTA PIN KODA DROŠĪBA

Atšķirībā no elektroniskā paraksta viedkartē, Latvijas virtuālajam elektroniskajam parakstam tā radīšanas līdzeklis (privātā atslēga) glabājas nevis viedkartē, bet uz iekārtas (servera) kā to norāda uzticama sertifikācijas pakalpojuma sniedzēja atbildē portālā *twitter.com*. Atbilde redzama attēlā 4.12.



4.12. att. PIN nr.1

Tas nozīmē to, ka elektroniskā paraksta radīšanai lietotājam ir nepieciešams autentificēties portālā *eparaksts.lv* un ievadīt savu *PIN* kodu. Fiziska viedkarte nav nepieciešama. Tas piešķir *PIN* kodam ļoti lielu nozīmi un līdz ar to arī paaugstinās drošības prasības pret tā ievadi un apstrādi. Līdz ar to arī Latvijas sabiedrībā rodas jautājumi par ievadītā *PIN* koda drošību, kā tas ir redzams attēlā [4.13]



4.13. att. PIN Nr. 2

Šī darba rakstīšanas laikā Jānis Bokta pilda tajā brīdī Latvijā vienīgā uzticamā sertifikācijas pakalpojuma sniedzēja VAS „Latvijas Valsts radio un televīzijas centrs” valdes priekšsēdētāja amata pienākumus.

Plašāka attēlā 4.13. redzamā saruna sociālajā portālā Twitter ir aplūkojama Pielikumā Nr.7. Tajā VAS „Latvijas Valsts radio un televīzijas centrs” pārstāvis uzsver, ka *PIN* slepenība tiek nodrošināta. Jānis Bokta par *PIN* koda pārsūtīšanu un apstrādi saka: „Sesijas laikā visas darbības tiek šifrētas, arī *PIN* ievade!”.

Virtuālā elektroniskā paraksta veidošanai nepieciešamajam *PIN* kodam prasība ir sastāvēt tieši no astoņiem simboliem, un to ir jāveido gan no cipariem, gan latīņu alfabēta burtiem kā tas ir redzams attēlā 4.14.

MANI DATI

Ievadiet jauno PIN:

PIN kods (tieši 8 simboli, iekļaut gan latīņu burtus, gan ciparus) *:

☒ Rādīt PIN

PIN kods atkārtoti *:

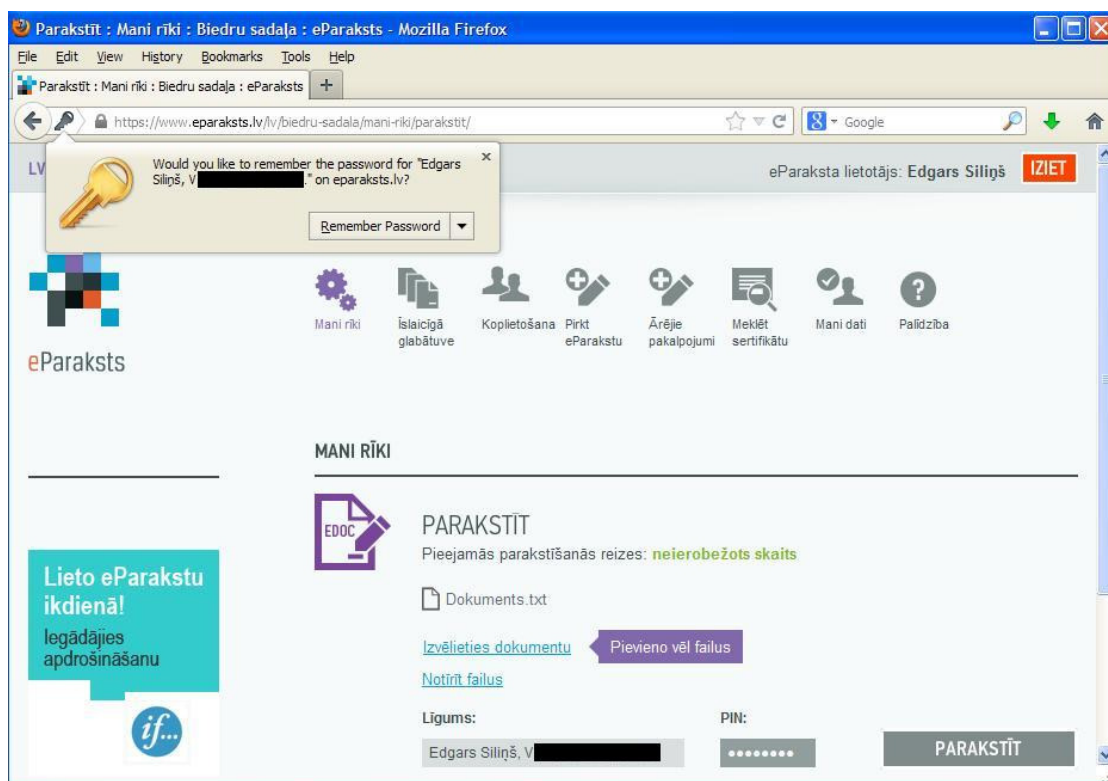
MAINĪT PIN **ATCELT**

4.14. att. **Nomainītais pin kods**

PIN kodu tikai no burtiem vai cipariem izveidot nav iespējams, jo tiek parādīts uznirstošs logs ar kļūdas paziņojumu.

Attēlā 4.14. darba autors nomaina sava virtuālā elektroniskā paraksta *PIN* kodu uz astoņu simbolu virkni „manspin1”

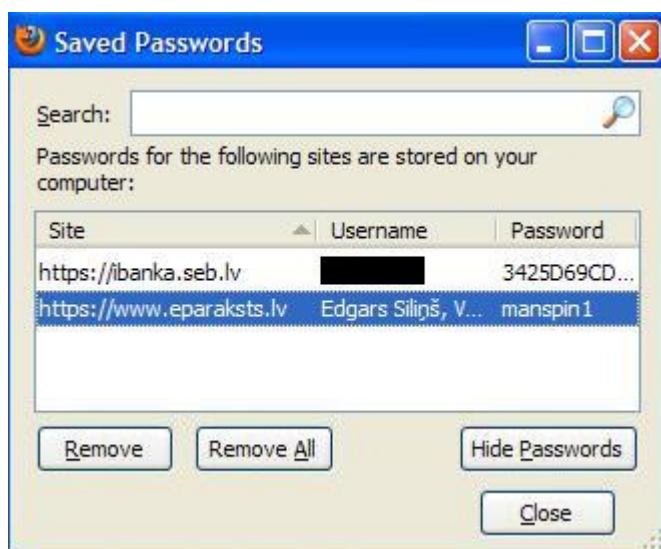
Attēlā 4.15 ir redzams, ka brīdī, kad tiek ievadīts *PIN* kods un nospiesta poga „PARAKSĪT”, interneta pārlūks piedāvā atcerēties ievadīto paroli (*PIN* kodu).



4.15. att. *PIN* koda saglabāšanas jautājums pārlūkā

Lietotājam, uz interneta pārlūka jautājumu atbildot apstiprinoši, ievadītais *PIN* kods tiek saglabāts pārlūka parolu glabātuvē. Instrukcija, kā tai piekļūt ir atrodama Pielikumā Nr.9.

Attēlā 4.16 ir redzams, ka ievadītais *PIN* kods tiek veiksmīgi saglabāts interneta pārlūkā nešifrēta un cilvēkam lasāma teksta veidā.



4.16. att. Saglabātā parole SEB ibankai un eparaksts.lv ievadītais *PIN* kods

Attēlā 4.16. redzamā informācija uzskatāmi parāda to, ka dokumenta parakstīšanas brīdī ir vismaz viens procesa izpildes posms, kad ievadītais *PIN* kods šifrēts netiek. Tas ir pretēji tam, ko attēlā 4.13. redzamajā sarunā Ilmāram Poikānam atbild Jānis Bokta, sakot, ka visos posmos *PIN* tiek šifrēts. Lietotāja un portāla savienojuma sesija, tiek šifrēta izmantojot *SSL* sertifikātu, tāpēc ir patiesi teikts, ka savienojuma pārraidītie dati tiek aizsargāti, bet par paša *PIN* koda šifrēšanu darba autoram ir šaubas. Ja pats *PIN* kods portālā netiek šifrēts, tad vēl aktuālāki kļūst šī darba nodaļā 4.2.2 aplūkotie *SSL* sertifikāta riski virtuālā elektroniskā paraksta portālam.

Tika veikts salīdzinājums starp drošības pasākumiem attiecībā pret *PIN* vai paroli slepenības nodrošināšanu un iespējamu lietotāja sesijas nekompromitēšanu. Rezultāti redzami tabulā 4.3

Tīmekļa vietņu paroli, PIN drošības salīdzinājums

	eParaksts.lv	Swedbank ibanka	SEB ibanka
Piedāvā atcerēties paroli/PIN?	Jā	Nē	Jā
Saglabātā parole/PIN strādā?	Netiek ievades laukā automātiski ievietota.	-	Nē
Paroles/PIN kļūdainas ievades reižu ierobežojums	nav	3	3
Sesijas laiks bez lietotāja darbībām	15 min	15 min	10 min

Salīdzinājumā redzams, ka ievadīto paroli *Swedbank* interneta bankā interneta pārlūks lietotājam atšķirībā no *SEB* interneta bankas un elektroniskā paraksta portāla nepiedāvā atcerēties. Tas automātiski izslēdz šo riska faktoru. *SEB* bankas interneta banka līdzīgi kā elektroniskā paraksta portāls piedāvā atcerēties un saglabāt ievadīto paroli. Kā redzams attēlā 4.16. *SEB* bankas saglabātā parole tiek šifrēta jau brīdī, kad lietotājs to ir ievadījis un nospiedis autentifikācijas datu apstiprināšanas pogu. Tika novērots, ka *SEB* bankas parole katru reizi, tiek šifrēta ar citu gala rezultātu. Nākošajā reizē, kad lietotājs apmeklē *SEB* interneta banku un ievada savu lietotāja vārdu, saglabātās parole šifrētā vērtība automātiski tiek ievietota tās ievades logā. Gadījumā, ja lietotājs nospiež autentifikācijas datu apstiprināšanas pogu, parole tiek atzīta par nepareizi ievadītu. Veicot salīdzinājumu, tika atklāts, ka virtuālā elektroniskā paraksta *PIN* koda ievadei nav kļūdaini ievadīto reižu skaita kontrole. Šis fakts kopā ar to, ka *PIN* kods nevar būt garāks par astoņiem simboliem nozīmē to, ka tā ievades realizācija virtuālā elektroniskā paraksta portālā *www.eparaksts.lv* var būt ievainojama gan pret pārlases, gan vārdnīcas uzbrukumu veikšanu. Ja ne automatizētu, tad cilvēka pašrocīgi veiktu noteikti.

Tika noskaidrots, ka nevienai no trīs aplūkotajām interneta vietnēm neaktīvas sesijas ilgums nepārsniedz piecpadsmit minūtes. Tas samazina nesankcionētas piekļuves risku, ja atvērta savienojuma sesija ir atstāta vaļā, dators nav noslēgts, bet pats tā lietotājs ir aizgājis prom no savas darbstacijas. Tādā gadījumā ļaundarim ir vismaz piecpadsmit minūtes elektroniskā paraksta portāla gadījumā, lai paspētu nonākt pie uzbrukuma upura datora un,

piemēram, mēģināt atminēt *PIN* kodu, paskatīties interneta pārlūkā saglabātās paroles vai kā citādi piekļūt sensitīvai informācijai. Darba autors vērš uzmanību, ka *www.eparaksts.lv* bija to portālu skaitā, kam tika 2012. gadā atklāta banku autentifikācijas ievainojamība.[44] To, izmantojot apvienojumā ar esošajiem *PIN* koda drošības riskiem, uzbrucējs varēja iegūt pilnu kontroli pār upura virtuālo elektronisko parakstu. Darba rakstīšanas brīdī banku autentifikācijas ievainojamība portālā *www.eparaksts.lv* ir novērsta.

Virtuālā elektroniskā paraksta *PIN* drošībai ir atklāti trīs riski:

1. Neierobežots kļūdaina *PIN* ievades pieļāvuma skaits,
2. *PIN* kods nevar būt garāks par astoņiem simboliem,
3. *PIN* kodu ir iespējams saglabāt nešifrētā veidā interneta pārlūkā.

Pirmajam no šiem riskiem risinājums ir tāds, ka ir nepieciešams virtuālā elektroniskā paraksta portāla izstrādātājiem papildināt tā funkcionalitāti, lai būtu iespējams kļūdaini ievadīt *PIN* kodu ne vairāk kā trīs reizes. Līdzīgi kā tas ir realizēts interneta banku vietnēs un elektroniskā paraksta viedkartēs.

Otrā riska risinājums ir pilnveidot virtuālā elektroniskā paraksta funkcionalitāti un *PIN* koda nosacījumus, lai tas varētu būt vismaz līdz divdesmit simboliem garš un ne īsāks par astoņiem simboliem. Tādā veidā tiktu uzlabota izmantoto *PIN* koda drošība un samazināta iespējamība tos atminēt.

Trešā riska risinājums ir ņemt piemēru no *SEB* un *Swedbank* interneta banku risinājumiem un iestrādāt līdzīgus mehānismus elektroniskā portāla interneta portāla *PIN* ievadei. Darba autors ierosina apvienot abus risinājumus, lai pēc iespējas uzlabotu *PIN* drošību. Ir nepieciešams veikt portāla uzlabojumus, lai interneta pārlūks līdzīgi kā *Swedbank* risinājumā neprasa vispār jautājumu atcerēties paroli un lietotāja ievadītais *PIN* kods obligāti ir jāšifrē, kad tas tiek ievadīts, kā tas ir *SEB* interneta bankai.

4.5.2 TREŠO PUŠU IZSTRĀDĀTĀJU RISINĀJUMI UN TO UZTICAMĪBA

Trešo pušu izstrādātājiem ir brīvi pieejamas Latvijas parakstītu elektronisko dokumentu apstrādes funkciju programmēšanas valodas *Java eDoc* bibliotēkas. Tās izstrādātājs var izmantot savos risinājumos, lai nodrošinātu tajos iespēju gan pārbaudīt parakstītus dokumentus, gan parakstīt elektroniskos dokumentus. Tas tiek panākts, izmantojot bibliotēkās esošas funkcijas, kas izstrādātājam ļauj piekļūt elektroniskā paraksta viedkartē esošajiem datiem un veikt ar tiem trešās puses risinājumam nepieciešamās darbības, piemēram, veidot elektronisko parakstu, veidot laika zīmogu, pārbaudīt parakstīta elektroniskā dokumenta derīguma u.c.

Izstrādātājs var brīvi lejupielādēt *java eDoc* bibliotēkas no uzticama sertifikācijas pakalpojumu sniedzēja interneta portāla.[82] Turpat arī ir nepieciešams lejupielādēt speciālu formu, kas ir jāaizpilda un jānosūta uzticamam sertifikācijas pakalpojumam uz norādītu elektroniskā pasta adresi. Atbildē izstrādātājs saņem licences failu, kas ir nepieciešams, lai ar bibliotēkām varētu strādāt. Licences teksta piemēru skatīt pielikumā Nr.8. Līdz ar šī faila nosūtīšanu un brīdi, kad bibliotēkas sāk strādāt, stājas spēkā bibliotēku lietošanas licences līgums. Tam ir šādas sadaļas: „Licences līgums”, „Bibliotēkas licence”, „1. Licences vispārējie noteikumi”, „2. Autortiesības”, „3. Jauninājumi un jaunas versijas”, „4. Kopēšana”, „5. Garantijas noteikumi”, „6. Preču zīmes”.

Pastāv liels risks saistībā ar trešo pušu risinājumiem, kas izmanto *Java eDoc* bibliotēkas, jo tie var viegli kļūt par vājāko posmu sertifikācijas pakalpojumu drošības ķēdē. Ja arī sertifikācijas pakalpojumu sniegšanas procedūras un tehnoloģijas ir izstrādātas un realizētas maksimāli droši un saskaņā ar pasaules labāko praksi, tad nevērīgs izstrādātājs, izmantojot *Java eDoc* bibliotēku funkcijas, visu drošību var sabojāt. Viens no veidiem, kā to izdarīt, ir ievadītā *PIN* koda neslēpšana tā, ka tas nešifrētā veidā kļūst pieejams kādā no risinājuma posmiem. Piemēram, atklūdošanas nolūkos ievadītais *PIN* kods tiek nešifrētā tekstā ierakstīts programmatūras izpildes žurnālfailos. Kaitniecisks izstrādātājs var pat speciāli iestrādāt slepenas sava risinājuma operācijas, kas visus ievadītos *PIN* kodus kopā ar atbilstošajiem un pieejamajiem sertifikātu datiem no ievietotās viedkartes uzkrāj slepenā datu bāzē vai pārsūta šo sensitīvo informāciju kādai ieinteresētai pusei.

Viens no risinājumiem šim riskam ir veikt trešo risinājumu un to programmkoda pārbaudes ar mērķi pārliecināties par to, vai tajā nav iestrādātas slepenas darbības, kas var kompromitēt viedkarti vai tajā esošos datus, un to, vai lietotāja ievadītie dati ir drošībā. Šis risinājums ir iespējams, jo uzticamam sertifikācijas pakalpojumam ir pieejama informācija par visiem izstrādātājiem, kam tas ir izsniedzis bibliotēku lietošanas licences. Par izstrādātāju pārbaudes veikšanu būtu jābūt atbildīgam vai nu pašam sertifikācijas pakalpojumam sniedzējam vai arī par sertifikācijas pakalpojumu sniegšanu uzraudzību atbildīgajai institūcijai, kas Latvijā darba rakstīšanas laikā ir Datu valsts inspekcija. Šis risinājums praktiski ir ļoti sarežģīti īstenojams, jo nav garantijas, ka pārbaudes laikā izstrādātājs kaitniecisko programmkodu ir noslēpis vai no risinājuma izņēmis, un uzreiz pēc pārbaudes veikšanas, tās koda daļas, kas atbild par lietotāja sensitīvo datu kompromitēšanu, uzstāda atpakaļ. Tāpat arī šādu pārbažu kvalitatīvai veikšanai būtu nepieciešami lieli finansiāli resursi, kas sertifikācijas pakalpojumus Latvijā padarītu vēl dārgākus.

Cits risinājums šim riskam ir iekļaut bibliotēku licences līgumā sadaļu, kur būtu ierakstīti noteikumi un drošības prasības risinājumiem, kuros šo bibliotēku funkcijas tiek

lietotas. Daži šādas nodaļas nosaukuma piemēri varētu būt: „Programmatūras izstrādes noteikumi”, „Izstrādes risinājumu drošības prasības” (vai noteikumi), „Bibliotēku izmantošanas drošības prasības” (vai noteikumi). Viena no šajā sadaļā obligāti iekļaujamām prasībām būtu ar mērķi, lai risinājumā, kurā tiek izmantotas šīs bibliotēkas, nevienā no tā izpildes posmiem, lietotāja ievadītais *PIN* kods nedrīkstētu būt pieejams (gan šifrētā, gan nešifrētā tekstā), tam ir būtu maksimāli droši aizsargātam no tā kompromitēšanas riskiem. Būtu nepieciešams licences līguma nosacījumus saskaņot ar Datu valsts inspekciju, lai tās formāts un saturs noteiktu izstrādātāja atbildību par lietotāja privāto datu aizsardzību.

Saskaņā ar esošajiem licences līguma nosacījumiem, uzsākot praktiski lietot *Java eDoc* bibliotēkas, izstrādātājs piekrīt un apņemas pildīt līguma saistības. Šāda licences līguma papildinājuma mērķi būtu noteikt izstrādātājam atbildību par sava risinājumu kvalitāti, drošību un it īpaši visu lietotāja ievadīto privāto datu drošību, kā arī kopumā uzlabot to trešo risinājumu kvalitāti, kur tiek izmantotas uzticama sertifikācijas pakalpojumu sniedzēja piegādātas bibliotēkas.

4.6 LATVIJAS ELEKTRONISKĀ PARAKSTA VIEDKARŠU RISKI, ŅEMOT VĒRĀ IGAUNIJAS ELEKTRONISKĀS IDENTIFIKĀCIJAS KARTES SEKMĪGU UZLAUŠANU

2012. gada aprīlī tika publicēts pētījuma pārskats „*Efficient Padding Oracle Attacks on Cryptographic Hardware*”, kur tiek parādīts, kā ekspluatēt dažādu iekārtu šifrētu atslēgu importa funkcijas, lai atklātu importētās atslēgas. [184] Tas tiek panākts, izmantojot papildinājuma orākula uzbrukumus, kur kļūdas paziņojumi, kas rodas no nepareizi papildināta nešifrēta teksta, tiek izmantoti kā blakus kanāls. [184] Starp citiem panākumiem pārskatā tiek aprakstīts veiksmīgs uzbrukums Igaunijas elektroniskās identifikācijas kartei. [184]

Tā kā Igaunijas elektroniskās identifikācijas kartes, tāpat kā Latvijas ieviestās elektroniskās identifikācijas kartes izmanto *PKCS#11* (publiskās atslēgas šifrēšanas standarts šifrēšanas marķiera saskarnei) standartu, tad nav izslēgta šādas ievainojamības esamība arī Latvijā ieviestajām kartēm.

Pētījuma rezultāti parāda, ka veiksmīgi uzbrukumi, izmantojot minēto metodi, ir iespējami, taču praktiski ļoti grūti vai pat neiespējami realizējami dzīvē. [184] Taču, kriptanalīzei un tehnoloģijām, attīstoties ir ļoti iespējams, ka pētījumā izmantotās uzbrukuma metodes tiks pilnveidotas un visas iekārtas un risinājumi, kur nebūs veikti ievainojamību novēršanas pasākumi, kļūs kompromitējamas. Labākajā gadījumā uzbrukuma pilnveidotājs

savu atklājumu paziņos publiski, lai atbildīgās iestādes un izstrādātāji var laicīgi veikt pretpasākumus. Sliktākajā gadījumā jaunās zināšanas tiks izmantotas kaitniecisku darbību veikšanai vai pārdotas kādam ieinteresētam ļaundarim.

Kā efektīvākais pretpasākums tiek minēts tas, ka ir nepieciešams *PKCS#1v1.5* vietā izmantot *OAEP* (optimāla asimetriskās papildināšanas shēma) papildinājumu shēmu, kas jau ir iekļauta *PKCS#11* standartā. [184, 45, 46] *OAEP* ir drošāks tādā ziņā, ka nešifrētā teksta papildināšanā tiek iesaistīta ne tikai nejauši izvēlēta vērtība, bet arī divas jaucējfunkcijas, kas šifrēšanas tekstu padara nelasāmu un tādu, ka to nevar izmantot par orākulu, lai uzbrucējs varētu iegūt sev nepieciešamo informāciju.

Tehniskajos risinājumos, ieviešot *OAEP* papildinājumu shēmu, izstrādātājam ir jābūt ļoti uzmanīgam, jo nekvalitatīvu uzstādījumu gadījumā ir iespējams papildinājuma orākula uzbrukums, kas ir daudz reizes efektīvāks par to, kas ir aprakstīts pētījuma pārskatā. [184,45,46]

4.7 CITI RISKI

Bez iepriekš aplūkotajiem ir arī citi riski, ko būtu vērts ņemt vērā, ieviešot, uzturot un attīstot drošus sertifikācijas pakalpojumus. Vairāki no tiem ir apskatīti turpmākajās nodaļās.

4.7.1 RSA ALGORITMA SPECIFISKIE RISKI

Darba autors šajā nodaļā neapskatīs visas RSA algoritma ievainojamības, jo vienmēr ir liela iespējamība, ka kāds publicēts pētījums netiek atrasts vai arī par ievainojamību netiek publiski ziņots vispār. [4]

RSA šifrēšanas algoritmam pastāv trīs uzbrukuma objekti: [4]

1. Sadalīt publisko atslēgu n pirmreizīnātajos; [4]
2. Atrast Eilera funkcijā $\phi(n)$ izmantojamo skaitli, kas iegūstams ar formulu (4.1)
$$E = (p-1)*(q-1) \quad (4.1)$$
3. Atrast privāto atslēgu d . [4]

Pirmais uzbrukuma objekts ir ļoti nozīmīgs, jo sadalot publisko atslēgu n pirmreizīnātajos tiek iegūti izvēlētie pirmskaitļi p un q , jo publiskā atslēga n tiek aprēķināta pēc formulas (4.2). [4]

$$n = p*q \quad (4.2)$$

Šie pirmskaitļi tiek pēc tam izmantoti privātās atslēgas ģenerēšanā, izmantojot Eilera funkciju $\varphi(n)$. [4] Ja uzbrucējs zina p vai q , tad viņš var aprēķināt privātās atslēgas vērtību. Drošības prasību dēļ p un q tiek izvēlēti ļoti lieli skaitļi, lai tos uzminēt un atminēt būtu pēc iespējas sarežģītāk. [4]

Otrais uzbrukuma objekts arī ir tieši saistīts ar izvēlētajiem p un q pirmskaitļiem, jo tā iegūšanai tie tiek izmantoti. [4] Veiksmīga uzbrukuma veikšanai uzbrucējs var tos pat nezināt, jo viņam pietiek zināt skaitli, kas tiek izmantots privātās atslēgas iegūšanai. [4] Ja uzbrucējs zina rezultātu formulai (4.1) tad viņš, izmantojot, Eilera matemātiskās funkcijas var izrēķināt upura privāto atslēgu d . [4]

Trešais uzbrukuma mērķis ir pati privātā atslēga d , kas tiek izmantota šifrēšanas un parakstīšanas operācijās. [4] Ja uzbrucējam tā ir zināma, tad viņam ir pilna pārvaldība pār upura elektroniskā paraksta radīšanas līdzekļiem, jo publiskās atslēgas e un n jau viņam ir zināmas. [4] Privātās atslēgas iegūšanai ir dažādi uzbrukuma veidi, kur ietilpst gan tās minēšanas mēģinājumi, gan matemātiski uzbrukumi, kas, piemēram, balstās uz izvēlēta šifrēta teksta izmantošanas metodēm. [4]

Izstrādājot *RSA* risinājumus ir obligāti jāveic visi nepieciešamie pasākumi, lai, ģenerējot p un q vērtības, tās uzreiz tiktu neatgriezeniski dzēstas no visām datora sistēmas komponentēm tā, lai nebūtu iespējams šīs vērtības vai to apstrādes pēdas nolasīt vai atgūt. Īpaša uzmanība jāpievērš, atkarībā no risinājuma, lai p un q nebūtu iespējams atgūt no datora operatīvās atmiņas vai cietā diska. Ja šīs prasības netiek nodrošinātas, tad, piemēram, iekšēja uzbrukuma riski var būt ievērojami. Darba autoram nav pārliecības par to, vai Latvijas uzticama sertifikācijas pakalpojumu sniedzēja risinājumā *RSA* īpatnības un papildus prasības pret drošību ir realizēts.

Šāda riska novēršanas risinājums ir veikt augstas kompetences esošā elektroniskā paraksta risinājuma pārbaudi, kur piedalītos arī vismaz viens profesionāls kriptologs. Pēc šādas pārbaudes vajadzētu būt publiski pieejamam kompetentam ziņojumam par pārbaudes rezultātiem. Šajā ziņojumā būtu jānorāda, vai esošais risinājums nodrošina paraksta radīšanas un paraksta privāto un publisko atslēgu radīšanas datu drošību, vai aparatūras platforma un vide atbilst kriptogrāfijas sistēmu un risinājumu labākās prakses drošības principiem, vai publiskās un privātās atslēgas radīšanas dati netiek kopēti, glabāti, sūtīti, vai padarīti pieejami trešajām pusēm utt.

Tā kā *RSA* algoritms šifrēšanas un elektronisko parakstu jomā tiek izmantots jau vairāk kā divdesmit gadus, pret to ir vērsti un veidoti daudz un dažādi uzbrukumi, no kuriem neviens nav izrādījies iznīcinošs. [128] Lielākā daļa veiksmīgo uzbrukumu parāda sekas un aspektus, kam ir jāpievērš stingra uzmanība ieviešot *RSA* algoritmu informācijas tehnoloģijas sistēmās

un risinājumos. [128] Tas parāda to, ka *RSA* kriptogrāfijas drošība ir ļoti atkarīga ne tik daudz kā no pašu šifrēšanas algoritmu drošības, bet vairāk no tās ieviesēja un izmantotāja, kas ir ļoti riskanti, īpaši sertifikācijas pakalpojumos, ja sertifikācijas pakalpojumu sniedzējs vai tā programmatūras un risinājumu piegādātājs netiek pietiekoši kvalitatīvi kontrolēts un pārbaudīts. [128]

Viens no risinājumiem, kā izvairīties no *RSA* kriptogrāfijas drošības riskiem ir tā vietā izmantot citus šifrēšanas un parakstīšanas risinājumus un algoritmus. Tā, piemēram, Amerikas Savienotajās valstīs Nacionālās drošības sistēmu komiteja ir izsludinājusi Nacionālās informācijas nodrošināšanas politiku par publiskajiem standartiem priekš drošas informācijas koplietošanas starp nacionālās drošības sistēmām *CNSSP-15*. [170] Šī politika nosaka valsts mērogā pārstāt izmantot *RSA* kriptogrāfiju un valsts drošības sistēmās elektroniskajam parakstam izmantot eliptisko līkņu digitālā paraksta algoritmu (*ECDSA*). Svarīgi ir atzīmēt, ka, atšķirībā no *RSA*, digitālā paraksta algoritms (*DSA*) ir paredzēts tikai elektroniskā paraksta radīšanai. *RSA* tiek izmantots gan datu šifrēšanai, gan elektroniskā paraksta radīšanai. Izsludinātās politikas realizācija ir iekļauta Amerikas Savienoto Valstu Nacionālās Drošības aģentūras izdotā B kategorijas kriptogrāfijas algoritmu kopumā, kas ir paredzēts valsts drošības informācijas apstrādei. [163] Izmantotie eliptisko līkņu algoritmi ir aprakstīti *FIPS 186-3* standartā. [163] [170]

Būtiska eliptisko līkņu kriptogrāfijas atšķirība no *RSA* kriptogrāfijas ir tas, ka tajā tiek izmantoti reāli skaitļi, nevis veseli. Tas ļauj samazināt nepieciešamo atslēgu garumus un ierobežo potenciālo risku apjomu.

4.7.1.1 PIEAUGOŠS ŠIFRĒŠANAS ATSLĒGAS GARUMS

Tā kā *RSA* algoritms balstās uz veselu skaitļu matemātiskajiem aprēķiniem, kur privātās un publiskās atslēgas vērtība ir tieši atkarīga no izvēlētajiem pirmskaitļiem p , q un e , pastāv ierobežojums attiecībā uz iespējamām skaitļu kombinācijām. Tāpēc, lai saglabātu šifrēšanas algoritma drošumu šie pirmskaitļi ir jāizvēlas ļoti lieli. Šī darba rakstīšanas laikā *RSA* algoritma izmantošanai jau tiek rekomendēts izmantot vismaz divi tūkstoši četrdesmit astoņu bitu garuma atslēgas. Tas nozīmē veselu pirmskaitli ar apmēram seši simti septiņpadsmit decimālzīmēm. Uz to arī daļēji balstās šī algoritma drošība, ka tik lielus skaitļus atkodēt vai publisko atslēgu n sadalīt reizinātājos, atrodot p un q , ir ļoti sarežģīti un laikietilpīgi. [119]

Laikam plūstot, tehnoloģijām attīstoties un plašāk lietojot *RSA* algoritmu, izmantoto atslēgu vēsture kļūst apzinātāka un plašāka, palielinās varbūtība un iespējas kompromitēt

esošās vai arī vecās atslēgas. Tāpēc Amerikas Savienoto valstu Nacionālais standartu un tehnoloģiju institūts publicēja ziņojumu *SP 800-57 „Rekomendācijas atslēgu pārvaldībai”*. Šajā ziņojumā tiek noteikts, ka līdz 2010. gadam RSA algoritma darbībā ir atļauts izmantot tādu atslēgas garumu, kas nav mazāks ar tūkstošs divdesmit četru bitu garumu. [174,182,202] Sākot ar 2030. gadu nav atļauts izmantot tādu atslēgu, kas būtu mazāka par trīs tūkstoši septiņdesmit divu bitu garumu. [174,182,202] Nav izslēgts, ka šīs rekomendācijas, pamatojoties uz jauniem kriptanalīzes atklājumiem, var mainīties un šie laika intervāli un atbilstoši atslēgu garumi var tikt noteikti atšķirīgi.

Šāda izmantoto atslēgu garuma novecošana rada lielu risku tieši elektroniskā paraksta jomā. Tā piemēram, dokuments, kas ir parakstīts 2010. gadā ar divi tūkstoši četrdesmit astoņu bitu garuma atslēgu var nebūt drošs pēc divdesmit gadiem. Atslēgu garuma maiņa atstāj tiešu ietekmi gan uz skaitļošanas patērētājam jaudām, patērēto laiku, kas nepieciešams algoritma darbību veikšanai (šifrēšana, atšifrēšana, parakstīšana, pārbaudīšana), gan izmantotajām tehnoloģijām. Jo lielāks atslēgas garums prasa lielāku apstrādei nepieciešamo vietu datu bāzēs, operatīvajās atmiņās, mikroshēmās un citos skaitļošanas sistēmu elementos.

4.7.1.2 ILGTERMIŅA ELEKTRONISKI PARAKSTĪTU DOKUMENTU GLABĀŠANA

Latvijas Republikas likuma Par grāmatvedību 10. pantā tiek noteikts glabāšanas laiks dažādiem uzņēmuma dokumentiem. [32] Dokumentu glabāšanas laiks var būt no pieciem līdz pat septiņdesmit pieciem gadiem. Visilgāk likums nosaka glabāt uzņēmuma attaisnojuma dokumentus par darbiniekiem aprēķināto mēnešalgu. [32]

Tehnoloģiju attīstība un maiņa ir nepārtraukts process. Strauji attīstās arī kriptanalīzes joma, kas nepārtraukti atrod jaunas ievainojamības esošajos kriptoloģijas risinājumos, vai atrod veidus, kā optimizēt un padarīt praktiski pielietojams iepriekš atklātās metodes.

Nemot vērā izmantoto atslēgu iespējamo kompromitēšanu un atslēgu garumu izmaiņas, laika gaitā, dokumentiem, kas tiek ilglaicīgi glabāti ir nepieciešama pārparakstīšana. Tas nozīmē jau parakstītu dokumentu parakstīt ar drošāku privāto atslēgu vai pavisam citu šifrēšanas, parakstīšanas algoritmu. Viens no risinājumiem pārparakstīšanai būtu, ja arhīvā glabātos dokumentus parakstītu ar speciāli tam domātu paraksta radīšanas datiem, kas ir izsniegti arhīva turētājam, piemēra Latvijas Valsts arhīvam. Tādā veidā nerastos problēmas ar visu dokumentu faktisko parakstītāju atrašanu un likšanu viņiem parakstīt savus dokumentus vēlreiz. Tādā scenārijā problēmas nerastos arī no tā, ja konkrētais parakstītājs pārparakstīšanas brīdī varētu būt jau zaudējis savas pilnvaras vai citādi nebūt vairs paraksttiesīgs. Gadījumā, ja dokumentus pārparaksta organizācija, kas uztur arhīvu, tad dokumenta parakstīšanas datu

kompromitēšanas gadījumā, tā autentiskumu varētu pierādīt, to salīdzinot ar šī konkrētā dokumenta pārparakstīto versiju, kas tiek glabāta arhīvā. Tikai šim arhīva dokumentam tad būtu radīts papildus aizsardzības slānis, izmantojot tajā brīdī aktuālākas drošības tehnoloģijas, kas garantētu tā autentiskumu. Visi dokumenti, kas būtu identiski oriģinālam vai konkurējoši par oriģināla statusu un nebūtu arhīva pārparakstīti, tiktu uzskatīti par juridiski bezspēcīgām kopijām vai oriģināla dokumenta viltojumiem.

Darba autors vērš uzmanību, ka šim risinājumam ir risks, ka arhīva organizācijas darbinieki tiek uzpirkti vai kā citādi ietekmēti kaitnieciskos nolūkos. Tāpēc, kamēr tiek izmantots *RSA* šifrēšanas algoritms, būtu nepieciešams izveidot risinājumu, ka pārparakstīšanu veic vismaz divas dažādas organizācijas, veidojot nevis divus atsevišķus elektroniskos parakstus, bet gan vienu. Tā kā *RSA* algoritmam ir spēkā formula (4.3), kur *e* ir publiskā atslēga, *d* ir privātā atslēga, *p* un *q* ir izvēlēti pirmskaitļi.

$$e \cdot d \bmod ((p-1) \cdot (q-1)) \equiv 1 \quad (4.3)$$

Saskaņā ar matemātikas likumiem, privāto atslēgu *d* var sadalīt divās daļās *d1* un *d2* tā, ka ir spēkā vienādojums (4.4)

$$e \cdot d1 \cdot d2 \bmod ((p-1) \cdot (q-1)) \equiv 1 \quad (4.4)$$

Tad šifrēšanas un atšifrēšanas funkcijas būtu atbilstoši formulām (4.5) un (4.6), kur *m* ir nešifrēts teksts, bet *c* ir šifrēts teksts.

$$c \equiv m^e \bmod ((p-1) \cdot (q-1)) \quad (4.5)$$

$$m \equiv c^{(d1 \cdot d2)} \bmod ((p-1) \cdot (q-1)) \quad (4.6)$$

Pēc matemātiskās likumiem vienādojumu var izteikt pēc vienādojuma (4.7).

$$m \bmod ((p-1) \cdot (q-1)) = (m^e)^{(d1 \cdot d2)} = (((m^e)^{d1})^{d2}) \quad (4.7)$$

Pēc aprēķiniem redzams, sadalot privāto atslēgu divos reizinātājos, matemātiskās funkcijas rezultāti nemainās. Šādā gadījumā *d1*, piemēram, ir tikai Valsts arhīva pārziņā, bet otra privātās atslēgas daļa *d2* ir izsniegta citai valstiski nozīmīgai organizācijai, piemēram Latvijas Bankai. Aprēķini rāda, ka privāto atslēgu drošības nolūkos var sadalīt pat vairākās daļās. Ja izmantotu šādu mehānismu, tad ļaundarim, lai pārparakstīšana tiktu veikta viņa interesēs, nāktos uzpirkt vai kā citādi ietekmēt nevis tikai viena Valsts arhīva darbiniekus, bet gan arī visu pārējo organizāciju darbiniekus, kuri ir atbildīgi par pārparakstīšanas atslēgas glabāšanu un dalību dokumentu pārparakstīšanas procedūrās. Šādā risinājumā, ja arī tiek konstatēta kaitnieciska darbības veikšana, tad, izmantojot matemātiskus pierādījumus, varēs saukt pie atbildības visas organizācijas, kuru pienākumos būs pārparakstīšanas veikšana. Tas ir tāpēc, ka radīt derīgu elektronisko parakstu varētu tikai tad, ja visi ir parakstījušies. Ja kaut viena iestāde nebūtu parakstījusies, tad pārparakstītais un kompromitētais dokuments netiktu atzīts par derīgu. Tas ir tāpēc, ka privātās atslēgas vērtībai, kas tiktu izmantota

pārparakstīšanas procedūrā trūktu viena daļa(reizinātāja). Tā rezultātā būtu publiskās atslēgas e un privātās atslēgas d neatbilstība.

Nododot elektroniskus dokumentus arhīvam, ir ļoti svarīgi nodrošināt un izstrādāt mehānismus, lai būtu iespējams dokumentu atvērt un pārbaudīt tā autentiskumu arī pēc septiņdesmit pieciem gadiem. 2011. gada 22. februāra informatīvajā ziņojumā par eParaksta praktiskās ieviešanas reālo situāciju un problēmām tā ieviešanā Latvijas Republikas Satiksmes ministrija par vienu no elektronisko dokumentu aprites problemātiku raksta: „Daudzi izvairās lietot e-dokumentus, jo nezina kā tos nodot Valsts arhīvam, bet pats arhīvs nespēj izstāstīt, kā tiks nodrošināta elektronisko dokumentu arhivēšana, saglabāšana un atvēršana pēc daudziem gadiem.”. [73] Ziņojuma saturs norāda, ka šajā nodaļā aprakstītā problēma Latvijā ir aktuāla arī pēc vairāk kā pieciem elektroniskā paraksta pastāvēšanas gadiem.

4.7.1.3 IZVĒLĒTA ŠIFRĒTA TEKSTA UZBRUKUMU RISKI

Ja sertifikācijas pakalpojumiem tiek izmantots *RSA* algoritms, tad ir svarīgi, lai dokumentu parakstīšana būtu pārdomāta. Ja tā nebūs, tad uzbrucējs varēs veikt sekmīgus uzbrukumus, iegūstot paraksta radīšanas līdzekļus vai arī viltojot upura parakstu uz sevis izvēlētiem dokumentiem. [4]

Viens no uzbrukuma veidiem, ko uzbrucējs var izmantot, ir izvēlēta šifrēta teksta izmantošana. [4] Piemēram, Alise sūta Bobam šifrētu vēstuli. Oskars noklausās pārraidītos datus un iegūst šifrēto tekstu c . [4] Oskars vēlas atrast tādu m , ko varētu aprēķināt pēc formulas (4.8), kur c ir Alises šifrētais teksts, d ir Alises privātā atslēga. [4]

$$m = c^d \quad (4.8)$$

Pēc tam Oskars izvēlas skaitli r , kas ir relatīvs pirmskaitlis ar Alises publisko atslēgu n un atbilst nosacījumam ($r < n$). [4] Izmantojot šos datus, Oskars izrēķina skaitli x pēc formulas (4.9), kur e ir Alises otra publiskā atslēga. [4]

$$x = r^e \bmod n \quad (4.9)$$

Pēc tam Oskars iegūst skaitli y , ko aprēķina pēc formulas (4.10). [4]

$$y = x * c \bmod n \quad (4.10)$$

Oskara uzbrukumam ir vajadzīgs arī skaitlis t , ko aprēķina pēc formulas (4.11). [4]

$$t = r^{(-1)} \bmod n \quad (4.11)$$

Zinot šo informāciju, Oskars iedod nošifrēt (parakstīt) sevis veidotu ziņojumu y . Alise to paraksta, kur *RSA* algoritma rezultātā šifrētā vērtība u atbilstu aprēķinam pēc formulas (4.12).

$$u = y^d \bmod n \quad (4.12)$$

Kad Oskars ir saņēmis atbildi no Alises, viņš, izmantojot iepriekš noklausīto šifrēt tekstu c , var izrēķināt Alises privātās atslēgas vērtību.

Aprēķina gaita:

$$t * u \bmod n = r^{(-1)} * y^d \bmod n = r^{(-1)} * x^d * c^d \bmod n = r^{(-1)} * r * c^d \bmod n = c^d \bmod n = m$$

Praktiski uzbrukuma aprakstā izmantotie piemēri būtu parakstāmo teksta ziņojumu jaucējkode. [4] Veiksmīga uzbrukuma gadījumā uzbrucējs iegūst Alises privāto atslēgu un var veiksmīgi Alises parakstu turpmāk viltot un lietot savām vajadzībām tik ilgi, kamēr Alise neaptur vai neanulē sava sertifikāta darbību. [4]

Cits scenārijs parāda, kā uzbrucējs, izmantojot izvēlēta šifrēta teksta uzbrukumu, var veiksmīgi viltot upura parakstu uz cita dokumenta. [4] Pieņemsim, ka Bobs ir notārs. Alise nosūta Bobam dokumentu, ko tas atsūta atpakaļ kā nošifrētu (parakstītu) ar savu personīgo atslēgu. [4] Oskaram ir nepieciešams Boba paraksts uz viņa sagatavota dokumenta $m1$. [4] Oskars izvēlas patvaļīgu skaitli x . [4] Viņš izrēķina skaitli y pēc formulas (4.12), kur e ir Boba publiskā atslēga. [4]

$$y = x^e \bmod n \quad (4.12)$$

Oskars izrēķina arī m pēc formulas (4.13). [4]

$$m = y * m1 \quad (4.13)$$

Izrēķināto tekstu m Oskars aizsūta Bobam parakstīt, kurš to arī izdara. [4] Tā rezultātā Oskars iegūst vērtību, kas iegūta pēc formulas $m^d \bmod n$, kur d ir Boba privātā atslēga. [4] No šīs saņemtās informācijas Oskars var iegūt Boba nošifrēta (parakstīta) dokumenta $m1$ vērtību $c1$ pēc formulas (4.13) [4]

$$c1 = (m^d \bmod n) * x^{(-1)} \bmod n = m1^d \bmod n \quad (4.13)$$

Šādā veidā, ja Bobs ir nepārdomāti parakstījis Oskara iesūtītu dokumentu, viņa paraksts var tikt viltots un uzlikts uz cita dokumenta, viņam to nezinot. [4] Šajā gadījumā uzbrucējam nav nepieciešams zināt ne Boba privāto atslēgu, ne kādu no izvēlētajiem pirmskaitļiem p un q , ne arī kādu no privātās atslēgas veidošanas starpvērtībām. [4] Pietiek tikai ar to, ka Bobs paraksta Oskara speciāli izveidotu tekstu. [4]

Vēl viens scenārijs, ko uzbrucējs var izmantot, ir uzģenerēt tekstus (tā jaucējkodus) $m2$ un $m3$ tādus, lai $m1$ varētu aprēķināt pēc formulas (4.13).

$$m1 = m2 * m3 \quad (4.13)$$

Formulā (4.13) $m1$ ir tā dokumenta tekstu, kuru uzbrucējs Oskars vēlas, lai upuris Bobs paraksta. [4] Lai veiktu veiksmīgu Boba paraksta viltošanu, Oskars aizsūta upurim parakstīt $m2$ un $m3$, tādā veidā iegūstot abu dokumentu parakstītās vērtības $c2$ un $c3$, kas aprēķināmas pēc formulām (4.14) un (4.15). [4]

$$c2 = m2^d \bmod n \quad (4.14)$$

$$c3 = m3^d \bmod n \quad (4.15)$$

Ņemot vērā, ka $m2$ un $m3$ tika veidots speciāli, lai savstarpējā reizinājumā radītu $m1$, Oskars var aprēķināt parakstītā $m1$ vērtību $c1$ pēc formulas (4.16) [4]

$$c1 = m1^d \bmod n = ((m2^d \bmod n) * (m3^d \bmod n)) \bmod n \quad (4.16)$$

Tādā veidā Oskars iegūst savu dokumentu $m1$ ar Boba parakstu. [4]

Lai no šāda veida uzbruktiem izvairītos ir svarīgi pirms parakstīt elektronisko dokumentu, tam veikt nelielas izmaiņas. [4] Pietiek ar nelielām kosmētiskām izmaiņām, lai dokumenta šifrēšanas laikā radītā jaucējkode vērtība tik uzmainīta tā, lai uzbrucējs izvēlēta šifrēta teksta uzbrukumu nevarētu veiksmīgi īstenot. [4] Īpaši svarīgi tas ir gadījumos, ja dokumenta adresāts ir vienīgais vai pirmais parakstītājs. [4]

4.7.1.4 KOPĒJA MODUĻA UZBRUKUMS

Ja RSA algoritms tiek nepārdomāti vai nekvalitatīvi iestrādāts un izmantots, tad viena no sekām, kas var rasties ir tas, ka ļaundaris var izmantot kopēja moduļa uzbrukumu („*common modulus attack*”). [4] Tas ir iespējams, ja, RSA algoritmā veidojot lietotājiem privātās un publiskās atslēgas, rodas situācija, ka publiskā atslēga n nemainās, bet mainās tikai e . [4] Ja, piemēram, tiek nošifrēts viens un tas pats dokuments m ar divām publiskajām atslēgām $e1$ un $e2$, kas ir relatīvi pirmskaitļi, tad atšifrēšanai nepieciešamā privātā atslēga nav nepieciešama, lai iegūtu šifrēto ziņojumu m . [4]

Piemēram, pakalpojuma sniedzējs nosūta diviem klientiem vienu un to pašu nezināmu dokumentu. [4] Abu dokumentu šifrētais teksts ir $c1$ un $c2$, ko iegūst pēc formulām (4.17) un (4.18)

$$c1 = m^{e1} \bmod n \quad (4.17)$$

$$c2 = m^{e2} \bmod n \quad (4.18)$$

Uzbrucējs Oskars zina publiskās atslēgas n , $e1$, $e2$ un abas nosūtītos, šifrētos dokumentus $c1$ un $c2$. [4] Ar to viņam ir pietiekoši, lai uzzinātu dokumenta saturu m . [4] Tā kā $e1$ un $e2$ ir relatīvi pirmskaitļi, tad, izmantojot paplašināto Eiklīda algoritmu, var atrast skaitļus r un s tādus, lai būtu spēkā vienādojums (4.19). [4]

$$r * e1 + s * e2 \bmod n = 1 \quad (4.19)$$

Tā kā, lai vienādojums būtu spēkā, skaitlim r vai s ir jābūt negatīvam, tiek atkārtoti lietots paplašinātais Eiklīda algoritms, lai atrastu $c1^{(-1)}$, pieņemot, ka r ir negatīvs. [4] No tā izriet vienādojums (4.20), pēc kura var aprēķināt šifrēto ziņojumu m . [4]

$$(c1^{(-1)})^{(-r)} * c2^s = m \bmod n \quad (4.20)$$

Praktiski šāds uzbrukums elektroniskā paraksta pašreizējā realizācijā nav aktuāls, bet jebkurā brīdī sertifikācijas pakalpojumu sniedzējs var sākt sniegt jauna formāta iespējas saviem klientiem. [4] Tā piemēram, iespēja paturēt tekstu noslēpumā un izsniegt tikai elektroniskos parakstus, ar ko tam tekstam var tikt klāt. [4] Piemēram, ja likums ļauj izmantot elektronisko parakstu testamentos, tad var būt scenārijs, ka testamenta rakstītājs atstāj tā tekstu pie notāra. [4] Viņš rada savam dokumentam divus elektroniskos parakstus, ar ko šim tekstam var tikt klāt un to izlasīt. [4] Šos abus parakstus viņš izsniedz diviem mantiniekiem, kuri attiecīgajā brīdī varēs ierasties pie notāra un iepazīties ar testamenta saturu. [4] Piemēram, abi mantinieki nevēlas gaidīt testamenta autora nāvi un ir apņēmušies uzzināt novēlējuma tekstu pēc iespējas ātrāk. [4] Ja abiem parakstiem ir viena un tā pati publiskā atslēga n , tad mantiniekiem ir iespējams uzzināt novēlējuma tekstu, izmantojot iepriekš aprakstītās matemātiskās darbības. [4] Ja testaments pirms parakstīšanas ir šifrēts ar jaucējfunkciju, tad mantinieki uzzinās jaucēj kodu. Ja jaucējfunkcija nav izmantota, tad mantinieki uzzinās testamenta tekstu un neapmierinātību gadījumā var sākt iedarboties uz testamentu ar mērķi, lai testamenta teksts tiek mainīts. [4] Jaucējfunkcijas izmantošanas gadījumā, ja tai ir atklāta jaucējsadursmes iespējamība, mantinieki var uzģenerēt citu testamentu ar identisku jaucēj kodu kā oriģinālam. [4]

Šis uzbrukums parāda vienu no aspektiem, kas jāņem vērā, kad ievieš RSA algoritmu drošības sistēmās. [4] Respektīvi, veidojot jaunas šifrēšanas privātās un publiskās atslēgas ir nepieciešams pārbaudīt, lai identiska publiskā atslēga n nebūtu nevienam citam esošam klientam jau izsniegta. [4] Labākajā gadījumā, pirms apstiprināt n vērtību, būtu nepieciešams pārbaudīt arī citu līdzīgu pakalpojumu sniedzēji izsniegtās publiskās atslēgas n vērtības. Tas ir nepieciešams, lai pēc iespējas garantētu n unikalitāti visiem tādu sertifikācijas pakalpojumu klientiem, kuru elektroniskā paraksta risinājums izmanto *RSA* šifrēšanas algoritmu. [4]

4.7.2 IZMANTOTO JAUCĒJFUNKCIJU VEIDOŠANAS TEHNOLOĢIJU RISKI

Elektroniskā paraksta risinājumi, kas izmanto *RSA* šifrēšanu, no parakstāmā satura izveido jaucēj kodu. Tehniski tiek parakstīts nevis pats parakstāmais saturs, bet gan tā noteikta garuma jaucēj kods, kam ir jābūt unikālam atkarībā no tā, kāds ir parakstāmais saturs. [171]

Šī darba rakstīšanas laikā pasaulē elektronisko parakstu veidošanā dominē jaucējfunkcijas *SHA-1* un *SHA-2*, kas aprakstītas *FIPS 180-2* standartā. [171,162] Abas šīs jaucējfunkcijas ir veidotas saskaņā ar *Merkle-Damgard* konstruktū.

Pasaules kriptanalīzei attīstoties esošajos risinājumos tiek atklāts ar vien vairāk risku un ievainojamību. Viena no galvenajām jaučējfunkciju un jaučējkodu prasībām ir tāda, lai nebūtu iespējamās kolīzijas. Tas nozīmē, lai nebūtu iespējams radīt divus identiskus jaučējkodus diviem dažādiem tekstiem. Darba rakstīšanas brīdī ir jau atklātas jaučējkodu kolīzijas *MD4*, *MD5*, *SHA-0* jaučējfunkcijām.[171] Ir izstrādātas metodes, kas pierāda *SHA-1* kolīziju iespējamību, bet faktiski tas vēl nav uzskatāmi parādīts. [152,171] Attiecībā uz *SHA-2* praktiskas ievainojamības vēl nav atklātas, bet nav izslēgts, ka tuvāko gadu vai gadu desmitu laikā veiksmīgas kriptanalīzes laikā netiek veikts veiksmīgs uzbrukums arī pret šo jaučējfunkciju. [152,171] Ja tā notiek un tiek kompromitēta *SHA-2* jaučējfunkciju saime, tad sekas elektroniskajiem parakstiem var būt graujošas. [152,171,172] Jau ir publicēti daži pētījumi par kolīziju iespējamību *SHA-2* jaučējfunkcijas risinājumos.[172] Tāpēc Amerikas Savienoto Valstu Nacionālais Standartu un Tehnoloģiju institūts 2007. gadā izziņoja publisku konkursu *SHA-3* jaučējfunkcijas radīšanai, kur viens no nosacījumiem ir tāds, lai tā tiktu radīta pēc atšķirīgiem principiem tā, lai veiksmīgs uzbrukums *SHA-2* jaučējfunkcijas saimei neradītu draudus *SHA-3* saimei. [185,171,173]

2012. gadā par konkursa uzvarētāju tika paziņots *Keccak* jaučējfunkcijas algoritms. [186] Viens no izvēlētajiem risinājumiem, kā pēc iespējas samazināt jaunā algoritma potenciālo ievainojamību un risku skaitu un garantēt lielāku tā drošību un ilgtermiņa stabilitāti, bija nodot visu konkursa dalībnieku iesniegtos risinājumus publiskai apspriedei, nenosakot konkursam beigu termiņu. [186] Tika meklēts un diskutēts par katru no risinājumiem līdz tika panākts valsts līmeņa speciālistu un publikas atzinums par labu konkursa uzvarētājam. [186] Bet arī šajā risinājumā pastāv risks, ka kāds no publiskās apspriedes dalībniekiem ir vienīgais ievērojis būtisku risku, bet ar nolūku par to klusē.

Šī darba rakstīšanas laikā Latvijā ieviestā elektroniskā paraksta nodrošināšanai vēl tiek izmantota *SHA-1* jaučējfunkcija, bet uzticams sertifikācijas pakalpojumu sniedzējs VAS „Latvijas Valsts radio un televīzijas centrs” gatavojas savu tehnoloģisko risinājumu pārbūvēt, lai tiktu izmantota *SHA-2* jaučējfunkcija, tādā veidā padarot pakalpojumu drošāku un uzticamāku. [16,45] Ar to arī tiek realizēts viens no Eiropas Savienības direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu pamata mērķiem veicināt tehnoloģisko attīstību.[11]

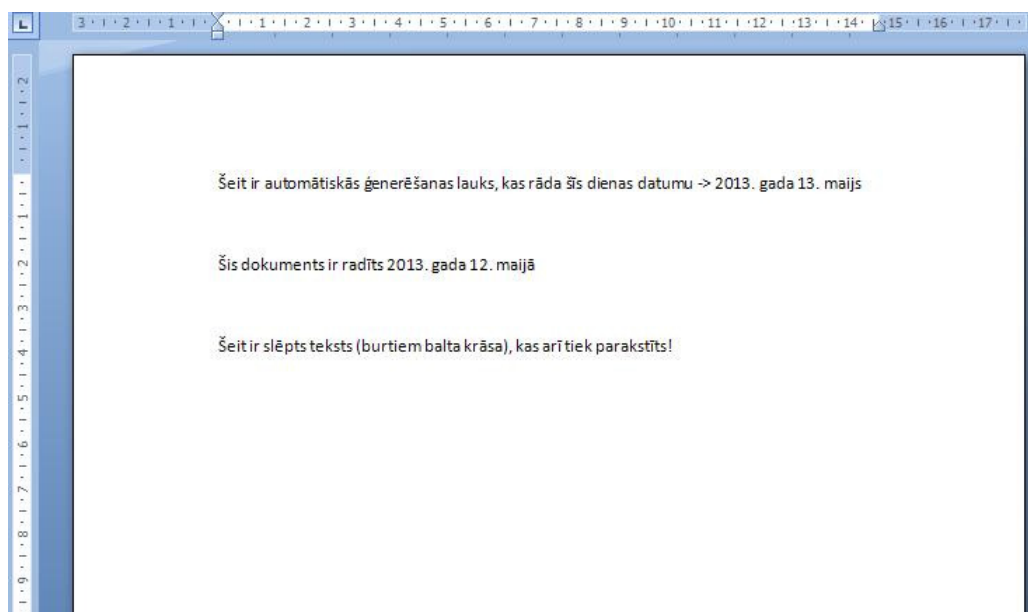
Jaučējfunkcijas maiņai uz jaunāku ir risks, ka jaunajai risinājuma arhitektūrai rodas nesavietojamības ar esošiem risinājumiem, piemēram, *SHA-2* sertifikāta ķēdes pārbaudi. [45] Darba autors uzskata, ka šis risks ir likumsakarīgs un nevar būt par pamatu, lai paliktu pie *SHA-1* jaučējkodu izmantošanas. Pakalpojuma tehnoloģiju attīstība ir noteikta iepriekš minētajā Eiropas Savienības direktīvā, tāpēc viens no šī riska risinājumiem ir veikt

pakalpojuma tehnoloģijas modernizēšanu pēc iespējas uzmanīgāk, laicīgi informējot iesaistītās puses un sagatavojot savietojamības risinājumus, ja tādi nepieciešami.[11]

4.7.3 ELEKTRONISKI DOKUMENTI AR MAINĪGU UN/VAI SLĒPTU SATURU

Parakstot fizisku dokumentu ar parastu parakstu, ir iespējams to paņemt rokā, aplūkot no visām pusēm, aptaustīt un redzēt pilnībā, kas tieši tiek parakstīts. Var droši teikt, ka cilvēks paraksta to, ko viņš redz. Ar elektroniskajiem dokumentiem ir pavisam savādāk, jo pašā pamatā elektronisks dokuments ir mašīnkoda dati, kas cilvēkam nav izlasāmi. Tāpēc ir radītas dažādas lietojumprogrammas, kas atspoguļo šos datus cilvēkam lasāmā un saprotamā formātā.

Parakstot elektronisko dokumentu ar elektronisko parakstu, cilvēkam tiek radīts iespaids, ka viņš paraksta tieši to, ko viņš redz. Elektroniskā vidē to garantēt ir sarežģīti. Var rasties neskaidras situācijas, ja elektroniskajā dokumentā tiek iekļauts mainīgs saturs. [45] Ja, piemēram, dokuments tiek veidots lietojumprogrammā Microsoft Word, minētie dati tiek veidoti cilvēkam lasāmā formā, kas rada iespaidu, ka viņš strādā papīra dokumentu. [45] Šajā gadījumā tas, ko cilvēks domā, ka viņš paraksta ir redzam attēlā 4.17



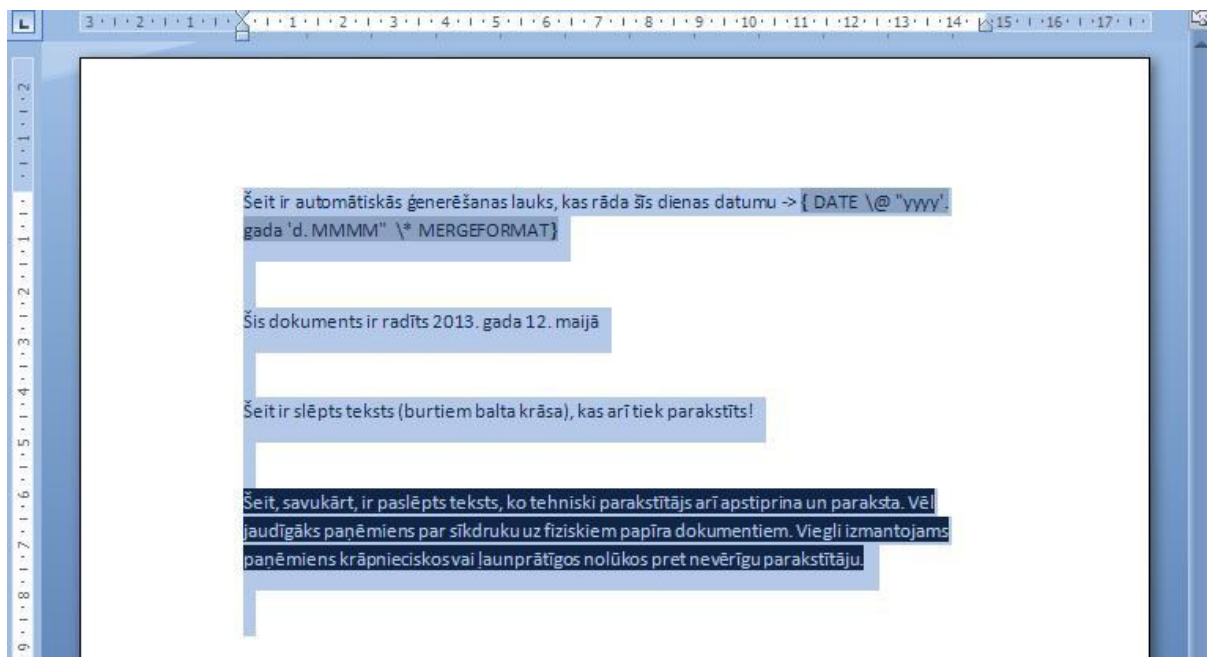
4.17 att. Parakstāma dokumenta piemērs

Lietojumprogrammās un elektroniskā vidē, lietojot elektronisko parakstu, ir jābūt ļoti uzmanīgam, jo ne viss, ko cilvēks redz ir viss patiesais dokumenta saturs. Ja uz papīra dokumenta viss tur ierakstītais fiziski ir statisks un nemaināms, elektroniskā vidē ir iespējams veidot elektroniskus dokumentus ar mainīgu saturu. Piemēram, lietojumprogrammā *Microsoft Word* ir iespēja veidot speciālus laukus, kas rāda konkrētās dienas datumu, kad tas tiek

atvērts. Ir iespējams arī veidot tādus laukus, kas veic aprēķinus vai loģiskus secinājumus no kādiem ieejas datiem.

Veidojot elektroniskiem dokumentus ir viegli iekļaut tā tekstā tādas daļas, kas cilvēkam nav redzamas. Piemēram, var uzrakstīt līguma dokumentā tekstu un to iekrāsot baltā krāsā. Tehniski šī informācija dokumentā ir un, ja tiek uzlikts elektroniskais paraksts, tad šī informācija tehniski arī tiek parakstīta.

Attēlā 4.17 redzamais dokuments, lai gan vizuāli nav redzams, satur gan tekstu iekrāsotu baltā krāsā, gan speciālu lauku, kas rāda to datumu, kas tā atvēršanas laikā ir iestatīts darbstacijai, uz kā tas tiek apstrādāts. Patiesā informācija, kas tiek parakstīta cilvēkam lasāmā formātā ir redzama attēlā 4.18



4.18 att. Patiesais saturs

Iezīmējot attēlā 4.17 redzamo tekstu, izveidotais datuma lauks iekrāsojas ar pelēku fonu. Nospiežot taustiņu kombināciju *Alt+F9*, tiek pārslēgts skata režīms, kas parāda lauku funkcijas, nevis šo funkciju atgrieztās vērtības. Tekstam ar balto burtu krāsu ir ietonēts melns fons, lai tas tiktu atklāts un cilvēkam viegli salasāms. Dokumentu manipulēšanas nolūkos burtu krāsas var veidot arī tādas, lai tie kļūtu redzamāki pie atšķirīga ekrāna kontrasta. Šajā dokumentā mainīgo saturu rada datuma lauks pirmajā rindā.

Ja šis dokuments tiek parakstīts 2013. gada 12. maijā ar elektronisko parakstu un laika zīmogu, viņš pirmajā rindā redzēs datumu, kas atbilst laika zīmoga uzlikšanas dienai. Ja šis parakstītais dokuments tiks atvērts tā paša gada 13. maijā, tad dokumentā jau rādīsies nevis datums „2013. gada 12. maijs”, bet „2013. gada 13. maijs”. Kad tiks veikta elektroniskā paraksta pārbaude, paraksts būs derīgs, jo tehniski dokuments mainīts nav. Tas ir tāpēc, ka, lai

gan parakstītājs domāja, ka viņš paraksta dokumentu, kur tekstā ir norādīts konkrēts datums, reāli viņš paraksta dokumentu, kam saturā ir iekļauta lietojumprogrammas funkcija, kā tas ir redzams attēlā 4.18. Dokumenta teksts tehniski mainīts netiek. Mainās tikai informācija, kas ir redzama lietotājam.

Dokumenti ar mainīgo saturu ir liels risks to parakstītājiem un nozīmē plašas iespējas tiem, kuri plāno veikt kaitnieciskas vai krāpnieciskas darbības. Piemēram, ļaundaris var iestrādāt dokumentā lauku un tajā ierakstīt funkciju, kas laika periodā līdz 2011.gada 1. janvārim rāda vienu teksta fragmentu, bet, ja dokuments tiek atvērts pēc šī datuma, tad tiek rādīts jau pavisam cits teksts. Darba autoram nav zināms neviens gadījums, kad dokumenta, piemēram, līguma vai tā teksta daļas ar mainīgu saturu likumiskums, atbilstība normatīvajiem aktiem vai tās saistību spēks tiktu vērtēta tiesā.

Šo risku par to, vai tas, ko lietotājs redz, ir tiešām tas, ko viņš paraksta, ir sarežģīti risināt. Viens ceļš ir mainīt likumdošanu, kur būtu nepieciešams paredzēt un noteikt kārtību kādā tiek izvērtēta elektronisko dokumentu leģitimitāte, ja tajos ir vizuāli vai mainīgs saturs (bilde, teksts, video u.c.). Piemēram, iekļaut likumā punktu, kas nosaka, ka parakstīts skaitās tas teksts, kas parakstīšanas brīdī ir bijis redzams vai attēlots. Tādā veidā, pārskatot iekļauto funkciju lauku formulas varētu noteikt, kurš teksta fragments parakstīšanas brīdī ir bijis redzams. Bet tas nerisinātu to, ka formulas var veidot atkarīgas ne tikai no datuma, bet arī no citiem datiem, piemēram, darbstacijas *IP* vai *MAC* adreses. Tādā gadījumā precīzi pateikt, kurš teksta fragments bijis redzams, būs ļoti sarežģīti vai pat neiespējami. Šādus gadījumus arī likumā var paredzēt, iekļaujot nosacījumu, ja nav iespējams noteikt mainīgo saturu, kas bija redzams dokumenta parakstīšanas brīdī tad, piemēram, dokuments tiek atzīts par neparakstītu vai neatbilstošu kādām elektroniski parakstāmu juridiski saistošu dokumentu izveidotām prasībām.

Cits variants ir risināt risku no tehnoloģiskās puses. Piemēram, izstrādāt speciālu elektronisko dokumentu formu, kas būtu jāizmanto, kad tiek sagatavots un elektroniski parakstīts līgums vai kāds cits juridisks dokuments, kur ir ļoti svarīgs tā tekstuālais saturs.

4.7.4 INFORMĀCIJAS PĀRTVERŠANA UN NOKLAUSĪŠANĀS

Elektroniskām iekārtām aktuāls ir sakaru izlūkošanas un pārtveršanas risks, kas ir viens no kiberuzbrukumu un informācijas drošības uzbrukumu veidiem. [1,2,3,140,177] Tā veikšanai parasti tiek izmantotas speciālas iekārtas vai metodes ar mērķi nolasīt informāciju, kas tiek izstarota vai pārraidīta. [1, 2,3,140,177] Šeit ietilpst gan elektromagnētiskā starojuma analīze,

gan nozarojuma ķēžu veidošana vados, mikroshēmās un citās elektroniskās sistēmās, kur tiek radīti vai pārraidīti dati un informācija. [1, 2,3,140,177]

Par sakaru izlūkošanas uzbrukuma mērķi var būt gan viedkartes, viedkaršu lasītāji, darbstacijas, šifrēšanas iekārtas, viedkaršu programmēšanas un personalizēšanas ierīces, datu pārraides vadi, datu ievades un izvades ierīces un viss cits, kas savas darbības veikšanai izmanto elektrisko strāvu. [1, 2,3,140,177] Viena no uzbrukuma pielietošanas jomām ir citādi nepieejamas informācijas iegūšana vai nolasīšana. [1, 2,3,140,177] Tas vistiešāk attiecas uz iekārtām, kas veic kriptogrāfiskas operācijas un datu šifrēšanu. [1, 2,3,140,177] Ja arī iegūto informāciju nav iespējams atšifrēt vai iegūt šifrēšanā izmantotās skaitliskās vērtībās, tad sakaru izlūkošanas uzbrukuma veicējs tik un tā var veikt šifrētā signāla plūsmas izpēti. [1,2,3,140,177] Tādā veidā, viņi var noskaidrot signāla avotu, adresātu, katras komunikācijas sesijas frekvenci un ilgumu, var iegūt izmantojamu informāciju, piemēram, komunikācijas veidu, iesaistītajām personām, un iespējamiem tās mērķiem. [1, 2,3,140,177]

Gan elektroniskajam parakstam, gan elektroniskās identifikācijas kartēm pastāv risks vismaz trīs sakaru izlūkošanas viedkaršu uzbrukuma veidiem: [1, 2,3,140,177]

1. fizisks uzbrukums, [1, 2,3,140,177]
2. vides uzbrukums, [1, 2,3,140,177]
3. programmatūras uzbrukums [1, 2,3,140,177]
4. blakuskanāla uzbrukums. [1, 2,3,140,177]

Fiziskie uzbrukumu viedkartēm un to sistēmām ir invazīvi. Piemēram, sakaru ķēdes izmaiņšana vai papildināšana ar speciālām zondēm, vai skaitļu ģenerēšanas elementiem vai papildus funkcijām, kas var ietekmēt viedkartes mikroshēmas darbību. [1, 2,3,140,177] Tādā veidā uzbrucējs var tieši iejaukties šifrēšanas procesos, kam sekas var būt arī iekodēto sertifikātu un parakstīšanas atslēgu nolasīšana un kompromitēšana. [1, 2,3,140,177] Tas uzbrucējam ļautu izmantot upura elektronisko parakstu tik ilgi, kamēr sertifikāta darbība netiks apturēta vai anulēta saskaņā ar sertifikācijas pakalpojumu sniedzēja procedūrām, kas aprakstītas tā sertifikācijas pakalpojumu sniegšanas noteikumos. [16,1, 2,3,140,177]

Fiziskie uzbrukumi viedkartēm mēdz būt iznīcinoši un laikietilpīgi. Ja, piemēram, uzbrucējs upurim viedkarti ir nozadzis vai nolaupījis, ir ļoti iespējams, ka upuris būs spējīgs par to paziņot sertifikācijas pakalpojumu sniedzējam pirms uzbrucējs būs spējīgs sekmīgi piekļūt viedkartē iestrādātajiem datiem un veikt ļaunprātīgas darbības ar upura elektronisko parakstu.[1, 2,3,140,177]

Vides uzbrukums nozīmē izmainīt ap karti esošo fizisko vidi tā, lai tās darbībā rastos dažādas kļūdas. To var panākt, piemēram, ar ultravioleto starojumu, temperatūras izmaiņām, apgaismojumu vai rentgena starojumu. Radot kļūdas un mikroshēmas nepareizu darbību,

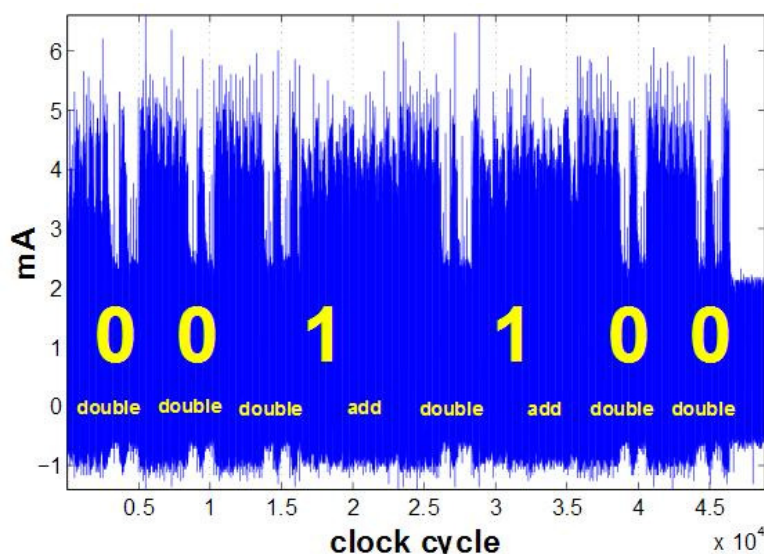
uzbrucējam var būt iespējams apiet kartes aizsardzības mehānismus vai iegūt papildus informāciju, kas var iekļaut arī tādu, kas ir slepena vai slēpta. [1, 2,3,140,177]

Blakus kanāla uzbrukums ir viens no upurim visnemanāmākajiem, jo ar tā palīdzību var tikt nolasīti izmantotās viedkartes dati tās lietotājam par to pat nezinot. Šis uzbrukums izmanto informāciju, ko rada iekārtas fiziskās īpašības brīdī, kad tiek izpildīti algoritmi. Tā veikšanai var izmantot gan laika skaitļošanas paņēmienus, gan enerģijas un starojuma mērījumus. [1, 2,3,140,177]

Ja kriptogrāfiskie algoritmi kartē ir iestrādāti pavirši, tad uz laika skaitļošanas paņemiens mēdz būt ļoti efektīvs. Ja algoritma izpildes laiks ir tieši atkarīgs no privātās atslēgas vērtības, tad no mazām atšķirībām datu apstrādes laikā prasmīgs uzbrucējs ir spējīgs izskaitļot viedkartes slēptos datus, kur ietilpst arī elektroniskā paraksta radīšanas līdzekļi. [140,177]

Līdzīgi var veiksmīgi izmantot arī informāciju par elektriskās iekārtas patērētās jaudām. Nolasot vai pārtverot šo informāciju un zinot izmantotos šifrēšanas algoritmus, uzbrucējam ir iespējams izsecināt un noteikt šifrēšanā izmantotos datus. Reizēm prasmīgam uzbrucējam pietiek tikai ar jaudas patēriņa laika līknes aplūkošanu, lai iegūtu sev nepieciešamo informāciju. [132,140,177]

Bez jaudas mērījumiem uzbrucējs var izmantot arī elektromagnētiskā starojuma analīzi. To ir grūtāk apstrādāt, jo mērījumos jāatfiltrē dažādu blakus starojumu troksnis. Lai veiksmīgi veiktu uzbrukumu viedkaršu darbībām, uzbrucējam ir jāpārzina izmantotie šifrēšanas algoritmi, lai iegūtos datus varētu precīzi interpretēt un nolasīt. [132,140,177,134] Attēlā 4.19 redzams mikroshēmas jaudas mērījumu analīze eliptisko līkņu šifrēšanas algoritma darbības laikā. [132,140,177,134]



4.19 att. Mikroshēmas izstarotās jaudas analīze eliptisko līkņu algoritmam [134]

Blakus kanāla uzbrukumi ir aktuāls risks ne tikai viedkartēm, bet tie var tikt vērsti pret jebkuru elektronisku iekārtu. [132,140,177,134] Tā, piemēram, 2004. gadā tika prezentēts pētījums „Plakanā ekrāna monitoru elektromagnētiskā starojumpārtveršanas riski” par veidiem, kā nolasīt iekārtas ekrāna darbības starojumu, iegūstot tā attēlu uz citas iekārtas, pašam uzbrucējam atrodoties pat vairāku metru attālumā no avota iekārtas.[159]

No aplūkotajiem sakaru izlūkošanas uzbrukumiem Latvijā ieviestajam elektroniskajam parakstam, pēc darba autora domām, vislielāko risku sagādā tieši elektromagnētiskā starojuma analīze un datu ievades nolasīšana. Tā piemēram, bibliotēkā publiskās pieejas datoram ir uzstādīts viedkaršu lasītājs, lai tās apmeklētāji varētu izmantot sertifikācijas pakalpojumus. Tajā pašā laikā blakus telpā vai uz ielas automašīnā sēž uzbrucējs ar speciālu ekipējumu un starojuma uztveršanas antenām, kas vērstas tieši pret konkrēto datoru. Ja viedkartei, tās lasītājam un datoram nav iestrādātas speciālas signāla starojuma bloķēšanas vai kropļošanas tehnoloģijas, tad prasmīgs uzbrucējs var veiksmīgi nolasīt un apstrādāt sertifikācijas pakalpojumos izmantoto iekārtu starojumu un iegūt sensitīvu informāciju. Cits scenārijs, ja starojuma nolasīšanas iekārtas tiek novietotas valsts Ministru kabineta telpās vai netālu no tām. Tādā gadījumā, ja valsts mēroga amata ieņēmēji izmanto parastas iekārtas, tad informācijas kompromitēšanas risks veiksmīgu uzbrukumu gadījumā ir ļoti liels.[159, 132,140,177,134]

Iespējamie tehnoloģiskie pretpasākumi sakaru izlūkošanas un uz viedkartēm tēmētiem uzbrukumiem ir viedkaršu un to lasītāju mikroshēmām iestrādāt papildus metāla apvalku un režģi, samazināt tranzistoru izmēru mikroshēmās. Tādā veidā var samazināt un kropļojot raidīto starojumu. Jaudīgs pretpasākums ir izmantotajos šifrēšanas algoritmos un procesos iekļaut nejaušus laika kavējumus vai iestrādāt mikroshēmām atšķirīga un nejauši izvēlēta ilguma skaitļošanas taktis. Tādā veidā, ja arī uzbrucējam būs izdevies starojumu veiksmīgi pārtvert, viņam nebūs iespējams informāciju pareizi interpretēt un nolasīt. [159, 132,140,177,134]

Pēc autora domām, ļoti svarīgs aizsardzības punkts ir tieši viedkaršu ražošanas un personalizācijas centri, kā arī pats sertifikācijas pakalpojumu datu centrs. Šajās vietās, gan statnēm, gan telpām jābūt starojuma necaurīdīgām un arī pašas iekārtas, datori, serveri un iekārtas, kas veic sensitīvo datu pārraidi vai apstrādi būtu jānodrošina ar aizsardzības mehānismiem, lai to darbības laikā raidīto starojumu nebūtu iespējams uztvert vai nolasīt pat atrodoties blakus telpā vai pašas iekārtas tuvumā. Piemēram, personalizācijas centra datoriem būtu jābūt specializētiem priekš to veicamajām darbībām, tiem būtu jāizmanto uzticama un

pārbaudīta operētājsistēma, kur par visu sistēmas procesu atbilstību visām drošības prasībām drošības amatpersona un speciālisti var pārliecināties.

Sakaru pārtveršanas un starojuma nolasīšanas risks kombinācijā ar iekšējo uzbrukumu veido ļoti lielu draudu. Tāpēc ir svarīgi, lai sertifikācijas pakalpojumu sniedzējs, veidojot infrastruktūru un drošības procedūras, būtu padomājis par visiem iespējamajiem riskiem gan savā pusē, gan klienta pusē (droši karšu lasītāji, drošas un augstas klases viedkartes).

4.7.5 CILVĒKU IZLŪKOŠANAS UN IEKŠĒJO UZBRUKUMU RISKI

Tāpat kā ir sastopami uzbrukumi no ārpuses, ir svarīgi padomāt arī par iekšējo uzbrukumu riskiem.

Iekšējs uzbrukums ir uzbrukums, ko ir veikusi persona no organizācijas iekšienes, kurai ir bijušas piekļuves tiesības tās iekšējiem resursiem un sistēmām, bet tās izmanto ne tādos veidos kā to ir paredzējis piekļuves tiesību piešķirējs. [1,2,167] Vēsturiski iekšējo uzbrukumu veicēji rada vislielākos draudus lielākai daļai kritisko informācijas sistēmu, jo tās ir pilnvarotas personas, kas veic nelegālas darbības ar nodomu bojāt vai nozagt kritiskus resursus. [1,2,130,201,49] Tie var būt darbinieki, kontrahenti, konsultanti, risinājumu, pakalpojumu piegādātāju darbinieki un atbalsta personāls. [1,2,130,201,49] Šī ir tā uzbrucēju grupa un uzbrukuma veids, pret ko ir visgrūtāk aizsargāties un sagatavoties. Šī uzbrucēju grupa var darboties savās interesēs, vai arī tie var būt ietekmēti vai pieaicināti no citām organizācijām, uzbrucēju grupām vai ārvalstu izlūkdienestiem. [1,2,130,201,49]

Iekšējo uzbrucēju motivācija var tikt saistīta ar personīgā labuma gūšanu, atriebību vai ideoloģiju. Šie uzbrucēji var būt noalgoti vai korumpēti tādā veidā, ka paveicot noziegumu, viņi tiek finansiāli stimulēti. [1,2,130,201,49] Citi var būt neapmierināti darbinieki, kas vēlas kaitēt organizācijai par kādu pāri darījumu. [1,2,130,201,49] Vai arī dažiem var būt ideoloģisku uzskatu atšķirības, kuri vēlas kaitēt organizācijas misijai vai mērķim. [1,2,130,201,49]

Papildus ļaunprātīgajiem uzbrucējiem ir arī tādi uzbrucēji, kas nav ar sliktu nodomu, bet tik un tā kaitējumu nodara. [1,2,130,201,49] Šādi uzbrukumi var būt iznākums dažādiem incidentiem, sev pieejamo resursu nepareiza izmantošana, nejauša kaitīga koda ievietošana no lejupielādēta faila u.c. [1,2,130,201,49]

Iekšējo uzbrukumu veicējiem nav nepieciešami īpaši resursi, rīki vai prasmes, lai nodarītu organizācijai kaitējumu. [1,2,130,201,49] Arī visnodalītākajās vidēs ir nepieciešama pietiekama apjoma uzticība darbiniekiem un personālam, lai tie varētu veikt savus darba pienākumus. [1,2,130,201,49] Iekšējie uzbrucēji parasti ir tādās pozīcijās vai lomās, lai apietu

visus drošības aspektus (konfidencialitāte, pieejamība, integritāte), un uzbrukums tiktu veikts tā, lai to būtu grūti asociēt ar pašu uzbrukuma veicēju. [1,2,130,201,49] Par vienu no bīstamākajiem iekšējiem uzbrucējiem tiek uzskatīts sistēmu administrators ar padziļinātām zināšanām par informācijas sistēmām un izmantotajiem drošības mehānismiem. [1,2,130,201,49] Lai gan potenciālais iekšējo uzbrucēju skaits ir ļoti mazs, nodarītā kaitējuma apjoms var būt ļoti liels. [1,2,130,201,49] Tā kā iekšējie uzbrucēji nevēlas tikt noķerti, viņi veiks nepieciešamās darbības, lai izvairītos no identificēšanas un atrašanas. [1,2,130,201,49] Dēļ sava uzticamā darbinieka statusa, šī veida uzbrucēji ir spējīgi paveikt kaitējumus, kas var tikt uzskatīti par pārāk riskantiem, lai tos veiktu kāds ārējs uzbrucējs. [1,2,130,201,49] Tas padara šos cilvēkus īpaši vērtīgus dažādu ārēju organizāciju acīs, piemēram, konkurentiem vai ārzemju izlūkdienestiem. [1,2,130,201,49]

Ne vienmēr iekšējā uzbrukuma iniciatīva nāk no organizācijas darbinieka, jo viņi ir pakļauti cilvēku izlūkošanas draudiem, kļūstot par vieniem no vājākajiem drošības ķēdes posmiem. [1,2,130,201,49] Šī disciplīna izmanto organizācijas darbinieku šantāžu, uzpirkšanu, izspiegošanu, piespiešanu, izspiešanu un sociālo inženieriju, lai panāktu no uzbrukuma upura vēlamu rezultātu. [1,2,130,201,49] Viens no aktuālākajiem riskiem mūsdienās ir kļuvis tieši sociālās inženierijas metožu izmantošanas aktualizēšanās. [1,2,130,201,49] Pie šīm metodēm pieder pikšķerēšana, baidatūra, inficētu e-pastu sūtīšana, speciālu situāciju radīšana, melošana vai citas manipulatīvas darbības ar mērķi panākt uzbrucējam vēlamu darbinieka rīcību vai reakciju. [1,2,130,201,49]

Kad šis darbs tika rakstīts, viens no jaunākajiem sociālās inženierijas uzbrukumiem, tika veikts neilgi pēc Bostonas sprādzieniem 2013. gada aprīlī. Ar izsūtīta un inficēta pikšķerēšanas e-pasta palīdzību tika iegūta autentifikācijas informācija *Associated Press* oficiālajam vietnes *Twitter* kontam. Tā rezultātā no iepriekš minētā konta tika izplatīta nepatiesa informācija par diviem sprādzieniem ASV Baltajā namā un tā laika prezidenta Baraka Obamas ciešanu tajos. Attēls 4.20 [126,195]



4.20 att. Uzbrukums *Associated Press* twitter kontam [126,195]

Tā kā šī darba rakstīšanas laikā Latvijā ir tikai viens uzticams sertifikācijas pakalpojumu sniedzējs VAS „Latvijas Valsts radio un televīzijas centrs” ar vidēji 252 darbiniekiem 2011. gadā (pēc pašu sniegtās informācijas), tad tas paver potenciāli 252 riska faktoros un potenciālus cilvēku izlūkošanas riskus, jo katram no visiem uzņēmuma darbiniekiem (ne tikai tiem, kas tieši strādā ar sertifikācijas pakalpojumu sniegšanu) ir piekļuve informācijai, ko uzbrucējs var izmantot. [123] Piemēram, visiem darbiniekiem ir piekļuve pārējo darbinieku kontaktinformācijai, vārdam, uzvārdam, amatam. To informāciju vien uzbrucējs var izmantot, lai uzzinātu nākošo uzbrukuma mērķi (darbinieku), kurš, piemēram, veiksmīga sociālā inženieringa gadījumā varēs sniegt viņam ļoti būtisku informāciju, piekļuvi vai pat neapzināti ļaut inficēt uzņēmuma datortīklu, tādā veidā iegūstot lielāku un tuvāku piekļuvi tieši sertifikācijas pakalpojumu sniegšanas procesiem vai pat sistēmām un sensitīviem datiem.

Datu valsts inspekcijas publiskotajā KPMG 2012. gada aprīlī veiktajā audita vērtējuma ziņojuma pirmajā lappusē (Pielikums 4) ir rakstīts: „(..) KPMG no 2. Marta līdz 24. Aprīlim veica LVRTC sertifikācijas pakalpojumu sniedzēja (turpmāk LVRTC SPS) CA auditu, kura laikā novērtēja LVRTC SPS izstrādātās procedūras, ieviestās kontroles, kā arī izstrādātās drošības prasības sertifikācijas pakalpojumu sniegšanai.”. No tā var secināt, ka auditā tika aplūkotas tikai tās VAS „Latvijas Valsts radio un televīzijas centrs” darbības funkcijas, kas ir saistītas ar sertifikācijas pakalpojumu sniegšanu. Tātad auditēta tika konkrēta struktūrvienība vai ierobežota darbinieku grupa, kas, tomēr, ir pakļauta sadarbībai un aktīvam kontaktam arī ar citiem VAS „Latvijas Valsts radio un televīzijas centrs” darbiniekiem. Tas pastiprina apzinātu vai neapzinātu iekšējo uzbrukumu vai sociālās inženierijas paņēmieni pielietošanas iespējamību. Piemēram, ja darbinieki, kas nodarbojas tieši ar sertifikācijas pakalpojumu sniegšanu iet ēst pusdienas kopā ar kolēģiem no citām uzņēmuma struktūrvienībām (vai pat departamentiem), tas jau paver plašākas iespējas ļaundariem, piemēram, ievērot patstāvīgās pusdienošanas vietas, sēsties netālu no uzņēmuma darbinieku kompānijas un noklausīties viņu sarunas, kas starp dažādu struktūrvienību darbiniekiem var būt vispārīgākas vai arī atklāt kādas detaļas, ko sociālie inženieri var veiksmīgi izmantot savās tālākajās darbībās.

Divdesmit pirmajā gadsimtā riskus rada uzņēmumu darbinieku aktivitāte sociālajos portālos un interneta vidē vispār. Uzbrukuma punkti ir gan personu interneta pārlūka vēsture, gan viņu aktivitātes sociālajos portālos. [1,2,130,201,49] Ar šo pieejamo informāciju prasmīgam cilvēku izlūkošanas uzbrukumu veicējam pietiek, lai, piemēram, izveidotu konkrētās personas psiholoģisko portretu, atrastu viņa īpašībās vājākos punktus, izstrādāt tieši upurim pielāgotus teikumus un jautājumus, ka uzbrukuma manipulācijai pretoties būtu praktiski neiespējami. [1,2,130,201,49] Upuris, iespējams, pats pēc tam brīnītos, kā viņš ir izpaudis tādu informāciju vai veicis konkrētu darbību. Potenciālos uzbrukuma mērķus bieži

vien ir iespējams viegli identificēt, aplūkojot personas, kas pārsūta vai veic atzīmi „man patīk” pakalpojuma sniedzēja vai darba devēja aktivitātēm. [1,2,130,201,49] Pastāv ļoti liela iespējamība, ka pirmie, kas ar šīm aktivitātēm sociālajos portālos mijiedarbosies, būs darbinieki, kas vēlas popularizēt sava darba devēja vai paša sasniegumus. Tāds piemērs ir redzams attēlā 4.21, kur Jānis Eiduks ir vienīgais, kurš ir konkrētu Satiksmes Ministrijas sīkziņu pāpublicējis saviem sekotājiem sociālajā portālā *Twitter*. [116]



4.12 att. Jāņa Eiduka pārsūtīta Satiksmes Ministrijas sīkziņa

Kā redzams attēlā 4.21 Satiksmes Ministrijas mājas lapas kontaktu sadaļā ir atrodams iestādes darbinieks Jānis Eiduks.



4.21. att. Jānis Eiduks Satiksmes Ministrijas publicēto kontaktu sarakstā

Nav izslēgts, ka līdzīgi savu identitāti gadās izpaust arī uzticama sertifikācijas pakalpojuma sniedzēja darbinieki, kam ir tieša vai netieša piekļuve sensitīvai sertifikācijas pakalpojumu informācijai. [1,2,130,201,49] Tādā veidā darbinieki mēdz neapzināti sevi atklāt uzbrucējiem. Viņi var konkrētās personas izlūkot ar mērķi izmantot vai ietekmēt kaitniecisku darbību veikšanas nolūkos. [1,2,130,201,49]

Riska novēršana vai tā iespējamības samazināšana veidi:

- **Darbinieku izglītošana** [153,166,49,48] - Viens no svarīgākajiem veidiem, kā izsargāties no apzinātiem vai neapzinātiem iekšējiem uzbrukumiem, ir darbinieku izglītošana par datu, informācijas, paroli un to glabāšanas drošības

jautājumiem. Viņus nepieciešams izglītēt arī par aktuālākajiem drošības riskiem saistībā ar sociālo inženieriju, pikšķerēšanu, baidatūru, citiem pasaulē bieži izmantotiem uzbrukumu paņēmieniem un to, kādas sekas var rasties uzņēmumam un pašam darbiniekam, ja kāda no datu vai informācijas drošības prasībām netiek ievērota.

- **Biometrijas izmantošana fiziskas personas identifikācijai.** [153] Tas nozīmē, ka cilvēks tiek atpazīts nevis pēc tā, kas viņam pieder (piemēram, viedkarte, magnētiskais mikroshēma u.c.), bet viņa unikālām raksturīgām pazīmēm, piemēram, seja, acs varavīksne, pirkstu nospiedums.[47,83] Tehnoloģijām attīstoties biometrijas nolasīšanas ierīces kļūst arvien lētākas un pieejamākas. Ar šāda veida tehnikas izmantošanu tiek izslēgts risks, ka darbinieks aizdod vai iedod savu piekļuves viedkarti citam kolēģim vai cilvēkam no malas. Bet netiek izslēgts risks par to, ka persona ar konkrēto piekļuvi var ielaist arī citus cilvēkus.
- **Pārraudzīšana (monitorings)** [153] – Nepieciešams veikt uzņēmuma svarīgas informācijas un datu, sistēmu darbības, darbinieku piekļuvju (gan fiziskiem, gan elektroniskiem objektiem) pārraudzīšanu. Ir svarīgi, lai par drošību atbildīgajam personālam būtu pieejama pilna informācija par sistēmas darbības datiem (kad, cikos, kurš darbinieks konkrētajam resursam ir slēdzies klāt, kurš ar kādu failu ir veicis kādas darbības utml.), piemēram, tādā veidā viegli pamanot vai laicīgi paredzot kādus konkrētus riskus vai topošus incidentus. Tā var arī redzēt, vai kādam darbiniekam ir iedotas pārāk lielas piekļuves tiesībās nekā viņam pienāktos. Ja ir pieejama pilna informācija, tad ir vieglāk gan atsekot, gan paredzēt iespējamus draudus un uz tiem laicīgi iedarboties.
- **Atrunātas un skaidras darbinieku atbildības** – Darba līgumos, instrukcijās un amatu aprakstos ir nepieciešams skaidri atrunāt katra konkrētās atbildības, ieņemamās lomas un darbības sfēras, kas jāpārtrauga. Tādā veidā tiek samazināts pārpratumu un bezatbildības risks, kā arī incidenta gadījumā ir skaidri zināms cilvēks, kurš par to ir atbildīgs un no kura ir jāprasa gan paskaidrojumi, gan ierosinājumi tā atkārtošanās novēršanai.
- **Konfidencialitātes līgums** – Ir nepieciešams slēgt ar darbinieku konfidencialitātes līgumu, kur būtu atrunātas tās lietas, kas tiek uzskatītas par komercnoslēpumu un neizpaužamu informāciju. Līgumā arī jābūt atrunātām darbinieku atbildībām, informācijas neizpaušanas ilgumam, prasībām pret informācijas glabāšanu un lietošanu, izņēmuma esamībām. Tas ir svarīgi, lai darbiniekiem būtu skaidri noteikumi un izpratne par atbilstošu apiešanos ar

saņemto un viņiem uzticēto informāciju, iespējamiem sodiem un sankcijām noteikumu neievērošanas gadījumā. Šāda līguma esamība nodrošina arī to, ka darbinieki kļūst uzmanīgāki saņemtās informācijas izmantošanā un tās glabāšanā. [51]

- **Drošības politikas** [166] – Katrā uzņēmumā nepieciešams izstrādāt datu drošības un privātuma aizsardzības politiku un ar to iepazīstināt visus darbiniekus. Šajā dokumentā būtu redzamas uzņēmuma drošības prioritātes, atrunātas procedūras, kontroles, prasības pret datu uzglabāšanu, lietošanu, incidentu novēršanu, reakciju uz tiem un aizsardzību no riskiem. Augstas drošības pakalpojumos, lai samazinātu darbinieku izlūkošanas iespējas, būtu noderīgi ierobežot vai reglamentēt viņu darbības sociālajos portālos. Piemēram, vai nu tādus nelietot vispār, ja lietot, tad tā, lai viņu darbības būtu redzamas tikai tiem cilvēkiem, kuriem viņi uzticas. Tas vajadzīgs, lai uzbrucējiem nebūtu plaši pieejama informācija par darbinieka aktivitātēm, lai nebūtu iespējams uzbrucējam izveidot viņa psiholoģisko portretu, tādā veidā atklājot konkrēta darbinieka lielākās vājības un ievainojamākās lietas. Svarīgi, lai darbinieku interneta pārlūkošanas vēsturi nebūtu iespējams iegūt trešajām personām. Šo informāciju uzbrucēji arī var izmantot, lai veidotu sekmīgus cilvēku izlūkošanas uzbrukumus.
- **Psiholoģisko risku novērtēšana** [130] – nepieciešams periodiski veikt darbinieku aptaujas un testus, lai pārbaudītu viņu psiholoģisko noturību, manipulējamību, pārlieku lielu uzticību un citas rakstura un psiholoģiskās īpašības, kas var padarīt konkrēto darbinieku par ietekmējamāku upuri uzbrucēja acīs. No šo aptauju rezultātiem būtu redzams, ar kuriem darbiniekiem nepieciešams veikt pārrunas vai sūtīt uz speciālām apmācībām, lai iespējamais riska faktorus konkrētajā darbiniekā pēc iespējas novērstu un padarītu viņu par stingrāku drošības ķēdes posmu. [130] Psiholoģisko risku novērtēšanai būtu jānotiek atsevišķā telpā. Visas personu aptaujas, testi, intervijas tiktu veiktas tikai šajā vienā telpā un obligāti novērtēšanas veicēja klātbūtnē. Katras dienas beigās visi iegūtie materiāli (testi, interviju pieraksti, anketas u.c.) būtu jāapstrādā, rezultāti jāsadokumentē un izmantotie materiāli neatgriezeniski jāiznīcina tās pašas dienas beigās. Nedrīkst pieļaut šo analīzes ieejas datu nonākšanu trešajām personām. Piemēram, ja kaut viena darbinieka aizpildīta psiholoģisko risku novērtēšanas anketa nonāk uzbrucēja rokās, tad viņš var iegūt pietiekošu informāciju, lai izstrādātu speciālu un pielāgotu uzbrukumu konkrētajai personai tādā līmenī, lai uzbrukuma izdošanās iespējamība būtu pēc iespējas lielāka.

Obligātai jābūt arī prasībai, lai ar psiholoģisko risku analīzes un novērtēšanas veicējs pats būtu uzticams un drošs.

- **Drošu iekārtu lietošana** – Datu un informācijas drošībā ir divi lielākie riski: iekārta un iekārtas operators(fiziska persona). Viens no veidiem, kā aizsargāties pret iekšējiem uzbrukumiem ir tieši drošu un speciālu aizsardzības iekārtu lietošana. Piemēram, iekšējais uzbrucējs ir kāds no darbiniekiem, kas nodarbojas ar viedkaršu personalizāciju. Šādā gadījumā iekšējo uzbrukumu ir iespējams veikt, pārējiem klāt esošajiem darbiniekiem to nemanot, paņemot līdzi kabatā jaunākās paaudzes elektroniskā starojuma nolasītāju vai kādu citu speciālu sakaru izlūkošanas tehniku. Tādā gadījumā datu noplūdes riskus var novērst, ievievojot skaitļošanas tehniku speciālos tiem paredzētos drošības seifos, kas ir ekranēti. [132,140,177,134] Kā arī pārējai ievades un izvades teknikai arī būtu jābūt drošai pret sakaru izlūkošanas tehniku. [132,140,177,134] Tāpat arī jābūt drošībā un aizsargātiem personalizācijas centrā esošajiem datu nesējiem un operatīvajām atmiņām. Ja gadījumā tajos glabājas kāda sensitīva informācija vai var atrast tās fragmentus, tad tādām iekārtām nepieciešami datu nozagšanas iespējamības novēršanas līdzekļi. [132,140,177,134] Piemēram, ja kāds uzbrucējs cenšas nesankcionēti atvērt skaitļošanas mašīnas korpusu, tad tā iekšpusē izplūst skābe, kas sabojā tās mikroshēmas, datu nesējas un padara to nefunkcionālu un ar neatgriezeniski dzēstiem jeb sabojātiem datiem. Līdzīgi kā drošības naudas maisiņos un koferos nesankcionētas piekļuves gadījumā izdalās tinte, kas padara naudu iezīmētu un praktiski nelietojamu.

Darba autors uzskata, ka ļoti būtiski ir veikt pilnu drošības un procesu auditu ne tikai uzņēmuma struktūrvienībai un procesiem, kas ir saistīti ar sertifikācijas pakalpojumu sniegšanu, bet gan visa uzņēmuma drošības politikām, to kvalitātei, nodrošināšanas procedūrām un darbības procesiem kopumā. Auditā noteikti būtu jāapskata tās procedūras un kontroles, kas attiecas uz darbinieku maiņām, darba tiesisko attiecību izbeigšanu, uzņēmuma lietoto paroļu maiņas un drošības politikām. Tādā veidā pakalpojuma ņēmējiem būtu lielāka pārliecība, ka arī blakus riski ir vērtēti un pārbaudīti.

4.7.6 LIKUMDOŠANAS RISKI

Latvijas Elektronisko dokumentu likums ir izveidots tā, ka ir iespējami vairāki riski saistībā ar dažiem no tā pantiem un punktiem. [14] Lai gan Latvijas Elektronisko dokumentu

likums ir jau vairākas reizes grozīts, vairāku risku iespējamība vēl nav izslēgta. [14] Likuma darbība un praktiskā funkcionalitāte tiesas prāvās vēl nav pārbaudīta, jo, no darba autoram pieejamās informācijas, nav bijušu attiecīgu incidentu un precedentu. Pēc darba autora domām, pēc tiesas prāvām, kas būtu saistītas ar Latvijas Elektronisko dokumentu likumu, radīsies nepieciešamība papildus likuma grozījumiem vai precizējumiem. Veicot salīdzinājumu ar Igaunijas Digitālā paraksta likumu, tika secināts, ka daži no šiem riskiem ir Igaunijas saistošajā likumdošanā nav aktuāli un ir novērsti.

4.7.6.1 DOKUMENTA PARAKSTĪTĀJA ATBILDĪBAS

Latvijas Elektronisko dokumentu likumā atšķirībā no Igaunijas Digitālā paraksta likuma nav atrunāts punkts, kas noteiktu iespēju elektroniskajam parakstam zaudēt savu likumisko spēku. [14,43] Tātad pat, ja ir pierādāms, ka sertifikāta īpašnieka paraksts ir uzlikts bez viņa ziņas, un nav iespējams pierādīt, ka šāds incidents ir radies viņa rupjas nolaidības dēļ, uzliktajam parakstam ir pilns juridiskais spēks kā ar roku veidotam parakstam. Tas nozīmē, ka Latvijā pat, ja sertifikāta turētājs labi rūpējas par savu datu un parakstīšanas rīku drošību un aizsardzību, viņš ir ļoti neaizsargāts. Piemēram, pret viņu vērš augstas klases sakaru izlūkošanas vai kāda cita veida uzbrukumu, pret ko civiliedzīvotājam būtu sarežģīti aizsargāties. Šī uzbrukuma rezultātā tiek radīts paraksts, ko nav veidojis pats sertifikāta turētājs. Šādā gadījumā uzbrukuma upurim ir jāuzņemas pilna atbildība par to informāciju, kas ir parakstīta ar viņam izsniegtu elektronisko parakstu. [14,43]

Šāda regulēja neesamība rada lielus riskus, ja elektroniskais paraksts tiek izmantots, lai autentificētos bankā. Šī darba rakstīšanas laikā interneta bankā autentificēties var tikai ar lietotāja identifikatora, paroles un speciāla koda ievadīšanu. Drošu elektronisko parakstu, lai autentificētos bankā izmantot, nav iespējams. Pašreizējā situācijā, ja, piemēram, tiek veikts nesankcionēts naudas pārskaitījums tad bankas konta īpašniekam ir iespēja, sazinoties ar banku, veikto naudas pārskaitījuma transakciju atcelt. Ja nesankcionēta naudas pārskaitījuma transakcijas apstiprināšanai tiek lietots elektroniskais paraksts, saskaņā ar Latvijas Republikas Elektronisko dokumentu likuma regulējumu, bankas konta un elektroniskā paraksta īpašniekam ir jāuzņemas pilna atbildība par parakstītajiem datiem. Tas nozīmē, ka bankas transakcijas atcelšana kļūst neiespējama, jo tiek lietots elektroniskais paraksts. Tādā veidā droša elektroniskā paraksta lietotājiem varētu rasties lieli zaudējumi. [14]

Ne Latvijā, ne Igaunijā, pēc darba autoram pieejamās informācijas, šo likuma punktu viennozīmīgums un darbības spēks, un efektivitāte nav pārbaudīta tiesā. [14,43,45]

Risinājums šim riskam būtu veikts Latvijas Republikas Elektronisko dokumentu likumā tādus grozījumus, kas paredzētu līdzīgu parakstītāja atbildību pret elektroniski parakstīto informāciju kā tas tiek noteikts Igaunijas Digitālā paraksta likumā, kur to regulē 3. panta 3. punkts. [14,43,45]

4.7.6.2 SERTIFIKĀTA ANULĒŠANAS VAI TĀ DARBĪBAS PAGaidu APTURĒŠANAS RISKI

Latvijas Elektronisko dokumentu likums nosaka speciālu kārtību un atbildības, kas ir jāievēro, ja ir nepieciešams sertifikātu slēgt vai uz noteiktu vai nenoteiktu laiku apturēt tā darbību.[14] Likuma 25. panta pirmās daļas 5. punkts nosaka parakstītāja pienākumu: *”nekavējoties pieprasīt, lai uzticams sertifikācijas pakalpojumu sniedzējs anulē kvalificētu sertifikātu vai aptur tā darbību, ja ir pamats uzskatīt, ka elektroniskā paraksta radīšanas dati izmantoti bez parakstītāja ziņas”*. [14]

Šajā nodaļā aplūkots risks balstās uz to, ka ne likumā, ne uzticama sertifikācijas pakalpojuma sniedzēja sertifikācijas pakalpojumu sniegšanas noteikumos nav atrunāts, kad tieši skaitās tas brīdis, kad sertifikāta darbība tiek apturēta. [14,16]

Uzticamam sertifikācijas pakalpojumu sniedzējam ir atsevišķa procedūra sertifikāta darbības apturēšanai (Sertifikācijas pakalpojumu sniegšanas noteikumu 3.9.2.2 nodaļa) un anulēšanai (Sertifikācijas pakalpojumu sniegšanas noteikumu 3.10.2. nodaļa), kas sastāv no vairākiem soļiem atkarībā no veida, kā sertifikāta apturēšana vai anulēšana tiek veikta. Saskaņā ar Sertifikācijas pakalpojumu sniegšanas noteikumu 3.9. un 3.10. nodaļām, virtuālā elektroniskā paraksta sertifikātus, kas tiek izmantoti interneta portālā *www.eparaksts.lv* nevar apturēt, tos var tikai anulēt. [14,16]

Sertifikāta darbību var apturēt divos veidos: [16]

1. Klientu apkalpošanas servisā, [16]
2. Palīdzības dienestā telefoniski. [16]

Pirmajā veidā apturēšanas procedūra sastāv no astoņiem punktiem, kas nosaka šādas darbības: pieprasījuma iesniegšana, pieprasījuma pārbaude, pieprasošās personas identificēšana, tās pilnvarotības pārbaude un autentificēšana, operatora autentificēšana, pieprasījuma apstrāde, apturēšanas amatpersonas autentifikācija, amatpersonas apstiprinājuma uzlikšana, parakstītāja informēšana. Līdz sertifikāta apturēšanai informācijas sistēmā veicamas septiņas secīgas darbības. [14,16]

Otrajā veidā procedūra ir īsāka un veicama telefoniski. [14,16] Tā sastāv no šādām darbībām: pieprasījuma izteikšana, slepenā jautājuma uzdošana pieprasītājam, atbildes sniegšana, sertifikāta apturēšana. Līdz sertifikāta apturēšanai informācijas sistēmā veicamas četras secīgas darbības. [14,16]

Sertifikācijas pakalpojumu sniegšanas noteikumu 3.9.2.3. apakšpunkts norāda, ka abos pieprasījuma veikšanas veidos patērētais laiks no apturēšanas pieprasījuma veikšanas līdz sertifikāta funkcionālai apturēšanai var ilgt līdz divdesmit četrām stundām jeb vienas pilnas dienas. [14,16] To pašu noteikumu 3.9.3.4. apakšpunktā norāda, ka laiks, uz kuru tiek apturēts sertifikāts, netiek ierobežots. [14,16]

Lai sertifikātu atjaunotu, nepieciešams iesniegt pieprasījumu rakstiskā veidā (Sertifikācijas pakalpojumu sniegšanas noteikumu 3.9.2.5 apakšpunkts) un tā izpilde var aizņemt vismaz deviņdesmit sešas stundas (Sertifikācijas pakalpojumu sniegšanas noteikumu 3.9.2.6 apakšpunkts). [14,16]

Sertifikāta darbības anulēšanas procedūras ir aprakstītas Sertifikācijas pakalpojumu sniegšanas noteikumu 3.10.2. un 3.10.2.1. apakšpunktos. [14,16] Pirmais apraksta darbību secību, kas jāpilda vispārīga anulēšanas pieprasījuma saņemšanai (piemēram, tas saņemts tiesas lēmuma formā). [14,16] Procedūra sastāv no šādām darbībām, ko izpilda drošības amatpersona: pieprasījuma saņemšana, pieprasījuma pārbaude, pieprasītāja pārbaude, drošības amatpersonas autentifikācija, sertifikāta anulēšana, pieprasītāja informēšana. [14,16] Līdz sertifikāta apturēšanai informācijas sistēmā veicamas piecas secīgas darbības. [14,16]

Otrs apakšpunkts precizē sertifikāta anulēšanas procedūru, ja to uzsāk pats lietotājs. Tā sastāv šādām darbībām: pieprasījuma iesniegšana, pieprasījuma pārbaude, pieprasītāja pārbaude, anulēšanas operatora autentificēšana, anulēšanas veikšana, drošības amatpersonas autentificēšana, anulēšanas apstiprināšana, pieprasītāja informēšana. [14,16] Līdz sertifikāta apturēšanai informācijas sistēmā veicamas septiņas secīgas darbības. [14,16]

Tātad saskaņā ar šī darba rakstīšanas laikā spēkā esošajām procedūrām, sertifikāta apturēšana vai anulēšanai nepieciešama ne vairāk kā viena diena kopš pieprasījuma izteikšanas, ne mazāk kā četras un ne vairāk kā septiņas secīgas darbības viena pieprasījuma veikšanas gadījumā. [14,16] Piemēram, rodas situācija – ar dažādu sakaru un vai cilvēku izlūkošanas metožu izmantošanu, ļaundari ir nelegāli ieguvuši lietotāja(upura) elektroniskā paraksta viedkartes *PIN* kodu. [14,16] Viņi sagūsta savu upuri, nolaupa viņam viedkarti, iekāpj automašīnā un aizbrauc. [14,16] Ļoti iespējams, ka, jau ceļā esot, viņi sāk izmantot jauniegūto sertifikātu elektronisko parakstu radīšanai un izmantošanai savu vai citu ieinteresēto pušu labā. [14,16] Tikmēr upuris steidzas zvanīt uz sertifikācijas pakalpojumu sniedzēja palīdzības dienestu, lai apturētu sava sertifikāta darbību. [14,16] Šajā gadījumā tam

ir nepieciešamas četras darbības. [14,16] Labākajā scenārijā upuris atbildi uz savu drošības jautājumu atceras, un iespējamais šoka stāvoklis netraucē viņam to nosaukt precīzi. [14,16] Tā rezultātā, viņam veicot četras secīgas darbības, sertifikāts ir veiksmīgi apturēts informācijas sistēmā un ļaundari sekmīgus parakstus radīt vairs nevarēs. [14,16] Piemēram, pa to laiku, kad tika veiktas noteiktās četras darbības sertifikāta darbības apturēšanai, ļaundari ir veiksmīgi paspējuši parakstīt vienu dokumentu. Risks slēpjas tajā gadījumā, ja jautājums par dokumenta paraksta derīgumu tiks pacelts Latvijas republikas tiesā. Pēc upura domām, sertifikātam būtu jāskaitās apturētam nevis tajā brīdī, kad ir veiktas attiecīgās darbības informācijas sistēmā, kas var ilgt līdz divdesmit četrām stundām, bet tajā brīdī, kad viņš ir ziņojis sertifikācijas pakalpojumu sniedzējam par konkrēto incidentu un izteicis pieprasījumu, ja tas ir pēc tam apstiprināts un izpildīts. Elektroniskais paraksts ir uzlikts laikā starp pieprasījuma veikšanu un attiecīgo izmaiņu informācijas sistēmā izpildi. Šis elektroniskais paraksts tiesā tiks uzskatīts par derīgu vai nē? Šī darba autoram nav informācijas par kādu esošu gadījumu Latvijas Republikas tiesā, kas uz šo jautājumu varētu atbildēt. Darba autors pieļauj, ka tāds paraksts tiks uzskatīts par derīgu atbilstoša likuma regulējuma vai attiecīgu procedūru neesamības dēļ. [14,16]

Iepriekšējā piemērā tika apskatīts ātrākais scenārijs. Ilgākajos scenārijos, kad tiek saglabāta upura nevainība rupjā nolaidībā, starp incidenta notikšanas faktu un sertifikāta faktisku apturēšanu var paiet pat vairākas dienas. Piemēram, incidents notiek darba brīvdienā, kad drošības amatpersona nav uz vietas vai palīdzības dienests nav sazvanāms, tad tuvākajā darba dienā tiek veikts pieprasījums apturēt sertifikātu, kura izpilde var aizņemt līdz divdesmit četrām stundām (Sertifikācijas pakalpojumu sniegšanas noteikumu 3.9.2.3. apakšpunkts). [14,16] Nav garantijas arī tam, ka drošības amatpersona būs tajā brīdī uzreiz sasniedzams. [14,16] Tā kā uzticamam sertifikācijas pakalpojumu sniedzējam ir jā rūpējas par pakalpojuma ilgtspējīgu un attīstību, drošības amatpersona pieprasījuma saņemšanas laikā var būt aizņemta svarīgā sanāksmē, kas nozīmē, ka apstiprināt pieprasījumu varēs tikai pēc tās beigām. [14,16] Šī maģistra darba autors pieļauj, ka sanāksme varētu tikt pārtraukta, ja pieprasītājs tajā laikā ieņem kādu valstiski nozīmīgu amatu. Šie paši gadījumi ir aktuāli arī sertifikāta anulēšanas procedūrās. To izpilde sastāv no vairākiem soļiem, kur katra veikšanai tiek patērēts laika apjoms, kas var kopsummā būt pietiekošs, lai ļaundari paspētu veiksmīgi izpildīt savus nelikumīgās kompromitētā sertifikāta izmantošanas darbības. [14,16]

Ņemot vērā to, ka Latvijas Elektronisko dokumentu likums nenosaka elektroniskā paraksta spēka zaudēšanu, ja tas ir izmantots bez tā īpašnieka ziņas un ir pierādīts, ka viņš nav vainojams rupjā nolaidībā vai speciālā nolūkā, un precizējumu neesamību par to, kad precīzi apturētais vai anulētais sertifikāts tiek uzskatīts par savu spēku zaudējušu, maģistra darba

autors secina, ka šāda gadījuma izskatīšana tiesā beigtos ar to, ka upurim būtu jāuzņemas pilna atbildība par nodarītajiem zaudējumiem un par visām darbībām, kas ir veiktas ar viņam izsniegto sertifikātu. [14,16] Tas ir uzskatāms par risku un problemātisku jautājumu, ko var risināt, sakārtojot atbilstošās procedūras un tiesību aktus tā, lai ne vienā no scenārijiem uzbrukuma upuris iespēju robežās neciestu zaudējumus. Darba autors uzskata, ka laika periods, kas ir nepieciešams no sertifikāta anulēšanas vai apturēšanas pieprasījuma līdz faktiskām izmaiņām informācijas sistēmā, ir maksimāli jāsamazina no esošajām stundām līdz minūtēm. Darba autors uzskata, ka nodrošināt iespēju jebkurā diennakts laikā un nedēļas dienā, piemēram, desmit minūšu laikā klientam anulēt vai apturēt sertifikāta darbību uzticamam sertifikācijas pakalpojumam sniedzējam var būt daudz lētāk nekā viena tiesvedība, kas var rasties, ja šis apskatītais risks netiks novērsts.

4.7.6.3 RISKI SAISTĪBĀ AR LAIKA ZĪMOGU

Lai gan Igaunijas un Latvijas elektronisko parakstu regulējošie likumi ir mazliet atšķirīgi prasībās pret laika zīmogu lietošanu un izsniegšanu, abām valstīm likumu formulējumi pieļauj dažādu risku esamību. [14,16,43,45] Ja vienā valsts likumā konkrēti riski ir novērsti, bet citi ir iespējami, tad otras valsts likumā iespējamie riski ir novērsti, bet citā likumā novērstie otrā ir aktuāli. [14,16,43,45] Tā kā darbā tiek aplūkots Latvijas Elektronisko dokumentu likuma realizācijas riski, tad Igaunijas Digitālā paraksta likuma riski aplūkoti netiek. [14,16,43,45]

Latvijas Elektronisko dokumentu likuma 18.panta septītā daļa nosaka: *"Drošs elektroniskais paraksts, kas radīts pēc kvalificēta sertifikāta anulēšanas vai laikā, kad sertifikāta darbība ir bijusi apturēta, nav derīgs."* [14,16,43,45] Likums ir formulēts tā, ka tiek pieļauta iespēja, ka dokumentu var parakstīt ar elektronisko parakstu arī tad, ja tā darbība konkrētajā brīdī ir apturēta vai anulēta. [14,16,43,45] Tātad parastā situācijā, ja elektroniskais paraksts(bez laika zīmoga) tiek uzlikts laikā, kad tā darbība ir apturēta, dokuments tiks parakstīts, bet, ja veiks paraksta pārbaudi, tas tiks atzīts par nederīgu. [14,16,43,45] Pēc laika sertifikāta darbība tiek atjaunota. [14,16,43,45] Tas nozīmē, ka, pārbaudot iepriekš parakstīto dokumentu tā sertifikāts tiks atzīts par derīgu. [14,16,43,45] Ja parakstītājs to paraksta ar laika zīmogu, tad visas iesaistītās puses var būt drošas tikai par laika zīmoga uzlikšanas brīdi, nevis sākotnējo parakstīšanas brīdi. [14,16,43,45] Uz šī pamata var tikt apšaubīta jebkura elektroniska dokumenta spēkā esamība. [14,16,43,45] Ja elektroniskais dokuments nav parakstīts ar laika zīmogu, vai tas ir uzlikts pēc sākotnējā paraksta pievienošanas, tad var būt

problemātiski pierādīt to, vai konkrētais dokuments nav bijis parakstīts laikā, kad sertifikāts ir bijis nederīgs. [14,16,43,45]

Risinājums būtu veikt grozījumus Latvijas Elektronisko dokumentu likumā, kas no likuma izņemtu iespēju atjaunot sertifikāta darbību, ja tas ir bijis apturēts. Tādā veidā atstājot iespēju sertifikāta darbību tikai anulēt. [14,16,43,45]

Latvijas Elektronisko dokumentu likuma 23. panta. 20. punktā nosaka uzticamam sertifikācijas pakalpojumu sniedzējam pienākumu nodrošināt, lai laika zīmogs norādītu starptautiski koordinētu laiku. [14,16,43,45] Pasaulē ir vairāk kā divdesmit laboratorijas, kas nodrošina universālā laika (*UTC*) kontroli Starptautiskā svaru un mēru biroja pārvaldībā(Francijs). [36,16] Šo uzturēto un kontrolēto laiku kā informācijas avotu izmanto vairāki pasaules laika serveri, kas nodrošina precīza laika rādījumu dažādām informācijas sistēmām. Tai skaitā arī elektroniskajam parakstam. [14,16,43,45] Likuma prasība tiek izpildīta un Latvijā pašlaik vienīgā uzticamā sertifikācijas pakalpojumu sniedzēja VAS „Latvijas Valsts radio un televīzijas centrs” sertifikācijas pakalpojumu noteikumu 8.1. punktā tas ir apstiprināts: *”eParaksts.lv SPS laika zīmoga radīšanai izmanto drošu, starptautiski koordinētu precīza laika avotu.”* [14,16,43,45]

Risks, kurš Igaunijas Digitālā paraksta likumā ir atrunāts un sakārtots, rodas tad, ja dažādu iemeslu dēļ nav iespējams noteikti uzlikto elektronisko parakstu precīzu laiku vai secību(Igaunijas Digitālā paraksta likuma 24.panta otrā daļa). [14,16,43,45] Tāda situācija var rasties, ja vienu elektronisko dokumentu paraksta, izmantojot dažādus sertifikācijas pakalpojumu sniedzēju pakalpojumus, kas atrodas dažādās laika zonās un izmanto atšķirīgus starptautiskos laika serverus. [14,16,43,45] Tās ir tehniskas iekārtas, kam piemīt tehniski ierobežojumi, konkrētas jaudas un ievainojamības. [14,16,43,45] To rādījumus var ietekmēt gan magnētiskās vētras vai pat specializēti sakaru izlūkošanas un elektromagnētiskā lauka uzbrukumi ar mērķi ietekmēt īslaicīgu laika rādījuma pareizību vai korektumu. [14,16,43,45] Var, piemēram būt konkrēti ligumi vai elektroniskā paraksta lietošanas situācijas, kad ir nepieciešams zināt precīzu paraksta uzlikšanas laiku vai secību. [14,16,43,45] Tādos gadījumos ieinteresētās puses var, veicot iepriekš minētos uzbrukumus, ietekmēt paraksta veidošanas procesu savā labā. [14,16,43,45] Dažādas laika un secības uzlikšanas nekonkrētības var rasties arī dažādu pakalpojumu sniedzēju elektroniskā paraksta izmantošanas formātu vai tehnoloģiju neatbilstību dēļ. Tāpēc Igaunijā ir atrunāts, ka šādos gadījumos tiek uzskatīts, ka visi paraksti ir uzlikti vienlaicīgi(Igaunijas Digitālā paraksta likuma 24.panta otrā daļa). [14,16,43,45] Latvijas Elektronisko dokumentu likumā tāda punkta nav, kas padara iespējamās problēmas saistībā ar precīza laika zīmoga uzlikšanas laika vai secības precizēšanu neskaidrību gadījumos. [14,16,43,45]

Šim riskam risinājums būtu iekļaut Latvijas Elektronisko dokumentu likumā analogiskus laika zīmoga darbību reglamentējošus punktus, kādi ir Igaunijas Digitālā paraksta likumā (24. panta otrā un trešā daļa). Tulkojumā uz latviešu valodu tie būtu: [14,16,43,45]

- 24.panta otrā daļa – „Ja nav iespējams noteikt oficiālo laiku un secību laika zīmogiem, ko ir izsnieguši atšķirīgi uzticami sertifikācijas pakalpojumu sniedzēji, tiek uzskatīts, ka laika zīmogi ir uzlikti vienlaicīgi” [43]
- 24.panta trešā daļa – „Uzticamam sertifikācijas pakalpojumu sniedzējam ir pienākums nodrošināt, lai nav iespējams izsniegt patiesu laika zīmogu, kas norādītu laiku pirms vai pēc tā faktiskas uzlikšanas, tādā veidā nemainot laika zīmogu uzlikšanas secību.” [43]

4.7.6.4 NEPĀRDOMĀTU LIKUMA GROZĪJUMU RISKI

2012. gada 10. oktobrī Latvijas Republikas Saeimas prezidijam tika iesniegts Satiksmes ministrijas izstrādāts likumprojekts „Grozījumi Elektronisko dokumentu likumā”, ko atbildīgā Tautsaimniecības, agrārās, vides un reģionālās politikas komisija 2012. gada 11. novembrī ir apstiprinājusi pirmajā lasījumā. [18] Otrajā lasījumā likumprojekts šī darba rakstīšanas laikā vēl nav izskatīts. [18]

Šis likumprojekts sevī ietver riskantas izmaiņas Latvijas Elektronisko dokumentu likuma 3. panta sestā daļa, to izsakot šādā redakcijā: ”(6) *Šis likums piemērojams tiklīdz, ciktāl citos normatīvajos aktos nav noteikta cita kārtība un nosacījumi dokumentu noformēšanā.*” [18,14] Tas nozīmē izslēgt no likuma iepriekš piemērotos izņēmumus elektroniskā paraksta lietošanai. Tas nozīmē, ja likumprojekts tiks apstiprināts, tad elektronisko parakstu varēs izmantot nekustamo īpašumu tiesību līgumiem, ģimeņu tiesību un mantojumu tiesību darījumos un arī galvojuma līgumos. [18,14]

Darba autors uzskata, ka pašlaik spēkā esošie izņēmumi Latvijas Elektronisko dokumentu likuma 3. panta sestajā daļā ir diezgan būtiski un sensitīvi darījumi un to iekļaušana elektroniskā paraksta pielietojumu sarakstā ne tikai paplašinās elektroniskā paraksta lietošanu, kā tas ir teikts iesniegtā likumprojekta anotācijā, bet arī padarīs to riskantāku un izaicinošāku kaitnieciskām darbībām. Tas var nodarīt lielus zaudējumus Latvijas iedzīvotājiem. [18,14] Darba autors uzskata, ka sertifikācijas pakalpojumu darbība un regulējums Latvijā nav pietiekoši pārbaudīta praksē un tiesu darbos, lai varētu uzskatīt, ka elektroniskā paraksta lietošana un tā regulējums Latvijā ir pietiekoši stabils un uzticams, lai būtu pieļaujama tā lietošana iepriekš minētajos gadījumos. [18,14] It īpaši, ja tajos pašlaik tiek prasīts notāra apstiprinājums, kas spēj garantēt, ka līguma vai darījuma slēdzēja puses

darbojas pēc brīvas gribas, ir rīcībspējīgas un viss atbilst atbilstošajos likumos noteiktajā kārtībā.[9,10,18,14,34,33] Elektronisko parakstu var likt arī attālināti un nav garantijas par to, vai tā īpašnieks to ir licis piespiedu kārtā vai pēc brīvas gribas, vai sertifikāts tajā brīdī ir derīgs (ja tiek parakstīts bez laika zīmoga), vai parakstu ir radījis tiešām pats elektroniskā paraksta īpašnieks, vai elektroniskajā dokumentā nav iestrādāts mainīgais saturs u.c. riska faktori, kas esošo izņēmuma gadījumos var radīt lielus zaudējumus un sekas. [9,10,18,14,34,33]

Risinājums šim riskam būtu Latvijas Elektronisko dokumentu likumā atstāt 3. panta sestajā daļā esošos izņēmumus un pirms apstiprināt grozījumus šajā likumā atbildīgajai komisijai ir nepieciešams rūpīgi izvērtēt iespējamos riskus, piesaistot arī nozares ekspertus un akadēmisko personālu, lai pēc iespējas nodrošinātu attiecīgo grozījumu pamatojamību un sabiedrības drošības garantējumu.[14] Būtu arī nepieciešama plašāka elektroniskā paraksta pielietošana mazāk sensitīvos darījumos, izmantojot dzīvās laboratorijas pieeju.[81] Tādā veidā tiktu ātrāk apgūti dažādi pielietojumu scenāriji, to riski praksē. Incidentu gadījumos iespējamais pāri darījums būtu mazāks nekā tad, ja tas notiktu ar tāda veida darījumiem, kādi pašlaik ir iekļauti Latvijas Elektronisko dokumentu likumā kā elektroniskā paraksta pielietojumu izņēmumi. [14]

4.7.6.5 PAKALPOJUMU SNIEDZĒJA DEFINĪCIJAS UN PRASĪBU RISKI

Latvijas Elektronisko dokumentu likuma 8. un 9. pants nosaka sertifikācijas pakalpojumu sniedzēju iedalījumu. Pakalpojumu sniedzēji tiek iedalīti divās kategorijās:[14]

1. Sertifikācijas pakalpojumu sniedzējs [14]

2. Uzticams sertifikācijas pakalpojumu sniedzējs [14]

Saskaņā ar saistošo likumu, sertifikācijas pakalpojumu sniedzējam nav nepieciešama speciālas atļaujas saņemšana un akreditācija Datu valsts inspekcijā ir brīvprātīga(Latvijas Elektronisko dokumentu likuma 8. panta otrā daļa). [14] Šo abu kategoriju definīcijās gan par Sertifikācijas pakalpojumu sniedzēju, gan par uzticamu sertifikācijas pakalpojumu sniedzēju var būt gan fiziska, gan juridiska persona. [14] Salīdzinājumam, Igaunijas Digitālā paraksta likums nosaka, ka sertifikācijas pakalpojumu sniedzēji var būt tikai juridiskas personas. [14,43] Starp fiziskām un juridiskām personām būtiska atšķirība ir to atbildības līmeņos, jo fiziskas personas Latvijā regulē civillikums, bet juridiskās personas – komerclikums.

Tātad tas viss nozīmē, ka Latvijā var veiksmīgi darboties vairāki sertifikācijas pakalpojumu sniedzēji, kuriem nav nepieciešamas speciālas atļaujas, un tie var nebūt atkreditēti Datu valsts inspekcijā. Darba autors uzskata, ka visi sertifikācijas pakalpojumu

sniedzēji neatkarīgi no tā, vai tie atbilst uzticama sertifikācijas pakalpojumu sniedzēja statusam vai nē, ir jākontrolē un jāuzrauga. Ja tas netiek darīts, tad rodas daudzi riski saistībā ar šādu pakalpojumu sniedzēju patvaļīgām darbībām. Piemēram, uzdošanās par uzticamiem sertifikācijas pakalpojumu sniedzējiem, parakstu viltošana, klientu krāpšana, viņu privāto sniegto datu iegūšana un izplatīšana. Neuzmanīgi pakalpojuma lietotāji varētu viegli kļūt par ļaunprātīgu pakalpojumu sniedzēju upuriem.

Risinājums šim riskam būtu Latvijas Elektronisko dokumentu likumā noteikt, ka sertifikācijas pakalpojumu sniedzējs var būt tikai juridiska persona un tiem paredzēt līdzīgas prasības, kādas tas ir uzticamiem sertifikācijas pakalpojumu sniedzējiem, uzmanīgi izvērtējot, kurus prasību punktus atstāt, kurus nē. [14]

Vēl viens risks rodas faktā, ka Latvijas Elektronisko dokumentu likumā gan no sertifikācijas pakalpojumu sniedzēja, gan no uzticama sertifikācijas pakalpojuma sniedzēja netiek prasīta parādu un nodokļu parādu neesamība, kā tas ir Igaunijas Digitālā paraksta likumā. [14,16] Saistošais likums nosaka tikai to, lai pakalpojumu sniedzējam ir pietiekoši finansu resursi tā darbības nodrošināšanai. Risks parādās tajā aspektā, ka pakalpojumu sniedzējam var būt daudzi parādsaistību līgumi noslēgti, kas nodrošina tam pietiekošus finansiālus resursus, lai izpildītu likuma prasības, bet tajā pašā laikā parādu esamība kā tāda liecina par iespējamām finansiālām problēmām nākotnē. Īpaši, ja pakalpojumu sniedzējam ir nodokļu parādi valstij, tad tas var liecināt arī par tā godprātību un likumisku darbību, kas var tālāk izpausties arī iekšējo procedūru un drošības prasību izpildē un kvalitatīva pakalpojuma sniegšanas garanta mazticamībā.

Risinājums būtu iekļaut Elektronisko dokumentu likumā prasību sertifikācijas pakalpojumu sniedzējiem būt bez parādsaistībām un bez nodokļu parādiem valstij.

4.7.6.6 PARAKSTA RADĪŠANAS DATU DEFINĪCIJAS RISKS

Eiropas Parlamenta un padomes Direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu 2. panta 4. punktā elektroniskā paraksta radīšanas dati tiek definēti: „4) *paraksta radīšanas dati*” ir unikāli dati, piemēram, kodi vai privātas šifrēšanas atslēgas, ko parakstītājs izmanto elektroniska paraksta radīšanai;” [11]

Latvijas Republikas Elektronisko dokumentu likuma 1. panta 6. punktā elektroniskā paraksta radīšanas dati tiek definēti šādi: ”6) *elektroniskā paraksta radīšanas dati* — tikai vienreiz radīti dati, kurus parakstītājs izmanto, lai radītu elektronisko parakstu;” [14]

Darba autors uzskata, ka paraksta pārbaudīšanas datu definīcija Elektronisko dokumentu likumā ir riskanta, jo atšķirībā no iepriekš minētās direktīvas definīcijas, tā nenosaka

parakstīšanas radīšanas datu unikalitātes prasību. Tas nozīmē, ka Latvijas Elektronisko dokumentu likums pieļauj iespēju, ka tiek dažādiem cilvēkiem izsniegti identiski paraksta radīšanas dati. Definīcijā tiek noteikta prasība, lai dati tiktu radīti tikai vienu reizi. Šāda definīcija, piemēram, ļauj vairākiem sertifikācijas klientiem vienu reizi izveidot elektroniskā paraksta radīšanas datus, bet visus veidojot identiskus, nevis unikālus, kā to nosaka direktīva.

Risinājums veikt pārdomātus Elektronisko dokumentu likuma grozījumus, pārņemot elektroniska paraksta radīšanas datu definīciju no Eiropas Parlamenta un padomes Direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu 2. panta 4. punkta. [14,16]

REZULTĀTI UN SECINĀJUMI

Eiropas Parlamenta un padomes Direktīvas 1999/93/EK divi galvenie mērķi ir: [11]

- 1) Veicināt brīvu konkurenci, [11]
- 2) veicināt tehnoloģiju attīstību. [11]

Latvijas Elektronisko dokumentu likuma realizācija nerealizē pirmo mērķi, jo valsts vēsturē ne vienu brīdi nav bijis vairāk par vienu uzticamu sertifikācijas pakalpojumu sniedzēju. Konkurences nav, uzraudzība neprofesionāla, kā rezultātā tehnoloģiju attīstībai nav motivācijas.

Atsevišķi tehnoloģiju attīstības gadījumi atzīmējami:

–pozitīvi vērtējams: darba rakstīšanas laikā VAS „Latvijas Valsts radio un televīzijas centrs” plāno pāriet no *SHA-1* uz *SHA-2* jaucējfunkciju izmantošanu, sekojot pasaules pieredzei;

–negatīvi vērtējams: izstrādāts un ieviests Elektronisko dokumentu likumam neatbilstošs tā saucamais virtuālais elektroniskais paraksts, bet tā drošība ir apšaubāma.

Desmit gadu laikā, kopš Latvijā tika apstiprināts Elektronisko dokumentu likums, vēl 2013. gadā sertifikācijas pakalpojumi netiek plaši lietoti un tie ir ieviesti nekvalitatīvi.

Darba autors secina, ka esošais sertifikācijas pakalpojumu risinājums ir ļoti nekvalitatīvs un neuzticams, par ko, piemēram, liecina biežās lietotāju sūdzības. Ir nepieciešama fundamentāla esošo risinājumu revīzija un pārstrāde. Nepieciešams veikt publisku iespējamo risinājuma apspriešanu un izvērtēšanu, piesaistot maksimāli daudzskaitlīgu un kompetentu akadēmisko personālu, iespējami daudz profesionāļu no pasaules, kas būtu aicināti ar personīgiem uzaicinājumiem, gan juridiskās, gan fiziskās personas, kam ir ievērojama pieredze līdzīgu vai līdzvērtīgu risinājumu veiksmīgā izstrādē. Noteikti būtu jāiesaista arī Madars Virza un Arnis Paršovs, kuru zinātniskie vadītāji Ron Rivest un Peeter Laud ir ievērojami profesionāli kriptologi.

Risinājuma ieviešanā būtu nepieciešams izmantot dzīves laboratorijas pieeju, maksimāli iesaistot pakalpojumu attīstībā sabiedrību un gala lietotājus, kā arī veidot ar viņiem uz attīstību un sadarbību orientētu atklātu un godīgu komunikāciju, bez informācijas slēpšanas vai maldināšanas.

Darba autors secina, ka bez nacionālas datu drošības skolas izveides ar profesionālas kriptoloģijas kompetenci Latvijas sertifikācijas pakalpojumiem un datu drošības jomai kā tādai perspektīvas nav. Ja tāda skola netiks veidota, tad vienīgais risinājums būs, ka ārēja

spiediena rezultātā par datu drošību un drošības risinājumu un pakalpojumu piegādi valstī rūpēsies ārzemju speciālisti un pakalpojumu sniedzēji. Šāds risinājums, savukārt, vērtējams kā nopietns nacionālas valsts drošības apdraudējums.

Kardināli nemainot esošos elektroniskā paraksta un ar sertifikācija pakalpojumiem saistītu Eiropas Savienības regulējumu ieviešanas realizācijas mehānismus, topošās Eiropas Savienības Regulas par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū prasības Latvijas valsts kvalitatīvi nespēs izpildīt, kā rezultātā tiks bremsēta iespējamā tautsaimniecības attīstība.

Darba autors vērš uzmanību tam, ka par vairāku apskatīto risku esamību var pārliecināties jebkurš lietotājs pat bez padziļinātām prasmēm informācijas tehnoloģijās.

IZMANTOTĀ LITERATŪRA UN AVOTI

- [1] E.L. Melnick, B.S. Everitt red., "Encyclopedia of Quantitative Risk Analysis and Assessment," Volume 1, John Wiley & Sons, 2008, p. 2176 pp. 429-435.
- [2] E.L. Melnick, B.S. Everitt red., "Encyclopedia of Quantitative Risk Analysis and Assessment," Volume 1, John Wiley & Sons, 2008, p. 2176 pp. 436-437.
- [3] E.L. Melnick, B.S. Everitt red., "Encyclopedia of Quantitative Risk Analysis and Assessment," Volume 1, John Wiley & Sons, 2008, p. 2176 p. 438-439.
- [4] APPLIED CRYPTOGRAPHY Second Edition Bruce Schneier John Wiley & Sons, 1996 784 pages pp.471-472
- [5] Juliano Rizzo, Thai Duong , "The CRIME attack" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://netifera.com/research/crime/CRIME_ekoparty2012.pdf
- [6] Grozījumi Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=158616><http://mk.gov.lv/doc/2005/IUMEPLANot.doc>
- [7] Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=121005>
- [8] 1998/0191(COD) - 13/12/1999 Final act [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.europarl.europa.eu/oeil/popups/summary.do?id=8172&t=f&l=en>
- [9] Civillikuma 2. Daļa – Mantojuma tiesības [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=90222>
- [10] Civillikuma 4. Daļa – saistību tiesības [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=90220>
- [11] Eiropas Parlamenta un padomes Direktīva 1999/93/EK (1999. gada 13. decembris) par Kopienas elektronisko parakstu sistēmu [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:LV:HTML>
- [12] EIROPAS PARLAMENTA UN PADOMES DIREKTĪVA 1999/93/EK par Kopienas elektronisko parakstu sistēmu. [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:24:31999L0093:LV:PDF>
- [13] Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.likumi.lv/doc.php?id=111613>

- [14] Elektronisko dokumentu likums [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=68521>
- [15] Elektronisko dokumentu likums 2003.04.08 19:13 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://dvi.gov.lv/edokumenti/read.php?c=edoc05&id=1049818390.108.8.0>
- [16] eParaksts. Sertifikācijas pakalpojumu sniedzēja Sertifikācijas pakalpojumu sniegšanas noteikumi [tiešsaiste]. - [atsauce 08.05.2013.]. Pieejams: https://www.eparaksts.lv/files/sps_sn_v2_9_3_lat.pdf
- [17] Fizisko personu datu aizsardzības likums [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=4042>
- [18] Grozījumi Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://titania.saeima.lv/LIVS11/SaeimaLIVS11.nsf/0/332CB05A02153D7CC2257AA300254673?OpenDocument#a>
- [19] Grozījumi Elektronisko dokumentu likumā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.likumi.lv/doc.php?id=139376>
- [20] Grozījumi Elektronisko dokumentu likumā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.likumi.lv/doc.php?id=158616>
- [21] Grozījumi Elektronisko identifikācijas karšu koncepcijā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=234590><http://mk.gov.lv/lv/mk/tap/?pid=40213846>
- [22] Grozījumi Ministru kabineta 2005.gada 28.jūnija noteikumos Nr.473 "Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.likumi.lv/doc.php?id=166355>
- [23] Grozījumi Ministru kabineta 2005.gada 28.jūnija noteikumos Nr.473 "Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.likumi.lv/doc.php?id=166355>
- [24] Grozījums Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=134126>
- [25] Grozījums Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=139376>

- [26] Grozījums Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.].
Pieejams: <http://likumi.lv/doc.php?id=158616>
- [27] Grozījums Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.].
Pieejams: <http://likumi.lv/doc.php?id=198815>
- [28] Grozījums Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.].
Pieejams: <http://likumi.lv/doc.php?id=88508>
- [29] Grozījums Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.].
Pieejams: <http://likumi.lv/doc.php?id=92549>
- [30] Grozījums Elektronisko dokumentu likumā [tiešsaiste]. - [atsauce 25.05.2013.].
Pieejams: <http://likumi.lv/doc.php?id=96222>
- [31] Informācijas sistēmās esošo dokumentēto datu un elektronisko dokumentu arhivēšanas noteikumi [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=60917>
- [32] LATVIJAS REPUBLIKAS LIKUMS Par grāmatvedību [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.likumi.lv/doc.php?id=66460>
- [33] Nekustamā īpašuma valsts kadastra likums [tiešsaiste]. - [atsauce 25.05.2013.].
Pieejams: <http://likumi.lv/doc.php?id=124247>
- [34] Notariāta likums [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://likumi.lv/doc.php?id=59982>
- [35] Noteikumi par elektronisko dokumentu izvērtēšanas veidu saglabāšanas kārtību un nodošanu valsts arhīvam glabāšanā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
likumi.lv/doc.php?id=85206
- [36] Noteikumi par tehniskajām un organizatoriskajām prasībām, kādām atbilst kvalificēts sertifikāts, uzticams sertifikācijas pakalpojumu sniedzējs, droši elektroniskā paraksta radīšanas līdzekļi, kā arī kārtību, kādā veicama droša elektroniskā paraksta verificēšana [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://likumi.lv/doc.php?id=112655>
- [37] Par darba grupu ar elektronisko dokumentu ieviešanu saistīto jautājumu risināšanai” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.vestnesis.lv/?menu=doc&id=9284>
- [38] Par darba grupu elektroniskā paraksta plašākas lietošanas nodrošināšanai <http://www.likumi.lv/doc.php?id=227457>
- [39] Par darba grupu elektronisko dokumentu ieviešanai” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.vestnesis.lv/?menu=doc&id=45>
- [40] Par Elektronisko identifikācijas karšu koncepciju [tiešsaiste]. - [atsauce 25.05.2013.].
Pieejams: www.likumi.lv/doc.php?id=205074

- [41] Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://dvi.gov.lv/edokumenti/read.php?c=edoc05&id=1057329095.109.7.0>
- [42] Valsts pārvaldes iekārtas likums [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.likumi.lv/doc.php?id=63545>
- [43] Digital Signatures Act [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30081K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=digitaalalkirja+seadus>
- [44] Arnis Paršovs, „Security Analysis of Internet Bank Authentication Protocols and their Implementations.” Master's Thesis, Faculty of Information technology Department of Computer Science Cyber Security, TALLINN UNIVERSITY OF TECHNOLOGY, 2012 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://math.ut.ee/~arnis/bankauth/thesis.pdf>
- [45] Privāta saruna ar Arni Pašrovu
- [46] Privāta saruna ar Madaru Virzu
- [47] Andris Rudzītis, „Biometrija pasaules ikdienā,” Sakaru pasaule, Feb. 2008 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.sakaru-pasaule.lv/main.php3?sub=view&RID=1558>
- [48] L. Lāce, Kāpēc sociālā inženierija ir efektīva? [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.esidross.lv/2013/04/10/kapec-sociala-inzenierija-ir-efektiva/>
- [49] Līva Lāce, Datu drošība uzņēmumā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.esidross.lv/2012/12/28/datu-drosiba-uznemuma/>
- [50] Ojārs Zvirbulis, „ADMINISTRATĪVĀ un KRIMINĀLĀ JUSTĪCIJA (VALSTS TIESĪBU APAŠNOZARE) Drošs elektroniskais paraksts Latvijā, Lietuvā un Igaunijā” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.ozvibr.lv/OUTSIDE/EME.pdf>
- [51] Platace Laura, Komerccnoslēpums, tā izpaušanas ierobežojumi un nosacījumi [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.lvportals.lv/print.php?id=249834#a3>
- [52] Bankas [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.fktk.lv/lv/tirgus_dalibnieki/kreditiestades/bankas1/
- [53] Datu Valsts inspekcija, E-dokumenti. Uzticamu sertifikācijas pakalpojumu sniedzēju sertifikācija [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://dvi.gov.lv/edokumenti/index.php?c=edoc05>
- [54] Drošs elektroniskais paraksts [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://lata.org.lv/wp-content/conf/Drosiba/LATA_eparaksts_ArnisParsovs.pdf

- [55] EDOC Java bibliotēkas [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.euso.lv/pages/products?lang=lv>
- [56] eID kartes Latvijā sāks izsniegt no 1. aprīļa [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.jelgavasvestnesis.lv/page/50&news_id=15189?action=vote_archive&id=127
- [57] Eiropas Savienības tiesību ceļvedis [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur-lex.europa.eu/lv/editorial/abc.pdf#page=86>
- [58] eparaksts.lv forums [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.eparaksts.lv/lv/forums/apskatit/131>
- [59] eparaksts.lv forums [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.eparaksts.lv/lv/forums/apskatit/999>
- [60] eparaksts.lv forums Sistēmas kļūda!? [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.eparaksts.lv/lv/forums/apskatit/681>
- [61] Iepirkumu uzraudzības birojs Iesniegumu izskatīšanas komisija L Ē M U M S Nr. 4-1.2/12-34 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.iub.gov.lv/files/lemumi/lem214377.pdf>
- [62] Informatīvais ziņojums "Par eParaksta praktiskās ieviešanas reālo situāciju un problēmām tā ieviešanā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=40208240>
- [63] Informatīvais ziņojums "Par eParaksta praktiskās ieviešanas reālo situāciju un problēmām tā ieviešanā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.mk.gov.lv/lv/mk/tap/?pid=40208240>
- [64] Informatīvais ziņojums "Par grozījumiem "Līgumā par droša elektroniskā paraksta ieviešanas pasākumu īstenošanu Latvijas Republikā" un koncepcijas "Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijā" īstenošanas gaitu" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30233302>
- [65] Informatīvais ziņojums "Par koncepcijas "Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā" īstenošanas gaitu" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30296997>
- [66] Informatīvais ziņojums "Par priekšlikumiem elektroniskā paraksta plašākas lietošanas nodrošināšanai" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=40224003>
- [67] Informatīvais ziņojums "Par priekšlikumiem elektroniskā paraksta plašākas lietošanas nodrošināšanai" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=40251614%20Par%20priek%C5%A1likumiem%20elektroni>

sk%C4%81%20paraksta%20pla%C5%A1%C4%81kas%20lieto%C5%A1anas%20nodro%C5%A1in%C4%81%C5%A1anai

[68] Informatīvais ziņojums "Par valsts un pašvaldību iestāžu (to skaitā arī iestāžu struktūrvienību) gatavību ar 2010.gada 1.janvāri pāriet uz dokumentu apriti starp iestādēm, izmantojot elektroniski parakstītus dokumentus" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=40112310>

[69] INFORMATĪVAIS ZIŅOJUMS "PAR GROZĪJUMIEM LĪGUMĀ PAR DROŠA ELEKTRONISKĀ PARAKSTA IEVIEŠANAS PASĀKUMU ĪSTENOŠANU LATVIJAS REPUBLIKĀ" UN KONCEPCIJAS „PAR DROŠA ELEKTRONISKĀ PARAKSTA NESĒJA IZVĒLI UN DORŠA ELEKTRONISKĀ PARAKSTA IEVIEŠANU LATVIJAS REPUBLIKĀ” ĪSTENOŠANAS GAITU” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLZino_220206_.doc

[70] Informatīvais ziņojums „Par koncepcijas „Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā” īstenošanas gaitu” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLZino_090408_epar.doc

[71] Informatīvais ziņojums „Par valsts un pašvaldību iestāžu (to skaitā arī iestāžu struktūrvienību) gatavību ar 2010.gada 1.janvāri pāriet uz dokumentu apriti starp iestādēm, izmantojot elektroniski parakstītus dokumentus” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLZino_130209_edok.492.doc

[72] Informatīvais ziņojums par elektroniskā paraksta ieviešanas pasākumu grafiku [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.mk.gov.lv/lv/mk/tap.?pid=30193999>

[73] Informatīvais ziņojums par eParaksta praktiskās ieviešanas reālo situāciju un problēmām tā ieviešanā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/SAMZino_220211_eparaksts.456.doc

[74] Informatīvais ziņojums par Komisijas ziņojumu Eiropas Parlamentam un Padomei “Ziņojums par direktīvas 1999/93/EK par Kopienas elektronisko parakstu sistēmu darbību” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLZino_110406_e_paraksts.doc

[75] Informatīvais ziņojums par koncepcijas "Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijā" īstenošanas gaitu" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30258576>

[76] Informatīvais ziņojums par priekšlikumiem elektroniskā paraksta plašākas lietošanas nodrošināšanai [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/SAMZino_081111_eparaksts.2936.doc

- [77] Informatīvais ziņojums par priekšlikumiem elektroniskā paraksta plašākas lietošanas nodrošināšanai [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/SAMZino_131112_eparaksts.1129.doc
- [78] INFORMATĪVAIS ZIŅOJUMS PAR VIENOŠANOS DROŠA ELEKTRONISKĀ PARAKSTA IEVIEŠANAI LATVIJĀ [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLZino_130605_e-par-vienos.doc
- [79] Informatīvais ziņojums par vienošanos droša elektroniskā paraksta ieviešanai Latvijā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30198857>
- [80] Informatīvais ziņojums „Par koncepcijas "Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā" īstenošanas gaitu” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLzino_280507.doc
- [81] Inovācijas atbalsta instrumenti un prakse [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.vraa.gov.lv/uploads/Handbook_latviski.pdf
- [82] Java EDOC bibliotēkas [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.eparaksts.lv/lv/palidziba/lejupielades/java-edoc-bibliotekas-1/>
- [83] Kas ir biometrija? [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://windows.microsoft.com/lv-LV/windows7/What-is-biometrics>
- [84] KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI Digitālā programma Eiropai. Document COM(2010) 245 final 19.5.2010 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:LV:PDF>
- [85] Koncepcijas projekts "Par droša elektroniskā paraksta finansēšanu atsevišķās iedzīvotāju mērķa grupās" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30296657>
- [86] Koncepcijas projekts "Par droša elektroniskā paraksta finansēšanu atsevišķās iedzīvotāju mērķa grupās"(informatīvā daļa) [tiešsaiste] . - [atsauce 25.05.2013.]. Pieejams: [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLKonc_290507.doc
- [87] Lattelecom [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.lattelecom.lv/Lattelecom_grupa/par_Lattelecom_grupu/Lattelecom/
- [88] Latvijas pasts. Aktualitātes [20.12.2005]" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.pasts.lv/lv/aktualitates/index.html;jsessionid=BE33CF514221307320DF8187C1FC2250?news_id=302

- [89] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES DARBA KĀRTĪBA 2008.gada 1.aprīlī plkst. 12:00TA-912 Informatīvais ziņojums "Par valsts akciju sabiedrības "Latvijas Pasts" problēmām, kas saistītas ar pasta pamatpakalpojumu nodrošināšanu Latvijas teritorijā" (papildus iekļautais jautājums) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/mksedes/saraksts/darbakartiba/?sede=2008-04-01#30336346>
- [90] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS 26.§ Konceptijas projekts par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2005-10-18>
- [91] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS NR 21 29.§ [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2005-04-19>
- [92] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS NR 21 53.§ Informatīvais ziņojums "Par valsts akciju sabiedrības "Latvijas Pasts" preses izdevumu piegādes pakalpojumu sniegšanas lauku apvidos radīto zaudējumu kompensēšanu [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2008-04-01#52>
- [93] LATVIJAS REPUBLIKAS MINISTRU KABINETA sēdes protokols nr. 35 2.§ Priekšlikumi par valsts akciju sabiedrības "Latvijas Pasts" turpmāko rīcību saistībā ar sertifikācijas pakalpojumu nodošanu citai institūcijai" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2008-05-28#2>
- [94] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS NR 59 14.§ Likumprojekts "Grozījumi Elektronisko dokumentu likumā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2012-10-23#14>
- [95] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS NR 70 41.§ Informatīvais ziņojums "Par priekšlikumiem elektroniskā paraksta plašākas lietošanas nodrošināšanai" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2012-12-11#41
- [96] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS Nr.11 67.§ Informatīvais ziņojums "Par eParaksta praktiskās ieviešanas reālo situāciju un problēmām tā ieviešanā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2011-02-22#67>

- [97] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS Nr.16"
[tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2007-02-27>
- [98] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS Nr.17 2.§
Informatīvais ziņojums "Par valsts un pašvaldību iestāžu (to skaitā arī iestāžu struktūrvienību)
gatavību ar 2010.gada 1.janvāri pāriet uz dokumentu apriti starp iestādēm, izmantojot
elektroniski parakstītus dokumentus" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2009-03-10#2>
- [99] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS Nr.2 28.§
Par Ministru kabineta 2009.gada 10.marta sēdes protokollēmuma (prot. Nr.17 2.§)
"Informatīvais ziņojums "Par valsts un pašvaldību iestāžu (to skaitā arī iestāžu
struktūrvienību) gatavību ar 2010.gada 1.janvāri pāriet uz dokumentu apriti starp iestādēm,
izmantojot elektroniski parakstītus dokumentus"" 3. un 4.punktā dotā uzdevuma izpildi
[tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2010-01-12#26>
- [100] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS Nr.24
[tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2006-04-25>
- [101] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS Nr.35
30.§ Informatīvais ziņojums par vienošanos droša elektroniskā paraksta ieviešanai Latvijā"
[tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2005-06-14>
- [102] LATVIJAS REPUBLIKAS MINISTRU KABINETA SĒDES PROTOKOLS Nr.35
33.§ Rīkojuma projekts "Grozījumi Elektronisko identifikācijas karšu koncepcijā" [tiešsaiste].
- [atsauce 25.05.2013.]. Pieejams:
<http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2011-06-07#33>
- [103] Latvijas sākotnējās nacionālās pozīcijas projekts par Komisijas ziņojumu Eiropas
Parlamentam un Padomei "Ziņojums par Direktīvas 1999/93/EK par Kopienas elektronisko
parakstu sistēmu darbību" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://mk.gov.lv/lv/mk/tap/?pid=30239782>
- [104] Likumprojekta "Grozījumi Elektronisko dokumentu likumā" sākotnējās ietekmes
novērtējuma ziņojums (anotācija) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
http://mk.gov.lv/doc/2005/SAMAnot_280812_edl.1663.doc
- [105] Likumprojekta „Grozījumi Elektronisko dokumentu likumā” Anotācija” [tiešsaiste]. -
[atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/doc/2005/IUMEPLAnot.doc>

- [106] Likumprojekts "Grozījumi Elektronisko dokumentu likumā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30259919>
- [107] Ministru kabineta rīkojuma projekta „Grozījumi Elektronisko identifikācijas karšu koncepcijā” sākotnējās ietekmes novērtējuma ziņojums (anotācija) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/SAMAnot_240511_eID.1331.doc
- [108] Noteikumu projekts "Grozījumi Ministru kabineta 2005.gada 28.jūnija noteikumos Nr.473 "Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un juridiskajām personām" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30305174> aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un
- [109] Par koncepcijas "Par droša elektroniskā paraksta nesēja izvēli un droša elektroniskā paraksta ieviešanu Latvijas Republikā" īstenošanas gaitu Informatīvais ziņojums par eParaksta praktiskās ieviešanas reālo situāciju un problēmām tā ieviešanā [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=30329510>
- [110] Par Microsoft Latvija [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.microsoft.com/lv-lv/about/default.aspx>
- [111] Par Ministru kabineta 2005.gada 19.aprīļa sēdes protokollēmumu (prot. Nr.21 29.§) "Informatīvais ziņojums Par elektroniskā paraksta ieviešanas gaitu [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.mk.gov.lv/lv/mk/tap/?pid=30196903>
- [112] Paskaidrojuma raksts Ministru kabineta noteikumu projektam „Grozījumi Ministru kabineta 2005.gada 28.jūnija noteikumos Nr.473 „Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://mk.gov.lv/doc/2005/IUMEPLPask_240907_edok.doc
- [113] Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULA par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū /* COM/2012/0238 final - 2012/0146 (COD) */ [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:LV:HTML>
- [114] Regulas, direktīvas un citi tiesību akti [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://europa.eu/about-eu/basic-information/decision-making/legal-acts/index_lv.htm
- [115] Rīkojuma projekts "Grozījumi Elektronisko identifikācijas karšu koncepcijā" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/tap/?pid=40213846>

- [116] Satiksmes ministrija twitter ziņa [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: https://twitter.com/Sat_Min/status/331707280749912064
- [117] SIA "EUSO" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.euso.lv/pages/;jsessionid=43B6FF274F2E6BDC67DEDAB581FAFF84>
- [118] SSL Report: eparaksts.lv (195.244.147.25) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.ssllabs.com/ssltest/analyze.html?d=www.eparaksts.lv>
- [119] Uzlauzta kārtējā RSA atslēga [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.antivirus.lv/news.php?l=lv&d=15.11.2005&n=1&w=1>
- [120] Valsts Datu inspekcija [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://dvi.gov.lv/>
- [121] VALSTS SEKRETĀRU SANĀKSMES P R O T O K O L S NR 49 51.§ Konceptijas projekts "Par droša elektroniskā paraksta finansēšanu atsevišķās iedzīvotāju mērķa grupās" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/vsssanaksmes/saraksts/protokols/?protokols=2007-12-13#51>
- [122] VALSTS SEKRETĀRU SANĀKSMES P R O T O K O L S Nr. 64 32.§ Noteikumu projekts "Grozījumi Ministru kabineta 2005.gada 28.jūnija noteikumos Nr.473 "Elektronisko dokumentu izstrādāšanas, noformēšanas, glabāšanas un aprites kārtība valsts un pašvaldību iestādēs un kārtība, kādā notiek elektronisko dokumentu aprite starp valsts un pašvaldību iestādēm vai starp šīm iestādēm un fiziskajām un juridiskajām personām" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://mk.gov.lv/lv/mk/mksedes/saraksts/protokols/?protokols=2007-11-13#32>
- [123] VAS Latvijas Valsts radio un televīzijas centrs (LVRTC) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.lvrtc.lv/lat/par_mums/
- [124] Vienošanās par grozījumiem 2005. gada 15. jūnija Līgumā par droša elektroniskā paraksta ieviešanas pasākumu īstenošanu, kas noslēgts starp Latvijas Republiku, VAS „Latvijas Pasts” un SIA „Lattelekom” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.mk.gov.lv/doc/2005/IUMEPLp1_220206_.doc
- [125] Bruce Morton, „CAs Support Standards and Regulations" [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://ssl.entrust.net/blog/>
- [126] Byron Acohido, Phishing gangs exploit videos of Boston, Texas [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.usatoday.com/story/tech/2013/04/19/phishing-gangs-exploit-boston-bombing--west-texas-fertilizer-explosion/2098397/>
- [127] Christopher Meyer, Jorg Schwenk, Lessons Learned From Previous SSL/TLS Attacks A Brief Chronology Of Attacks And Weaknesses [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eprint.iacr.org/2013/049.pdf>

- [128] Dan Boneh, Twenty Years of Attacks on the RSA Cryptosystem [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf>
- [129] J. Salowey et al, AES Galois Counter Mode (GCM) Cipher Suites for TLS [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://tools.ietf.org/html/rfc5288>
- [130] Marco Strano, INSIDE ATTACK: what prevention? [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.dvara.net/hk/ins_attack_english_strano.pdf
- [131] Morris Dworkin, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>
- [132] Poul Kocher, J. Jaffe, B. Jun Differential Power Analysis [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.cryptography.com/public/pdf/DPA.pdf>
- [133] S.M. Bellovin Problem Areas for the IP Security Protocols [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.cs.columbia.edu/~smb/papers/badesp.pdf>
- [134] Siddika Berna Örs Yalçın, Side-channel attacks on hardware implementations of cryptographic algorithms [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://web.itu.edu.tr/~orssi/dersler/cryptography/slides.pdf>
- [135] Schedule for CA evaluations [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://wiki.mozilla.org/CA>
- [136] Schedule for CA evaluations [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: https://wiki.mozilla.org/CA:Schedule#Schedule_for_CA_evaluations
- [137] 56387 : SSLv2 Protocol Multiple Weaknesses [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://osvdb.org/56387>
- [138] 74829 : SSL Chained Initialization Vector CBC Mode MiTM Weakness (BEAST) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://osvdb.org/74829>
- [139] A few technical details about the case by TURKTRUST [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: www.turktrust.com.tr/files/tech-details.pdf
- [140] Adam Matthews, Low Cost Attacks on Smart Cards The Electromagnetic Side-Channel [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.escrow4softwares.com/media/18514/low_cost_attacks_on_smart_cards_the_electromagnetic_side_channel.pdf
- [141] An attack against SSH2 protocol [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.mail-archive.com/openssl-dev@openssl.org/msg10664.html>
- [142] Analysis of the SSL 3.0 protocol [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.schneier.com/paper-ssl.pdf>

[143] BEAST [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://vnhacker.blogspot.com/2011/09/beast.html>

[144] BEAST vs HTTPS [tiešsaiste]. [atsauce 25.05.2013.]. Pieejams:
<http://youtu.be/BTqAIDVUvrU>

[145] Browse - computer tips - dump display print ssl certificate [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
http://www.davekb.com/browse_computer_tips:dump_display_print_ssl_certificate:txt

[146] Bug 518098 - Add E-ME root certificate [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
https://bugzilla.mozilla.org/show_bug.cgi?id=518098#c66

[147] Bug 665814 - (CVE-2011-3389) Rizzo/Duong chosen plaintext attack (BEAST) on SSL/TLS 1.0 (facilitated by websockets -76) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
https://bugzilla.mozilla.org/show_bug.cgi?id=665814

[148] Bug 825022 - Deal with TURKTRUST mis-issued *.google.com certificate [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: https://bugzilla.mozilla.org/show_bug.cgi?id=825022

[149] BUREAU INTERNATIONAL DES POIDS ET MESURES, BIPM Annual Report on Time Activities [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
http://www.bipm.org/utls/en/pdf/time_ann_rep/Time_annual_report_2011.pdf

[150] Cipher Suite [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<http://www.networking4all.com/en/support/tools/site+check/cipher+suite/>

[151] Cipher Suite Mitigation for BEAST [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
<https://www.phonefactor.com/resources/CipherSuiteMitigationForBeast.pdf>

[152] Classification and Generation of Disturbance Vectors for Collision Attacks against SHA-1 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eprint.iacr.org/2008/469.pdf>

[153] CNET, Prepare for your greatest security risk: An inside attack [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.techrepublic.com/article/prepare-for-your-greatest-security-risk-an-inside-attack/1033524>

[154] Commerce Department Announces Winner of Global Information Security Competition [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:
http://www.nist.gov/public_affairs/releases/g00-176.cfm

[155] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245:EN:NOT>

- [156] Compression and Information Leakage of Plain text [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.iacr.org/cryptodb/archive/2002/FSE/3091/3091.pdf>
- [157] Don't Fire An Employee And Leave Them In Charge Of The Corporate Twitter Account [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.forbes.com/sites/susanadams/2013/02/01/dont-fire-an-employee-and-leave-them-in-charge-of-the-corporate-twitter-account/>
- [158] DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-507.971+01+DOC+PDF+V0//EN&language=EN>
- [159] Electromagnetic Eavesdropping Risks of Flat-Panel Displays [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf>
- [160] Electronic communication, open networks safety: electronic signatures, common regulatory framework 1998/0191(COD) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.europarl.europa.eu/oel/popups/ficheprocedure.do?lang=en&reference=1998/0191%28COD%29#tab-0>
- [161] Encryption Ciphers [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.wormly.com/help/ssl-tests/encryption-ciphers/aspopup/1>
- [162] Federal Information Processing Standards Publication 180-2, SECURE HASH STANDARD [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>
- [163] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, „Digital Signature Standard (DSS)” [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
- [164] Here Come The XOR Ninjas [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://bug665814.bugzilla.mozilla.org/attachment.cgi?id=540839>
- [165] How To Verify SSL Certificate From A Shell Prompt [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.cyberciti.biz/faq/test-ssl-certificates-diagnosis-ssl-certificate/>
- [166] Internal Network Security [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.123helpme.com/internal-network-security-view.asp?id=158965>
- [167] Internet Security Glossary [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://tools.ietf.org/html/rfc2828>

- [168] KPMG's Inside Trader: What The Auditor, and Skechers, Don't Want To Talk About [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.forbes.com/sites/francinemckenna/2013/04/22/kpmgs-inside-trader-what-the-auditor-and-skechers-dont-want-to-talk-about/?utm_campaign=forbestwittersf&utm_source=twitter&utm_medium=social
- [169] Mitigating the BEAST attack on TLS [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://community.qualys.com/blogs/securitylabs/2011/10/17/mitigating-the-beast-attack-on-tls>
- [170] National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.cnss.gov/Assets/pdf/CNSSP_No%2015_minorUpdate1_Oct12012.pdf
- [171] National Institute of Standards and Technology , „ Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA–3) Family” Federal Register vol. 72, No. 212, Nov. 2007 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://csrc.nist.gov/groups/ST/hash/documents/FR_Notice_Nov07.pdf
- [172] New Collision attacks Against Up To 24-step SHA-2 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eprint.iacr.org/2008/270.pdf>
- [173] NIST Selects Winner of Secure Hash Algorithm (SHA-3) Competition [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.nist.gov/itl/csd/sha-100212.cfm>
- [174] NIST Special Publication 800-57, RECOMMENDATION FOR KEY MANAGEMENT Part 3: Application-Specific Key Management Guidance [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf
- [175] On the Security of RC4 in TLS [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.isg.rhul.ac.uk/tls/>
- [176] Pending Certificate List [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.mozilla.org/projects/security/certs/pending/#E-ME>
- [177] Practical Electro-Magnetic Analysis Non-Invasive Attack Testing Workshop NIAT-2011 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/03_deBeer.pdf
- [178] Proposal for a European Parliament and Council Directive on a common framework for electronic signatures/* COM/98/0297 final - COD 98/0191 */[tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur->

lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=EN&type_doc=COMfinal&an_doc=1998&nu_doc=297

[179] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0136:FIN:EN:PDF>

[180] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=EN&type_doc=COMfinal&an_doc=2012&nu_doc=238

[181] RC4 in TLS is Broken: Now What? [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://community.qualys.com/blogs/securitylabs/2013/03/19/rc4-in-tls-is-broken-now-what>

[182] Recommendation for Key Management – Part 1: General (Revision 3) [tiešsaiste, atvērt sp800-57_part1_rev3_general.pdf dokumentu]. - [atsauce 25.05.2013.]. Pieejams: <http://csrc.nist.gov/publications/PubsSPs.html#800-57-part1>

[183] Recommendation for Key Management: Part 2: Best Practices for Key Management Organization [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.sslcertificate.com/knowledgebase-category.html?category_id=570 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams:

[184] Romain Bardou et al, Efficient Padding Oracle Attacks on Cryptographic Hardware [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://hal.inria.fr/docs/00/70/47/90/PDF/RR-7944.pdf>

[185] SHA-3 Competition (2007-2012) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://csrc.nist.gov/groups/ST/hash/sha-3/index.html>

[186] SHA-3 Selection Announcement [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_selection_announcement.pdf

[187] Slaying BEAST: Mitigating the latest SSL/TLS Vulnerability [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://blog.phonefactor.com/2011/09/23/slaying-beast-mitigating-the-latest-ssl-tls-vulnerability/>

[188] SSL BEAST [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.webopedia.com/TERM/S/ssl_beast.html

[189] SSL Server Rating Guide [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide_2009c.pdf

[190] SSL Server Test [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <https://www.ssllabs.com/ssltest/analyze.html?d=ibanka.seb.lv%20>[18

[191] Symantec Completes Acquisition of VeriSign's Security Business [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.symantec.com/about/news/release/article.jsp?prid=20100809_01

[192] The 15 worst data security breaches of the 21st Century [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the-21st-century>

[193] The BEAST summary - TLS, CBC, Countermeasures (Update 4) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://blog.zoller.lu/2011/09/beast-summary-tls-cbc-countermeasures.html>

[194] The BEAST summary - TLS, CBC, Countermeasures (Update 4) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://phiral.net/Beast-SSL.rar>

[195] Timeline of AP hacking, reaction [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.usatoday.com/story/tech/2013/04/23/ap-twitter-hack-was-trivial/2107427/>

[196] TURKTRUST CA Problems [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: http://www.securelist.com/en/blog/208194063/TURKTRUST_CA_Problems

[197] Verisign authentication services [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.verisign.com/>

[198] VeriSign hit by hackers [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://blogs.csoonline.com/data-protection/2013/verisign-hit-hackers>.

[199] Vulnerability Summary for CVE-2011-3389 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3389>

[200] Vulnerability Summary for CVE-2013-2566 [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566>

[201] What is Inside View Vulnerability and How Can You Prevent It? [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://www.guidance-consulting.com/articles/85-inside-view-vulnerability.html>

[202] What's the deal with 2048-bit keys [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://ssl.entrust.net/blog/?p=107>

[203] Windows Root Certificate Program - Members List (All CAs) [tiešsaiste]. - [atsauce 25.05.2013.]. Pieejams: <http://social.technet.microsoft.com/wiki/contents/articles/2592.windows-root-certificate-program-members-list-all-cas.aspx>

PIELIKUMI

1. pielikums. Portāla Eparaksts.lv SSL sertifikāts 1 [145]

```
C:\>"C:\Program Files\GnuWin32\bin\openssl.exe" x509 -in  
C:\eparakstslv_ssl_sertifikats\VeriSignClass3PublicPrimaryCertifica  
tionAuthority-G5.crt -noout -text
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

18:da:d1:9e:26:7d:e8:bb:4a:21:58:cd:cc:6b:3b:4a

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For
authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5

Validity

Not Before: Nov 8 00:00:00 2006 GMT

Not After : Jul 16 23:59:59 2036 GMT

Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006
VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Cer
tification Authority - G5

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

Modulus (2048 bit):

00:af:24:08:08:29:7a:35:9e:60:0c:aa:e7:4b:3b:
4e:dc:7c:bc:3c:45:1c:bb:2b:e0:fe:29:02:f9:57:
08:a3:64:85:15:27:f5:f1:ad:c8:31:89:5d:22:e8:
2a:aa:a6:42:b3:8f:f8:b9:55:b7:b1:b7:4b:b3:fe:
8f:7e:07:57:ec:ef:43:db:66:62:15:61:cf:60:0d:
a4:d8:de:f8:e0:c3:62:08:3d:54:13:eb:49:ca:59:
54:85:26:e5:2b:8f:1b:9f:eb:f5:a1:91:c2:33:49:
d8:43:63:6a:52:4b:d2:8f:e8:70:51:4d:d1:89:69:
7b:c7:70:f6:b3:dc:12:74:db:7b:5d:4b:56:d3:96:
bf:15:77:a1:b0:f4:a2:25:f2:af:1c:92:67:18:e5:
f4:06:04:ef:90:b9:e4:00:e4:dd:3a:b5:19:ff:02:
ba:f4:3c:ee:e0:8b:eb:37:8b:ec:f4:d7:ac:f2:f6:
f0:3d:af:dd:75:91:33:19:1d:1c:40:cb:74:24:19:
21:93:d9:14:fe:ac:2a:52:c7:8f:d5:04:49:e4:8d:
63:47:88:3c:69:83:cb:fe:47:bd:2b:7e:4f:c5:95:

ae:0e:9d:d4:d1:43:c0:67:73:e3:14:08:7e:e5:3f:
9f:73:b8:33:0a:cf:5d:3f:34:87:96:8a:ee:53:e8:
25:15

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

X509v3 Key Usage: critical

Certificate Sign, CRL Sign

1.3.6.1.5.5.7.1.12:

0_].[0Y0W0U..image/gif0!0.0...+.....k...j.H.,{..0%.#ht

tp://logo.verisign.com/vslogo.gif

X509v3 Subject Key Identifier:

7F:D3:65:A7:C2:DD:EC:BB:F0:30:09:F3:43:39:FA:02:AF:33:31:33

Signature Algorithm: sha1WithRSAEncryption

93:24:4a:30:5f:62:cf:d8:1a:98:2f:3d:ea:dc:99:2d:bd:77:
f6:a5:79:22:38:ec:c4:a7:a0:78:12:ad:62:0e:45:70:64:c5:
e7:97:66:2d:98:09:7e:5f:af:d6:cc:28:65:f2:01:aa:08:1a:
47:de:f9:f9:7c:92:5a:08:69:20:0d:d9:3e:6d:6e:3c:0d:6e:
d8:e6:06:91:40:18:b9:f8:c1:ed:df:db:41:aa:e0:96:20:c9:
cd:64:15:38:81:c9:94:ee:a2:84:29:0b:13:6f:8e:db:0c:dd:
25:02:db:a4:8b:19:44:d2:41:7a:05:69:4a:58:4f:60:ca:7e:
82:6a:0b:02:aa:25:17:39:b5:db:7f:e7:84:65:2a:95:8a:bd:
86:de:5e:81:16:83:2d:10:cc:de:fd:a8:82:2a:6d:28:1f:0d:
0b:c4:e5:e7:1a:26:19:e1:f4:11:6f:10:b5:95:fc:e7:42:05:
32:db:ce:9d:51:5e:28:b6:9e:85:d3:5b:ef:a5:7d:45:40:72:
8e:b7:0e:6b:0e:06:fb:33:35:48:71:b8:9d:27:8b:c4:65:5f:
0d:86:76:9c:44:7a:f6:95:5c:f6:5d:32:08:33:a4:54:b6:18:
3f:68:5c:f2:42:4a:85:38:54:83:5f:d1:e8:2c:f2:ac:11:d6:
a8:ed:63:6a

2. pielikums. Portāla eparaksts.lv SSL Sertifikāts nr.2 [165]

```
C:\>"C:\Program Files\GnuWin32\bin\openssl.exe" s_client -showcerts -connect epa
raksts.lv:443
```

Loading 'screen' into random state - done

CONNECTED(00000730)

depth=2 /C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5

verify error:num=20:unable to get local issuer certificate

```
verify return:0
```

— — —

Certificate chain

0 s:/C=LV/ST=Riga/L=Riga/O=Valsts AS Latvijas Valsts radio un televīzijas centr
s/OU=Sertifikācijas pakalpojumu daļa/OU=Terms of use at www.verisign.com/rpa (c)
05/CN=www.eparaksts.lv

i:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://
www.verisign.com/rpa (c)10/CN=VeriSign Class 3 Secure Server CA - G3

-----BEGIN CERTIFICATE-----

MlIF+TCCBOGgAwIBAgIQRe2iYwqi6nQg40UbotscoDANBgkqhkiG9w0BAQUFADCBC
tTELMakGA1UEBhMCVVMxZmFzAVBgNVBAAoTDIzlcmITaWduLCBJbmMuMR8wHQYDVQQLEwExZWZXXJpU2lnbiBUcnVzdCBOZXRX3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2UgYXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykyMDEvMC0GA1UEAxMmVmVyaVNpZ24gQ2xhc3MgMyBTZWNN1cmUGU2VydmVyeIENBIC0gRzMwHhcNMTE5MDAwMDAwWHcNMTCxMTE3MjM1OTU5WjCB5TELMakGA1UEBhMCCTFYxDALBgNVBAGTBFIJpZ2ExDTALBgNVBAcUBFIJpZ2ExPjA8BgNVBAAoUNVZhbnHN0cyBBUyBMYYXR2aWphcyBWYWxzZHMgcmlkaW8gdW4gdGVsZXZpemlqYXMgY2VudHJzMSgwJgYDVQQLFb9TZXJ0aWZpa2FjaWphcyBwYWthbHBvanVtdSBkYWxhMTMwMQYDVQQLFb9TZXJtcyBvZiB1c2UgYXQgd3d3LnZlcmlzaWduLmNvbS9ycGEgKGMpMDUxGTAXBgNVBAMUEHd3dy5lcGFyYWtzdHMubHYwgEiMA0GCSqGSIsb3DQEBAQUAA4IBDwAwggEKAAoIBAQDLQ2jiPoDWuug+9+wRo6UekPhVQwS4jqgmK0/C59ictJ8jdTrZ3mOVaz379F52Qe+b nP8vYfvnGOAPHzvHTZepgJnVSK0Il6ItRuVaVRgYl5z3hBeftzNmXB+yda2r12U/QAL7fdxG42nZzVfyf5blfUbF1rZFVNK7X0Jya3Xh4cJn4wzhNT5x+y/MPbU6IGjrARgWtYXeQ++rYCJZ/wyR/8eWe8M/vwk3x8b+ZdM3BdjEYSMeT9ywa+dd/gjtHOLMu4Q1xyNdM6kngkpVll6nQeUKv7xeWK/JZJQ0z8BnP9XFHADhLw8irdPMV3/GU7UaKCdUVyaoDKQxEEwMxOexAgMBAAGjggHRMIIBZTAJBgNVHRMEAjAAMAsGA1UdDwQEAwIfFoDBFBgNVHR8EPJA8MDqgOKA2hjRodHRwOi8vU1ZSU2VjdXJILUczLWNybC52ZXJpc2lnbi5jb20vU1ZSU2VjdXJIRzMuY3JsMEQGA1UdIAQ9MDswOQYLIZIAYb4RQEHFwMwKjAoBggrBgEFBQCcARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYTAdBgNVHSUEFjAUBggrBgEFBQCDAQYIKwYBBQUHAwIwHwYDVR0jBBgwFoAUDURcFINEwYJ+HSCrJfObY9i+eaUwdgYIKwYBBQUHAOEaiBoMCOGCCSGAQUFbZABhhho

dHRwOi8vb2NzcC52ZXJpc2lnbi5jb20wQAYIKwYBBQUHMAKGNh0dHA6Ly9TVIJT
ZWN1cmUtRzMtYWlhLnZlcmlzaWduLmNvbS9TVIJTZWN1cmVHMy5jZXIwbGyYIKwYB
BQUHAQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUS2u5
KJYGDlvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3Zz
bG9nbzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQCqEWesrBJD5nwfMtInwpO4tQct
vLD0zpDbQ7VbNX1E1ge9x2QzkkzC7yrYd6YLaRk/aASEbfwMMW4ZrS2yjBrbK/qP
jVzfs3VROfObf9aNqbE/BqgC3iuaPk+6vU6PIJkUp/rdTtM/sX11XqW+gl1IRUEI
YZCiv5ckdCVQdHMQFaOE7xZNEWWM4TeY2FAL7hFLLRPkRgANqxcfcFFO5r1gxH0K
1oz2yOTKvcT9+WqbUoVSDhrZidKZLrppB6K3SHSoj6z+eG53xKJEiYImZUm/Ot8q
CV170y2WyXr1OH47ScAG8BAOvkMhpHLHXmC/vktYy9MGCbvHihXXJV/8W40o
-----END CERTIFICATE-----

1 s:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://
www.verisign.com/rpa (c)10/CN=VeriSign Class 3 Secure Server CA - G3
i:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc.
- For authorized use only/CN=VeriSign Class 3 Public Primary Certification Auth
ority - G5
-----BEGIN CERTIFICATE-----

MIIF7DCCBNsgAwIBAgIQbsx6pacDIam4zrz06VLUKTANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxZzAVBgNVBAoTDIzlcm1TaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWXZJp
U2lnbiwgSW5jLiAtIEZvciBhdXR0b3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmtpYyBQcm1tYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwWhcNMjAwMjA3MjM1OTU5WjCBtTEL
MAkGA1UEBhMCVVMxZzAVBgNVBAoTDIzlcm1TaWduLCBJbmMuMR8wHQYDVQQLExZW
ZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXRJcyBvZiB1c2UgYXQg
aHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYyYkxMDEvMC0GA1UEAxMmVmV
aVNpZ24gQ2xhc3MgMyBTZW51cmUgU2VydMvYIENBIC0gRzRwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCh4QfwgxF9byrJZenraI+nLr2wTm4i8rCrFbG
5bt1jRPTc5v7QIK1K9OEJxoiy6Ve4mbE8riNDTB81vzSXtig0iBdNGIeGwCU/m8
f0MmV1gzgzsChew0E6RJK2GfWQS3HRKNKEdCuqWHQsV/KNLO85jiND4LQyUhhDK
tpo9yus3nABINYyPUHjoRWPNGUFP9ZXse5jUxHGzUL4os4+guVOc9cosI6n9FAbo
GLSa6Dxugf3kzTU2s1HTaewSulZub5tXxYsU5w7HnO1KVGrJTcW/EbGuHGeBy0RV
M5I/JJs/U0V/hhrzPPptf4H1uErT9YU3HLWm0AnkGHs4TvoPAgMBAAGjggHfMIIB
2zA0BggrBgEFBQcBAQQoMCYwJAYIKwYBBQUHMAKGNh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTASBgNVHRMBAf8ECDAGAQH/AgEAMHAGA1UdIARpMGcwZQYLYIZIAyB4
RQEHFwMwVjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nw
czAqBggrBgEFBQcCAjAeGhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMDQG
A1UdHwQtMCswKAAwCwGI2h0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMtZzUu
Y3JsMA4GA1UdDwEB/wQEAwIBBjBtBggrBgEFBQcBDARhMF+hXaBbMFkwVzBVFglp
bWFnZS9naWYwITAfMAcGBSsOAwIaBBSP5dMahqyNjmvDz4Bq1EgYlHsZLjAlFiNo
dHRwOi8vbG9nbz52ZXJpc2lnbi5jb20vbnNsb2dvLmdpZjZjAoBgNVHREEITAfB0w
GzEZMBcGA1UEAxMQVmVyaVNpZ25NUETJLTItNjAdBgNVHQ4EFgQUUDURcFINEwYJ+

HSCrJfQBY9i+eaUwHwYDVR0jBBgwFoAUf9Nlp8Ld7LvWMAnzQzn6Aq8zMTMwDQYJ
KoZIhvcNAQEFBQADggEBAAyDJO/dwwzZWJz+NrbrioBL0aP3nfPMU++CnqOh5pfB
WJ11bOAdG0z60cEtBcDqbrlicFXZIDNAMwfCZYP6j0M3m+oOmmxw7vacgDvZN/R6
bezQGH1JSsqZxxkoor7YdyT3hSaGbYcFQEFn0Sc67dxIHSLNCwuLvPSxe/20majp
dirhGi2HbnTTiN0eIsbfFrYrghQKIFzyUOyvzv9iNw2tZdMGQVPtAhTItVgooazg
W+yzf5VK+wPlrSbb5mZ4EkrZn0L74ZjmQoObj49nJOhhGbXdzbULJgWOw27EyHW4
Rs/iGAZeqa6ogZpHFt4MKGwlJ7net4RYxh84HqTEy2Y=

-----END CERTIFICATE-----

2 s:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc.

- For authorized use only/CN=VeriSign Class 3 Public Primary Certification Auth

ority - G5

i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority

-----BEGIN CERTIFICATE-----

MIIE0DCCBDmgAwIBAgIQJQzo4DBhLp8rftXz4/TANBgkqhkiG9w0BAQUFADBf
MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAsT
LkNsYXNzIDMgUHVibGljIFByaW1hcngQ2VydGlmaWNhdGlubiBBdXRob3JpdHkw
HhcNMDYxMTA4MDAwMDAwWhcNMjExMTA3MjM1OTU5WjCBYjELMAkGA1UEBhMCVVMx
FzAVBgNVBAoTDlZlcm1TaWduLCBJbmMuMR8wHQYDVQQLEwZWZXJpU2lnbiBUcnVz
dCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2lnbiwSW5jLiAtIEZv
ciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzZWZXJpU2lnbiBDbGFzcyAz
IFB1YmtpYyBQcm1tYXJ5IENlcjZmljYXRpb24gQXV0aG9yaXR5IC0gRzUwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAgIKXo1nmAMqudL007cfLw8
RRy7K+D+KQL5VwijZIUUVJ/XxrcxiV0i6CqqpKzj/i5Vbext0uz/o9+B1fs70Pb
ZmlVYc9gDaTY3vjgw2IIPVQT60nKWVSfJuUrjxuf6/WhkeIzSdhDY2pSS9KP6HBR
TdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KII8q8ckmcY5fQGBO+QueQA5N06tRn/
Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+rCpSx4/VBEnkjWNH
iDxp8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7IP59zuDMKz10/NieWiu5T6CUVAgMB
AAGjggGbMIIBlZAPBgNVHRMBAf8EBTADAQH/MDEGA1UdHwQqMCgwJqAkoCKGIGh0
dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA4GA1UdDwEB/wQEAwIBBjA9
BgNVHSAENjA0MDIGBFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuVyaXNpZ24uY29t
aXNpZ24uY29tL2NwczAdBgNVHQ4EFgQUf9Nlp8Ld7LvWMAnzQzn6Aq8zMTMwbQYI
KwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQU
j+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9nby5naWYwNAYIKwYBBQUHAQEEDAmMCQGCCsGAQUFBzABhhodHRwOi8v
b2NzcC52ZXJpc2lnbi5jb20wPgYDVR0lBDcwNQYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDAwYJYIZIA Yb4QgQBBgpgkhgBhvhFAQgBMA0GCSqGSIb3DQEBAQUA
A4GBABMC3fjohgDyWvj4IAxZiGIHs73Tvm7WaGY5eE43U68ZhjTresY8g3JbT5K
ICDDPLq9ZVTGr0SzEK0saz6r1we2uIFjxflLuUqZ87NMwwq14lWAyMfs77oOghZ
tOxFNfeKW/9mz1Cvxm1XjRI4t7mi0VfqH5pLr7rJhJ+xr3/

-----END CERTIFICATE-----

Server certificate

subject=/C=LV/ST=Riga/L=Riga/O=Valsts AS Latvijas Valsts radio un televizijas ce
ntrs/OU=Sertifikācijas pakalpojumu daļa/OU=Terms of use at www.verisign.com/rpa
(c)05/CN=www.eparaksts.lv
issuer=/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https
://www.verisign.com/rpa (c)10/CN=VeriSign Class 3 Secure Server CA - G3

No client certificate CA names sent

SSL handshake has read 4987 bytes and written 322 bytes

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA

Server public key is 2048 bit

Compression: NONE

Expansion: NONE

SSL-Session:

Protocol : TLSv1

Cipher : DHE-RSA-AES256-SHA

Session-ID: DDA8191EB1CE0421934CC75AC2B8F94C72BA860E82921854B77B2DC57ADF9584

Session-ID-ctx:

Master-Key: C7F3D60BA68AADCB13B460BAE80B0DD4EC3345662D4297A8BE3B4532909A3303
1BD00C4E5DCE4707A31B1D2D7BF91A6A

Key-Arg : None

Start Time: 1366656045

Timeout : 300 (sec)

Verify return code: 20 (unable to get local issuer certificate)

3. pielikums. SSL pārbaužu kopsavilkuma tabula

	GlobalSign	Qualys SSL Labs	SSLShopper	BlueSSL	Digicert	Wormly	VeriSign	Secure128	Networking4all	GOGETSSL	The H Security	COMODO
Overall rating	F	F	-	-	-	79%	-	-	7/11	-	-	-
SSL Certificate is not expired	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed
Site is listed in the certificate	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed
Organisation details are listed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed
Encryption strength is at least 1024-bit	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed
Signature Algorithm is strong	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed
Accepting low encryption cipher suites	ALARM	ALARM	-	-	-	ALARM	-	-	ALARM	-	-	ALARM
No Debian weak key present	Passed	Passed	-	-	-	-	-	-	Passed	-	-	-
No known security issues for this Certificate Authority	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed	Passed
SSL 2.0	Failed	Failed	-	-	-	Failed	-	-	-	-	-	Failed
SSL 3.0	Passed	Passed	-	-	-	Passed	-	-	-	-	-	Passed
Compression(CRIME attack vulnerability)	Failed	Failed	-	-	-	-	-	-	-	-	-	Failed
BEAST attack vulnerability	Failed	Failed	-	-	-	-	-	-	-	-	-	-
URL	https://ssllcheck.globalsign.com/en_US/sslcheck?host=www.eparaksts.lv	https://www.ssllabs.com/ssltest/analyze.html?d=www.eparaksts.lv	https://www.bluessl.com/en/ssltest	https://www.bluessl.com/en/ssltest	http://www.digicert.com/help/	https://www.wormly.com/test_ssl/https://www.eparaksts.lv/i/195.244.147.25/p/443	https://ssl-tools.verisign.com/#certChecker	http://www.secure128.com/resource/ssl-certificate-installation-checker.aspx	http://www.networking4all.com/en/support/tools/site+check/report/?fqdn=www.eparaksts.lv&protocol=https	http://www.gogotssl.com/check-ssl-installation/	http://www.h-online.com/nettools/tools	https://sslanalyzer.comodoca.com/?url=www.eparaksts.lv

4. pielikums. KPMG Vērtējums par USPS atbilstību 2005. Gada 12. Jūlija Ministru kabineta noteikumiem Nr.514 [41,54]



KPMG Baltica SIA
Vesetas iela 7, Rīga, LV-1013_Latvija

Tālrunis +371 67038000_Fakss +371
67038002_Internets www.kpmg.lv

Jānim Boktam
VAS "Latvijas Valsts radio un televīzijas centrs"
valdes priekšsēdētājam
Ērgļu iela 7,
Rīga, LV-1012

Mūsu ats. 07-2012/01

2012. gada 24. aprīlis

A. god. Boktas kungs

Vērtējums par USPS atbilstību 2005. gada 12. jūlija Ministru kabineta noteikumiem Nr.514

Saskaņā ar noslēgto līgumu 2011. gada 10. novembrī noslēgto līgumu Nr. ESP- 2011/10 starp VAS "Latvijas Valsts radio un televīzijas centru (turpmāk LVRTC) un SIA KPMG Baltics (turpmāk KPMG), KPMG no 2. marta līdz 24. aprīlim veica LVRTC sertifikācijas pakalpojuma sniedzēja (turpmāk LVRTC SPS) CA auditu, kura laikā novērtēja LVRTC SPS izstrādātās procedūras, ieviestās kontroles, kā arī izstrādātās drošības prasības sertifikācijas pakalpojumu sniegšanai. Audita pamatā tika izmantota KPMG izstrādāta, uz „WebTrust for Certification Authorities” programmu balstīta novērtēšanas matrica, kas pilnībā iekļauj prasības, kas minētas sertifikācijas pakalpojumu sniegšanas noteikumos.

Detalizēts KPMG atzinums tika nodots LVRTC SPS 2012. gada 24. aprīlī. Mūsu atzinums neiekļauj izmaiņas procedūrās un kontrolēs, ja tās tikušas ieviestas pēc 2012. gada 24. aprīļa. Mēs veicām auditu saskaņā ar attiecīgiem starptautiskiem CA audita veikšanas standartiem, kas iekļāva procedūras, kuras mēs uzskatījām par nepieciešamām, lai iegūtu pietiekamu informācijas un pierādījumu kopumu, uz kura varētu balstīt mūsu atklājumus un rekomendācijas.

LVRTC SPS procedūras bija visaptverošas un detalizētas, tās iekļāva nepieciešamās politikas, instrukcijas LVRTC SPS darbiniekiem, kā arī dažādus organizatoriskus un sistēmas arhitektūras dokumentus. No saņemtajām un analizētajām procedūrām un veiktajiem testiem KPMG bija iespējams izprast arī LVRTC SPS informācijas sistēmas detalizētu uzbūvi.

Audita laikā mēs ieguvām pārliecību, ka LVRTC SPS kontroles un procedūras ir pietiekamas un atbilstošas gan Latvijas Republikas normatīvajiem aktiem, gan attiecīgiem starptautiskajiem standartiem uz 2012. gada 24. aprīli, lai sniegtu profesionālu, kvalitatīvu un drošu pakalpojumu.

KPMG Baltica SIA, Latvijā reģistrēta sabiedrība ar ierobežotu atbildību un KPMG neatkarīgu dalībnieku, kuras sastāvā ir Šveices uzņēmumu KPMG International Cooperative (KPMG International), tās daļbaltne

Tomēr audita laikā KPMG atklāja atsevišķas jomas, kuras tuvākajā laikā būtu jāuzlabo vai jāpapildina kontroles:

Latvijas nacionālajam standartam LVS ETSI TS 101 456 "Politikas prasības sertifikācijas pakalpojumu sniedzējiem, kas izsniedz kvalificētos sertifikātus" (ETSI TS 101 456)

- USPS darbībā nav atklātas neatbilstības standartā izvirzītajām prasībām.

Latvijas nacionālajam standartam LVS ETSI TS 102 023 "Politikas prasības laika zīmoga pakalpojumu sniedzējiem" (ETSI TS 102 023)

- USPS darbībā nav atklātas neatbilstības standartā izvirzītajām prasībām.

Latvijas nacionālajam standartam LVS ISO/IEC 17799 "Informācijas tehnoloģija. Prakses kodeksa informācijas drošības pārvaldībai";

- SPS izmantotās produkcijas videi programmatūras jauninājumi tiek uzstādīti neregulāri. Šī ir neatbilstība LVS ISO/IEC 17799 sadaļai 12.6
- Darbības nepārtrauktības plāns, iespējams, ir neaktuāls, jo satur neaktuālas atsauces uz citām procedūrām, novecojušu informāciju par iesaistītajiem darbiniekiem, nesatur atsauces uz esošajiem plāniem. Šis atklājums tika konstatēts arī iepriekšējā akreditācijas auditā; Šī ir neatbilstība LVS ISO/IEC 17799 sadaļai 14.1.5.

Latvijas nacionālajam standartam LVS CWA 14167-1:2004 "Drošības prasības uzticamām elektronisko parakstu sertifikātu pārvaldības sistēmām. 1.daļa: Vispārīgas drošības prasības";

- USPS darbībā nav atklātas neatbilstības standartā izvirzītajām prasībām.

Latvijas nacionālajam standartam LVS CWA 14167-2:2004 "Drošības prasības uzticamām elektronisko parakstu sertifikātu pārvaldības sistēmām. 2.daļa: Kriptogrāfiskais modulis parakstīšanas operācijām, ko īsteno sertifikācijas pakalpojumu sniedzēji. Aizsardzības profils (MCSO-PP)"

- USPS darbībā nav atklātas neatbilstības standartā izvirzītajām prasībām.

Latvijas nacionālajam standartam LVS ISO/IEC 12207 "Informācijas tehnoloģija. Programmatūras dzīves cikla procesi".

- USPS darbībā nav atklātas neatbilstības standartā izvirzītajām prasībām.

ABCD

Jānim Bokšam
*Vērtējums par U.S.P.S atbilstību 2005. gada 12. jūlija
Ministru kabineta noteikumiem Nr. 514
2012. gada 24. aprīlis*

Jebkuras izmaiņas LVRTC SPS aprakstītajās kontrolēs, turpmāka projekta attīstība vai informācijas izmaiņas var radīt jaunus riskus, jo esošās kontroles var kļūt neatbilstošas, kā arī atbilstība pret standartiem var mainīties. Mūsu LVRTC SPS procedūru un kontroles novērtējums pret Sertifikācijas pakalpojumu sniegšanas noteikumiem neaizsargā LVRTC SPS pret neatbilstību nākotnes standartiem un pret iespējamām sistēmas kļūdām vai krāpšanas gadījumiem.

Šis atzinums ir veidots LVRTC SPS vadībai iesniegšanai Datu valsts inspekcijai akreditācijai. Izņemot akreditācijas vajadzībām, bez KPMG iepriekšējas rakstiskas piekrišanas, to nedrīkst citēt, atsaukties uz to vai nodot jebkurai trešajai pusei.

Šis atzinums ir parakstīts ar drošu elektronisko parakstu.

Ar cieņu,

Armine Movsisjāna
Partnere

5. pielikums. Open ID tīmekļa vietnes informācija (www.open-id.lv)

Par mums - SIA "Open ID" - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Par mums - SIA "Open ID"

open-id.lv/par-mums

Google

OPEN ID

PAR MUMS
PROJEKTI
VAKANCES
KONTAKTI

Par OPEN ID

2010. gadā tika dibināts jauns, inovatīvs, spēcīgs un strauji augošs uzņēmums SIA „OPEN ID”.

SIA „OPEN ID” ir uzņēmums, kurā apvienotas zināšanas, nepieciešamās iemaņas un pieredze, lai īstenotu ikviena klienta pārdrošākās idejas IT pasaulē. Mēs piedāvājam daudzveidīgu risinājumu klāstu un dažādu tehnoloģiju apvienojumus mūsu projektos. Mēs rūpējamies ne tikai par veiksmīgu projektu ieviešanu, bet arī par to uzturēšanu.

SIA "OPEN ID" mērķis ir sasniegt komfortablu sadarbību ar saviem klientiem, kā rezultātā mūsu attīstītie projekti būtu pieejami un saprotami pēc iespējas plašākam iedzīvotāju lokam. Esam veidojuši un stiprinājuši sadarbību ar vairākiem Latvijas IT uzņēmumiem un valsts iestādēm, kā rezultātā ir plašas zināšanas par tendencēm kopējās industrijas attīstībā.

SIA „OPEN ID” ir veikts audits par tā atbilstību starptautiskajam standartam "ISO/IEC 12207:2008 Informācijas tehnoloģija – Programmatūras dzīves cikla procesi". Šāds audits atzinums apliecina uzņēmuma spēju nodrošināt saviem klientiem sistēmanalīzes, programmatūras projektēšanas, izstrādes, testēšanas un ieviešanas, klientu apkalpošanas, starptautiskam standartam atbilstošā kvalitātes un drošības līmeni.

Kompetence

- PKI projektu ieviešanā
- IS arhitektūras izstrādē
- IS izstrādē
- IS uzturēšanā
- Programmatūras risinājumi
- Datu uzturēšanas un drošības risinājumi

5 iemesli nākt pie mums

1. Pieredze + Uzticamība + Racionālas izmaksas = Kopējs ieguvums;
2. Profesionāla attieksme, un Jūs saņemsiet tieši to risinājumu, kas Jums ir nepieciešams;
3. Izdarīsim visu nepieciešamo, lai no Jūsu puses piepūle būtu minimāla;
4. Augsti vērtējam Jūsu laiku, naudu un mūsu savstarpējās attiecības;
5. Ar mums ir viegli strādāt. Mēs runājam klientam saprotamā valodā un informējam viņus par procesa gaitu.

Rekvizīti

/ SIA „OPEN ID”

VIENOTAIS REĢ. NR. 40103276621
MADONAS IELA 27 – 93, RĪGA, LV - 1084
NOR. KONTA NR. LV68HABA0551027797926
AS "SWEDBANK"; KODS: HABALV22

Projekti - SIA "Open ID" - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Projekti - SIA "Open ID"

open-id.lv/projekti

Google

OPEN ID

PAR MUMS
PROJEKTI
VAKANCES
KONTAKTI

Projekti

eParaksts



eParaksts ir unikāls, elektronisks personas identifikācijas apliecinājums, kas pievienots datorā sagatavotam dokumentam. eParaksts ir ar roku parakstīta dokumenta ekvivalents elektroniskā formātā un apliecina tā piederību konkrētai fiziskai personai, kas pārstāv juridisko personu. eParaksta izmantošana nodrošina elektroniskā dokumenta autentiskumu un apstiprina parakstītāja identitāti.

- eparaksts.lv

Pēc *VAS Latvijas Valsts radio un televīzijas centra* pasūtījuma izstrādājam Eiropā unikālu timekdi bāzētu elektroniskā paraksta risinājumu. Izstrādātais portāls ļauj cilvēkiem droši un juridiski saistoši parakstīt dokumentus, bez nepieciešamības iegādāties viedkaršu lasītājus un uztraukties par draiveru savietojamību ar lietotāja izmantoto operētājsistēmu. Atsakoties no viedkartēm, panākts ievērojami zemāks lietotāja izmaksu sliekšnis.

Izveidotais risinājums izmanto jau esošo E-Me infrastruktūru, tā panākot gan zemākas izmaksas no valsts puses, gan arī nodrošinot zemākas uzturēšanas izmaksas.

Projektā iesaistītie partneri:

- SIA Cube
- SIA Asketic
- SIA Euso

6. pielikums. EUSO izstrādātāja tīmekļa vietne (www.euso.lv)

EUSO • Informācijas Tehnoloģijas - elektroniskais paraksts, Java EDoc bibliotēkas, e-paraksta integrācija - Mozilla Fi...

File Edit View History Bookmarks Tools Help

www.euso.lv/pages/;jsessionid=43B6FF274F2E6BDC67DEDA8581FAFF84

Google



Informācijas Tehnoloģijas

LV EN

Par mums

Pakalpojumi

Produkti

Tehnoloģijas

Kontaktinformācija

KLIENTU ATBALSTS

Lietotāja vārds:

Parole:

Pieslēgties

JAVA RESURSI

- > Java
- > Oracle
- > IBM
- > JBoss.ORG



SIA "EUSO" ir IT uzņēmums, kas veic programmatūras risinājumu izstrādi un ieviešanu uzņēmumiem un valsts iestādēm.

Uzņēmums dibināts 2000. gadā ar mērķi attīstīt programmatūras izstrādes pakalpojumus uz J2EE tehnoloģijas platformas.

Galvenie darbības virzieni:

- Informācijas sistēmu izstrāde un ieviešana
- Datu apmaiņas sistēmu izstrāde un ieviešana
- E-komercijas risinājumu izstrāde un ieviešana
- Uzņēmumu lietojumprogrammu integrācija
- Konsultācijas IT risinājumu jautājumos



Esam kompetenti partneri elektroniskā paraksta ieviešanā – jaunu lietojumu izstrādē un integrācijā. VAS Latvijas Pasts uzdevumā esam izstrādājuši programmatūras komponentu **EDOC Java bibliotēkas**, kas nodrošina visas galvenās funkcijas elektronisko dokumentu apstrādei.

Izmantojot EDOC Java bibliotēkas, esam izstrādājuši lietojumprogrammu **SignAnywhere Free**, kas paredzēta elektroniskā paraksta pievienošanai dokumentiem, izmantojot E-ME izsniegtās viedkartes.

Esam izstrādājuši Microsoft .NET klašu bibliotēku **EDocLibraries.NET**, kas .NET programmatūras izstrādātājiem ļauj savos risinājumos ātri un vienkārši ieviest EDOC formāta elektronisko dokumentu veidošanas un pārbaudes funkcionalitāti.



Burtu ĀBECE iPhone, iPad, Android
Latviešu, krievu un angļu valodas burtu ābece pirmsskolas vecuma bērniem, kā arī pieaugušajiem.

Copyright © 2001 - 2013 SIA EUSO. All Rights Reserved.
Oracle and Java are registered trademarks of Oracle and/or its affiliates.

7. pielikums. Jāņa Boktas un Ilmāra Poikāna saruna par PIN drošību([twitter.com](https://twitter.com/ilmarmors/status/294814632907005954))

(<https://twitter.com/ilmarmors/status/294814632907005954>)



Ilmārs Poikāns
@ilmarmors

Follow

@JanisBokta Kādā formā lietotāja pārlūkprogrammā ievadītais virtuālā e-paraksta PIN kods tiek nosūtīts LVRTC?

Reply Retweet Favorite More

6:31 AM - 25 Jan 13



Janis Bokta @JanisBokta 25 Jan

@ilmarmors šifrētā veidā, visos posmos no klienta līdz hsm, sistēmas uzturētājs tam netiek klāt!

Details



Ilmārs Poikāns @ilmarmors 25 Jan

@JanisBokta V epar. lietotājs pēc dok. upload, lai to parakstītu, ievada PIN, ko pārlūks nosūta LVRTC serverim, kur kods to redz kādā formā?

Details



Janis Bokta @JanisBokta 26 Jan

@ilmarmors Vēlreiz, HSM iekārta v.parakstam ir EAL4+, tieši tāpat kā kartīgai! Sesijas laikā visas darbības tiek šifretas, arī PIN ievade!

Details



Ilmārs Poikāns @ilmarmors 26 Jan

@JanisBokta Laikam jāpārfrāzē jautājums - ja ir root pieeja uz eparaksts.lv, tad tiešām nekādi nav iespējams pārtvert virt.p. PIN?

Details



Janis Bokta @JanisBokta 27 Jan

@ilmarmors scenārijs tāds pats kā kartīgai, LVRTC netiek klāt klienta PIN!

Details

8. pielikums. Java eDoc bibliotēku licences līguma teksts

product: EDOC Java Libraries
version: 2.0
customer: Jebkura fiziska vai juridiska persona
type: Standard
number: ###
serial: *[serial number]*
validity: Perpetual
generated: *[licence generation date]*

JAVA programmatūras bibliotēka

Licencētais produkts: JAVA programmatūras bibliotēka
Produkta īpašnieks: VAS Latvijas Valsts Radio un Televīzijas centrs (LVRTC), vienotais reģ.nr. 40003011203
Licences lietotājs: Jebkura fiziska vai juridiska persona
Licences numurs: ###

LICENCES LĪGUMS

JAVA programmatūras bibliotēkas (turpmāk tekstā — „Bibliotēka”) Licences Līgums (turpmāk tekstā — “Līgums”)
ir līgums par LVRTC programmatūras izmantošanu, kas noslēgts starp Produkta īpašnieku un jebkuru produkta lietotāju, (turpmāk tekstā – Lietotājs). Bibliotēka ietver programmatūru, ieskaitot visus kļūdu labojumus,
jauninājumus un papildinājumus, kuri saņemti atbilstoši Līguma darbības laikā un atbilstoši noteikumiem, kā arī dokumentāciju papīra
vai elektroniskā formātā. Programmatūra, kas ietverta Bibliotēkā, tiek licencēta Līgumā noteikto programmatūras izmantošanas tiesību apjomā.
Lietojot Bibliotēku, Lietotājs ir pieņēmis LVRTC noteiktos Līguma noteikumus.
Ja Lietotājs nepiekrīt šī Līguma noteikumiem, tad Lietotājs nedrīkst izmantot Bibliotēku un 14 dienu laikā no Licences saņemšanas brīža tā jāatgriež LVRTC.
Līgums ir spēkā kopā ar LVRTC Licenci, kas tiek nosūtīta Lietotājam pēc Lietotāja pieprasījuma saņemšanas.
Līgums stājas spēkā ar brīdi, kad Licence ir nosūtīta Lietotājam un Bibliotēka ir sākusi darboties.

BIBLIOTĒKAS LICENCE

Bibliotēku aizsargā starptautiskie un Latvijas Republikā spēkā esošie normatīvie akti, kas regulē autortiesības, autortiesību līgumi, kā arī citi normatīvie akti, kas regulē intelektuālā īpašuma aizsardzību, un līgumi.
Bibliotēkas lietošana tiek licencēta, nevis pārdota.
1. LICENCES VISPĀRĒJIE NOTEIKUMI

Līgums piešķir Lietotājam šādas tiesības:

a) Lietotājam ir atļauts instalēt, lietot, piekļūt, darbināt un veikt citas darbības, kas saistītas ar Bibliotēkas lietošanu atbilstoši licences tipam, kāds norādīts šajā Līgumā

b) Visas tiesības, kas Lietotājam nav piešķirtas ar šo Līgumu, saglabā LVRTC.

c) Bibliotēka tiek licencēta kā vienots produkts un tās komponentus (moduļus) nedrīkst atdalīt, pārtaisīt vai izjaukt atsevišķi.

d) Sākotnējais Bibliotēkas Lietotājs var nodot Bibliotēkas Licenci saistību tiesību pārņēmējam. Šai atsavināšanai ir jāietver visi ar Bibliotēkas Licenci piegādātie materiāli (ieskaitot visas tā sastāvdaļas, drukātos materiālus, jauninājumus un šo Līgumu). Lietotājs apņemas nodrošināt, ka Licence ieguvējs pārņems visas ar šo Līgumu pielīgtais Lietotāja saistības izpildīt visus Līguma noteikumus. Bibliotēku nedrīkst ne iznomāt, ne patapināt, ne arī nodot trešajām personām nekādā citā veidā, kas nav norādīts Līgumā.

e) Lietotājam, pārkāpjot Līguma noteikumus, LVRTC ir tiesības vienpusēji, rakstveidā paziņojot Lietotājam, izbeigt šo Līgumu, vienlaicīgi anulējot izsniegto Licenci. Šādā gadījumā Lietotājam ir jāiznīcina visi Bibliotēkas un tās komponentu eksemplāri LVRTC noteiktajā termiņā.

f) Gadījumā, ja Bibliotēku nokopējusi vai instalējusi trešā puse Lietotāja vietā, tad Lietotājs ir atbildīgs par šīs trešās puses rīcību un tās nodarītajiem zaudējumiem. Lietotājs var nodot Bibliotēku kā nedalāmu komponenti trešajai pusei (programmatūras izstrādes kompānijai) tikai un vienīgi kā integrācijas elementu uz izstrādes brīdi Lietotāja lietojumprogrammās. Trešā puse (programmatūras izstrādes kompānija) programmatūras izstrādes laikā vai pēc tam nepārmanto Licence izmantošanas tiesības. Lietotājam ir jāveic visi iespējamie pasākumi, lai Lietotāja darbinieki, pārstāvji vai trešās puses lietotu Bibliotēku tikai atbilstoši Līguma noteikumiem.

2. AUTORTIESĪBAS

Visas autora mantiskās un personiskās tiesības uz Bibliotēku (ieskaitot pakotnē iekļautos failus), dokumentāciju un Bibliotēkas eksemplāriem pieder LVRTC, un tās aizsargā autortiesību un intelektuālā īpašuma tiesību reglamentējošie normatīvie akti un starptautiskie līgumi. Līgums piešķir Lietotājam tiesības uz šo Bibliotēku izmantošanu tikai tādā veidā, kā tas ir noteikts Līgumā.

3. JAUNINĀJUMI UN JAUNAS VERSIJAS

Lietotājam Licence Līguma darbības laikā ir tiesības saņemt visus sagatavotos kļūdu labojumus un jauninājumus bez maksas. Programmatūras jauninājumi pilnībā vai daļēji aizstāj esošo Bibliotēkas versiju.

Bibliotēkas jaunā versija ir tādu jauninājumu kopums, kas pilnībā aizstāj esošo Bibliotēkas versiju. Lai nodrošinātu pāreju uz Bibliotēkas jaunāko versiju, nepieciešama Jaunas versijas atjaunošanas licence.

Lietotājam pilnībā vai daļēji papildinot vai atjauninot Bibliotēku, jāievēro Līguma noteikumi.

4. KOPĒŠANA

Bibliotēkas vai tās komplektācijā iekļautos drukātos materiālus drīkst kopēt Lietotāja iekšējām vajadzībām, taču pašas Bibliotēkas autortiesības tiek aizsargātas ar speciālo programmatūras aizsardzības sertifikātu.

5. GARANTIJAS NOTEIKUMI

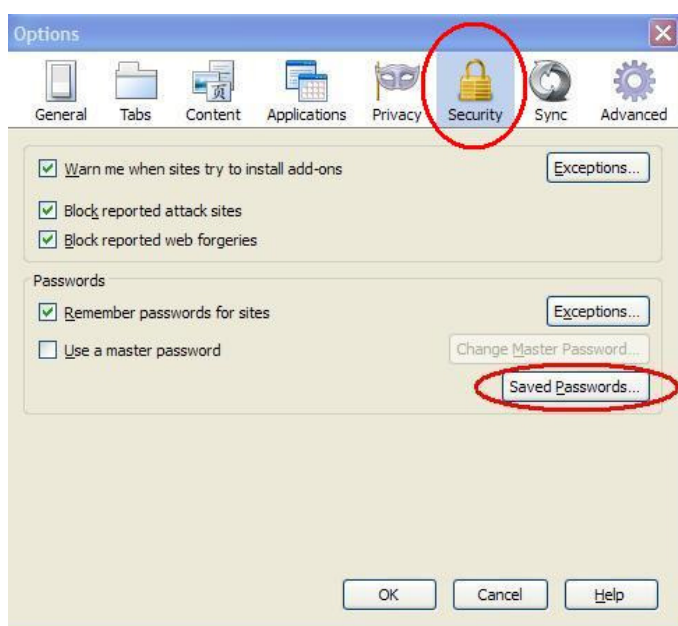
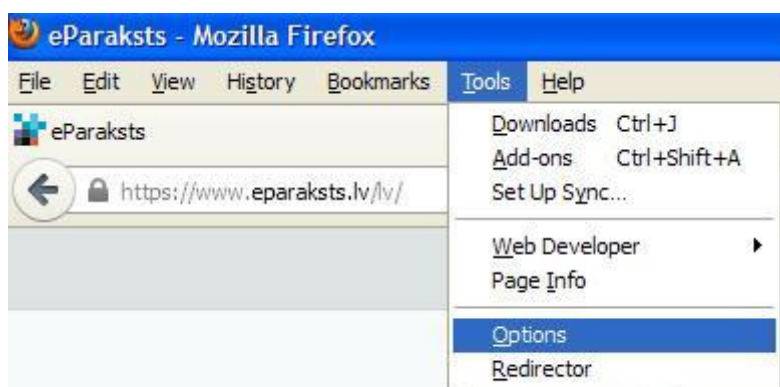
Bibliotēkas lietošana un tās piemērotība Lietotāja vajadzībām ir Lietotāja kompetencē.

LVRTC negarantē, ka Bibliotēka atbilst Lietotāja prasībām, ka tā ir bez kļūdām un ir pasargāta no darbības pārtraukumiem.

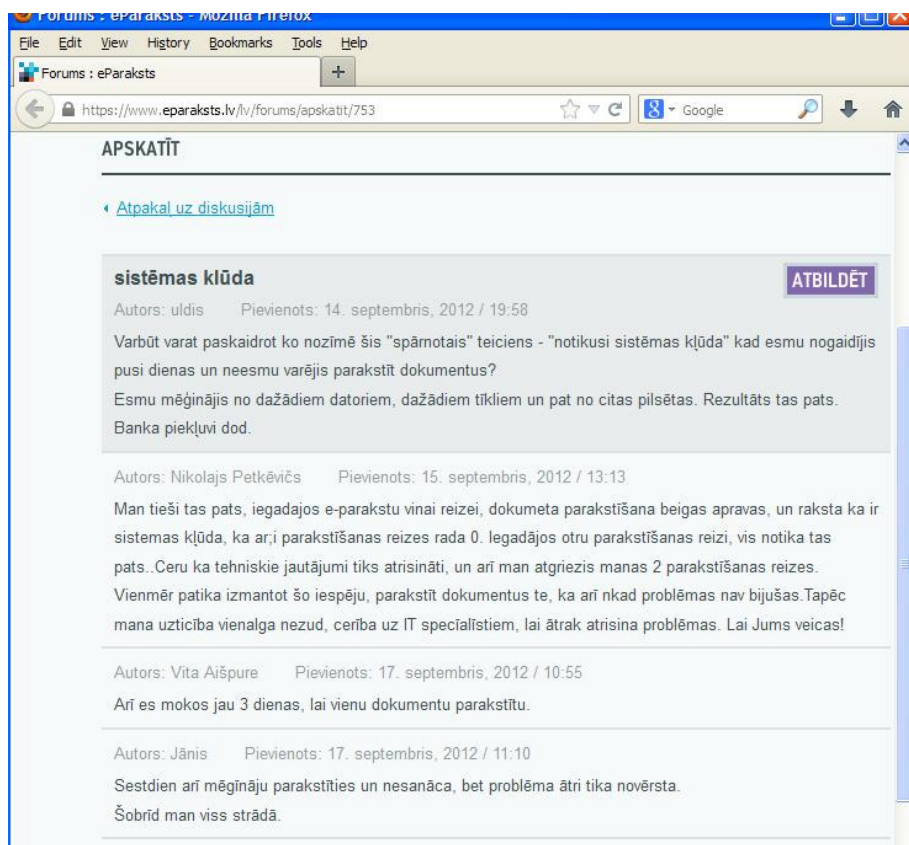
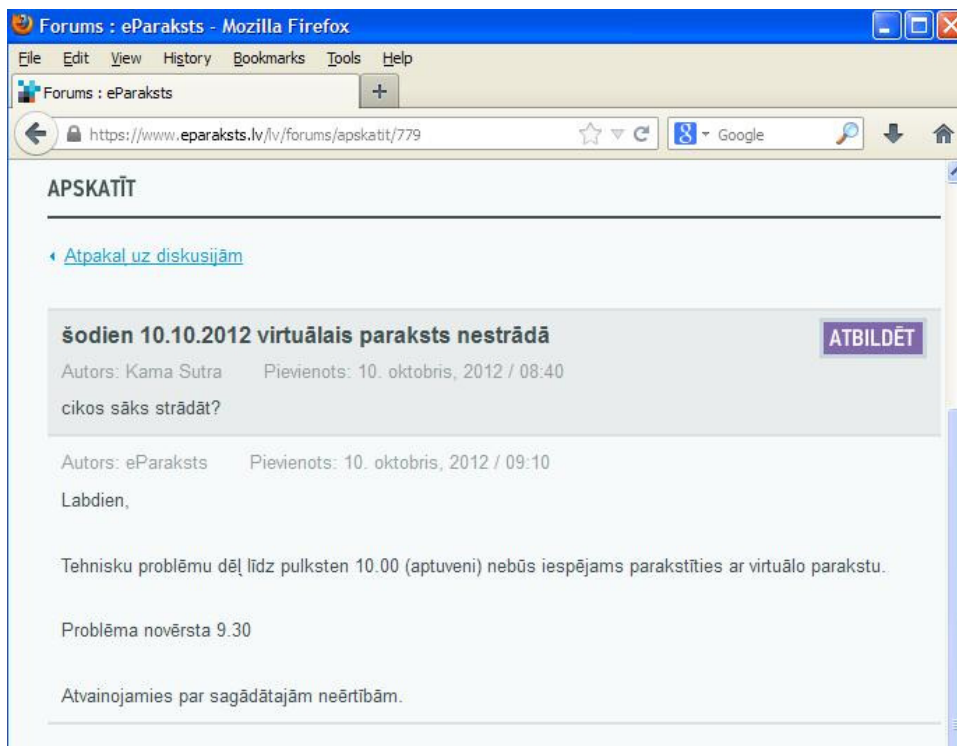
6. PREČU ZĪMES

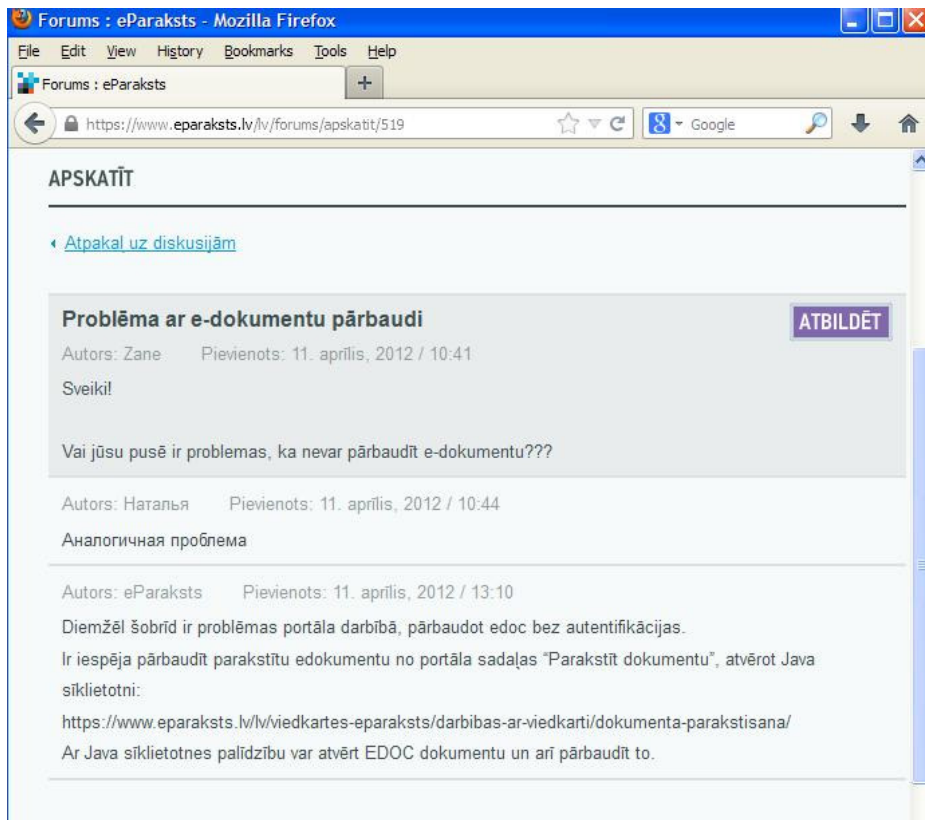
JAVA ir reģistrēta preču zīme. Arī citu produktu un firmu nosaukumi, kas minēti tekstā, var būt šo produktu un firmu īpašnieku preču zīmes.

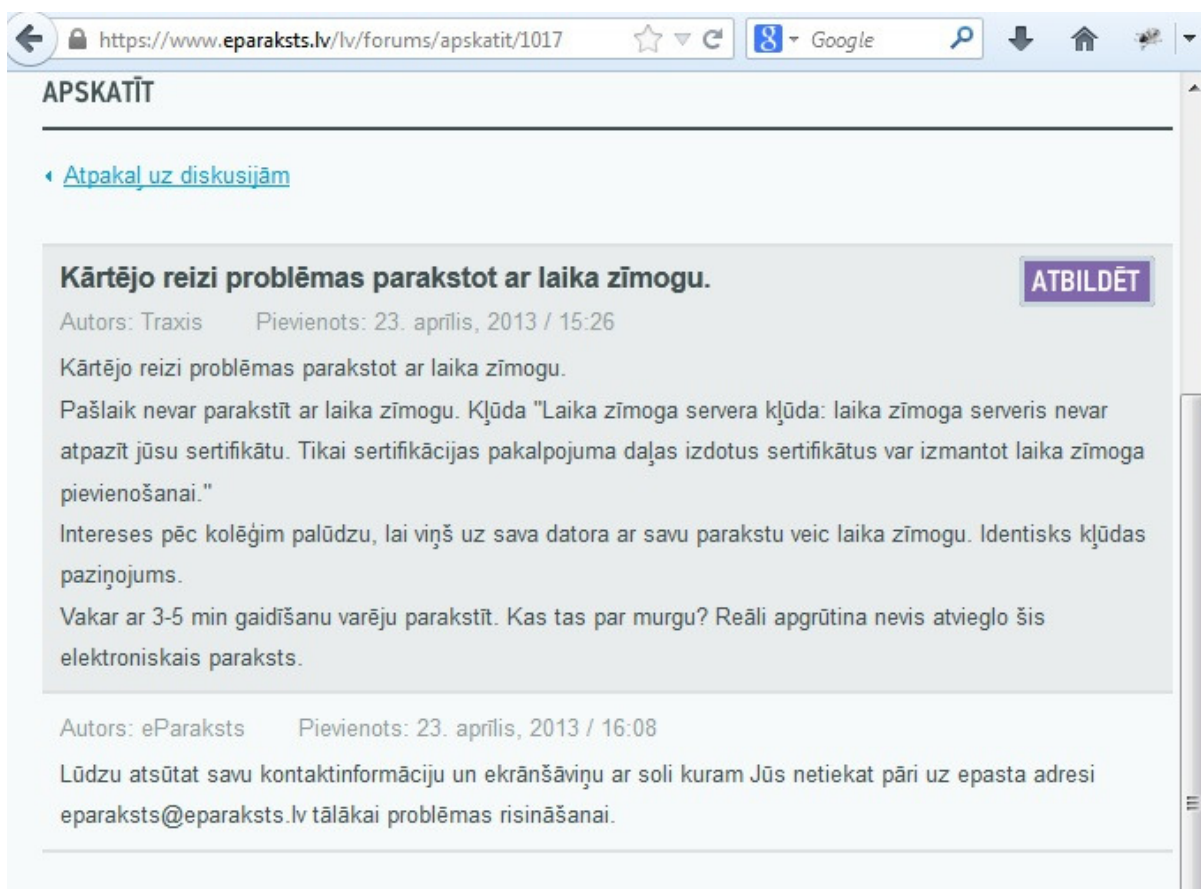
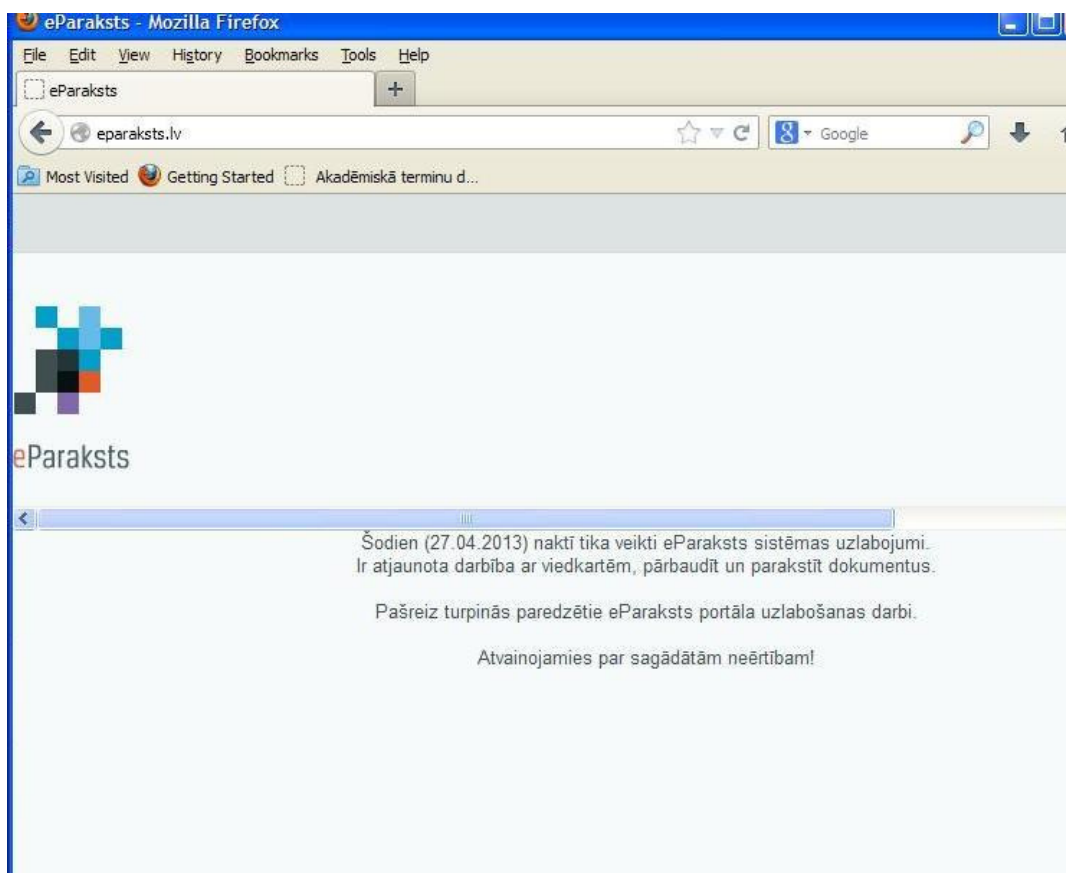
9. pielikums. Mozilla Firefox interneta pārlūkā saglabāto paroli atklāšana



10. pielikums. Sertifikācijas pakalpojumu sniedzēja tehniskas problēmas.







11. pielikums. Arnis Paršovs Datu Valsts inspekcijai par Latvijas pasta neiekļaušanu uzticamu sertifikācijas pakalpojumu sniedzēju reģistrā. [45]

Arnis Paršovs

personas kods 050886-11968

tālrunis: +371 29354127, elektroniskais pasts arnis@parsovs.lv

IESNIEGUMS

Balvos 15.01.2013.

Datu valsts inspekcijai
info@dvi.gov.lv

Par uzticamu sertifikācijas pakalpojumu sniedzēju VAS "Latvijas Pasts"

Atbilstoši Elektronisko dokumentu likuma 20.panta otrās daļas 5.punktam uzraudzības iestāde uztur tiešsaistes režīmā brīvi pieejamu uzticamu sertifikācijas pakalpojumu sniedzēju (turpmāk – USPS) reģistru un atbilstoši 22.panta sestajai daļai uzraudzības iestāde nekavējoties anulē darbību izbeiguša, par maksātnespējīgu pasludināta vai sertifikācijas pakalpojumu sniegšanu apturējušā USPS akreditāciju, informāciju par to iekļaujot USPS reģistrā.

Lūdzu sniegt informāciju par USPS VAS "Latvijas Pasts" statusu un skaidrojumu par to, kāpēc informācija par šo USPS nav atrodama USPS reģistrā, lai gan Datu valsts inspekcijas 2006.gada pārskatā ir pieejama informācija, ka Datu valsts inspekcija ir akreditējusi minēto USPS.

12. pielikums. Datu Valsts inspekcijas atbilde Arnim Paršovam par VAS „Latvijas Pasts” statusu [45]



LATVIJAS REPUBLIKAS DATU VALSTS INSPEKCIJA

Blaumenāņu iela 11/13 - 15, Rīga, LV - 1011, tālr. : (+371) 67223131, fakss: (+371) 67223556, e-pasts: info@dvi.gov.lv

Rīga

15.02.2013. Nr.1-2/1114
Uz 15.01.2013.

Arnim Paršovam
amis@parsovs.lv

Par atbildes sniegšanu

Datu valsts inspekcija, atbildot uz Jūsu iesniegumu par uzticamu sertifikācijas pakalpojumu sniedzēju VAS „Latvijas Pasts”, informē, ka informācija par uzticama sertifikācijas pakalpojuma sniedzēja VAS „Latvijas Pasts” anulēšanu ir izņemta no uzticama sertifikācijas pakalpojumu reģistra, jo, sākot ar 2011.gada gada 1.jūniju tika gandrīz pilnībā likvidēta VAS „Latvijas Pasts” sertifikācijas institūcijas un ar to saistītā servisu infrastruktūra, atstājot tikai to infrastruktūras daļu, kas nepieciešama, lai saskaņā ar LR spēkā esošajiem normatīvajiem aktiem nodrošinātu ar VAS „Latvijas Pasts” sertifikātiem elektroniski parakstīto dokumentu pārbaudi tiešsaistes režīmā, ko iespējams veikt Web vietnē <https://www.e-me.lv/eDoc>.

Direktore

S.Plūmiņa

Šis dokuments ir elektroniski parakstīts ar drošu elektronisko parakstu un satur laika zīmogu.

Zagorska, 67223131

13. pielikums. Datu Valsts inspekcijas atbilde Arnim Paršovam [45]



LATVIJAS REPUBLIKAS DATU VALSTS INSPEKCIJA

Blaumaņa iela 11/13 - 15, Rīga, LV - 1011, tālr. : (+371) 67223131, fakss: (+371) 67223556, e-pasts: info@dvi.gov.lv

Rīga

13.02.2013.Nr.1-2/1041

Uz 08.01.2013.

Arnim Paršovam

amis@parsovs.lv

Par atbildes sniegšanu

Datu valsts inspekcija, atbildot uz Jūsu iesniegumu par drošības pārbaudes atzinumu, sniedz šādu informāciju:

1. Datu valsts inspekcijas savā mājas lapā nepārtrauktā tiešsaistes režīmā sadaļā „E-dokumenti, Uzticamu sertifikācijas pakalpojumu sniedzēju reģistrs” (http://www.dvi.gov.lv/edokumenti/pak_sniedz/kpmg.pdf) ir brīvi pieejams SIA „KPMG Baltics” 2012.gada 24.aprīļa „Vērtējums par USPD atbilstību 2005.gada 12.jūlija Ministru kabineta noteikumiem Nr.514”, kas satur visu Elektronisko dokumentu likuma 20.panta otrajā daļā noteikto informāciju, tai skaitā, sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes atzinums, kurā ir norādīta visa Ministru kabineta 2003.gada 1.jūlija noteikumu Nr.358 „Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi” 13.pantā noteiktā informācija. Iepriekšminētajā vērtējumā ir atrodamas ziņas:

1.1. par sertifikācijas pakalpojuma sniedzēja parakstītu apstiprinājumu par to, ka pārbaude notikusi noteiktajā laika posmā – Vērtējumā ir norādīts, ka CA audits ir veikts VAS „Latvijas Valsts radio un televīzijas centrs” no 2.marta līdz 24.aprīlim saskaņā ar 2011.gad 10.novembrī starp VAS „Latvijas Valsts radio un televīzijas centrs” un SIA KPMG Baltics noslēgto līgumu Nr. ESP-2011/10;

1.2. par eksperta personas datiem – Vērtējumā ir norādīts eksperta vārds, uzvārds, amats;

1.3. par informāciju par eksperta atbilstību Elektronisko dokumentu likuma 13.panta otrajā daļā noteiktajām prasībām – Vērtējumā ir norādīts, ka auditu ir veikusi Datu valsts inspekcijas apstiprinātajā sarakstā iekļautā persona - SIA „KPMG Baltics”, savukārt saskaņā ar Elektronisko dokumentu likuma 13.panta otro daļu iepriekšminētajā sarakstā drīkst iekļaut tikai tās personas, kuras atbilst Elektronisko dokumentu likuma 13.panta otrās daļas prasībām;

1.4. par laikposmu, par kuru veikta pārbaude – Vērtējumā ir norādīts, ka audits ir veikts par laika posmu līdz 2012. gada 24. aprīlim;

1.5. par eksperta vērtējumu, secinājumu un lēmumu par sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības atbilstību normatīvajiem aktiem, kuri reglamentē sertifikācijas pakalpojumu sniegšanu - Vērtējumā eksperts ir veicis auditu par VAS „Latvijas Valsts radio un televīzijas centrs” atbilstību Ministru kabineta 2003. gada 1. jūlija noteikumu Nr.358 „Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi” 10.panta, gan 2005.gada 12.jūlija Ministru kabineta noteikumi Nr.514 „Noteikumi par tehniskajām un organizatoriskajām prasībām, kādām atbilst kvalificēts sertifikāts, uzticams sertifikācijas pakalpojumu sniedzējs, droši elektroniskā paraksta radīšanas līdzekļi, kā arī kārtību, kādā veicama droša elektroniskā paraksta verificēšana” 2.panta prasībām.

Līdz ar to Datu valsts inspekcija ir nodrošinājusi Elektronisko dokumentu 20.panta otrajā daļā 5.punkta izpildi.

2. Datu valsts inspekcija saskaņā ar Elektronisko dokumentu likuma 21.panta pirmo daļu kā uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzības iestāde ir devusi norādījumus VAS „Latvijas Valsts radio un televīzijas centrs” novērst audita laikā konstatētās nepilnības.

Direktore

S.Plūmiņa

Šis dokuments ir elektroniski parakstīts ar drošu elektronisko parakstu un satur laika zīmogu.

Zagorska, 67223131

14. pielikums. Arņa Paršova iesniegums Datu valsts inspekcijai 08.01.2013 [45]

Arnis Paršovs

personas kods 050886-11968

tālrunis: +371 29354127, elektroniskais pasts arnis@parsovs.lv

IESNIEGUMS

Balvos 08.01.2013.

Datu valsts inspekcijai
info@dvi.gov.lv

Par drošības pārbaudes atzinumu

Ministru kabineta noteikumu Nr.358 "Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi" 13. punkts nosaka prasības pārbaudes atzinumam.

Jūsu 13.11.2012. vēstulē Nr.1-2/7419 norādītā tiešā saite uz KPMG Baltics SIA sniegto atzinumu (http://www.dvi.gov.lv/edokumenti/pak_sniedz/kpmg.pdf) nesatur šādas prasītās ziņas:

1. sertifikācijas pakalpojumu sniedzēja parakstītu apstiprinājumu par to, ka pārbaude notikusi noteiktajā laikposmā;
2. eksperta personas datus;
3. informāciju par eksperta atbilstību Elektronisko dokumentu likuma 13.panta otrajā daļā noteiktajām prasībām;
4. laikposmu, par kuru veikta pārbaude;
5. eksperta vērtējumus, secinājumus un lēmumu par sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības atbilstību normatīvajiem aktiem, kuri reglamentē sertifikācijas pakalpojumu sniegšanu (eksperta lēmums sniegts tikai par atbilstību Ministru kabineta noteikumiem Nr.514).

Lūdzu:

1. nodrošināt Elektronisko dokumentu likuma 20.panta otrās daļas 5.punkta izpildi un ievietot uzticamu sertifikācijas pakalpojumu sniedzēju reģistrā uzticama sertifikācijas pakalpojumu sniedzēja VAS "Latvijas Valsts radio un televīzijas centrs" informācijas sistēmu, iekārtu un procedūru drošības pārbaudes atzinumu;
2. sniegt informāciju, vai Datu valsts inspekcija kā uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzības iestāde atbilstoši Elektronisko dokumentu likuma 21.panta pirmajai daļai ir devusi norādījumus uzticamam sertifikācijas pakalpojumu sniedzējam VAS "Latvijas Valsts radio un televīzijas centrs" novērst neatbilstību LVS ISO/IEC 17799, kuru auditors konstatējis arī iepriekšējā akreditācijas pārbaudē.

15. pielikums. VAS „Latvijas Valsts radio un televīzijas centrs” atbilde Arnim Paršovam par auditiem. [54]



LATVIJAS VALSTS
RADIO UN TELEVĪZIJAS CENTRS

VAS "Latvijas Valsts radio un televīzijas centrs"

Vienotais reģistrācijas Nr. 40003011203, Ērgļu iela 7, Rīga, LV-1012

Tālrunis: 67108704, fakss: 67315577, e-pasts: lvrtc@lvrtc.lv

17.09.2012. Nr. 60AD00.2/844
Uz 31.08.2012.

Arnim Paršovam
arnis@parsovs.lv

Par sertifikācijas pakalpojuma auditiem

VAS „Latvijas Valsts radio un televīzijas centrs” (turpmāk – LVRTC), atbildot uz Jūsu 31.08.2012. iesniegumu, sniedz sekojošu informāciju.

Izpildot Elektronisko dokumentu likumā un Ministru kabineta 2003.gada 1.jūlija noteikumos Nr. 358 „Sertifikācijas pakalpojumu sniegšanas informācijas sistēmu, iekārtu un procedūru drošības pārbaudes kārtība un termiņi” noteikto, par LVRTC kā uzticama sertifikācijas pakalpojumu sniedzēja (turpmāk – USPS) informācijas sistēmām, iekārtām un procedūrām, kā arī par pakalpojuma funkcionalitātēm tika veikti sekojoši auditi:

1. Saskaņā ar 29.07.2009.gada līgumu Nr.11-2008/1 SIA „KPMG Baltics” laika periodā no līguma noslēgšanas dienas līdz 14.08.2009. veica ikgadējo USPS auditu. Līguma summa par izpildītajiem pakalpojumiem ir LVL 9500.00, bez pievienotās vērtības nodokļa.
2. Saskaņā ar 19.02.2010. līgumu Nr.2010/1 SIA „KPMG Baltics” laika periodā no 05.03.2010. līdz 14.04.2010. veica ikgadējo USPS auditu. Līguma summa par izpildītajiem pakalpojumiem ir LVL 7000.00, bez pievienotās vērtības nodokļa.
3. Saskaņā ar 25.02.2010. līgumu Nr. ITC-LVRTC-2/2010, (LVRTC reģistrācijas Nr.14/2010 ESP) SIA „IT Centrs” laika periodā no 01.03.2010. līdz 06.04.2010. veica funkcionalitātes auditu. Līguma summa par izpildītajiem pakalpojumiem ir LVL 19 500.00, bez pievienotās vērtības nodokļa.
4. Saskaņā ar 08.08.2010. līgumu Nr. RAS-C2010/22 SIA „KPMG Baltics” laika periodā no līguma noslēgšanas līdz 01.04.2011. veica funkcionalitātes auditu. Līguma summa par izpildītajiem pakalpojumiem ir LVL 14 400.00, bez pievienotās vērtības nodokļa.
5. Saskaņā ar 25.03.2011. līgumu Nr. 2011/ITA/3 SIA „KPMG Baltics” laika periodā no 28.03.2011. līdz 28.04.2011. veica ikgadējo USPS auditu. Līguma summa par izpildītajiem pakalpojumiem ir LVL 8880.00, bez pievienotās vērtības nodokļa.
6. Saskaņā ar 10.11.2011. līgumu Nr. ESP-2011/10 SIA „KPMG Baltics” laika periodā no 02.03.2012. līdz 20.04.2012. veica ikgadējo USPS auditu, kā arī laika periodā no 16.11.2011. līdz 14.12.2011. eID ieviešanas risinājuma funkcionalitātes auditu. Līguma summa par izpildītajiem pakalpojumiem ir LVL 27 010.00, bez pievienotās vērtības nodokļa. Uz doto brīdi ir veikta samaksa par izpildītajiem pakalpojumiem LVL 13 690.00, bez pievienotās vērtības nodokļa apmērā.

Ievērojot Publisko iepirkumu likuma 3.panta ceturto daļu, attiecībā uz augstāk norādītajiem līgumiem tika piemērots Publisko iepirkumu likuma piemērošanas izņēmums. Vienlaikus norādām, ka atbilstoši LVRTC iepirkumu kārtībai Publisko iepirkumu likuma 3. panta ceturtais daļas ietvaros, LVRTC uzaicina vismaz 3 pretendentes iesniegt savus piedāvājumus attiecīgā pakalpojuma sniegšanai, kur, izvērtējot iesniegtos piedāvājumus, tiek izvēlēts pretendents, kas atbilst noteiktām nolikuma vai tehniskās specifikācijas prasībām (zemākā cena vai saimnieciski izdevīgākais piedāvājums).

Šis dokuments ir parakstīts ar drošu elektronisko parakstu un satur laika zīmogu.

Valdes priekšsēdētājs, prokurists Jānis Bokta.

Pužule 67108778
tatjana.puzule@lvrtc.lv

16. pielikums. Arņa Paršova vēstule VAS „Latvijas Valsts radio un televīzijas centrs” par auditiem. [54]

Arnis Paršovs

personas kods 050886-11968

tālrunis: +371 29354127, elektroniskais pasts amis@parsovs.lv

IESNIEGUMS

Balvos 31.08.2012.

VAS “Latvijas Valsts radio un televīzijas centrs”
valdes priekšsēdētājam Jānim Boktam
lvrtc@lvrtc.lv

Par sertifikācijas pakalpojumu auditiem

Lūdzu sniegt informāciju par ārējiem jeb neatkarīgajiem auditiem vai novērtējumiem (atbilstības auditiem, drošības testiem, ielašanās testiem u.c.), kas veikti par uzticama sertifikācijas pakalpojumu sniedzēja VAS “Latvijas Valsts radio un televīzijas centrs” piedāvātajiem sertifikācijas pakalpojumiem, par katru no auditiem norādot:

1. laika posmu, kurā audits veikts;
2. auditoru, kas veicis auditu (tajā skaitā juridiskā persona, kuru auditors pārstāv);
3. audita izmaksas;
4. vai tika veikts publisks iepirkums;
5. audita veids un uzdevums.

17. pielikums. „Qualyslabs SSL server rating guide” [189]

SSL Server Rating Guide

version 2009c (1 February 2013)

Copyright © 2009-2013 SSL Labs (www.ssllabs.com)

Abstract

The Secure Sockets Layer (SSL) protocol is a standard for encrypted network communication. We feel that there is surprisingly little attention paid to how SSL is configured, given its widespread usage. SSL is relatively easy to use, but it does have its traps. This guide aims to establish a straightforward assessment methodology, allowing administrators to assess SSL server configuration confidently without the need to become SSL experts.



Introduction to the 2009c Release

The SSL threat landscape changed significantly since the original rating guide was published in 2009. The original guide is thus no longer entirely suitable for use today. In addition, we now have several years of experience using the criteria in real life, and we know what works well and what not so much.

Our plan is to update the rating criteria to take all this new information into account. However, because that process will take several months to complete and because an update to the guide is long overdue, we have decided to release a small patch release, labeling it 2009c. This document.

The purpose of this release is to keep the original rating criteria relevant for a little while longer, until the next version is ready. The text of the original document remains as is, but the following changes apply:

- SSL 2.0 is not allowed (F).
- Insecure renegotiation is not allowed (F).
- Vulnerability to the BEAST attack caps the grade to B.
- Vulnerability to the CRIME attack caps the grade to B.
- The score (0-100) is now shown any more, in order to focus on the grade, which is more useful. Future versions of the guide will probably remove the score altogether.

In addition, we've taken the opportunity to remove the old configuration advice, directing the readers to our *SSL/TLS Deployment Best Practices* document instead.

Methodology Overview

Our approach consists of three steps:

1. We first look at a certificate to verify that it is valid and trusted. A server that fails this step is always assigned a zero score.
2. We inspect server configuration in three categories:
 - a. Protocol support
 - b. Key exchange support
 - c. Cipher support
3. The final score—a number between 0 and 100—is a combination of the scores achieved in the individual categories. A zero score in any category forces the total score to zero.

Because small differences between configurations are sometimes less important, we also assign letter grades to servers. Letter grades are generally more useful—it is instantly clear

that a server given an A is well configured. [Table 1](#) shows how a numerical score is translated into a letter grade.

Table 1. Letter grade translation

Numerical Score	Grade
score >= 80	A
score >= 65	B
score >= 50	C
score >= 35	D
score >= 20	E
score < 20	F

Our methodology is purposefully designed to be straightforward and practical. Advanced users may prefer to dig deep into the finer details of SSL (e.g., which ciphers are better than others), but we feel that such an approach, although intellectually challenging, would make this guide less useful in practice.

What This Guide Does Not Cover

Our immediate goal is to focus on those configuration problems whose presence can be determined remotely and without manual assessment. It is only a fully automated approach that makes it possible to perform a large-scale assessment of SSL configuration practices. Our aim is to scan all SSL servers on the public Internet.

In focusing on automation, we have decided not to look for certain problems. We will list those problems in this guide, and hopefully find ways to enhance our automation to include them in a future version of this guide. Some of those problems are listed here:

Certificate quality

Three certificate types are currently in use: domain-validated, organisation-validated and extended-validation (EV) certificates. This guide requires a certificate to be correct, but does not go beyond this basic requirement. The domain-validated and organisation-validated certificates are generally treated in the same way by the current generation of browser software, and thus offer similar assurance to users. EV certificates are treated significantly better and, generally, they are recommended for high-value web sites. Without a reliable way to determine the purpose of a web site, however, there is little that this guide can do to assess whether a certificate used on an arbitrary site is suitable for the purpose of the site.

Session hijacking issues in web applications

There are several ways in which web applications can subvert SSL and make it less effective. For example, session cookies that are not marked as secure can be retrieved by a determined attacker, leading to session hijacking and thus application compromise.

Such problems are not the fault of SSL, but they do affect its practical applications nevertheless. Detecting web application-specific problems is non-trivial to perform in an automated fashion, and this version of the guide does not attempt to do it. We leave this problem for the consideration in the future. In the meantime, to remove any doubt that might exist about the seriousness of the above-mentioned issues, we will state that *any application that incorrectly implements session token propagation should be awarded a zero score.*

What Should My Score Be?

We don't know. In order to tell you whether you've configured your SSL server correctly, we would need to know what your site does. Because different web sites have different needs, it is not possible for us to choose any one configuration and say that it works for everyone. But we can do two things. First, we can give you some general configuration advice and tell you what you should never do. Second, we can give you some general guidance using examples of what other web sites do. If that's what you are interested in, skip to the end of this document for more information.

Is SSL Enough?

No. A non-trivial web site cannot be secure if it does not implement SSL, but SSL is not enough. SSL deals with only one aspect of security, and that is the security of the communication channel between a web site and its users. SSL does not and cannot address a number of possible security issues that may exist on a web site. View SSL as a foundation on which to build, but the foundation alone is not enough.

Acknowledgements

The first version of this guide was written by [Ivan Ristic](http://blog.ivanristic.com)¹, and subsequently enhanced by the contributions from the following individuals, listed in alphabetical order: Christian Bockermann, Christian Folini, Robert Hansen, Ofer Shezaf and Colin Watson.

Certificate Inspection

Server certificate is often the weakest point of an SSL server configuration. A certificate that is not trusted (i.e., is not ultimately signed by a well-known certificate authority) fails to prevent man-in-the-middle (MITM) attacks and renders SSL effectively useless. A certificate that is incorrect in some other way (e.g., a certificate that has expired) erodes trust and, in the long term, jeopardises the security of the Internet as a whole.

¹ <http://blog.ivanristic.com>

For these reasons, any of the following certificate issues immediately result in a zero score:

- Domain name mismatch
- Certificate not yet valid
- Certificate expired
- Use of a self-signed certificate
- Use of a certificate that is not trusted (unknown CA or some other validation error)
- Use of a revoked certificate

Note

Some organisations create their own (private) CA certificates, a practice that is entirely legitimate, provided such CA certificates are distributed, in a safe manner (e.g., through the use of customised browsers) to all those who need it. Without the access to such certificates we may not be able to verify that a site we are inspecting has a trusted certificate, but we believe that such sites will be relatively rare. Such issues can be considered on a case-by-case basis.

Scoring

SSL is a complex hybrid protocol with support for many features across several phases of operation. To account for the complexity, we rate the configuration of an SSL server in three categories, as displayed in [Table 2](#). We calculate the final score as a combination of the scores in the individual categories, as described in the “Methodology Overview” section.

Table 2. Criteria categories

Category	Score
Protocol support	30%
Key exchange	30%
Cipher strength	40%

The sections that follow explain the rating system for each of the categories.

Protocol Support

First, we look at the protocols supported by an SSL server. For example, both SSL 2.0 and SSL 3.0 have known weaknesses. Because a server can support several protocols, we use the following algorithm to arrive to the final score:

1. Start with the score of the best protocol.
2. Add the score of the worst protocol.
3. Divide the total by 2.

Table 3. Protocol support rating guide

Protocol	Score
SSL 2.0	20%
SSL 3.0	80%
TLS 1.0	90%
TLS 1.1	95%
TLS 1.2	100%

Key Exchange

The key exchange phase serves two functions. One is to perform authentication, allowing at least one party to verify the identity of the other party. The other is to ensure the safe generation and exchange of the secret keys that will be used during the remainder of the session. The weaknesses in the key exchange phase affect the session in two ways:

- Key exchange without authentication allows an active attacker to perform a MITM attack, gaining access to the complete communication channel.
- Public cryptography is used during key exchange: the stronger the server's private key, the more difficult it is to break the key exchange phase. A weak key, or an exchange procedure that uses only a part of the key (the so-called exportable key exchanges), can result in a weak key exchange phase that makes the per-session secret keys easier to compromise.

Table 4. Key exchange rating guide

Key exchange aspect	Score
Weak key (Debian OpenSSL flaw)	0%
Anonymous key exchange (no authentication)	0%
Key length < 512 bits	20%
Exportable key exchange (limited to 512 bits)	40%
Key length < 1024 bits (e.g., 512)	40%
Key length < 2048 bits (e.g., 1024)	80%
Key length < 4096 bits (e.g., 2048)	90%
Key length >= 4096 bits (e.g., 4096)	100%

Cipher Strength

To break a communication session, an attacker can attempt to break the symmetric cipher used for the bulk of the communication. A stronger cipher allows for stronger encryption and thus increases the effort needed to break it. Because a server can support ciphers of varying

strengths, we arrived at a scoring system that penalises the use of weak ciphers. To calculate the score for this category, we follow this algorithm:

1. Start with the score of the strongest cipher.
2. Add the score of the weakest cipher.
3. Divide the total by 2.

Table 5. Cipher strength rating guide

Cipher strength	Score
0 bits (no encryption)	0%
< 128 bits (e.g., 40, 56)	20%
< 256 bits (e.g., 128, 168)	80%
>= 256 bits (e.g., 256)	100%

SSL Configuration Advice

The configuration advice from the original document has been superseded by a standalone document with comprehensive coverage of this topic. You can download the [SSL/TLS Deployment Best Practices](#)² document from the SSL Labs web site.

For Consideration in Future Releases

We have left a number of open issues for future consideration:

Perfect forward secrecy bonus points

Some key exchange mechanisms allow for perfect forward secrecy. Perfect forward secrecy is a property that ensures that short-term session keys cannot be compromised after a compromise of a long-term secret key (which was used in the generation of the short-term keys). We should consider giving bonus points to those servers that allow only the key exchange mechanisms that allow for forward secrecy.

Differences between encryption algorithms

Should the choice of encryption algorithms affect server score? For example, it is said that RC4 is not as strong as once thought, so its availability might warrant negative points.

Default ciphers

In SSL v3 and later, clients provide servers with a list of cipher suites they are willing to use. We want to determine whether servers typically select the first mutually acceptable cipher suite for a session, or if there is a logic behind the suite selection. If the latter,

² <https://www.ssllabs.com/projects/best-practices/>

then we might want to consider giving a better grade to the servers that make better choices.

SSL v2 support

Should servers that support SSL v2 be awarded a zero score in the protocol category? A zero score for the entire test?

About SSL

The Secure Sockets Layer (SSL) protocol is a standard for encrypted network communication. It was conceived at Netscape in 1994; version 2.0 was the first public release. SSL was later upgraded to 3.0, and, with further minor improvements, standardised under the name TLS (*Transport Layer Security*). TLS v1.2, the most recent version, is defined by [RFC 5246](http://www.ietf.org/rfc/rfc5246.txt)³.

About SSL Labs

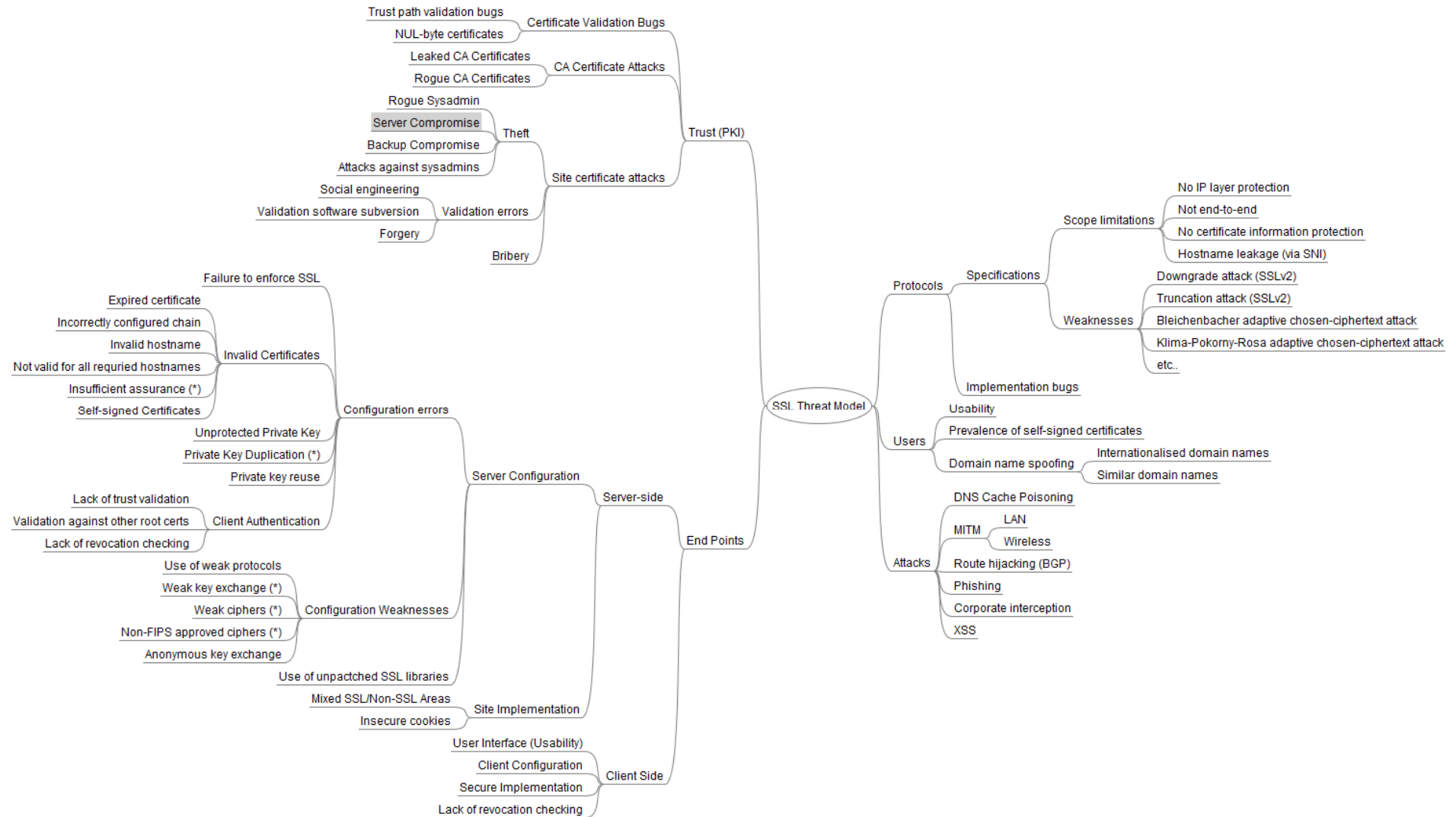
[SSL Labs](https://www.ssllabs.com)⁴ is a computer security research organisation that, unsurprisingly, focuses on the SSL standard. Our aim is to discuss the rarely mentioned aspects of SSL, promote its correct usage, and generally inspire everyone to do their part to promote security. Unlike in some other areas (e.g., application security), security is relatively easy to achieve when it comes to SSL. Thus we believe that there are no excuses for a lack of security.

³ <http://www.ietf.org/rfc/rfc5246.txt>

⁴ <https://www.ssllabs.com>

18. pielikums. „SSL threat model”

(https://www.ssllabs.com/downloads/SSL_Threat_Model.png)



19. pielikums. Droša Elektroniskā paraksta nesēju veidi.

(<https://www.eparaksts.lv/lv/palidziba/eparaksta-neseju-veidi/>)

	Virtuālais eParaksts	eParaksts eID kartē	eParaksts viedkartē
eParaksta nesēja veids:			
Nepieciešamais darbam:	DATORS + INTERNETS	DATORS + INTERNETS + EID KARTE + KARTES LASĪTĀJS	DATORS + INTERNETS + VIEDKARTE + KARTES LASĪTĀJS
eParaksta saņemšana:	Jāapmeklē Klientu apkalpošanas centrs , iepriekš aizpildot un izdrukājot pieteikumu: www.eparaksts.lv . Nav jāapmeklē SEB bankas klientiem, eID kartes un viedkartes īpašniekiem. Pieteikšanās notiek tiešsaistē	Jāapmeklē PMLP 2 reizes – pirmo reizi, lai iesniegtu pieteikumu par eID kartes izgatavošanu un otro reizi, lai saņemtu eID karti	Jāapmeklē Latvijas Pasts 2 vai 3 reizes – pirmo reizi, lai iesniegtu pieteikumu par viedkartes izgatavošanu, otro reizi, lai saņemtu viedkarti un PIN kodu , trešo reizi, ja esat norādījuši dažādas pasta nodaļa PIN kodu saņemšanai .
Datora sagatavošana darbam:	Nav nepieciešama	Jāinstalē speciāla programmatūra	Jāinstalē speciāla programmatūra
Izgatavošanas laiks:	Var lietot uzreiz	2-10 dienas	10 dienas kopš personas pieteikuma saņemšanas
Izmaksas:	Abonēšanas uz 1 gadu ar neierobežotu parakstīšanas reižu skaitu vai maksa par parakstīšanas reizēm, cenrādis	Vienreizējā maksa par eID KARTI ar iekļautām 120 parakstīšanās reizēm (karte jāatjauno ik pēc 5 gadiem) - 10.00 LVL; (20.00 LVL par paātrināto izgatavošanu) + vienreizējā maksa par kartes LASĪTĀJU, skat. Tirdzniec. vietas	Vienreizējā maksa par VIEDKARTI (karte jāatjauno ik pēc 2 gadiem) 9.90 LVL + vienreizējā maksa par kartes LASĪTĀJU, skat. Tirdzniec. vietas , + maksa par parakstīšanās reizēm, cenrādis
Vai eParaksts ir drošs?	Jā, jo tikai VAS „Latvijas Valsts radio un televīzijas centrs” (LVRTC) pārvaldītajam elektroniskajam parakstam (eParakstam), ir tāds pats juridiskais spēks kā cilvēka fiziskam parakstam, un tas, atbilstoši likumam, ir vienīgais drošais elektroniskais paraksts Latvijā.	Jā, jo tikai VAS „Latvijas Valsts radio un televīzijas centrs” (LVRTC) pārvaldītajam elektroniskajam parakstam (eParakstam), ir tāds pats juridiskais spēks kā cilvēka fiziskam parakstam, un tas, atbilstoši likumam, ir vienīgais drošais elektroniskais paraksts Latvijā.	Jā, jo tikai VAS „Latvijas Valsts radio un televīzijas centrs” (LVRTC) pārvaldītajam elektroniskajam parakstam (eParakstam), ir tāds pats juridiskais spēks kā cilvēka fiziskam parakstam, un tas, atbilstoši likumam, ir vienīgais drošais elektroniskais paraksts Latvijā.
Pielietojumi:	Parakstīt dokumentus	Parakstīt dokumentus , ielogoties portālos, ceļot	Parakstīt dokumentus , ielogoties portālos
Parakstāmo dokumentu formāti:	eDOC un PDF formāti	eDOC	eDOC
Derīguma termiņš:	beztermiņa	Kartes derīguma termiņš ir 5 gadi	Kartes derīguma termiņš ir 2 gadi