Vilniaus Universiteto
Komunikacijos fakulteto
Informacijos ir komunikacijos katedra

Karolis Rubinas

Informacijos sistemų vadybos magistrantūros studijų programos studentas

Elektroninio parašo diegimo problemos

Magistro darbas

Vadovas Doc. dr. Valdas Undzėnas

Vilnius, 2011

Pildo magistro baigiamojo darbo autorius

Karolis Rubinas
(magistro baigiamojo darbo autoriaus vardas, pavardė)

Elektroninio parašo diegimo problemos
(magistro baigiamojo darbo pavadinimas lietuvių kalba)

Public Key Infrastructure implementation problems
(magistro baigiamojo darbo pavadinimas anglų kalba)

Patvirtinu, kad magistro baigiamasis darbas parašytas savarankiškai, nepažeidžiant kitiems asmenims priklausančių autorių teisių, visas baigiamasis magistro darbas ar jo dalis nebuvo panaudoti kitose aukštosiose mokyklose.

_____
(magistro baigiamojo darbo autoriaus parašas)

Sutinku, kad magistro baigiamasis darbas būtų naudojamas neatlygintinai 5 metus Vilniaus universiteto Komunikacijos fakulteto studijų procese.

_____
(magistro baigiamojo darbo autoriaus parašas)

Pildo magistro baigiamojo darbo vadovas

Magistro baigiamąjį darbą ginti _____
(įrašyti – leidžiu arba neleidžiu)

_____ _____
(data) (magistro baigiamojo darbo vadovo parašas)

Pildo instituto / katedros, kuruojančios studijų programą, reikalų tvarkytoja

Magistro baigiamasis darbas įregistruotas

_____
(instituto / katedros, kuruojančios studijų programą, pavadinimas)

_____ _____
(data) (instituto / katedros reikalų tvarkytojos parašas)

Pildo katedros, kuruojančios studijų programą, vadovas

Recenzentu skiriu _____
(recenzento vardas, pavardė)

_____ _____
(data) (katedros vadovo parašas)

Pildo recenzentas

Darbą recenzuoti gavau. _____ _____
(data) (recenzento parašas)

REFERATO LAPAS

Karolis Rubinas,

Elektroninio parašo diegimo problemos: magistro darbas / Karolis Rubinas; mokslinis vadovas Valdas Undzėnas; Vilniaus universitetas. Komunikacijos fakultetas. Informacijos ir komunikacijos katedra. – Vilnius, 2011. – 57, [1] lap. – Mašinr. – Santr. Angl. – Bibliogr.: lap. 52 – 55 (33 pavad.)

UDK indeksas 004. 056.55

Reikšminiai žodžiai: elektroninis parašas, reikalavimai, sertifikatų centras, sertifikatas, kvalifikuotas sertifikatas, veiklos nuostatai, Gyventojų registro sertifikatų centas, skaitmeninių sertifikatų centras, registrų centro sertifikatų centras, parašo taisyklės, laiko žymos tarnyba, elektroninio parašo infrastruktūra.

Magistro darbo objektas – elektroninis parašas.

Darbo tikslas – nustatyti priežastis, kodėl elektroninio parašo technologija taip sunkiai diegiama Lietuvoje, ir pasiūlyti būdus, kaip diegimą galima būtų palengvinti.

Darbo uždaviniai:

1. Išsiaiškinti elektroninio parašo veikimo principus.
2. Išnagrinėti ir pateikti el. parašo pritaikymo galimybes ir sritis.
3. Išanalizuoti ir pateikti, kur ir kaip asmenys turėtų įsigyti el. parašo naudojimui būtinus dokumentus ir įrangą.
4. Atlikti el.parašo įdiegimo lygio analizę kitose šalyse.
5. Suformuluoti galimas diegimo problemos priežastis.
6. Išanalizuoti ir palyginti Lietuvoje veikiančių sertifikavimo centrų veiklos nuostatus ir parašo taisykles, išskirti informacijos trūkumus.
7. Pateikti pasiūlymus, kaip palengvinti el. parašo technologijos diegimą Lietuvoje.

Remiantis egzistuojančiais el. parašo apibūdinimais, galima teigti: el. parašas – tai skaitmeninė technologija, leidžianti ne tik pasirašyti dokumentą el. būdu, bet ir identifikuoti pasirašiusįjį asmenį, užtikrinant dokumento originalumą. Išanalizuoti viešojo rakto infrastruktūrai skirti standartai bei teisiniai dokumentai. Nustatyta, kad didžiausia problema kuriant ir vystant el. parašo infrastruktūrą – jai keliami aukšti reikalavimai. Reikalavimų privalu laikytis, norint sukurti patikimą ir kvalifikuotą el. parašo infrastruktūrą.

Palyginus Lietuvoje esamą situaciją su kitomis pasaulio šalimis, matyti, jog svetur ši technologija pažengusi gerokai toliau ir plačiau. Nors Lietuvoje įstatyminė bazė parengta anksčiau

nei kitose, daugiau sertifikatų centrų turinčiose šalyse (Latvija, Lenkija, Vokietija, Indija). Įvertinus situaciją Lietuvoje, nustatyta jog iš penkių sertifikavimo paslaugas teikiančių institucijų, kvalifikuotus sertifikatus išduoda trys: UAB „Skaitmeninio sertifikavimo centras“, VĮ „Registrų centras“ bei Gyventojų registro tarnyba. Daroma prielaida, kad „UAB Omnitel“ ir „UAB Bitė Lietuva“ į šį sąrašą nepatenka, nes netenkina daugumos šiame darbe paminėtų ir nepaminėtų reikalavimų.

Magistro darbas gali būti naudingas tiek privačioms verslo įmonėms, tiek valstybinėms organizacijoms, ketinančioms teikti sertifikavimo paslaugas, taip pat žmonėms norintiems labiau suprasti el. parašo veikimą, paskirtį ir naudą.

TURINYS

SANTRUMPŲ SĄRAŠAS

El. – elektroninis.

CA – *Certificate Authorities*, sertifikatų centras.

CP – *Certificate Policy*, sertifikatų taisyklės.

CPS – *Certificate Practice Statement*, veiklos nuostatai.

CRL – *Certificate Revocation List,* atšauktų sertifikatų sąrašas.

GRSC – Gyventojų Registro Sertifikavimo Centras.

OCSP – *Online Certificate Status Protocol,* užklausų sistema realiu laiku.

RCSC – Registrų Centro Sertifikatų Centras.

RSA – *Rivest Shamir Adelman*, algoritmo pavadinimas.

SCA – Signature creation Application, parašo formavimo programa.

sPIN – *secure Personal Identification Number,* saugus asmeninis identifikavimo numeris.

SSC – Skaitmeninio Sertifikavimo Centras.

SSCD – *Secure Signature Creation Device,* saugus parašo formavimo įrenginys.

ĮVADAS

Informacinė visuomenė sąlygojo daugybę pokyčių organizacijų veikloje. Svarbiausias iš jų – tai tradicinės dokumento sampratos pasikeitimas. Organizacijose šiuo metu vis svarbesnę vietą užima elektroniniai dokumentai (toliau el. dokumentai), kurių teisinė galia turėtų būti tokia pati, kaip ir spausdintų dokumentų. El. dokumentų parengimas bei siuntimas kompiuterių tinklais yra daug pigesnis ir greitesnis būdas, nei siuntimas paprastu paštu. Šie kriterijai tampa ypatingai svarbūs, plėtojantiems tarptautinį verslą.

Naudojant el. dokumentus iškyla dvi problemos: 1) kaip pasirašyti dokumentą, t. y. kaip užtikrinti gavėjui, jog gauti duomenys yra tokie patys, kokius perdavė siuntėjas (nebuvo pakeisti) ir 2) kaip identifikuoti dokumentą pasirašiusįjį asmenį? Dėl šių priežasčių, buvo išrastas elektroninis parašas, tačiau Lietuvoje šios technologijos pritaikymas kol kas kelia daug sunkumų.

El. paršo įstatymas Lietuvoje priimtas dar 2000 m. Žiūrint į šios technologijos diegimo lygį Lietuvoje (t.y. kaip plačiai ši technologija naudojama, kiek apie ją žmonių žino ar bent yra girdėję), tai rezultatai yra labai menki.

Praktikoje el. parašo technologijos pritaikymas labai platus: bankuose, statistikos departamente, elektroniniam balsavimui, susirašinėjimui su Vyriausybe, Sodroje, mokesčių inspekcijoje, tarptautiniam ir vietiniame versle, ir t. t. Ilgą laiką el. parašui vystytis trukdė bankai, nes jų išduodamos klientų identifikavimo priemonės, jungimuisi prie el. bankininkystės, klaidingai buvo laikomos el. parašu. Nemažai problemų sukelia ir politiniai veiksniai, pvz., tam priešinasi dalis Seimo.

Svarbiausi šaltiniai, tiesiogiai susiję su el. parašu: el. parašo įstatymas, direktyvos (pradinis taškas, be kurio kvalifikuoto el. parašo technologija išvis nebūtų įmanoma), standartai (dokumentai nusakantys, kaip ir kokių reikalavimų reikia laikytis kuriant viešojo rakto infrastruktūrą); CP ir CPS (dokumentai, kuriais įstaigos įrodo, kad laikosi ir kaip atitinka minėtus standartus), techninė literatūra (skirta programuotojams, joje vyrauja šifravimo algoritmai, programų kodai, jų šablonai ir kt).

Darbo objektas. El. parašas ir viešojo rakto infrastruktūra.

Darbo tikslas. Nustatyti priežastis, kodėl elektroninio parašo technologija taip sunkiai diegiama Lietuvoje, ir pasiūlyti būdus, kaip diegimą galima būtų palengvinti.

Darbo uždaviniai:

1. Išsiaiškinti elektroninio parašo veikimo principus.
2. Išnagrinėti ir pateikti el. parašo pritaikymo galimybes ir sritis.

3. Išanalizuoti ir pateikti, kur ir kaip asmenys turėtų įsigyti el. parašo naudojimui būtinus dokumentus ir įrangą.
4. Atlikti el.parašo įdiegimo lygio analizę kitose šalyse.
5. Suformuluoti galimas diegimo problemos priežastis.
6. Išanalizuoti ir palyginti Lietuvoje veikiančių sertifikavimo centrų veiklos nuostatus ir parašo taisykles, išskirti informacijos trūkumus.
7. Pateikti pasiūlymus, kaip palengvinti el. parašo technologijos diegimą Lietuvoje.

Darbe buvo pasirinkti **tradicinės dokumentų analizės, indukcijos, dedukcijos ir palyginimo metodai**. Būtent šie metodai, geriausiai padeda pasiekti išsikeltus uždavinius ir tikslą. Pasirinktas tradicinės dokumentų analizės metodas išryškina analizuojamos medžiagos esmę. Palyginimo metodas, tai vienas iš kokybinių tyrimo metodų, kuris pagrįstas logika ir samprotavimais, kai gretinant kelis objektus išskiriami jų panašumai ir skirtumai. Indukcijos metodas tai „*samprotavimo būdas, kai ištyrus kai kuriuos vienos klasės objektus ir nustačius, kad jie turi tam tikrą savybę, padaroma apibendrinančio pobūdžio išvada, kad tą savybę turi visi tos klasės objektai*“ [PRLP]. Kai kuriais atvejais, formuojant išvadą, nepakanka ištirti kelis klasės objektus, reikia ištirti visus objektus. Visų klasės objektų ištyrimas vadinamas pilnąja indukcija, nes išvada visuomet yra teisinga, o tai, faktiškai, yra dedukcija. Dedukcija tai dar vienas naudojamas tyrimo metodas, kai remiantis logikos dėsniais iš kelių teisingų teiginių suformuojamas naujas teiginys ar išvada. Svarbiausi šaltiniai, skirti nagrinėjamai problematikai yra standartai, sertifikatų centrų veiklos nuostatai ir sertifikatų centrų parašo taisyklės. Būtent šiems dokumentams pagrinde ir taikomi minėti tyrimo metodai.

Darbas susideda iš keturių dalių. Pirmoje dalyje apibrėžiama el. parašo samprata: kas tai yra, kam ši technologija naudojama ir kam reikalinga, kaip ji veikia, kas ją sudaro, kur ją įsigyti. Antra dalis skirta apžvalgai: apžvelgiama pagrindinė literatūra, įvardinamos galimos el. parašo diegimo kliūtys, keliamų reikalavimų sritys, analizuojamas ištirtumas – kas yra padaryta kaimyninėse ir kitose šalyse. Trečioje dalyje analizuojami standartų reikalavimai viešojo rakto infrastruktūrai, jos komponentams, pateikti konkretūs reikalavimai, jie suskirstomi į grupes. Ketvirta dalis skirta sertifikatų centrų, Lietuvoje išduodančių kvalifikuotus sertifikatus, dokumentų palyginimui. Analizuojami svarbiausi sertifikatų centrų dokumentai: parašo taisyklės ir veiklos nuostatai. Tarpusavyje gretinami trijų sertifikatų centrų - UAB „Skaitmeninio sertifikavimo centro", VĮ „Registrų centro" ir Gyventojų registro tarnybos - dokumentai bei vertinama, kurio iš šių centrų teikiama paslauga yra kokybiškesnė.

1. APIE ELEKTRONINĮ PARAŠĄ

1.1. Elektroninio parašo poreikis

Sparčiai besivystant informacinei visuomenei, vis daugiau atsiranda visokių el. dokumentų: brėžiniai, ataskaitos, sąskaitos, sutartys, apskaitos dokumentai ir t. t. Kol nebuvo kompiuterių visi įvairių sričių dokumentai buvo spausdinami ant popieriaus ir patvirtinami antspaudu ir/arba parašu. Tačiau dvidešimto amžiaus pabaigoje tokie dokumentai pradėjo būti tvarkomi kompiuteriais, o išsivysčius telekomunikacijoms jie buvo ir perduodami. Toks perdavimas yra žymiai greitesnis ir pigesnis, nei tai būtų daroma paprastu paštu. Be to el. dokumentų saugojimas reikalauja daug mažiau vietos. Greitas ir pigus dokumentų perdavimas ypač svarbus yra tiems, kas užsiima tarptautiniu verslu, o el. komercija be el. dokumentų iš vis neegzistuoja.

Kokia parašo ar antspaudo esmė? Ant atspausdinto lapo padėtas parašas ar antspaudas patvirtina, jog autorius pritaria dokumente esančiai informacijai, informacija nėra iškraipyta, taip pat, identifikuojamas asmuo ar įstaiga, kurie yra atsakingi už patvirtintą dokumentą bei jo turinį. Toks pat patvirtinimas bei asmens ar įstaigos identifikavimas turi būti ir el. dokumentuose, kad juos gavęs žmogus iš karto matytų, jog el. dokumentas pasirašytas konkretaus asmens bei pateikti duomenys nebuvo pakeisti ar iškraipyti siuntimo metu. Visa tai užtikrina el. parašas.

1.2. Kas yra elektroninis parašas?

„*El. parašas – duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti*“ [EPĮ0; KARY]. El. parašas suteikia didesnį saugumą finansinėms transakcijoms atlikti, o asmenų bendravimas su įvairiomis institucijomis tampa patogesnis ir greitesnis. Žiūrint iš techninės pusės, el. parašas – tai produktas duomenų šifravimo sistemos, kuri užšifruodama duomenis (dokumentą) paverčia juos nesuprantama simbolių seka, o dešifruodama simbolių seką atstato pradinę, suprantamą duomenų formą.

1.3. Šifravimo mechanizmas

Kaip buvo minėta anksčiau, el. parašas – tai šifravimo sistemos produktas. Duomenims šifruoti yra taikomi du šifravimo metodai: simetrinis ir asimetrinis. El. parašas naudoja būtent asimetrinį šifravimo metodą. „*Tai skaitmeninis metodas. Todėl dažnai vietoje termino "el. parašas" naudojamas „skaitmeninis parašas"* " [VAUN]. Norint toliau šnekėti apie el. parašą ir suprasti jo veikimo principą, būtina išsiaiškinti, kaip veikia asimetrinė šifravimo sistema.

Pagrindinis skirtumas tarp simetrinio ir asimetrinio šifravimo metodų yra toks, kad šifravimui simetriniu metodu sugeneruojamas tik vienas raktas, o asimetriniu – du matematiškai tarpusavy susieti raktai. Jei dokumentas buvo užšifruotas asimetrinio metodo vienu poros raktu, tai dešifruoti įmanoma tik kitu poros raktu. Deja, naudojant ši metodą, duomenų šifravimo bei dešifravimo greitis yra daug mažesnis, nei tai būtų daroma simetriniu metodu. Svarbus faktas tai, kad jei vienas iš poros raktų yra žinomas tretiesiems asmenims, atskleisti kito poros rakto praktiškai neįmanoma.

Sugeneruotos poros raktai turi savo pavadinimus. Vienas raktas yra privatusis (private), jis duodamas parašo savininkui, kitas – viešasis (public), jį gali sužinoti bet kuris norintis. Privatusis raktas privalo būti saugomas itin griežtai: kompiuteryje, intelektualioj kortelėj (smartcard), o pasiekiamas turi būti tik įvedus slaptažodį ar/ir biometrinius duomenis (pvz., pirštų atspaudus). Šių raktų ilgis, priklausomai nuo reikalaujamo saugumo lygio, gali būti nuo 512 iki 4096 bitų. T.y. nuo 64 iki 512 simbolių (8 bitai = 1 simbolis). Paprastai tokius raktus sugeneruoja tokios paslaugos tiekėjai, nors tai padaryti gali ir pats asmuo, jeigu žino kaip.

1.4. Elektroninio parašo istorija

Šifruojant asimetriniu metodu, dažniausiai naudojamas „RSA" algoritmas. Šį algoritmą sukūrė trys Masačiusetso instituto profesoriai: R. **R**ivest, A. **S**hamir ir L. **A**dleman. Pagal jų pavardžių pirmas raides ir buvo pavadintas šis algoritmas. Asimetrinio šifravimo būdas buvo sukurtas 1978 m. Tokį atsiradimą paskatino simetrinio šifravimo metodo trūkumas. Simetrinis metodas turi tik vieną raktą, todėl jį sužinoję tretieji asmenys, gali ne tik perskaityti užšifruotą informaciją, bet ir siųsti klaidingą informaciją kito žmogaus vardu. Dar daugiau, jeigu siunčiamą informaciją norima paskleisti tarp daug gavėjų, tai kiekvienam iš jų saugiai perduoti raktą yra labai sunku ir nepatogu. Tuo tarpu naudojant viešojo rakto infrastruktūrą (Public Key Infrastructure – PKI) pastaroji problema dingsta. Viešasis raktas yra prieinamas visiems norintiems, todėl nereikia rūpintis dėl saugaus perdavimo ar rakto slaptumo. [HFPS]

1.5. Elektroninio parašo naudojimas

Susigeneravus raktų porą, tuoj pat galima pasirašinėti dokumentus. Deja, toks parašas neturės jokios juridinės galios. Parašas turi būti susietas su pasirašančiuoju asmeniu, t. y. turi būti patvirtinimas, jog raktai priklauso asmeniui. Ir tai reikia padaryti oficialiai. Todėl asmens duomenys kartu su viešuoju raktu pateikiami oficialioms institucijoms, kurios sudaro to asmens sertifikatą, pasirašo jį savo elektroniniu parašu, perduoda jį užsakiusiam asmeniui ir pagal užklausas teikia visiems kitiems, kam prireikia tikrinti to asmens el. parašus.

1.5.1. Sertifikatas

Norint dokumentus pasirašinėt el. parašu, visų pirma, reikia turėti sertifikatą. „*Sertifikatas – tai elektroninio pavidalo liudijimas, patvirtinantis, kad šifravimo raktų pora priklauso sertifikate nurodytam asmeniui.*“ [VAUN]. Sertifikatai gali būti dviejų rūšių: paprastieji ir kvalifikuoti. Kvalifikuotus sertifikatus išduoda tik nustatytus reikalavimus atitinkantys sertifikavimo centrai (Certificate Authorities – CA).

Pagal standartą X.509 kiekviename sertifikate privalo būti toki duomenys:

- sertifikato versija;
- unikalus sertifikato numeris;
- sertifikatą išdavusios įstaigos duomenys (pavadinimas, adresas, ...);
- sertifikato galiojimo laikas (pradžios ir pabaigos datos);
- asmens duomenys (vardas, pavardė);
- viešasis raktas, atitinkantis asmens turimą privatųjį raktą;
- papildomi duomenys (rakto naudojimo sąlygos, sertifikato naudojimo paskirties apribojimai, privataus rakto naudojimo terminai ir t.t.). [HFPS]

Sertifikavimo sistema yra sukurta tam, kad būtų galima patikrinti, jog pasirašyti el. duomenys iš tikro priklauso sertifikate nurodytam asmeniui. Dar tiksliau kalbant, reikia paliudyti, jog viešasis raktas priklauso tam asmeniui, kurio vardu yra pasirašyti duomenys. Tokį vaidmenį atlieka sertifikavimo centrai (CA).

1.5.2. Dokumento pasirašymas

Kai turime raktų porą ir sertifikatą, galima pradėti pasirašinėti dokumentus. El. parašo kūrimo metu sukuriami papildomi duomenys, vadinami santrauka. Tai pasirašomų duomenų, pasirašymo laiko, vietos, sertifikato nuorodos, parašo taisyklių nuorodos ir t. t. santrauka. Jos ilgis paprastai yra nuo 16 iki 20 simbolių. Gauta santrauka užšifruojama siuntėjo privačiuoju raktu ir taip gaunamas el. parašas. Tuomet jis yra pridedamas prie dokumento, kuris toliau įrašomas į laikmeną arba siunčiamas kompiuterių tinklais.

1.5.3. Dokumento tikrinimas

Gavėjas priėmęs „siuntinį“ jį perskaito. Jei dokumento tipas nėra labai svarbus arba turinys toks, kokio ir tikėtasi, gavėjas gali net nesidomėti dokumento autentiškumu ir tikėti tuo ką mato. Tačiau, jei reikalingas patvirtinimas, tuomet vykdoma parašo tikrinimo (dešifravimo) procedūra. Atskirai paimami atsiųsti duomenys (pasirašyti duomenys, pasirašymo laiko, vietos, sertifikato nuorodos, parašo taisyklių nuoroda ir t.t. – tai atviri duomenys) ir iš jų, tuo pačiu principu, kaip ir parašo formavimo metu, suformuojama santrauka. Lygiagrečiai vykdoma kita operacija. Iš gauto dokumento atsiųstos duomenų visumos paimama nuoroda į siuntėjo sertifikatą. Nuoroda į sertifikatą reikalinga tam, kad sužinotume siuntėjo viešąjį raktą. Nuoroda į sertifikatą visuomet yra saugoma el. parašo viduje. El. parašą paveikus viešuoju raktu atstatoma siuntėjo sudaryta santrauka. Tuomet gautos dvi santraukos yra lyginamos tarpusavy ir jeigu santraukos identiškos, tai duomenys tikrai nebuvo iškraipyti siuntimo metu, o siuntėjo tapatybė yra patvirtinama. Iki pilnos laimės ir užtikrintumo, reikia įsitikinti, jog nuorodą į sertifikatą atsiuntė ir dokumentą pasirašė, vienas ir tas pats asmuo. Tokią paslaugą teikia sertifikatus teikiančios įstaigos. Taip pat reikia atkreipti dėmesį į tai, ar dokumentas nebuvo pasirašytas tuomet, kai buvo pasibaigęs asmens sertifikato galiojimo laikas.

1.6. Sertifikatų įsigijimas

Norint pradėti naudotis el. parašu reikia susigeneruoti privačiojo ir viešojo raktų porą. Tam, kad el. parašas turėtų teisinę galią, reikia sertifikato, kuris oficialiai susieja raktų porą su savininku. Kol kas Lietuvoje yra trys registruoti kvalifikuotus sertifikatus sudarantys sertifikavimo paslaugų teikėjai:

- UAB „Skaitmeninio sertifikavimo centras“;
- VĮ „Registrų centras“;

- Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. [IVPK]

Paprastai, raktų porą suteikia sertifikatą išduodanti įstaiga ir vartotojui nebereikia tuo rūpintis pačiam. Tačiau ne viskas auksas, kas auksu žiba: imkime kad ir „Registrų centrą“. Sertifikatas kriptografinėje USB laikmenoje arba valstybės tarnautojo pažymėjime dviems metams kainuoja 127,60 lt. Pasibaigus sertifikato galiojimo terminui, jis pratęsiamas dviems metams už tą pačią, 127,60 lt sumą. Atrodytų daug, tačiau lyginant su SSC (Skaitmeninio Sertifikavimo Centras) teikiama paslauga, čia už **kvalifikuotą** (gali išduoti ir nekvalifikuotus. Tokie sertifikatai yra pigesni) sertifikatą metams reikia sumokėti 150 lt., o už USB ar kitokias laikmenas reikia sumokėti atskirai. Pasibaigus sertifikato galiojimo terminui, jis pratęsiamas vieneriems metams už tą pačią, 150 lt. sumą. Lyginant su pirmąja įstaiga, SSC paslauga yra daugiau negu dvigubai brangesnė.

Sertifikavimo paslaugą teikia ir didieji Lietuvos mobiliojo ryšio operatoriai:

- UAB „Bitė Lietuva“;
- UAB „Omnitel“. [IAER]

Šių operatorių teikiama paslauga vadinasi šiek tiek kitaip. Vietoj „elektroninis parašas“ paslauga vadinama „mobilusis elektroninis parašas“. Šios paslaugos pagrindinis skirtumas tas, kad kiekvienai pasirašymo operacijai reikia išsiųsti sms žinutę su savo, pasirašymui skirtu, kodu (sPIN). [SODR]. Trumposios žinutės išsiuntimas atstoja pasirašymo faktą. Omnitel svetainėje apie paslaugos kainą yra teigiama: „*Šiuo metu nėra taikomi jokie mokesčiai naudojantis Lietuvoje*“. Reikia pripažinti, taip ir yra. Paskambinus į klientų aptarnavimo centrą, buvo patvirtinta jog siunčiamos žinutės nieko nekainuoja. Naudojantis Bitės paslaugomis taikomas mėnesinis, 1 lt mokestis. Be to, reikia sumokėti nepilnai 15 lt už paslaugos įjungimą.

Lietuvos Respublikos Ryšių reguliavimo tarnyba **registruoja kvalifikuotus sertifikatus sudarančius sertifikavimo paslaugų teikėjus** ir viešai skelbia tik Lietuvoje įregistruotų ir prižiūrimų paslaugų teikėjų (sudarančių kvalifikuotus sertifikatus) sąrašą. Į šį sąrašą nei UAB „Omnitel“, nei UAB „Bitė Lietuva“ nepatenka. Todėl, pagal Informacinės visuomenės plėtros komiteto tinklalapyje paskelbtą informaciją galima teigti, jog šie mobilaus ryšio operatoriai teikia nekvalifikuotus sertifikatus.

2. EL. PARAŠO DIEGIMO APŽVALGA

2.1. El. parašo diegimo kliūtys

El. parašo atsiradimas Lietuvoje yra naujovė, bet tai naujovei įdiegti reikia įveikti eilę problemų. El. parašo procese dalyvauja keturi dalyviai:

- sertifikavimo centrai;
- pasirašantieji asmenys;
- parašo tikrintojai;
- laiko žymos tarnybos.

Kiekvienam iš šių dalyvių egzistuoja daugybė dokumentų. Tai taisyklės ir reikalavimai, kurių privalo laikytis visi dalyviai. Pvz.: reikalavimai sertifikavimo centrų (toliau CA) veiklai ir naudojamai įrangai; reikalavimai el. parašo struktūrai, pasirašymo įrangai, procedūroms bei aplinkai; reikalavimai el. parašo tikrinimo aplinkai ir procedūroms; reikalavimai laiko žymų tarnybų (toliau TSA – Time Stamp Authorities) veiklai ir įrangai.

2.2. PKI dalyviams keliami reikalavimai

Didžiausi reikalavimai yra keliami CA, t. y. jų teikiamoms paslaugoms bei įrangai. Šių paslaugų ir įrangos kokybė turi būti įvertinta atitinkamų institucijų, kurios, vėl gi, turi laikytis atitinkamų vertinimo procedūrų bei taisyklių. Viena iš tokių institucijų buvo EESSI (European Electronic Signature Standardization Initiative). Ji parengė įrangos ir procedūrų atitikties nustatytiems reikalavimams vertinimo vadovus. Kadangi ši institucija buvo tam ir sukurta, tai įgyvendinus tikslą, ji buvo panaikinta 2004 m. El. parašo diegime turi dalyvauti ir valstybė: „*CA pasirengimo atlikti savo funkcijas lygiui įvertinti valstybės turi būti parengusios CA savanoriškos akreditacijos reikalavimus ir akreditavimo tvarką.*“ [VAUN]

Dar vienas bendras ir svarbus reikalavimas CA, el. parašo kūrėjams ir tikrintojams bei TSA yra toks, kad jų naudojama įranga turi būti gauta iš gamintojų, kurie privalo turėti patikimų kokybės kontrolės institucijų išduotus sertifikatus ar pažymėjimus. Taigi iš čia išplaukia dar vienas reikalavimas įrangos gamintojams – jie patys turi pasirūpinti išleidžiamos įrangos įvertinimu pagal atitikties nustatytus reikalavimus.

2.3. El. parašo priežiūros institucija

Pagal Elektroninio parašo įstatymą ir Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimą Nr. 2108 CA (tokių valstybėje skaičius neribotas) turi būti prižiūrimi aukštesnės institucijos. „Tokia el. parašo priežiūros institucija turėtu akredituoti, tikrinti CA veiklą“ [VAUN]. Lietuvos respublikos, Elektroninio parašo įstatymo, 14 straipsnio 1 punktas teigia: „*Elektroninio parašo priežiūros institucijos funkcijas atlieka Vyriausybės įgaliota institucija*“[EPĮ0]. Lietuvoje tai daro Lietuvos Respublikos Ryšių reguliavimo tarnyba. Dar svarbu paminėti, jog priežiūros institucijos negali būti susijusios su el. parašo įrangos gamintojais ar paslaugos tiekėjais, jokia bendra veikla. [EPĮ0]

2.4. Problematika

Nors pasaulyje elektroninio parašo infrastruktūra, kurią sudaro techninė bei programinė įranga, teisės aktai ir standartai, buvo pradėta plėtoti 1989 metais ir buvo pristatytas pirmasis produktas, leidęs pasirašyti dokumentus skaitmeniniu parašu, tačiau Lietuvoje ši technologija dar nėra labai populiari. Elektroninio parašo įstatymas, kuris reglamentuoja elektroninio parašo kūrimą, tikrinimą galiojimą, parašo naudotojų teises ir atsakomybę, nustato sertifikavimo paslaugas ir reikalavimus jų teikėjams bei el. parašo priežiūros institucijos teises ir funkcijas, Lietuvoje buvo priimtas 2000 metais [EPNT]. Nemažai išleista ir poįstatyminių aktų, atrodytų jog belieka tik diegti šią technologiją ir plėsti, tačiau iki šiol pasiekti rezultatai (Sertifikavimo centrų skaičius, klientų skaičius ir naudojamumas) yra menki. „Apie realų, masiškai naudojamą elektroninį parašą daugelis tikriausiai išgirdo neseniai vykusios parodos „InfoBalt 2007“ metu“ [GYRE], todėl natūralu, jog kyla klausimas: kas gi stabdo, kas trukdo šios technologijos diegimą ir vystymąsi?

Viena iš galimų priežasčių, kuri ilgą laiką stabdė elektroninio parašo plėtrą, yra bankai, kurių išduodamos klientų identifikavimo priemonės, skirtos prisijungimui prie internetinės bankininkystės sistemų, buvo klaidingai laikomos elektroniniu parašu [EVLI]. Kita daug realesnė priežastis yra sunkumai, susiję su atitinkamų tarnybų steigimu ar techninių ir programinių sprendimų priėmimu, kaip:

1. **Sertifikavimo centrai (CA –** Certificate Authorities). Norint įsteigti sertifikavimo centrą, kuris vėliau būtų laikomas kaip kvalifikuotus sertifikatus išduodanti įstaiga, reikia, jog minėta įstaiga atitiktų Vyriausybės nustatytus reikalavimus kuriuos, savaime suprantama, nėra taip lengva įgyvendinti.

2. **Laiko žymos tarnybos (TSA – Time Stamp Authorities)**. Tam, kad elektroninio parašo vartotojas gautų laiko žymą, jis turi kreiptis į laiko žymos tarnybą, kuriai vėl keliama daug reikalavimų.

3. **Programinė įranga**. Tiek sertifikavimo centrai, tiek laiko žymos tarnybos, tiek elektroninio parašo vartotojai, naudoja atitinkamą programinę įrangą, kuriai taip pat keliami aukšti reikalavimai.

4. **Techninė įranga**. Programinė įranga nekabo ore, ji egzistuoja tik tam tikroje techninėje įrangoje, kuri nėra išimtis ir jai lygiai taip pat keliami įvairūs saugumo reikalavimai.

Kaip matosi yra daugybė reikalavimų, kurių įgyvendinimas atsiremia į kainą, laiką ir patikimumą.

2.5. El. parašo technologijos ištirtumas

2.5.1. Kas padaryta kaimyninėse valstybėse

Latvijoje 2002 metų pabaigoje parlamentas patvirtino elektroninių dokumentų įstatymą. 2005 m. liepos mėn. Latvijos paštas tapo pirmuoju kvalifikuotu elektroninio parašo paslaugos teikėju, taip pat buvo akredituotas kaip kvalifikuotų sertifikatų išdavimo centras. Dabartinė Latvijos rinkos situacija yra tokia, kad jie turi laiko žymos tarnybą, naudoja saugaus parašo kūrimo įrangą (SSCD – Secure Signature Creation Device). Klientų programinė įranga, kuri skirta dokumento pasirašymui, laiko žymos gavimui bei parašo patikrinimui, duodama nemokamai. Per darbo savaitę apytiksliai uždedama 10 laiko žymų [EREG].

Lenkijoje elektroninio parašo įstatymas buvo priimtas 2001 metais, kuris buvo kuriamas laikantis Europos sąjungos direktyvos (99/93/EC). Šios technologijos diegimas prasidėjo 2002 metais. Galima sakyti jog nuo įstatymo išleidimo elektroninis parašas turėjo tokią pačią teisinę galią, kokią turi ir paprastas parašas [WAPA]. Dabar Lenkija turi keturis kvalifikuotus sertifikatus išduodančius sertifikavimo centrus.

Rusijoje elektroninis parašas dar nėra paplitęs. Jį naudoja tik federalinis iždas (Federal Treasury), siunčiant dokumentus į savo regioninius filialus. Savo sertifikavimo centrų neturi, o naudojasi Microsoft kompanijos sertifikatais. Rusijos federalinio iždo direktoriaus pavaduotojo Alexei Popov teigimu planuojama diegti viešojo rakto infrastruktūra, kurios numatomi vartotojai bus didieji bankai, federalinis iždas ir tikriausiai bankų klientai, kurie vykdys piniginius apmokėjimus. Kaip matyti nei paprasti piliečiai, nei įmonės negalės naudotis elektroninio parašo paslaugomis. Panašu jog norintiems užsiiminėti elektronine komercija, Rusija dar nėra pati tinkamiausia vieta tai pradėti [ELME].

Baltarusijoje elektroninio parašo įstatymo projektas dar tik neseniai buvo paduotas į parlamento posėdį svarstymui (2009 m.), todėl apie rezultatus dar anksti kalbėti [MIDO].

2.5.2. Kas padaryta ES ir kitose valstybėse

Vokietijoje elektroninio parašo įstatymas išleistas 2001 metais. Nuo to laiko viešojo rakto infrastruktūra yra intensyviai plėtojama. Dabar jau yra dešimt akredituotų įstaigų, iš kurių šešios yra sertifikavimo centrai, teikiantys kvalifikuotus sertifikatus ir laiko žymas, trys sertifikavimo centrai, kurie teikia tik kvalifikuotus sertifikatus, ir viena įstaiga, kuri teikia tik laiko žymas. Visų šių įstaigų veiklą prižiūri „Federalinė tinklų agentūra“ (Bundesnetzagentur). Analogiška institucija Lietuvoje yra Lietuvos Respublikos Ryšių reguliavimo tarnyba. Taip pat minėta vokiečių institucija yra šakninis sertifikavimo centras (root), kuris turi teisę steigti ar naikinti kitus jam pavaldžius sertifikavimo centrus [BNET].

Italija turi 16 sertifikavimo centrų ir dar yra 18 tokių, kurie jau pasitraukė iš rinkos arba pakeitė savo vardą. Visus šiuos centrus prižiūri „Nacionalinis IT viešajame administravime centras“ (CNIPA – Centro Nazionale per Informatica nella Pubblica Amministrazione) [CNIP]. Taip pat CNIPA yra parengusi dokumentą („skaitmeninio parašo naudojimo techninis vadovas“), kuris skirtas padėti pavieniams vartotojams ir kompanijoms naudotis elektroniniu parašu. Šiame dokumente yra atskiras skyrius, kuriame pateikiama konkreti programinė įranga, kurią vartotojai gali parsisiųsti nemokamai ir instrukcijos, kaip ja naudotis [CNGA]. Iš to galima daryti išvadą, jog nei vienas iš sertifikavimo centrų nėra prisirišęs prie savo programinės įrangos ir, turint sertifikatus iš įvairių sertifikavimo centrų, elektroninį parašą galima formuoti su viena programa. Panašu, jog sistema yra centralizuota ir patogi, žiūrint iš vartotojo pusės.

Nors Indija laikoma trečiojo pasaulio šalimi, bet ji turi neblogai išvystytą viešojo rakto infrastruktūrą. Yra vienas šakninis sertifikavimo centras, kuris įsteigtas 2007 metais pagal X.509 standartą. Yra kiti sertifikavimo centrai, kurių sertifikatus pasirašo šakninis sertifikavimo centras. Yra įstaiga, prižiūrinti ir reguliuojanti visų kvalifikuotų sertifikavimo centrų darbą, kuri vadinasi „Controller of Certifying Authorities” (CCA). Iš viso Indijoje yra septyni kvalifikuotus sertifikatus teikiantys sertifikavimo centrai [COCA].

Labai įdomus sertifikavimo centrų pasiskirstymas Amerikoje. Ten sertifikavimo centrai steigiasi ir priklauso ne visai valstybei, bet konkrečiai valstijai. Tokių valstijų, kuriom priklauso akredituoti sertifikavimo centrai yra septynios (Utah, Oregon, North Carolina, California, Washington, Nebraska, Texas) ir pastebimas toks dėsningumas, jog kiekviena iš septynių valstijų turi po 2-4 akredituotus sertifikavimo centrus. Dar daugiau, visur kartojasi beveik tie patys

sertifikavimo centrai: VeriSign, Inc., ID Certify, Inc., Digital Signature Trust Company, kurie yra puikiai žinomi visame pasaulyje [TPKI].

Beveik visos valstybės, kurios jau yra įsidiegę ir naudoja elektroninio parašo technologiją, įstatymus yra priėmusios apie 2000 metus (+/- 2 metai). Tai kodėl gi vienos valstybės sugeba išvystyti ir išpopuliarinti šią technologiją, o kitos ne, kokie reikalavimai trukdo vystytis šiai technologijai?

3. REIKALAVIMAI PKI TARNYBOMS IR JŲ NAUDOJAMAI ĮRANGAI

3.1. Reikalavimai sertifikavimo centrų struktūrai

Paprastai kiekvieno sertifikavimo centro paskirtis ir funkcijos sutampa, todėl norint vykdyti tas funkcijas reikalingos atitinkamos sertifikavimo centro tarnybos:

1. **Registravimo tarnyba**. Ji iš asmenų priima būtinus duomenis sertifikatams sudaryti, patikrina juos ir perduoda sertifikatų sudarymo tarnybai. sertifikavimo centras gali turėti kelias tokias tarnybas, pavyzdžiui, įvairiose vietovėse.

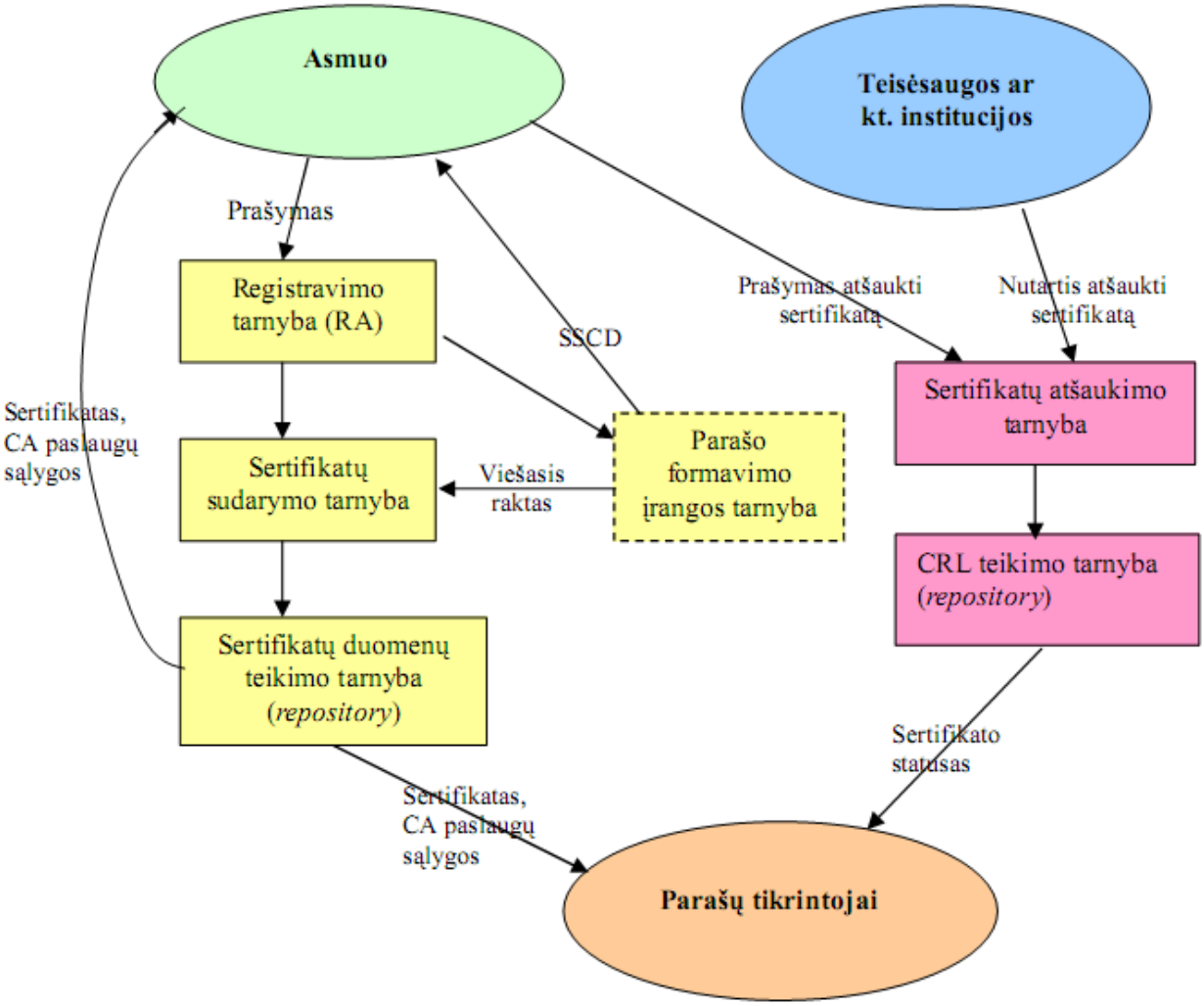
2. **Sertifikatų sudarymo tarnyba**. Ji iš registravimo tarnybos gautų asmens duomenų ir viešojo rakto sudaro sertifikatą, pasirašo jį savo elektroniniu parašu ir atiduoda sertifikatų duomenų teikimo tarnybai.

3. **Sertifikatų duomenų teikimo tarnyba**. Sertifikatas atiduodamas jo savininkui ir užrašomas į sertifikatų duomenų bazę – katalogą. Iš pastarosios pagal užklausas sertifikatų duomenys teikiami elektroninių parašų tikrintojams.

4. **Sertifikatų atšaukimo tarnyba**. Šios tarnybos funkcijos yra nutraukti sertifikato galiojimą paprašius pačiam sertifikato savininkui, teisėsaugos institucijų sprendimu, paprašius asmeniui, kuriam atstovauja sertifikato savininkas. Tai turi būti atliekama greitai, sugaištant ne daugiau nustatyto laiko. Informacija apie atšauktus sertifikatus kaupiama atšauktų sertifikatų sąraše (CRL – Certificate Revocation List), kuris periodiškai perduodamas CRL teikimo tarnybai.

5. **CRL teikimo tarnyba**. Ji informaciją apie atšauktus sertifikatus laiko pas save ir operatyviai pagal užklausas teikia elektroninių parašų tikrintojams. Tie elektroniniai parašai, kurie buvo sukurti sertifikato galiojimo laikotarpiu, išlieka galiojantys. Elektroninis parašas, sukurtas negaliojant ar nesant sertifikatui, yra negaliojantis [VAUN].

Sertifikavimo centrui neturint tokios struktūros (1 pav.), jo veikla negalima. Be to tai nėra labai sunku įgyvendinti, lyginant su kitais reikalavimais.



1 pav. Sertifikavimo centro struktūra [VAUN].

3.2. Reikalavimai sertifikavimo centrų veiklai

Tam, kad sertifikavimo centras galėtų pradėti savo veiklą, pirmiausia jis turi parengti veiklos nuostatus (CPS - Certification Practice Statement). Veiklos nuostatai – tai pagrindinės sertifikavimo centro veiklos taisyklės, kuriose detaliai aprašyti sertifikavimo centro atliekami veiksmai. Registruodamasis elektroninio parašo priežiūros institucijoje, sertifikavimo centras turi pateikti savo veiklos nuostatus, pagal kuriuos (gali būti ir kitų dokumentų) minėta institucija nusprendžia, ar sertifikavimo centras yra tinkamas vykdyti savo funkcijas, ar ne. Jeigu tinkamas, tada išduodamas leidimas sertifikatų centrui, kuris turi užtikrinti tokias veiklas:

1. **Sertifikavimo centro veiklos nuostatų rengimas**. Sertifikavimo centras turi parengti savo veiklos nuostatus (CPS), kurie atitiktų pasirinktas sertifikato taisykles (CP) ir užtikrintų patikimą paslaugų teikimą, ir paskelbti internete paslaugų teikimo sąlygas.
2. **Raktų tvarkymas**. Sertifikavimo centras turi užtikrinti:

a) kad raktai būtų kuriami kontroliuojamoje aplinkoje, naudojant saugią elektroninio parašo įrangą (SSCD) ir dalyvaujant bent dviems įgaliotiems darbuotojams;

b) Sertifikavimo centro privačiojo rakto konfidencialumą ir saugumą;

c) sertifikatuose esantiems sertifikavimo centro parašams tikrinti skirto viešojo rakto saugumą ir autentiškumą bei šio rakto saugų teikimą elektroninio parašo naudotojams;

d) kad sertifikavimo centras nelaikytų ir nekopijuotų abonentams parengtų privačiųjų raktų;

e) kad sertifikavimo centro privatusis raktas būtų naudojamas saugiai ir tik sertifikatams bei CRL sąrašams pasirašyti, o pasibaigus šio rakto galiojimo laikui, jis būtų sunaikinamas;

f) saugų raktų porų kūrimą, kai juos savo abonentams teikia sertifikavimo centras, ir privačiųjų raktų slaptumą;

g) saugios parašo formavimo įrangos (SSCD), jei sertifikavimo centras ją teikia savo abonentams, saugų rengimą.

3. **Sertifikatų tvarkymas**. Sertifikavimo centras turi užtikrinti:

a) kad abonentai iki sutarties pasirašymo būtų tinkamai informuoti apie sertifikatų teikimo ir naudojimo sąlygas bei šių sąlygų laisvą teikimą elektroninėmis priemonėmis;

b) kad būtų tinkamai patikrinta asmens, kuriam sudaromas sertifikatas, tapatybė ir kiti jo duomenys;

c) kad jau anksčiau užregistruoto asmens prašymas sudaryti naują arba atnaujinti senąjį sertifikatą pagal patikslintus asmens duomenis būtų išsamus ir sankcionuotas;

d) sertifikatų sudarymo saugumą, padedantį išsaugoti jų autentiškumą;

e) kad sertifikatų duomenys esant užklausai būtų teikiami abonentams ir elektroninių parašų tikrintojams;

f) savalaikį sertifikatų atšaukimą ar galiojimo sustabdymą remiantis prašymais asmenų, kurie turi teisę pateikti tokį prašymą, ir patikrinus jų tapatybę.

4. **Valdymas ir veikla.** Sertifikavimo centras turi užtikrinti, kad:

a) jo organizacinė struktūra, administracinės ir valdymo procedūros būtų patikimos;

b) jo informacija ir visa paslaugoms teikti reikalinga įranga būtų tinkamai apsaugota;

c) personalas būtų reikiamos kvalifikacijos ir laikytųsi sertifikavimo centro nustatytų taisyklių ir paslaugų teikimo tvarkos;

d) būtų naudojama patikima sertifikatų tvarkymo sistema, apsaugota nuo modifikavimo;

e) tik įgalioti asmenys turėtų prieigą prie patikimos sertifikatų tvarkymo sistemos ir ji būtų naudojama teisingai su minimaliu sutrikimų pavojumi;

f) fizinė prieiga prie kritinių paslaugos vietų (pvz., sertifikatų sudarymo ir pasirašymo) būtų kontroliuojama;

g) nesėkmės atveju, įskaitant sertifikatams pasirašyti naudojamo sertifikavimo centro privačiojo rakto kompromitaciją, paslaugų teikimas būtų kaip galima greičiau atstatytas;

h) būtų minimizuota potenciali abonentų ir elektroninio parašo tikrintojų žala sertifikavimo centrui nutraukus veiklą, ir su sudarytais sertifikatais susijusi informacija kaip įrodinėjimo priemonė būtų teikiama teismams bet kuriuo metu to prireikus;

i) būtų laikomasi teisės aktų reikalavimų (pvz., asmens duomenų teisinės apsaugos įstatymo);

j) visa sutartyje su abonentu nurodyta informacija, susijusi su sertifikatais, būtų užrašoma ir saugoma nurodytą laiką, kad galima būtų ją panaudoti kaip įrodinėjimo priemonę teisme;

k) būtų apdrausta sertifikavimo centro civilinė atsakomybė. To reikia, kad sertifikavimo centras galėtų padengti abonentų nuostolius savo klaidos arba nenumatytais atvejais;

l) sertifikavimo centro veikla būtų nutraukiama vadovaujantis įstatymais. Šiuo atveju turi būti nutraukiamas galiojimas visų sertifikavimo centro sudarytų sertifikatų, o atšauktų sertifikatų sąrašas (CRL) perduotas kitam sertifikavimo centrui arba elektroninio parašo priežiūros institucijai. [VAUN].

Akivaizdu, jog reikalavimai veiklai yra žymiai griežtesni, labiau apibrėžti ir jų yra kur kas daugiau. Tai gali būti tik viena iš priežasčių, kodėl sunkiai diegiama elektroninio parašo technologija.

3.3. Reikalavimai laiko žymos tarnyboms, jų veiklai

Laiko žymos tarnyba (TSA) - tai patikima trečioji šalis, kuri vartotojui kreipusis uždeda laiko žymą, kuri yra kaip įrodymas, jog elektroninis parašas buvo sukurtas ne vėliau, negu žymoje nurodytas laikas. Kaip TSA turi kurti žymas ir valdyti žymos kūrimo procesą, kad jomis galėtų pasitikėti vartotojai, nusako tokie reikalavimai:

1. **TSA veiklos nuostatai ir jų skelbimas:**

   a) TSA savo veikla turi užtikrinti patikimą laiko žymos paslaugų teikimą;

   b) TSA turi parengti savo veiklos nuostatus ir juos bei laiko žymos paslaugų teikimo sąlygas paskelbti internete visiems vartotojams.

2. **Raktų tvarkymas:**

   a) TSA turi užtikrinti, kad bet kokie kriptografiniai raktai būtų generuojami laikantis standartų;

b) TSA turi užtikrinti savo privačiojo rakto konfidencialumą ir vientisumą;

c) TSA turi užtikrinti pasitikinčioms šalims platinamo TSA viešojo rakto ir bet kurių kitų susijusių parametrų vientisumą ir autentiškumą;

d) TSA sertifikato galiojimo ir atitinkamo privačiojo rakto naudojimo trukmė turi būti ribota, atsižvelgiant į naudojamus duomenų santraukos apskaičiavimo ir parašo kūrimo algoritmus bei laiko žymoms pasirašyti naudojamo rakto ilgį;

e) TSA turi užtikrinti, kad jos privatusis raktas laiko žymoms pasirašyti nebebūtų naudojamas pasibaigus sertifikate nustatytam terminui;

f) TSA turi užtikrinti laiko žymoms pasirašyti naudojamo kriptografinio modulio saugumą, viso jo gyvavimo ciklo metu.

3. **Laiko žymos kūrimas:**

a) TSA turi užtikrinti, kad laiko žymos būtų kuriamos saugiai ir į jas būtų įtraukiamas teisingas laikas;

b) TSA turi užtikrinti, kad jos laikrodis paskelbtu tikslumu būtų sinchronizuotas su universaliuoju laiku UTC.

4. **TSA valdymas ir darbas:**

a) TSA turi užtikrinti, kad administracinės ir valdymo procedūros atitiktų pripažintus standartus;

b) TSA turi užtikrinti, kad jos informacija ir kitoks turtas būtų tinkamai apsaugoti;

c) TSA turi užtikrinti, kad personalas ir samdomi darbuotojai stiprintų ir palaikytų TSA veiksmų patikimumą ir kad darbuotojų sukčiavimo galimybės būtų sumažintos iki minimumo;

d) TSA turi užtikrinti, kad fizinė prieiga prie kritinių paslaugos vietų (laiko žymos formavimo ir pasirašymo) būtų kontroliuojama ir fizinis pavojus jos turtui būtų minimizuotas;

e) TSA turi užtikrinti, kad TSA sistemos komponentai būtų saugūs ir būtų naudojami teisingai, su minimaliu sutrikimų pavojumi;

f) TSA turi užtikrinti, kad tik įgalioti asmenys turėtų prieigą prie TSA sistemos;

g) TSA sistemoje naudojami komponentai (kriptografinis modulis, kt.) turi būti apsaugoti nuo modifikavimo;

h) TSA turi užtikrinti, kad atsitikus įvykiams, turintiems įtakos laiko žymų teikimo saugumui, įskaitant TSA privačiojo rakto kompromitaciją arba pastebėjus laikrodžio sutrikimus, vartotojai būtų tinkamai informuojami;

i) TSA turi užtikrinti, kad būtų minimizuota potenciali vartotojų žala TSA nutraukiant veiklą, ir, kas ypač svarbu, kad būtų nepertraukiamai teikiama informacija, reikalinga anksčiau sukurtų laiko žymų teisingumui patikrinti;

j) TSA turi užtikrinti, kad nebūtų pažeidžiami įstatymų ir kitų teisės aktų reikalavimai, pvz., asmens duomenų apsauga;

k) TSA turi užtikrinti, kad visa reikiama informacija, susijusi su laiko žymų kūrimu, audito tikslams būtų užrašoma ir saugoma atitinkamą laiką, kad, reikalui esant, galima būtų ją panaudoti kaip įrodinėjimo priemonę teisme. [VAUN].

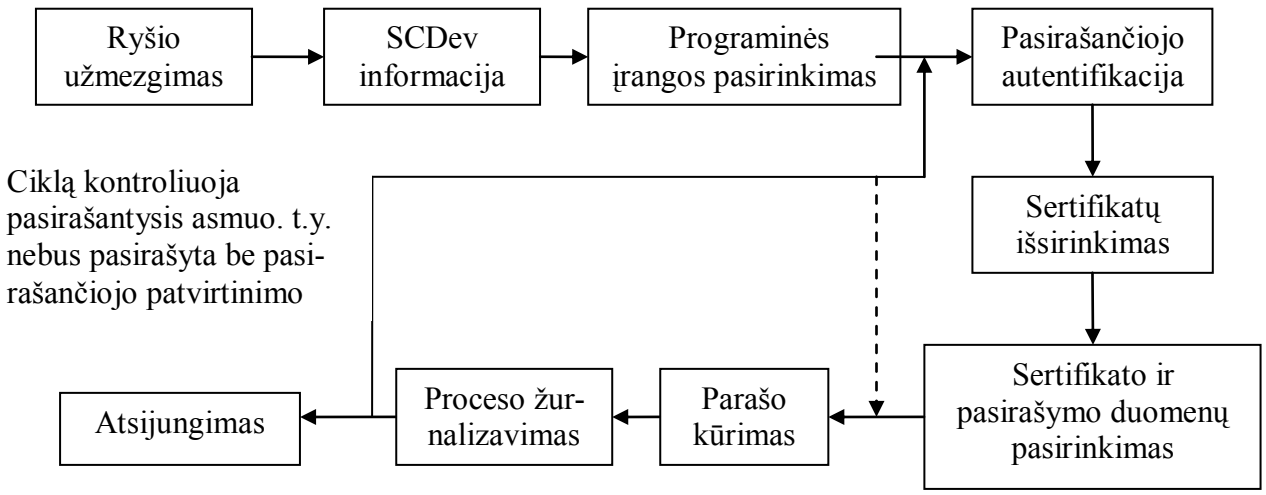
Vėl matosi didelis kiekis reikalavimų, taigi turime dar vieną galimą kliūtį, diegiant elektroninio parašo technologiją.

3.4. Reikalavimai programinei įrangai

3.4.1. Kliento programinė įranga

Programinė įranga reikalinga ne tik sertifikavimo centrams, laiko žymų tarnyboms, bet ir klientams, kurie naudosis elektroniniu parašu. Žemiau pateiktas sąrašas reikalavimų, kuriuos turi tenkinti kliento programinė įranga (aplikacija):

1. Sąveikos nuoseklumas. Formuojant parašą, komunikatorius (SSC - SCDev/SCA Communicator) užmezga ryšį tarp parašo kūrimo įrenginio (SCDev) ir parašo kūrimo aplikacijos (SCA). Šis komponentas yra labai jautrus saugumo atžvilgiu, todėl bet koks veiklos sutrikimas (pvz., dėl piktavališko bandymo įsiskverbti į sistemą) gali sugadinti parašą. 2 pav. iliustruoja, kokia eilės tvarka vyksta sąveika.



2 pav. Įvykių seka tarp parašo formavimo įrenginio ir programos [CWA0].

Brūkšninė linija rodo, jog vienokia parašo formavimo įranga gali reikalauti vartotojo autentifikacijos kiekvieno parašo formavimo metu, kitokia gali reikalauti autentifikacijos tik vieną kartą, kol nebus išjungta programa ar atjungtas parašo formavimo įrenginys. Jeigu parašo kūrimo programa suteikia galimybę pasirinkti, kurį variantą naudoti, tuomet tokia konfigūravimo funkcija privalo būti apsaugota, t. y. tik pasirašantysis asmuo turi teisę keisti tokius nustatymus.

2. Fizinio ryšio kūrimas. Parašo formavimo aplikacija privalo turėti bent vieną fizinį ryšį su parašo formavimo įrenginiu. Tokiems įrenginiams, kai ryšys užmezgamas dinamiškai (pvz., įkišant USB raktą ar kortelę į atitinkamą lizdą), turi būti užtikrinti šie dalykai:

a) pakankamas elektros srovės padavimas, o įtampa negali išeiti už nustatytų normų. Tokiu būdu bus užtikrintas stabilus įrenginio veikimas;

b) taktų generatoriaus veikimas atitinkamu dažniu. Tokiu būdu sinchronizuojamas bitų perdavimas;

c) parašo formavimo aplikacija turi palaikyti perdavimo protokolus, kuriuos naudoja parašo kūrimo įrenginys.

3. Parašo formavimo įrenginio funkcijos pasirinkimas. Toks reiškinys gali būti realizuotas įrenginyje (pvz., USB rakte), kuris savyje turi ne vieną, o kelias funkcijas. Dar daugiau, parašo formavimo įrenginio funkcijos gali būti dalis didesnės aplikacijos, kuri turi daugiau funkcijų, ne tik parašo kūrimo (pvz., namų bankininkystės programa). Jeigu yra naudojamas toks multifunkcinis įrenginys, tuomet parašo formavimo aplikacija turi pasirinkti vieną iš tokių.

4. Sertifikatų išsirinkimas. Parašo formavimo įrenginyje gali būti keli sertifikatai (pvz., pasirašančiojo sertifikatai su skirtingomis pareigomis arba sertifikatai skirtingiems pasirašymo raktams). Jeigu taip yra, tuomet toks įrenginys turėtų pateikti tokią informaciją:

a) kaip pasirinkti sertifikatą;

b) nuorodą į sertifikatą; (Pasirašantis asmuo gali turėti kelis sertifikatus. Pasirašydamas jis turi nurodyti, kurį sertifikatą naudos);

c) atskirti, kuris sertifikatas priklauso kuriai sertifikatų grandinei.

Priklausomai nuo parašo formavimo įrenginio gamintojo saugumo taisyklių sertifikato pasirinkimas gali būti atviras arba uždaras, t. y. pasirašantysis asmuo sertifikatą gali pasirinkti bet kada arba tik autentifikavęsis.

5. Parašo formavimo duomenų pasirinkimas. Parašo formavimo įrenginyje gali būti įrašyti keli parašo formavimo duomenys (privatieji raktai), tuomet žmogui turi būti sudaryta galimybė,

sąlygos pasirinkti reikiamą, t. y. tą, kuris atitinka pasirašančiojo tikslą ar ketinimus. Pasirinkus norimus parašo formavimo duomenis (privatųjį raktą), turi būti nurodomas ir tą raktą atitinkantis sertifikatas, tai užtikrina įrenginio atpažinimo žymė (Token), kuri turi informaciją, žyminčią ryšį tarp sertifikato ir nuorodos į parašo formavimo duomenis.

6. Pasirašančiojo autentifikavimas. Jeigu parašo formavimo įrenginys neturi autentifikacijos duomenų įvedimo įrenginio, tuomet komunikatoriaus (tarp programos ir įrenginio) komponentas iš autentifikacijos komponento saugiu kanalu gauna pasirašančiojo autentifikacijos duomenis ir su atitinkama komanda pasiunčia viską į parašo formavimo įrenginį tam, kad būtų palyginti duomenys. Rezultatas turėtų būti vienas iš šių:

a) patikrinimas sėkmingas;

b) patikrinimas nesėkmingas;

c) patvirtinimas užblokuotas dėl per didelio nesėkmingų bandymų skaičiaus.

Rezultatas grąžinamas atgal į autentifikacijos komponentą, kuris vartotojui išmeta atitinkamą pranešimą.

7. Skaitmeninio parašo (santraukos) skaičiavimas. Paskutinis parašo formavimo procesas yra santraukos skaičiavimas. Santrauka yra sukuriama pačiame parašo formavimo įrenginyje, kuris ją turi pateikti kaip bitų seką.

8. Saugumo reikalavimai komunikatoriaus (tarp programos ir įrangos) komponentui:

a) tam, kad dėl fizinės sąsajos veikimo sutrikimo nebūtų blogai sukurtas parašas, visų šio komponento palaikomų fizinių sąsajų parametrai neturi išeiti už nustatytų normų ribų;

b) jeigu tarp parašo kūrimo aplikacijos ir parašo kūrimo įrenginio yra naudojamas bevielis ryšys, komunikatorius turi turėti priemones draudžiančias slapta sekti ar kitaip įsiterpti į šį ryšį.

c) komunikatorius turi būti apsaugotas nuo bet kokio neautorizuoto modifikavimo. [CWA0].

3.4.2. Paslaugos teikėjų ir klientų parašo kūrimo programinė įranga

Žemiau pateiktas sąrašas reikalavimų, kuriuos turi tenkinti paslaugos teikėjų gaminama ir teikiama vartotojams programinė įranga, parašams kurti ir tikrinti:

1. **Saugus kanalas**. Tai reikalavimai kanalui, kad būtų apsaugoti pasirašomi duomenys, kol jie keliauja į saugų parašo formavimo įrenginį:

a) baziniai saugaus kanalo reikalavimai. Pirma, programinė įranga turi apsaugoti nuo tyčinio ar atsitiktinio pasirašomų duomenų iškraipymo, t. y. užtikrinti pasirašomų duomenų vientisumą. Antra, kanalas turi užtikrinti vartotojo duomenų konfidencialumą, t. y. užtikrinti vartotojo autentifikacijos duomenų, pasirašomų duomenų ir jų komponentų slaptumą;
b) viešųjų pasirašymo terminalų reikalavimai. Tam, kad nebūtų atskleisti ar netinkamai panaudoti pasirašančiojo autentifikacijos duomenys bei pasirašomi duomenys, visi su parašu susiję duomenys turi būti ištrinami po kiekvienos pasirašymo operacijos. Toks terminalas negali kopijuoti ar kaip nors kitaip užlaikyti šių elementų;
c) pasirašomų duomenų ir parašo atributų apsaugos reikalavimai. Programinė įranga turi užtikrinti, kad pasirašomi duomenys ar jų dalys nėra sukeisti. T. y. dokumento peržiūros (preview) metu vartotojo matomi duomenys turi išlikti tokie patys ir pasirašymo metu.

2. **Jei parašo kūrimo programos išskaidytos.** Moduliai sudarantys parašo kūrimo programą gali būti pasiskirstę per kelias skirtingas platformas, tai reiškia jog yra grėsmė, kad informacija gali būti perduodama nepatikimais komunikaciniais ryšiais, nepatikimomis programų sąsajomis ar nepatikimais programinės/techninės įrangos moduliais. Taigi, programinė įranga turi užtikrinti, jog kelias, kuriuo vartotojo autentifikacijos duomenys, pasirašomi duomenys bei jų elementai keliauja iš vieno programos komponento į kitą (pvz., tarp skirtingų programos ar techninės įrangos modulių), būtų saugūs ir garantuotų duomenų vientisumą ir konfidencialumą.
3. **Sistemos, tiesiogiai nedalyvaujančios parašo formavimo metu.** Tai sisteminiai ar programiniai procesai, kurie dalyvauja toje pačioje aplinkoje (pvz., operacinėje sistemoje) kaip ir pasirašymo programinė įranga, tačiau nėra naudojami, nereikalingi parašo formavimo metu. Todėl turi būti užtikrinta apsauga, kad joks nepatikimas procesas neįsiterptų į pasirašymo procesą.
4. **Parašo patvirtinimas po pasirašymo.** Labai rekomenduojama, kad vartotojui būtų sudaryta galimybė pačiam patvirtinti, jog skaitmeninis parašas buvo susietas su reikiamais pasirašomais duomenimis ir parašo atributais.
5. **Reikalavimai pasirašomiems duomenims.** Pasirašomus duomenis privalo sudaryti:
    a) pasirašomas dokumentas;
    b) pasirašančiojo sertifikatas, kurį jis pats pasirenka;
    c) pasirašomo dokumento duomenų tipas (pvz. doc, avi, jpg, ir t.t.), kad tikrintojas žinotų su kokia programa atverti duomenis. [CWA0].

Žinoma, pasirašomus duomenis gali sudaryti ir daugiau parašo atributų, tačiau aukščiau išvardinti yra privalomi, o likę dedami priklausomai nuo elektroninio parašo formato (BES, EPES, ES-T, ES-C, ES-X).

3.4.3. Paslaugos teikėjų ir klientų parašo tikrinimo programinė įranga

Yra reikalaujama, jog parašas turi būti patikimai patvirtintas, o pats patvirtinimas būtų korektiškai atvaizduotas.

1. **Bendrieji reikalavimai.** Visi parašo tikrinimo sistemos komponentai turi būti realizuoti saugioje aplinkoje. Tai aplinka, kurioje atmintis, duomenų apdorojimas ir procesai yra apsaugoti nuo neteisėtų modifikacijų ar nepageidaujamos veiklos. Tokiai aplinkai įgyvendinti turi būti pasirinkta kuri nors iš šių priemonių:

   a) saugumo priemonės programinėje įrangoje. Saugumas, kuris gali būti pasiektas, priklauso nuo operacinės sistemos saugumo lygio. Kompiuteriuose su standartine operacine sistema derėtų turėti papildomas apsaugos priemones;

   b) saugumo priemonės „Tamper-evident" modulyje. Tai toks procesas ar įrenginys, kuris saugomame objekte leidžia lengvai aptikti nepageidaujamą veiklą. Todėl, net jei ir nepavyksta apsisaugoti nuo nepageidaujamos veiklos ar bandymo kažką neteisėtai modifikuoti, vartotojas gali tai aptikti. Kompiuteriuose su standartine operacine sistema toks modulis galimas tik kaip atskiras išorinis įrenginys;

   c) saugumo priemonės „Tamper-resistant" modulyje. Tai toks modulis, kuris nepageidaujamą veiklą ar neteisėtas modifikacijas padaro beveik neįmanomas saugomame objekte ar sistemoje. Kompiuteriuose šiuo metu tokie moduliai įmanomi tik kaip atskira išorinė įranga. Tai jau nebepriklauso nuo to, kokia operacinė sistema yra naudojama.

   Be abejo galima naudoti ne kurią nors vieną priemonę, o jų kombinacijas, tačiau tuomet reikia nepamiršti, jog bendras sistemos saugumas bus lygus silpniausios priemonės saugumo lygiui.

2. **Reikalavimai „tamper-evident" ir „tamper-resistant" moduliams:**
   a) instaliavimo metu turi būti užtikrintas visų komponentų programinės ir techninės įrangos integralumas ir autentiškumas;
   b) duomenys ir procesai esantys saugioje aplinkoje turi būti apsaugoti nuo neteisėtų modifikacijų;
   c) turi būti atpažįstamos saugios aplinkos įrenginių neteisėtos modifikacijos.

3. **Instaliavimo ir tikrinimo prielaidos.** Parašo tikrinimo programinės įrangos tiekėjas turėtų pateikti įrankį, su kuriuo vartotojas bet kuriuo metu galėtų patikrinti, ar jo programinė įranga kaip nors nebuvo pakeista po instaliacijos. Kai tik tikrinimo įranga yra paruošiama darbui, vartotojas privalo galėti aptikti bet kokią manipuliaciją prieš atliekant parašo patvirtinimo procesą.
4. **Būtinos sąlygos.** Visa sistema turi būti saugi, kas reiškia, kad bet kokia informacija gauta iš bet kurios sistemos dalies turi būti tiksli ir neiškraipyta**:**
    a) **patvirtinimo procesas.** patvirtinimo procesas turi aiškiai, demonstratyviai parodyti el. parašo patvirtinimą, kaip to reikalauja parašo taisyklės;
    b) **elektroninio parašo pasirinkimas patvirtinimui.** Vartotojo sąsaja turi leisti vartotojui pasirinkti pasirašomą dokumentą ir jei galima, elektroninį parašą;
    c) **tinkamų parašo taisyklių pateikimas.** Vartotojo sąsaja parašo tikrintojui turi pateikti patikimu, nedviprasmišku ir nemanipuliuojamu būdu parašo taisyklių identifikatorių, parašo taisyklių programos aprašymą ir sąlygas susijusias su el. parašu;
    d) **pasirašomo dokumento pateikimas.** Vartotojo sąsaja parašo tikrintojui turėtų pateikti patikimu, nedviprasmišku ir nemanipuliuojamu būdu nedviprasmišką pasirašomą dokumentą. Gali būti taip, kad dokumente yra įterptas kodas ar makro komandos taip, kad patvirtintojui yra pateikiamas kažkas kito, negu jis pasirašė.Tuomet sąsaja turi duoti kokį nors įspėjantį pranešimą, apie galimą bandymą pakenkti.
    e) **pasirašiusiojo ir papildomos informacijos pateikimas.** Vartotojo sąsaja, parašo tikrintojui turi pateikti patikimu, nedviprasmišku ir nemanipuliuojamu būdu pasirašiusiojo vardą. Šis vardas kartu su sertifikatų centro vardu turi būti išgauti iš pasirašančiojo sertifikato. Kita informacija, kaip pasirašymo laikas, pasirašiusiojo gyvenamoji vieta, taip pat turėtų būti pateikta. Jei vykdomas pirminis tikrinimas, turi būti pateikiama viena iš trijų būsenų:
        - patikrinimas baigtas;
        - patikrinimas nesėkmingas;
        - patikrinimas nebaigtas.

        Jei vykdomas vėlesnis patikrinimas, tuomet turi būti pateikta viena iš dviejų būsenų:
        - patikrinimas baigtas;
        - patikrinimas nesėkmingas;

f) **Ilgalaikio galiojimo elektroninio parašo užklausa.** Jei reikia ilgalaikio galiojimo parašo, tuomet vartotojo sąsaja turi leisti tikrinančiajam užfiksuoti informaciją, kuri leistų el. parašui galioti ilgesnį laiką [CWA1].

3.4.4. Laiko žymos protokolo reikalavimai

Laiko žymos protokolą sudaro klientas – paprastas vartotojas, ir serveris – tarnyba, todėl ir reikalavimai dalinasi į dvi dalis:

1. Reikalavimai kliento įrangai
    a) reikalavimai formuojant užklausas į TSA;
        - nepateikti praplėtimo (extension) laukų;
        - kuriant informacijos, kuriai bus dedamas laiko štampas, maišos funkciją, naudoti SHA-1, MD5, RIPEMD-160 algoritmus. (Dabar MD5 jau nerekomenduojamas, nes nėra toks saugus kaip anksčiau);
    b) reikalavimai tikrinant gautus atsakymus iš TSA;
        - turi būti palaikomas ir suprantamas tikslumo (accuracy) laukas;
        - turi būti palaikomos nurodymų (ordering) lauko reikšmės – „missing“ arba „FALSE“;
        - turi būti palaikomas parametras „nonce“;
        - praplėtimo (extension) laukas būti neprivalo;
        - parašui sukurti turi būti palaikomi SHA-1 ir RSA algoritmai;
        - kuriant parašą RSA algoritmo rakto ilgis turi būti 1024 arba 2048 bitų ilgio;
        - DSA algoritmui naudojamų pirminių skaičių (p ir q) ilgis negali būti mažesnis negu 1024 bitų;
2. Serverio reikalavimai:
    a) reikalavimai formuojant užklausas į TSA;
        - turi būti palaikomas parametras „nonce“;
        - turi būti palaikomas parametras „certReq“;
        - praplėtimo (extension) laukas būti neprivalo;
        - turi būti atpažįstami maišos algoritmai, SHA-1, MD5, RIPEMD-160;
    b) reikalavimai atsakymams iš TSA;
        - genTime parametras turi atvaizduoti laiką vienos sekundės tikslumu;
        - laiko accuracy lauke tikslumas turi būti nemažesnis nei viena sekundė;
        - turi būti palaikomos nurodymų (ordering) lauko reikšmės – „missing“ arba „FALSE“;

- praplėtimo (extension) laukas būti neprivalo;
- jei „extension“ laukas yra, tada jis negali būti kritinis, esminis;
- turi būti naudojama atitinkama, laiko žymos protokolą naudojančio serverio, vardo struktūra, kuri yra aprašyta ISO 9594-6 standarte;
- turi būti palaikomi maišos algoritmai, SHA-1, MD5, RIPEMD-160;
- parašui sukurti turi būti palaikomi SHA-1 ir RSA algoritmai;
- kuriant parašą RSA algoritmo rakto ilgis turi būti 1024 arba 2048 bitų ilgio; [ETSI].

Akivaizdžiai matosi, jog kliento programinė įranga negali būti bet kokia. Tai dar vienas akmenukas į elektroninio parašo diegimo problemų darželį.

3.5. Reikalavimai techninei įrangai

Pagrindinis įrenginys, kuriam keliami didžiausi saugumo reikalavimai yra saugaus parašo formavimo įrenginys (toliau SSCD – Secure Signature Creation Device). Šie įrenginiai yra trijų tipų:

1 tipas. Šio tipo įrenginys skirtas tik raktų poros sugeneravimui. Sugeneruoti raktai (viešasis ir privatusis), turi būti perkelti į 2 tipo įrangą, todėl turi būti užtikrintas saugus perdavimo kanalas.

2 tipas. Šio tipo įrenginys skirtas elektroninio parašo kūrimui. Privatusis raktas gaunamas iš 1 tipo įrangos, todėl būtina užtikrint saugų perdavimo kanalą. Taip pat šis įrenginys yra asmeninis kiekvienam vartotojui ir, norint juo pasinaudoti, riekia įvesti autentifikacijos kodą, todėl čia turi būti užtikrinta betarpiška sąsaja su vartotoju arba saugus perdavimo kanalas.

3 tipas. Šio tipo įrenginys yra kombinacija 1 tipo ir 2 tipo įrangos. T.y. jame sugeneruojama raktų pora ir juo formuojamas elektroninis paršas. Todėl privatusis raktas niekad į išorę nepatenka. Šiuo įrenginiu pasinaudoti galima tik suvedus autentifikacijos duomenis, todėl kaip ir 2 tipo įrenginyje čia turi būti užtikrinta betarpiška sąsaja su vartotoju arba saugus perdavimo kanalas [CWA9].

2 ir 3 tipo įranga - tai yra visiem gerai žinomos lustinės kortelės ar USB laikmenos. 3 tipo įranga laikoma saugiausia. Lietuvoje, tokio tipo įrangai priskiriamos gyventojų registrų centro išduodamos asmens tapatybės kortelės.

4. LIETUVOJE KVALIFIKUOTUS SERTIFIKATUS IŠDUODANČIŲ SERTIFIKAVIMO CENTRŲ VEIKLOS NUOSTATAI IR SERTIFIKATO TAISYKLĖS

Ankstesniuose skyriuose kalbėta apie vartotojų įrangos reikalavimus, tačiau yra daugybė organizacinių, veiklos reikalavimų paslaugų teikėjams: ką daryti, kaip daryti, naudojant jau aptartą įrangą. Iš tikrųjų tai yra specialus dokumentas, kuriame aprašoma, kaip turi būti vykdomos funkcijos, kad būtų tenkinami keliami reikalavimai. Toks dokumentas vadinamas **veiklos nuostatais** (CPS – Certification Practice Statement). Tai tokios CA veiklos taisyklės, kuriose smulkiai aprašyta CA vykdoma veikla. Pagal šį dokumentą el. parašą prižiūrinti institucija sprendžia, ar išduoti leidimą veiklai, ar ne.

Kitas dokumentas, kuriame išreikšti reikalavimai yra parašo taisyklės (CP – Certificate Policy). Kad naudotojų grupės (pvz. bankai, valstybinės įstaigos) pasitikėtų CA išduodamais sertifikatais, jos parengia dokumentą, kuriame yra išdėstomi reikalavimai, ką turėtų daryti CA sudarant, tvarkant ir naudojant sertifikatus. Abu šie dokumentai yra viešai prieinami ir pateikti kiekvieno CA svetainėse.

Lietuvoje yra trys, kvalifikuotus sertifikatus teikiantys, sertifikavimo centrai: SSC – UAB „Skaitmeninio sertifikavimo centras“, RCSC – „VĮ Registrų centro sertifikavimo centras“, GRSC - Gyventojų registro tarnybos sertifikavimo centras prie LR vidaus reikalų ministerijos. Todėl ir bus analizuojami sertifikavimo teikėjų veiklos nuostatai ir sertifikato taisyklės (taisyklės, nustatančios kriptografinėje USB laikmenoje įrašomų sertifikatų sudarymo ir tvarkymo reikalavimus, sertifikavimo paslaugų teikėjo bei sertifikatų naudotojų teises ir pareigas) panašumai bei skirtumai, didesnį dėmesį skiriant skirtumams. Jų išryškinimui, Lietuvos sertifikatų centrai lyginami su „Verisign“ (labiausiai pažengusiu sertifikatų centru pasaulyje)

4.1. Veiklos nuostatų palyginimas

Pastebėtina tai, jog RCSC ir SSC priedus yra pateikę pačiuose veiklos nuostatuose, todėl jų apimtis žymiai didesnė, nei GRSC veiklos nuostatų. Nors sertifikavimo centrų veiklos nuostatų puslapių skaičiaus standartas (IETF RFC 3647) ir neapibrėžia, tačiau lyginant su Verisign (jų veiklos nuostatus sudaro 121 puslapis) – mūsų vidutiniškai du kartus trumpesni. Taigi, gali būti, jog mūsų sertifikavimo centrų nuostatuose yra praleista daug punktų. Gal būt taip yra todėl, kad mūsų vartotojams nėra poreikio.

Verta paminėti, jog SSC savo veiklos nuostatų kiekviename puslapyje skelbia: *„© SSC CA, 2005. Visos teisės saugomos. Jokia šio dokumento turinio dalis negali būti atgaminta ar platinama jokia forma ir jokiomis priemonėmis be išankstinio raštiško UAB „Skaitmeninio sertifikavimo centras“ sutikimo“*. [SSC1] Remiantis LR Autorių teisių ir gretutinių teisių įstatymu, 5 straipsniu, konstatuojama, jog autorių teisių objektais nelaikomi:

a) idėjos, procedūros, procesai, sistemos, veiklos metodai, koncepcijos, principai, atradimai ar atskiri duomenys;
b) teisės aktai, oficialūs administracinio, teisinio ar norminio pobūdžio dokumentai (sprendimai, nuosprendžiai, nuostatai, normos, teritorijų planavimo ir kiti oficialūs dokumentai), taip pat jų oficialūs vertimai.

Kyla klausimas: ar jie rėmėsi LR Autorių teisių ir gretutinių teisių įstatymu rengdami CPS? Todėl gali kilti abejonių dėl šio sertifikavimo centro kvalifikacijos bei veiklos patikimumo.

Dar vienas dalykas, kuris krenta į akis tai, kad GRSC nuostatuose nėra turinio, todėl labai apsunkina skaitytoją, nes visiškai neaiški dokumento struktūra.

4.1.1. Ginčų sprendimo tvarka

Sertifikavimo centrai veiklos nuostatuose pateikia ginčų tarp sertifikavimo centro ir klientų (sertifikato naudotojų ar parašo tikrintojų) ginčų sprendimo tvarką, kuri šiek tiek skiriasi:

- GRSC: „*Visi ginčai, susiję su sertifikatų sudarymu ir tvarkymu, sprendžiami vadovaujantis LR įstatymais*“. [GRSC]
- RCSC: „*Bet kokie ginčai tarp CA ir sertifikatų naudotojų sprendžiami derybų keliu. Neišsprendus ginčo, jis sprendžiamas teismo tvarka*“. [RCSC]
- SSC: „*Bet kokie ginčai <...> sprendžiami geranoriškomis šalių derybomis, konsultacijomis. Jei tokie nesutarimai negali būti išspręsti derybų keliu, juos sprendžia kompetentingas SSC CA buveinės vietos teismas*“. [SSC1]
- VeriSign: Ginčai tarp sertifikatų naudotojų sprendžiami derybų keliu, o jei į ginčą yra įsivėlęs pats Verisign, tuomet ginčas sprendžiamas federaliniame arba valstijos teisme tam skiriant 60 dienų laikotarpį. [VCPS]

Ginčų sprendimą derybų keliu nurodo RCSC ir SSC, tačiau neaiški lieka SSC pozicija dėl ginčų sprendimo, jei derybų kelias negalimas. Matyt, ginčą sprendžia „kompetentingas buveinės vietos teismas“.

4.1.2. Viešai teikiama informacija

Pastebėtina tai, jog vienintelis iš tirtų sertifikavimo centrų SSC apriboja vartotojams informacijos apie sertifikatų statusą gavimą OCSP būdu (Online Certificate Status Protocol): *„<...> turi teisę apriboti OCSP užklausų skaičių iki 10 užklausų vienam naudotojui per 24 valandas. Asmenims, kuriems dėl jų veiklos prigimties dažnas OCSP naudojimas yra būtinas, būtina sudaryti atskirą sutartį su SSC CA*“. [SSC1]

Sertifikavimo centrai veiklos nuostatuose pateikia, kokio tipo informaciją ir kada jie skelbia savo internetinėje svetainėje. Apie atšauktų sertifikatų sąrašus informacija pateikta atskirai, tačiau RCSC ir GRSC išskiria kito turinio dokumentus, tokius kaip prašymų šablonai ar CA veiklos tikrinimo išvados, kuriuos įsipareigoja paskelbti iškart po jų patvirtinimo arba gavimo. SSC tokio pobūdžio informacijos nepateikia. Verisign įsipareigoja visada skelbti: sertifikatų taisykles, veiklos nuostatus, abonentų sutarties sąlygas (subscriber agreements) ir pasitikinčių šalių susitarimus [SSC1; RCSC; GRSC; VCPS]

4.1.3. Veiklos tikrinimas

Visuose analizuojamų sertifikavimo centrų veiklos nuostatuose pateikiami veiklos tikrinimo procesai, metodai, reikalavimai. GRSC ir RCSC savo veiklą įsipareigoję tikrinti ne rečiau kaip kartą per vienerius metus, o SSC patikrinimų dažnumo nenurodo. GRSC ir RCSC aiškiai apibrėžia, kas gali tikrinti jų veiklą (tikrintojai), tai yra sertifikavimo paslaugų teikėjo auditorius ir saugumo pareigūnas. Labai keistai ir neskaidriai atrodo tai, jog SSC patys įvertina savo veiklos atitikimą CP ir CPS. Nėra kvalifikacinių ar kitų reikalavimų tikrintojui. Sertifikatų centrai (GRSC ir RCSC) pateikia skirtingas tikrinamas veiklos sritis (1 lentelė) savo veiklos nuostatuose.

1 lentelė. Tikrinamos veiklos sritys

Veiklos sritis	**SSC**	**RCSC**	**GRSC**	**VERISIGN**
Fizinis saugumas	-	+	+	+
Sertifikatą sudaryti prašančiųjų asmenų tapatybės tikrinimo procedūra	-	+	-	+
Sertifikavimo paslaugos ir jų teikimo procedūros	-	+	+	+
Programinės įrangos ir sistemos prieigos kompiuterių tinklų saugumas	-	+	+	+
Personalo patikimumas	-	+	-	+
Registracijos žurnalų ir sistemos tvarkymo procedūros	-	+	+	+
Informacijos atsarginių kopijų darymas	-	+	+	+
Archyvų tvarkymo procedūros	-	+	+	+

Įrašai apie CA struktūros keitimus	-	+	-	+
Įrašai apie techninės ir programinės įrangos tikrinimą ir priežiūrą	-	+	+	+

SSC apie tikrinamas veiklos srtis nepateikia jokios informacijos (žr. 1 lentelę), todėl galima teigti, jog tikrinamos sritys ne tik nėra apibrėžtos, bet kyla klausimas, ar apskritai kas nors yra tikrinama. [SSC1; RCSC; GRSC; VCPS].

4.1.4. Sertifikatų savininkų vardų sudarymas

Sudarydami sertifikatų savininkų vardus sertifikavimo centrai laikosi to pačio standarto rekomendacijų, tik skirtingų versijų (2 lentelė). Didelių skirtumų tarp šių versijų nepastebėta, pabrėžiama tik tai, jog SSC rekomendacijose yra elektroninio pašto adreso laukelis ir laukeliai juridinių asmenų informacijai įrašyti (žr. 1, 2, 3 priedus).

2 lentelė. Naudojami standartai sertifikatų savininkų vardų sudarymui

Sertifikatų centrai	**SSC**	**RCSC**	**GRSC**	**VERISIGN**
Standarto rekomendacijos	X.501	X500	X.500	X.501

SSC konstatuoja, jog sertifikatuose yra galimas pseudonimų naudojimas, tačiau sertifikavimo tarnybos privalo turėti tinkamą įrodymą, kad yra ryšys tarp to vardo (pseudonimo) ir subjekto, kuriam priklauso vardas. GRSC ir RCSC pseudonimų sudarant sertifikatus naudoti neleidžia.

4.1.5. Sertifikato galiojimo nutraukimas ir sustabdymas

Reikšmingų skirtumų sertifikato galiojimo nutraukimui tarp sertifikavimo centrų nepastebėta, tačiau šiokie tokie yra (3 lentelė). Normalu, jog GRSC automatiškai nutraukia sertifikato galiojimą pasibaigus asmens tapatybės kortelės galiojimui, kiti sertifikavimo centrai to nedaro, nes jie neišduoda minėto tipo lustinių kortelių. Reikia atkreipti dėmesį į tai, jog ši lentelė sudaryta remiantis išskirtais punktais veiklos nuostatuose, ji pagrįsta ne spėliojimu, o konkrečiomis nuostatomis, todėl, neradus punkto 3-oje lentelėje dedamas minusas. Todėl, kai kuriais atvejais, gali pasirodyti, jog sertifikavimo tarnybų elgesys (pozicija) yra nelogiškas. Pavyzdžiui, kai pažeidžiamas CA privačiojo rakto ir naudojamos sertifikatų tvarkymo sistemos saugumas, keliantis pavojų sudarytų sertifikatų patikimumui, GRSC ir RCSC pabrėžiama, jog sertifikatų savininkams iš karto nutraukiamas sertifikato galiojimo laikas (tai galima padaryti ir be sertifikato savininko žinios

ir tik vėliau jį informuoti). SSC šiuo konkrečiu atveju įsipareigoja informuoti sertifikato savininką, o kokių veiksmų imasi vėliau, lieka neįvardinta (tikėtina, jog sertifikato galiojimas nutraukiamas, bet gi tai ir turi būti įvardinta veiklos nuostatuose).

3 lentelė. Sertifikato galiojimo nutraukimas

Sertifikato galiojimas nutraukiamas	**SSC**	**RCSC**	**GRSC**
Sertifikato savininko prašymu	+	+	+
Paaiškėjus, kad sertifikato duomenys daugiau nėra teisingi	-	+	+
Paaiškėjus, kad sertifikatas buvo sudarytas remiantis neteisingais duomenimis	+	+	+
CA nutraukia veiklą ir joks kitas sertifikavimo paslaugų teikėjas neperima sertifikavimo veiklos	-	+	+
CA sprendimu, paaiškėjus, kad sertifikato savininkas nesilaiko sertifikato naudojimosi sąlygų	-	+	+
Sertifikato savininkui praradus sertifikatą atitinkančių parašo formavimo duomenų kontrolę	+	+	+
Remdamasis sertifikato galiojimo apribojimais, nurodytais sertifikate jį sudarant	+	+	+
Kai sertifikato savininkas nusprendžia nutraukti susitarimą su sertifikatą jam sudariusiu CA	-	+	-
Kai pažeidžiamas CA privačiojo rakto ir naudojamos sertifikatų tvarkymo sistemos saugumas, keliantis pavojų sudarytų sertifikatų patikimumui	-	+	+
Sertifikato savininkui pažeidus elektroninio parašo naudojimą reglamentuojančius teisės aktus arba sutarties su sertifikavimo paslaugų teikėju sąlygas	+	-	+
Asmens, kuriam pagal sertifikate nurodytą informaciją pasirašantis asmuo turi teisę atstovauti, prašymu	+	-	-
Gavus pranešimą, kad sertifikato savininkas tapo neveiksnus	+	+	+
Gavus pranešimą, kad sertifikato savininkas mirė	+	+	+
Kitais LR įstatymų numatytais atvejais	+	-	+
Nutraukiamas visais atvejais, nustojus galioti asmens tapatybės kortelei, kurioje įrašyti sertifikatai	-	-	+

Visi sertifikavimo centrai sustabdo sertifikato galiojimą, tokiais atvejais:

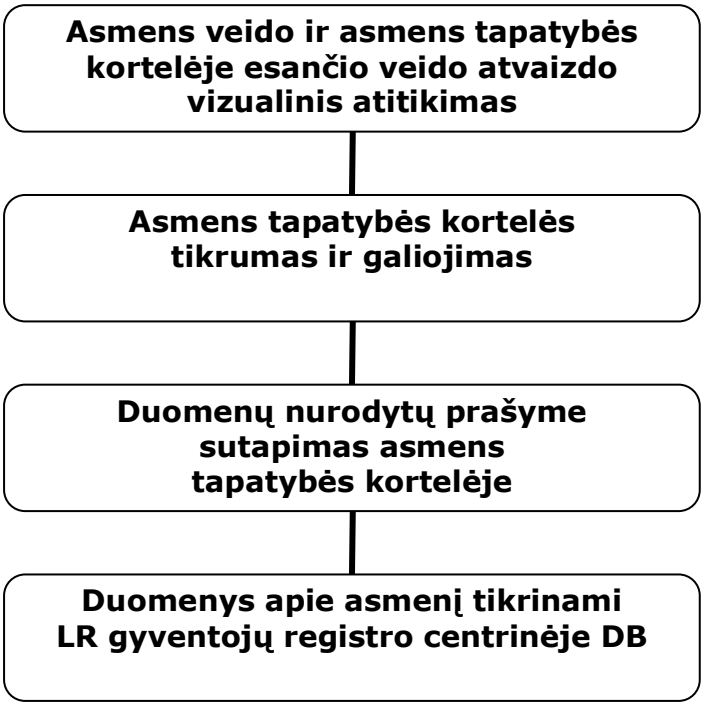
1) gavus sertifikato savininko prašymą;
2) teisėsaugos institucijų reikalavimu, siekiant užkirsti kelią nusikaltimams;
3) gavus informacijos ar kilus įtarimui, kad sertifikato duomenys yra neteisingi arba sertifikato savininkas prarado sertifikatą atitinkančių parašo formavimo duomenų kontrolę.

Prašymus, sustabdyti sertifikato galiojimą visuose aptariamuose sertifikavimo centruose, gali teikti sertifikato savininkas ir teisėsaugos institucijos. RCSC tokį prašymą gali teikti ir CA įgaliotasis asmuo (pavyzdžiui, saugumo administratorius), o SSC - asmenys, kuriems pagal

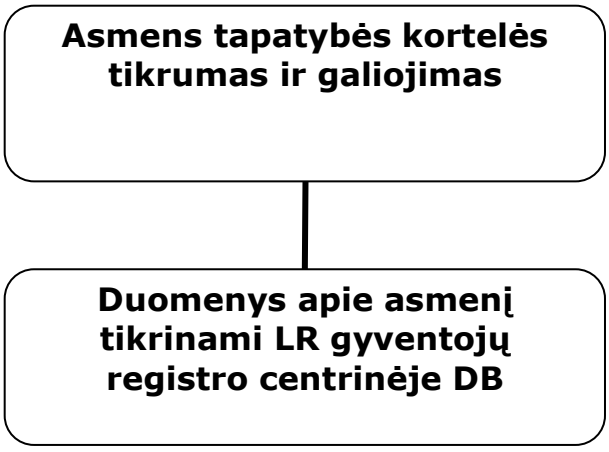
sertifikate nurodytą informaciją pasirašantis asmuo turi teisę atstovauti (turima omenyje juridinį asmenį). [SSC1; RCSC; GRSC]

4.1.6. Asmens tapatybės tikrinimas

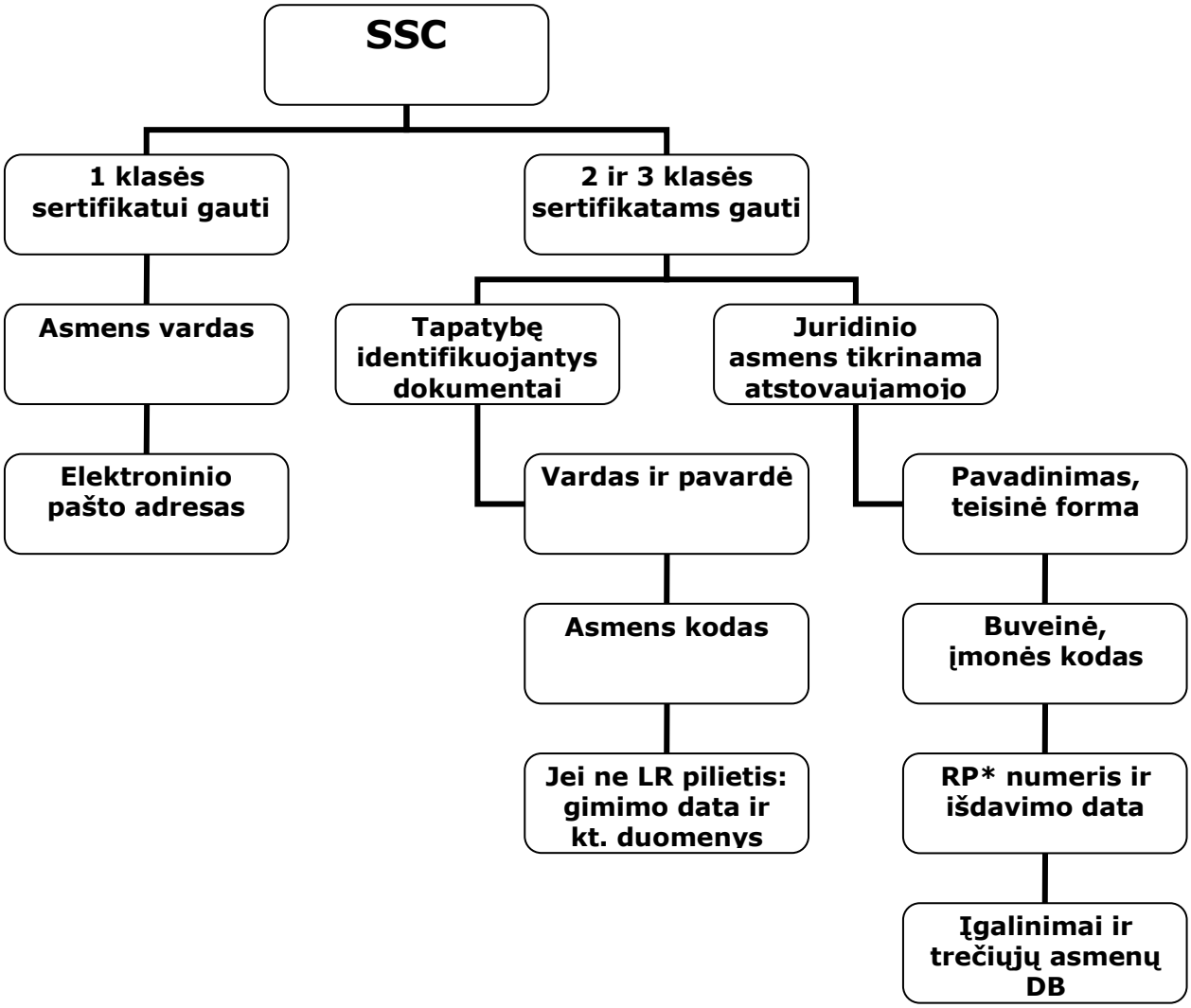
Šiame veiklos nuostatų skyriuje pastebėta skirtumų ir netgi trūkumų (neaiškumų). Kiekvienas sertifikavimo centras asmens tapatybę tikrina skirtingai, todėl pateikiamos kiekvienos iš jų tikrinimo schemos (3, 4, 5 pav).



3 pav. GRSC asmens tapatybės tikrinimas



4 pav. RCSC asmens tapatybės tikrinimas



5 pav. SSC asmens tapatybės tikrinimas

Pastebėta tai, jog vienintelis GRSC įvardina bei pabrėžia, jog tikrina asmens veido ir asmens tapatybės kortelėje esančio veido atvaizdo vizualinį atitikimą bei tikrina prašyme nurodytų duomenų atitikimą su asmens tapatybės dokumente (kortelėje, pase) nurodyta informacija. Tačiau šiame skyriuje, analizuojant SSC veiklos nuostatus, kyla svarbesnis klausimas: kur SSC tikrina asmens tapatybės duomenis? SSC veiklos nuostatuose tik konstatuojama: *„SSC RA patikrina, ar pateikti visi paraiškoje reikalaujami duomenys, o esant reikalui, pareikalauja papildomų dokumentų ir paaiškinimų. Surinkęs visus reikalaujamus dokumentus, SSC RA priima sprendimą, ar asmuo gali tapti sertifikavimo sistemos klientu“.* [SSC1] Daugiau duomenų nepateikta. [GRSC], [RCSC]

4.1.7. Sertifikavimo paslaugų teikėjų užtikrinimai

Visi analizuoti sertifikavimo paslaugų tiekėjai užtikrina, jog:

1) sudaromi kvalifikuoti sertifikatai atitinka elektroninio parašo įstatyme kvalifikuotiems sertifikatams nustatytus reikalavimus (SSC tik 3-os klasės sertifikatams);
2) kvalifikuoti sertifikatai atitinka Lietuvos standarto LST ETSI TS 101 862 „Kvalifikuoto sertifikato profilis“ sertifikatų sandarai nustatytus reikalavimus;
3) kriptografinių raktų poros generavimo procedūra yra saugiai susieta su sertifikato sudarymo procedūra;
4) saugi parašo formavimo įranga sertifikato savininkui perduodama saugiai;
5) privačiam raktui generuoti naudojama Lietuvos standarto LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“ trečiojo saugumo lygmens (SSCD Type 3) reikalavimus atitinkanti saugi parašo formavimo įranga;
6) sudarytame sertifikate nurodyti asmens identifikavimo duomenys yra unikalūs ir nepriskirtini kitam asmeniui;
7) sertifikatams sudaryti naudotų duomenų konfidencialumas ir integralumas užtikrinamas viso sertifikato gyvavimo ciklo metu [SSC1], [RCSC], [GRSC].

4.1.8. Negaliojančių sertifikatų sąrašų skelbimas

Visi minėti sertifikavimo centrai sertifikatų galiojimą siūlo tikrinti dviem būdais:

1) sertifikatų sąraše (CRL);
2) naudojant užklausų sistemą realiu laiku (OCSP), 24 val. per parą.

Sąrašai skelbiami kas savaitę, tačiau aktualioje negaliojančių sertifikatų sąrašo versijoje, kitos versijos paskelbimo laiką nurodo tik RCSC ir GRSC. [SSC1], [RCSC], [GRSC]

4.1.9. Duomenų apie sertifikavimo centrų veiklą kaupimas

GRSC kaupia šiuos duomenis apie veiklą:

1. Dokumentai:
    a) prašymai;
    b) sutartys.
2. Sertifikatų valdymo sistemos techninės priežiūros žurnalas:
    a) kriptografinės įrangos gyvavimo ciklo įvykiai;

b) sertifikatų gyvavimo ciklo įvykiai ir kt.;

3. Elektroninis sistemos audito žurnalas:
    a) privačiųjų kriptografinių raktų publikavimo įvykiai ir kt.
4. Elektroninis sistemos saugumo diagnostikos žurnalas:
    a) visi su sistemos saugumu susiję įvykiai. [GRSC]

RCSC kaupia šiuos duomenis apie operacijas:

1. Operacijų žurnalas:
    a) sertifikato statuso keitimas;
    b) CRL generavimo ir publikavimo įrašai ir kt.
2. CA sistemų veiklos registravimo žurnalai:
    a) sistemų veiklos sutrikimai, klaidos.
3. Diagnostikos žurnalas:
    a) sistemų veikimo analizė;
    b) diagnostika;
    c) sutrikimų šalinimas ir kt.
4. Klaidų žurnalas:
    a) sistemų sutrikimai ir klaidos, nurodant sutrikimo laiką, šaltinį, aprašymą ir detalią informaciją. [RCSC]

SSC fiksuoja šiuos reikšmingus įvykius:

1. Rakto galiojimo laikotarpio tvarkymas:
    a) CA rakto generavimas, saugojimas, atstatymas ir kt.;
    b) kriptografinės įrangos veikimo laikotarpio tvarkymas.
2. Sertifikatų galiojimo laikotarpio tvarkymo įvykiai:
    a) prašymai ir kt.,
    b) sertifikatų ir CRL generavimas ir sudarymas ir kt.
3. Saugumas:
    a) sėkmingi ir nesėkmingi bandymai prieiti prie PKI sistemos;
    b) saugos profilių pokyčiai ir kt.
4. Informacija apie prašymus sudaryti sertifikatus:
    a) asmens, priimančio prašymą, tapatybė;
    b) metodai, taikomi nustatyti identifikavimo dokumentų tikrumą, jei tokie metodai taikomi ir kt. [SSC1]

Šių žurnalų įrašus GRSC ir SSC peržvelgia kartą per savaitę, o RCSC kartą per mėnesį.

4.1.10. Atsarginės kopijos ir archyvai

Sertifikavimo centrai daro įvairias duomenų bazių ar programinės įrangos atsargines kopijas ir vieni didesnį dėmesį skiria duomenų bazėms, o kiti operacinei sistemai (4 lentelė).

4 lentelė. Atsarginės kopijos

Duomenų tipas	**SSC**	**RCSC**	**GRSC**	**VERISIGN**
Operacinių sistemų konfiguracijos duomenų kopijos	-	-	+	+
Pilnos operacinių sistemų kopijos	-	-	+	-
Sertifikatų duomenų bazės kopijos	-	+	+	+
Negaliojančių sertifikatų sąrašų kopijos	+	+	+	+
Sistemos audito žurnalo kopijos	-	-	+	+
Instaliacinio disko su sistemos programine įranga	-	+	-	+
Instaliacinio disko su CA ir RA taikomosiomis programomis	-	+	-	+
WWW serverio ir saugyklos instaliaciniai diskai	-	+	-	-
Asmenų, kuriems yra sudaryti sertifikatai, duomenys	+	+	-	+
CA sistemos operacijų ir veiklos registravimo žurnalai	-	+	-	-
Saugyklos (*repository*) duomenų kopija	-	+	-	-

GRSC saugo duomenis remiantis LR dokumentų ir archyvų įstatymo nustatyta tvarka. RCSC archyvas saugomas laikantis Registrų centro numatytos vidinės tvarkos ir LR dokumentų ir archyvų įstatymo. SSC atsargines duomenų kopijas daro visų archyvuojamų duomenų ar dokumentų, tačiau neužsimena apie duomenų bazių, taikomųjų programų ar operacinių sistemų atsargines kopijas. Duomenys GRSC ir RCSC archyvuose saugomi 10 metų, tolesnis jų saugojimas užtikrinamas Dokumentų ir archyvų įstatymo nustatyta tvarka. SSC minimalus archyvavimo laikotarpis yra 5 metai. Duomenų archyvuose saugomi įvairaus turinio dokumentai (5 lentelė). [SSC1; RCSC; GRSC; VCPS]

5 lentelė. Sertifikavimo centrų archyvai

Archyvuoja	**SSC**	**RCSC**	**GRSC**	**VERISIGN**
Asmenų prašymų registravimo duomenis	+	-	+	-
Asmenų, kuriems buvo sudaryti sertifikatai, DB	-	+	-	-
Veiklos registravimo žurnalai	-	+	+	+
Pasibaigusio galiojimo sertifikatų duomenis	-	-	+	+
Negaliojančių sertifikatų sąrašus	+	+	+	+
CA sistemos operacijų žurnalus	-	+	**?**	+

CA priklausančių raktų istoriją nuo jų sugeneravimo iki sunaikinimo	-	+	-	+
Susirašinėjimo informaciją su tarnybomis ir sertifikatų naudotojais (paslaugų vartotojais)	+	+	-	-
Asmens tapatybės patvirtinimo informaciją	+	-	-	-
Sertifikatų DB	+	+	-	+

4.1.11. Sertifikavimo paslaugų teikėjo veiklos nutraukimas

Visi minėti sertifikavimo centrai ne vėliau kaip prieš vieną mėnesį įsipareigoja informuoti sertifikatų savininkus ir kitus asmenis ar institucijas apie savo veiklos nutraukimą. GRSC įsipareigoja per vieną mėnesį po paskelbimo apie veiklos nutraukimą sukauptus veiklos duomenis perduoti veiklos perėmėjui ar elektroninio parašo priežiūros institucijai, kurie turi užtikrinti duomenų, reikalingų sertifikato statusui tikrinti, teikimą sertifikatais pasitikinčioms šalims. RCSC nutraukia sertifikatų galiojimą (neįvardinta kada), jei nėra veiklos perėmėjo. SSC gali nutraukti sertifikatų galiojimą po vieno mėnesio nuo veiklos nutraukimo paskelbimo. [SSC1; RCSC; GRSC]

4.1.12. Saugumo priemonės

Dažniausiai skirtinguose sertifikatų centruose taikomos skirtingos saugumo priemonės. SSC taikomos biometrines priemonės, RCSC – identifikacinių kortelių sistema, GRSC – biometrinės įėjimo kontrolės sistema. Saugiam kriptografinių raktų porų generavimui sertifikavimo centrai taiko šiuos reikalavimus: LST ISO/IEC 15408 „Informacijos technologija. Saugumo metodai. Informacijos technologijų saugumo įvertinimo kriterijai“ trečiojo saugumo lygmens (SSCD Type 3) reikalavimai; FIPS PUB 140-2 „Saugos reikalavimai kriptografiniams moduliams“ trečiojo saugumo lygmens reikalavimai; LST CWA 14168 „Saugi parašo formavimo įranga EAL 4“ ir kitus. Sertifikatų centrai generuoja skirtingo dydžio kriptografinius raktus (6 lentelė).

6 lentelė. Kriptografinių raktų dydžiai

Rakto tipas	**GRSC**	**RCSC**	**SSC**		**VERISIGN**
			1kl. 2 kl.	**3 kl.**	
Šakninės sertifikavimo TS*	4096 bitai	4096 bitai	-	-	1000 bitų
Nuostatų sertifikavimo TS*	2048 bitai	2048 bitai	-	-	1024 bitai
Darbinės	2048 bitai	2048 bitai	-	-	1024 bitai

sertifikavimo TS*					
Asmenų	2048 bitai	2048 *arba* 1024 bitai	512 bitų	1024 bitai	1024 bitai

*TS – tarnybinė stotis.

Kriptografinių raktų galiojimo terminai asmenims taip pat skiriasi (7 lentelė), o sertifikato galiojimo pradžios terminas paprastai sutampa su sertifikato sudarymo data.

7 lentelė. Kriptografinių raktų galiojimo terminai

Sertifikatų centrai	**GRSC**	**RCSC**	**SSC**			**VERISIGN**
			1 kl.	2 kl.	3 kl.	
Trukmė metais	3	1-2	2	2-5	2-5	2-5

Analizuojami sertifikavimo centrai veiklos nuostatuose pateikia kompiuterių saugumo priemones (8 lentelė). Reikia atkreipti dėmesį į tai, kad minusai ties Verisign stulpeliu reiškia, jog savo veiklos nuostatuose ties skyrium „kompiuterių saugumas“ apie šias saugumo priemones nėra nieko užsimenama. Tiksliau sakant tos priemonės nėra taip smulkiai detalizuotuos. Greičiausiai jos išsibarstę po kitus skyrius.

8 lentelė. Kompiuterių saugumo priemonės

Priemonė	**GRSC**	**RCSC**	**SSC**	**VERISIGN**
OS ir taikomųjų programų lygiu numatytas privalomas registravimasis	+	+	-	-
Savo nuožiūrai palikta prieigos kontrolė	-	+	+	-
Prisijungimams reikiamų duomenų kaupimo tikrinimas	-	+	-	-
Įgalinti atskirti pareigas, leistinas sistemoje	+	+	+	-
Prisijungiančių asmenų pareigų identifikavimas ir autentifikavimas	+	+	+	-
Kriptografinės informacijos apsauga, perduodant ją tinklu	+	+	-	-
Archyvo apie kompiuterius ir duomenis tvarkymo istorijos fiksavimo kontrolė	-	+	-	-
Patikimas darbuotojų ir jų pareigų kaitos fiksavimas	-	+	-	-
Nesankcionuotos prieigos prie kompiuterinių resursų valdymas ir informavimas	+	+	-	-

SSC, GRSC ir RSCS naudoja ugniasienes (firewalls) siekdamos apsaugoti gamybinį tinklą nuo įsiveržimo iš vidaus ir iš išorės bei apriboti priėjimo prie produkcijos sistemų galimybę. [SSC1; RCSC; GRSC; VCPS]

4.1.13. Sertifikavimo veiklos nuostatų administravimas

Nuostatų pakeitimai gali būti esminiai ir neesminiai. Siūlymus keisti, peržiūrėti veiklos nuostatus gali teikti tiek sertifikavimo paslaugų teikėjas, darbuotojai, tiek ir sertifikatų naudotojai. Esminių pakeitimų atveju parengtas naujos nuostatų redakcijos projektas turi būti teikiamas suinteresuotoms šalims pastaboms ir pasiūlymams, paskelbiant projektą internete:

- GRSC – 30 kalendorinių dienų laikotarpiui;
- SSC – 15 dienų laikotarpiui;
- RCSC – informacijos nepateikia. [SSC1; RCSC; GRSC]

4.2. Sertifikatų taisyklių palyginimas

Sertifikatų taisyklės, tai taisyklių pilnas dokumentas, kuris nusako bendrų saugumo reikalavimo lygį ir CA išduodamų sertifikatų taikymą tarp dalyvių. „*Sertifikato taisyklėmis (CP) sertifikato naudotojas GALI naudotis, norėdamas nustatyti ar sertifikatas ir jį išleidusi institucija yra pakankamai patikima, kad jį būtų galima taikyti kurioje nors srityje.*“ [SSCP]

Lyginant bendrą dokumento struktūrą labai išsiskiria GRSC dokumentas, kuris pirmiausia nėra standartiniame „pdf“ formate, turinys ir jo pateikimas labiau primena referatą nei oficialų dokumentą, o dokumento struktūra ir skyrių pavadinimai tik pradžioje sutampa su tais, kurie yra naudojami tokio tipo dokumentuose. Tuo tarpu SSC patys įspėja skaitytoją, jog dokumento struktūra atitinka RFC 2527 standartą. RCSC nors ir nieko šiuo klausimu nepamini, bet aiškiai matosi, jog jų dokumentas rengtas taip pat remiantis šiuo standartu. [RFC3]

Iš trijų Lietuvoje kvalifikuotus sertifikatus išduodančių įstaigų tik vienas GRSC įsipareigoja konsultuoti sertifikatų naudotojus. GRSC ir RCSC draudžia savo veiklą 100.000 litų sumai vienam draudiminiam įvykiui, vienerių metų laikotarpiui ir įsipareigoja atlyginti ne didesnę kaip minėto dydžio žalą. Tuo tarpu SSC konstatuoja, jog neprisiima jokios finansinės atsakomybės išduotų sertifikatų savininkams. Nuostoliai atlyginami pagal SSC civilinės atsakomybės draudimą (daugiau informacijos šiuo klausimu nerasta). [GRCP; RCCP; SSCP]

4.2.1. Sertifikatų savininkų įsipareigojimai

Sertifikatų savininkai yra įpareigoti teikti tikslią ir pilną informaciją CP ir CPS nustatyta tvarka, tinkamai pasirūpinti, kad kiti asmenys nepanaudotų jų privačiojo kriptografinio rakto ir jo aktyvavimo duomenų, naudoti viešojo ir privačiojo raktų porą tik pagal paskirtį, nurodytą sertifikate. Jie privalo sutikti, kad CA atsakomybė yra ribojama ir leisti naudoti ir saugoti asmens duomenis, taip kaip apibrėžta CP ir CPS. Privačiojo rakto sukompromitavimo atveju, sertifikato savininkas privalo nedelsiant ir visiškai nutraukti jo naudojimą. SSC kaip sertifikato savininko įsipareigojimą pateikia sertifikavimo veiklos nuostatų perskaitymą.

Sertifikatų savininkai privalo nedelsiant informuoti kai prarandama parašo formavimo duomenų kontrolė, kai atskleisti elektroninės laikmenos aktyvavimo duomenys, apie privačiojo rakto sukompromitavimą, kai privatusis raktas buvo pamestas, pavogtas ir kai pastebėti sertifikato netikslumai arba reikalingi pakeitimai jame. [GRCP; RCCP; SSCP]

4.2.2. Sertifikavimo centrų pareigos prieš pasirašant sertifikato savininkui sutartį

GRSC ir RCSC veiklos nuostatuose aiškiai išskirta, kokią informaciją sertifikavimo centrai privalo pateikti sertifikato savininkui, prieš pasirašant sutartį (žr. 9 lentelę).

9 lentelė. CA pareigos prieš sutartį

Sertifikatų sudarymo ir tvarkymo sąlygose privalomi pateikti	**GRSC**	**RCSC**
Sertifikavimo paslaugų teikėjo pavadinimas ir kontaktai	+	-
Sertifikatų naudojimo paskirties apribojimai	+	+
Sertifikato galiojimo tikrinimo, nutraukimo ir sustabdymo procedūros	+	+
Sertifikavimo paslaugų teikėjo pareigos ir atsakomybė	+	+
Sertifikato savininko pareigos ir atsakomybė	+	+
Pasitikinčių šalių pareigos ir atsakomybė	+	-
Garantiniai CA įsipareigojimai ir draudimo programos	+	-
Sutarčių, CP, CPS identifikacija ir nuorodos	+	+
Rinkliavos už teikiamas sertifikavimo paslaugas	+	-
Taikomų piniginių lėšų sugrąžinimo taisyklių aprašas ir nuorodos	+	-
Taikomos teisės nustatymas, skundų procedūra, ginčų sprendimo mechanizmai	+	+
Taikomų asmens duomenų apsaugos taisyklių aprašas ir nuorodos	+	-
Informacija apie sertifikavimo paslaugų teikėjo statusą	+	-
Jei buvo atliktas auditas, pateikiama audito ataskaita	+	-

Pažymėtina tai, jog SSC sertifikato taisyklėse tokio skyriaus nėra, tačiau lentelėje esantys elementai egzistuoja, tik jie yra išsibarstę po visą dokumentą. Iš pateiktų lentelėje duomenų matyti, jog daugiausiai informacijos sertifikato savininkui pateikia GRSC, tačiau kiekis ne visada geriau už kokybę. [GRCP] , [RCCP], [SSCP]

4.2.3. Sertifikavimo veiklos reikalavimai

GRSC sertifikato taisyklėse konstatuojama, jog sertifikavimo veiklos procedūros, saugumo, techniniai ir personalo reikalavimai turi būti detalizuoti sertifikavimo veiklos nuostatuose, kurie turi atitikti sertifikato taisykles. Nors pagal šių dokumentų rengimo standartą reikalaujama, kad tokia informacija būtų patiekta ir šiame dokumente. RCSC ir SSC sertifikavimo veiklos procedūrų, saugumo, techninius ir personalo reikalavimus pateikia kaip priklauso. Visi analizuojami sertifikavimo centrai pateikia personalo patikimumo kontrolę. Geriausiai pastebimi panašumai vyrauja tarp GRSC ir RCSC:

1. Bendri reikalavimai:
    a) aukštasis išsilavinimas, kompetencija (žinios, patirtis, kvalifikacija);
    b) pareigybių aprašymai, kuriuose turi būti nurodyti reikalavimai įgūdžiams ir patirčiai;
    c) personalo vykdomos administracinės ir valdymo procedūros bei procesai atitiktų CA informacijos saugumo valdymo procedūras.
2. Reikalavimai su sertifikatų sudarymu ir tvarkymu susijusioms pareigoms:
    a) vadybininkams reikalinga patirtis (el. parašo technologijų srityje, informacijos saugumo ir rizikos valdyme);
    b) ypatingo pasitikėjimo pareigoms būtinas diplomatiškumas, kurias apima:
        1) saugumo pareigūnus;
        2) sistemos administratorius;
        3) sistemos operatorius;
        4) sistemos auditorius.
3. CA neturi įdarbinti asmenų, kuriais nebūtų galima pasitikėti dėl teistumo ar kitokių kaltinimų nusikalstama veikla. [GRCP], [RCCP]

Lyginant su GRSC ir RCSC reikalavimais SSC reikalavimai atrodo mažiau apibrėžti ir nėra toki konkretūs, tačiau jie yra: *„CA veiklą vykdantis personalas PRIVALO būti techniškai ir profesiškai kompetentingu. Kiekviena atitinkama CA savo CPS TURĖTŲ aprašyti kitas, šį išskirtinį klausimą detalizuojančias, nuostatas ir su tuo susijusius dalykus“*.[SSCP] Personalo kontrolės priemonės reikalavimus sudaro biografiniai, kvalifikaciniai, patirties ir leidimų reikalavimai, tokie kaip ankstesnio darbo patirtis, rekomendacijos, išsilavinimas, teistumas, kreditinės / finansinės informacijos patikrinimas, sodros įrašų tikrinimas ir kita informacija.

4.2.4. Sertifikato saugojimo kriptografinės laikmenos

Paprastai kiekvienas sertifikavimo centras sertifikatus įrašo į jų pačių išduodamas kriptografines laikmenas. Kokias laikmenas išduoda Lietuvoje veikiantys kvalifikuotus sertifikatus išduodantys CA, iliustruoja žemiau pateikta lentelė (žr. 10 lentelę).

10 lentelė. Kriptografinės laikmenos

Laikmena	**GRSC**	**RCSC**	**SSC**
Asmens tapatybės kortelė	+	-	-
Valstybės tarnautojo pažymėjimas	+	+	-
Lustinė kortelė		+	+
USB raktas	-	+	+
SMART SIM mobilaus telefono kortelė	-	-	+

Asmens tapatybės kortelė bei valstybės tarnautojo pažymėjimas yra lustinės kortelės, o į kitokio tipo lustinę kortelę GRSC sertifikatų neįrašo, todėl lentelėje, GRSC celė ties lustine kortele, tuščia. Įdomus faktas tai, jog RCSC internetinėje svetainėje pateiktame dažniausiai užduodamų klausimų sąraše teigiama: „*Ar galima įsigyti RCSC sertifikatą kliento asmeninėje sertifikatų laikmenoje?* - Taip, galima. Įrašoma tik į kriptografines sertifikatų laikmenas.“ [RDUK] tik prieš tai darant rekomenduotina įsitikinti ar nesikeičia sertifikato savininko atsakomybė ir CA prisiimama atsakomybė. [GRCP; RCCP; SSCP]

IŠVADOS

Sparčiai besivystant informacinei visuomenei neišvengiamai daugėja elektroninių dokumentų. Tokių dokumentų klastojimas nėra sudėtingas, todėl autentiškumo užtikrinimas tampa labai svarbus. Tam buvo sukurta ir pradėta taikyti tokia technologija, kaip elektroninis parašas. Pastebėta:

1. El. parašas tai papildomi duomenys kurie logiškai sujungti su pasirašomu dokumentu pastarojo autentiškumui užtikrinti. Ši technologija padeda užtikrinti pasirašyto dokumento integralumą bei identifikuoti pasirašiusįjį asmenį, taip apsaugant siunčiamo dokumento turinį. El. parašo veikimo principas pagrįstas kriptologijos mokslu, t.y. duomenų užšifravimu bei dešifravimu.
2. El. parašas gali būti reikalingas bankams, statistikos departamentui, elektroniniam balsavimui, susirašinėjimui su vyriausybe, Sodroje, mokesčių inspekcijoje, tarptautiniame ir vietiniame versle, pavieniams asmenims ir t. t.
3. Kvalifikuoto el. parašo ir sertifikavimo paslaugas šiuo metu Lietuvoje teikia UAB „Skaitmeninio sertifikavimo centras“, VĮ „Registrų centras“ bei Gyventojų registro tarnyba. Įsigyti el. parašo įrangą, bei sertifikatą gali bet kuris žmogus, turintis asmens kodą, pateikęs asmens tapatybę patvirtinantį dokumentą, susimokėjęs atitinkamą mokestį už suteikiamą paslaugą.
4. Lietuvoje, kaip ir daugelyje kitų elektroninį parašą naudojančių valstybių, įstatyminė el. parašo bazė buvo sukurta 2000m., tačiau pirmoji kvalifikuotus sertifikatus teikianti institucija (SSC) buvo sukurta tik 2005 m. Tokį ilgą laiko tarpą lėmė tai, kad valstybė, taupant lėšas, nutarė nekurti atitinkamos valstybinės institucijos. 2007 m. antroje pusėje lyginant su ES vidurkiu, el. parašo diegimas ir naudojimas Lietuvoje nebuvo lėtas, tačiau buvo tikslinga tai paspartinti vykdant valstybės tarnautojų pažymėjimų ir daugiafunkcinės lustinės asmens tapatybės kortelės projektus.
5. Viešojo rakto infrastruktūros diegimas yra labai ilgas ir sudėtingas procesas, kuriam yra keliami aukšti reikalavimai. Be to el. parašo technologijos yra brangios ir šiuo metu mažai pelningos, todėl pelno siekiančios organizacijos neskuba užimti šios rinkos dalies. El. parašo technologijai ilgą laiką vystytis trukdė bankai. Jų išduodamos klientų identifikavimo priemonės, naudojamos prisijungiant prie internetinės bankininkystės sistemų, buvo klaidingai laikomos elektroniniu parašu.

   Žiūrint iš vartotojo pusės, beveik nėra reklamos, todėl daugelis vartotojų net nežino ir nėra girdėję apie elektroninio parašo technologiją ir jos teikiamą naudą. Be to, paprastam vartotojui ir nėra didelės būtinybės naudoti šią technologiją, nes šiuo metu elektroninį parašą galima naudoti tik dokumentų pasirašymui.

Kita priežastis yra sunkumai, susiję su atitinkamų tarnybų steigimu ar techninių ir programinių sprendimų priėmimu. Egzistuoja daug įvairių dokumentų, standartų, teisės aktų, kuriuose pilna reikalavimų. Tokie reikalavimai el. parašo infrastruktūros kūrėjus įspraudžia į labai siaurus rėmus. Tam, kad būtų įgyvendinta tokie kiekiai reikalavimų, reikia gerų specialistų, kurie sugebėtų juos realizuoti. Norint pasamdyti aukštą kvalifikaciją turinčius specialistus, reikės daug piniginių lėšų. Taip pat lėšų reikės įrangai bei technologijoms, nekalbant apie laiką, kurio prireiks įgyvendinant visus reikalavimus. Akivaizdu, jog reikalavimų visuma yra pagrindinė ir pati didžiausia priežastis, dėl kurios el. parašo technologija taip sunkiai skinasi sau kelią.

6. Atlikus konkrečių įstaigų - UAB „Skaitmeninio sertifikavimo centro“, VĮ „Registrų centro“ ir Gyventojų registro tarnybos - veiklos nuostatų ir parašo taisyklių analizę–palyginimą tarpusavyje galima teigti: GRSC sertifikavimo veiklos nuostatuose ir sertifikatų taisyklėse yra daug nuorodų į reglamentuojančius LR įstatymus, standartus ar kitus dokumentus. Tai yra gerai. Tačiau nuostatai ir taisyklės yra nemažai nukrypę nuo jų rengimo standarto. GRSC veiklos nuostatuose ir parašo taisyklėse praleista daug punktų, greičiausiai dėl to, jog tokių punktai nėra aktualūs vartotojams.
7. Visų technologijų diegimas ar plėtra priklauso nuo aukščiausius postus užimančių asmenų. Tokiu atveju, pirmiausia, reikėtų valdžios atstovams parodyti, jog el. parašo technologija yra tikrai saugi, patikima ir ją galima pritaikyti daugelyje sričių. Reikėtų daugiau lėšų skirti šios technologijos reklamai ir diegimui. Taip atsirastų didesnė paklausa, kas lemtų savaiminį šios technologijos naudojimo augimą. Įstaigoms, kurios jau išduoda sertifikatus, ar tos, kurios dar tik ketina steigtis, rekomenduotina daugiau vadovautis parengtais standartais ir lygiuotis į didžiausias, labiausiai pažengusias kompanijas, tokias kaip Verisign. Gilinantis į techninius dalykus, programavimo darbus turėtų atlikti tik patirtį ir aukštą kvalifikaciją turintys programuotojai, kitaip vadinami „Senior programers“. Tęsiant šią temą, reikėtų atlikti apklausą kvalifikuotus sertifikatus išduodančiuose sertifikatų centruose, siekiant išsiaiškinti, kuriuos dalykus buvo sunkiausia įgyvendinti. Taip pat derėtų apklausti ir Informacinės visuomenės plėtros komitetą prie Susisiekimo ministerijos, dėl kokių priežasčių dažniausiai sertifikatų centrai nebuvo registruojami, kaip kvalifikuotus sertifikatus išduodantys.

SUMMARY

Karolis Rubinas, Public Key Infrastructure implementation problems.

The main object is a digital signature. The aim of this work is to find out the difficulties, witch prevents Public Key Infrastructure implementation. Goals was to: clear up the definition of a digital signature, find out how digital signature works and what is it for; analyze the structure and introduce it to the reader; compare the existing PKI situation in Lithuania with other countries; identify possible problems implementing a digital signature; compare Lithuanian qualified CA's CP and CPS.

Taking digital signature definitions into generalization, it is possible to conclude, that this is a digital technology, witch enables the user not only to sign the digital document and identify the person who signed, but also keeps the document from distortion and makes it unique. After analyzing the standards and legal documents I may say that the biggest problem implementing and developing PKI is REQUIREMENTS. In every step there are requirements witch you have to fulfill if you want to create a trustworthy and qualified PKI. Comparing the existing situation in Lithuania Digital signature in other countries is way more used and spread even though juridical base was completed by Lithuanians earlier than other countries, with more CAs. In addition it was revealed that there are five CAs in Lithuania, but only three of them produce qualified certificates. These are: UAB „Skaitmeninio sertifikavimo centras", VĮ "Registrų centras" and „Gyventojų registro tarnyba". "„UAB Omnitel" and „UAB Bitė Lietuva" is not included in this list. This may be because of lack of meeting most of the requirements that were mentioned and those were not mentioned in this work.

This work could be useful for business companies as well as for public organizations witch want to offer digital signature service. Also this is useful for digital signature users, who want to understand more about the digital signature operation, its purpose and benefits.

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS

[BNET] Bundesnetzagentur. ACCREDITED CERTIFICATION SERVICE PROVIDERS. State of 12.02.2010. Prieiga per internetą: <http://www.bundesnetzagentur.de/cln_1912/EN/Areas/ElectronicSignature/CertificationServiceProviders/certificationserviceproviders_node.html#doc11642bodyText1>

[CNGA] Centro nazionale per i'informatica nella pubblica amministrazion. GUIDA ALLA FIRMA DIGITALE. 2009 04. Prieiga per internetą: <http://www.cnipa.gov.it/html/docs/GuidaFirmaDigitale2009_a.pdf >

[CNIP] Centro nazionale per i'informatica nella pubblica amministrazion. ELENCO PUBBLICO DEI CERTIFICATORI. 2010 04 08. Prieiga per internetą: <http://www.cnipa.gov.it/site/it-IT/Attivit%C3%A0/Firma_digitale/Certificatori_accreditati/Elenco_certificatori_di_firma_digitale/>

[COCA] Controller Of Certifying Authorities. PKI FRAMEWORK, RCAI, LICENSED CA'S. 2008. Prieiga per internetą: < http://cca.gov.in/rw/pages/index.en.do>

[CWA0] Cen Workshop Agreement. CWA 14170. SECURITY REQUIREMENTS FOR SIGNATURE CREATION APPLICATIONS. May 2004. Prieiga per internetą: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf >

[CWA1] CWA 14171. GENERAL GUIDELINES FOR ELECTRONIC SIGNATURE VERIFICATION. May 2004. Prieiga per internetą: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf>

[CWA9] Cen Workshop Agreement. CWA 14169. SECURE SIGNATURE-CREATION DEVICES. March 2004 Prieiga per internetą: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf>

[ELME] Ellen Messmer. RUSSIA'S FEDERAL TREASURY GETS PKI ROLLOUT MOVING. *NetworkWorld.com*, 09/12/05 Prieiga per internetą:

<http://www.networkworld.com/weblogs/security/009945.html>

[EPĮ0] ELEKTRONINIO PARAŠO ĮSTATYMAS. 2000 m. liepos 11 d. Nr. VIII-1822 Vilnius.

[EPNT] ELEKTRONINIS PARAŠAS NETRUKUS TAPS KASDIENYBE. Best in Lithuania Nr. 4, 2008. Prieiga per internetą: <http://www.bestinlt.lt/Straipsnis-17-Elektroninis_parasas_netrukus_taps_kasdienybe>

[EREG] Ēriks Eglītis. PKI DEVELOPMENTS, LATVIA. Eparaksts eme. 2007. Prieiga per internetą: <http://info.e-me.lv/?page_id=39>

[ETSI] Time stamping profile. ETSI TS 101 861 V1.2.1. March 2002. Prieiga per internetą: <http://docbox.etsi.org/EC_Files/EC_Files/ts_101861v010201p.pdf>

[EVLI] Evaldas Liutkus. ELEKTRONINIO PARAŠO TAIKYMAI LIETUVOJE. Pasaulis realisto akimis. 2009 Prieiga per internetą: <http://blog.liutkus.eu/elektroninio-paraso-taikymai-lietuvoje>

[GYRE] Gytis Repečka. ELEKTRONINIS PARAŠAS. KAS TAI? Balsas.lt 2008. Prieiga per internetą: <http://www.balsas.lt/naujiena/175605/gytis-repecka-elektroninis-parasas>

[GRCP] Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. SERTIFIKATO TAISYKLĖS. 2009-03-25. Prieiga per internetą: <http://www.gyvreg.lt/html/teises_aktai/NSC%20CP%20v1.1.doc>

[GRSC] Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos. SERTIFIKAVIMO VEIKLOS NUOSTATAI. Versija: 2.0. 2009-11-25. Prieiga per internetą: <http://www.nsc.vrm.lt/docs/NSC%20CPS%20v2.pdf>

[HFPS] R.Housley, W.Ford, W.Polk, D.Solo. INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE AND CRL PROFILE. 1999. Prieiga per internetą: <http://www.clizio.com/S3/documenti/RFC/rfc2459.txt.pdf>

[IAER] Elektroninio Parašo infrastruktūros diegimas ir naudojimo skatinimas Lietuvoje. Ignalina IAERPA Konferencija 2007. Prieiga per interentą: <www.inppregion.lt/get.php?f.37331>

[IVPK] Informacinės Visuomenės plėtros komiteto prie Susisiekimo ministerijos interneto svetainė. Prieiga per internetą: <http://www.ivpk.lt/main.php>

[KARY] Rytis Kalinauskas. ELEKTRONINIS PARAŠAS IR ELEKTRONINIS DOKUMENTAS. 2003. Prieiga per internetą: <www.ivpk.lt/renginiai/pranesimai/r.kalinauskas.ppt>

[MIDO] Mikhail Doroshevich. DRAFT LAW ON ELECTRONIC DIGITAL SIGNATURE PASSED THE FIRST HEARINGS AT BELARUSIAN PARLIAMENT. 02/06/2009 Prieiga per internetą: <http://www.e-belarus.org/news/200906021.html>

[PRLP] Plečkaitis, Romanas. LOGIKOS PAGRINDAI. Vilnius: Tyto Alba, 2004. p. 316-318 ISBN 9986-16-322-6

[RCCP] Registrų centras. RCSC KVALIFIKUOTŲ SERTIFIKATŲ TAISYKLĖS. Versija 3.0. Galioja nuo 2010.11.24. Prieiga per internetą: <http://www.registrucentras.lt/bylos/rcsc/cp_v3_0.pdf>

[RCSC] Registrų centras. RCSC SERTIFIKAVIMO VEIKLOS NUOSTATAI. Versija: 2.0. 2008-03-05. Prieiga per internetą: <http://www.registrucentras.lt/bylos/rcsc/cps_v2_0.pdf >

[RDUK] Registrų centro svetainė. DAŽNIAUSIAI UŽDUODAMI KLAUSIMAI. Žiūrėta 2011-04-07. Prieiga per internetą: <http://www.registrucentras.lt/rcsc/diegimas/duk.php>

[RFC3] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. November 2003. Prieiga per internetą: <http://www.apps.ietf.org/rfc/rfc3647.html#sec-4.6.5>

[SODR] SODRA EDAS: Instrukcija pradedančiam vartotojui. Prieiga per internetą: <www.parasas.lt/DigiDoc/DigiDoc-instrukcija.pdf>

[SSC1] UAB „skaitmeninio sertifikavimo centras“. SERTIFIKAVIMO VEIKLOS NUOSTATAI. Versija: 1.0. 205-03-01. Prieiga per internetą: <http://repository.ssc.lt/files/cps/ssc_trusted_root_cps_v1-0-0[LT].pdf >

[SSCP] „UAB Skaitmeninio Sertifikavimo Centras“. SERTIFIKATO TAISYKLĖS. Versija 1.0. 2007.12.28. Prieiga per internetą: <http://repository.ssc.lt/files/cp/ssc_trusted_root_cp_v1-0-0[LT].pdf>

[TPKI] J. Dumortier, S. Kelm, H. Nilsson, G. Skouma, P. Eecke. THE LEGAL AND MARKET ASPECTS OF ELECTRONIC SIGNATARES. Study for the European Commission - DG Information Society. October 2003. Prieiga per internetą: <http://www.pki-page.info/eu/>

[VAUN] Valdas Undzėnas. ELEKTRONINIO PARAŠO INFRASTRUKTŪRA IR ELEKTRONINĖ KOMERCIJA. Vilnius – 2003. Prieiga per internetą: <http://uosis.mif.vu.lt/~valund/KONSPEKTAI/Elektroninis%20parasas.pdf>

[VCPS] VeriSign Certification Practice Statement. Version 3.8.1. February 01, 2009. Prieiga per internetą: <http://www.verisign.com/repository/CPSv3.8.1_final.pdf>

[WAPA] Waldemar Pawlak. INTERNAL TRADE REGULATION. Ministry of economy. 2007 Prieiga per internetą: <http://www.mg.gov.pl/English/ECONOMY/Internal%20Trade%20Regulation>

PRIEDAI

1 priedas. Sertifikato dalis pagal X.500 standartą

Unikalaus vardo lauko žymėjimas ir jo paskirtis	Nurodoma reikšmė
Sertifikavimo paslaugu teikėjo unikalus vardas	
C (angl. Country), šalis	LT
O (angl. Organization), organizacija	Gyventoju registro tarnyba prie LR VRM – i.k. 188756767
OU (angl. Organization Unit), organizacijos padalinys	Nacionalinis sertifikavimo centras (NSC)
CN (angl. Common Name)	Nacionalinis sertifikavimo centras (IssuingCA)
Fizinio asmens, sertifikato savininko unikalus vardas	
G (angl. Given Name)	Asmens vardas
SN (angl. Surname)	Asmens pavardė
CN (angl. Common Name)	Asmens vardas, pavardė
Serijinis numeris	Asmens kodas

2 priedas. Sertifikato dalis pagal X500 standartą

DN vardo lauko žymėjimas ir jo paskirtis	Nurodoma reikšmė
CA sudarytojo DN	
C (*Country* – šalis)	LT
O (Organizacija)	VI Registru Centras - I.k. 124110246
OU (*Organization Unit* – organizacijos padalinys)	Registru Centro Sertifikavimo Centras
CN (*Common Name*)	VI Registru Centras RCSC (IssuingCA)
Sertifikato savininko DN	
CN (*Common Name* – asmens vardas)	Asmens vardas, pavardė
Serijinis numeris	Asmens kodas
C (*Country* – šalis)	Šalis (ISO 3166 code)

3 priedas. Sertifikato dalis pagal X.501 standartą

Atributas	*Įrašas*
Valstybė (C=)	"LT", arba netaikoma.
Pasirašytojas (CN=)	Vardas, pavardė arba pseudonimas
Juridinis asmuo (O=)	Į juridinio asmens atributą įrašoma: • Galutinio Naudotojo juridinio asmens pavadinimas
Atstovavimo teisė	Nurodoma: - Pasirašytojo teisės veikti juridinio asmens vardu; - įgalinimų apimtis; - įgalinimų pagrindas; - įgalinimų trukmė (terminas).
Vietovė (L=)	Nurodoma vietovė (adresas), kurioje yra Galutinis Naudotojas, arba netaikoma.
Įprastinis pavadinimas (CN =)	Šiame atribute įrašoma: • juridinio asmens pavadinimas (jei atributas yra sertifikate, kurimo pasirašomas kodas/objektas); • vardas (pavadinimas) (jei atributas yra fizinio asmens sertifikate).
Elektroninio pašto adresas (E =)	Elektroninio pašto adresas (jei atributas yra fizinio asmens sertifikate).