Vilniaus universitetas
Komunikacijos fakultetas

Audrius Mašidlauskas,
Informacijos sistemų vadybos programos studentas

Elektroninis parašas: teisinis reglamentavimas ir praktiniai įgyvendinimo aspektai Lietuvoje

MAGISTRO DARBAS

Vadovas: Dr. Irmantas Aleliūnas

Vilnius, 2008

Magistro darbo lydraštis

Pildo magistro baigiamojo darbo autorius
Audrius Mašidlauskas (magistro baigiamojo darbo autoriaus vardas, pavardė) Elektroninis parašas: teisinis reglamentavimas ir praktiniai įgyvendinimo aspektai Lietuvoje (magistro baigiamojo darbo pavadinimas lietuvių kalba) Electronic signature: legal regulation and practical aspects of implementation in Lithuania (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 bakalauro / 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) _____ _____ (2008 05 ___) (magistro baigiamojo darbo vadovo parašas)
Pildo instituto / katedros, kuruojančios studijų programą, reikalų tvarkytoja
Magistro baigiamasis darbas įregistruotas _____ (instituto / katedros, kuruojančios studijų programą, pavadinimas) _____ _____ (2008 05 ___) (instituto / katedros reikalų tvarkytojos parašas)
Pildo instituto / katedros, kuruojančios studijų programą, vadovas
Recenzentu skiriu _____ (recenzento vardas, pavardė) _____ _____ (2008 05 ___) (instituto / katedros vadovo parašas)
Darbą recenzuoti gavau. _____ _____ (2008 05 ___) (recenzento parašas)

Referato lapas

Mašidlauskas, Audrius
(studento pavardė) (studento vardas)

Ma601, *Elektroninis parašas: teisinis reglamentavimas ir praktiniai įgyvendinimo aspektai Lietuvoje*: magistro darbas
Mašidlauskas Audrius; mokslinis vadovas Dr. Aleliūnas Irmantas; Vilniaus universitetas.
(studento pavardė, vardas) (vadovo pavardė, vardas)

Komunikacijos fakultetas. Informacijos ir komunikacijos katedra. – Vilnius, 2008. – 75, [2] lap.: lent. – Mašinr. – Santr. angl. – Bibliogr.: p. 65–68 (51 pavad.).**
UDK indeksas 004.056055

Raktiniai žodžiai*: elektroninis parašas, asimetrinis šifravimas, PKI infrastruktūra, elektroninio parašo standartai, elektroninis parašas valstybinėse institucijose.*

Magistro darbo objektas – elektroninis parašas. Darbo tikslas - Nustatyti ir išanalizuoti priežastis, lemiančias ribotą elektroninio parašo naudojimą Lietuvoje. Pateikti principinę elektroninio parašo formavimo technologiją bei taikomus šifravimo algoritmus; Apžvelgti elektroninio parašo teisinį reglamentavimą ir atitikimą elektroninio parašo direktyvai; Apžvelgti bei išanalizuoti elektroninės valdžios, įskaitant ir elektroninio parašo ilgalaikę strategiją; Įvertinti dabartinę asmens tapatybės kortelių (su identifikacijos ir elektroninio parašo sertifikatais) projekto įgyvendinimo situaciją; Apžvelgti Lietuvos ir kelių Europos valstybių situaciją praktiškai taikant elektroninį parašą; Išnagrinėti elektroninės valdžios sistemas naudojančias elektroninį parašą; Ištirti ar valdžios institucijos nagrinėja užklausimus, atsiųstus elektroniniu paštu ir pasirašytus elektroniniu parašu; Įvertinti dabartinį visuomenės požiūrį į elektroninio parašo infrastruktūrą;
Naudojantis mokslinės literatūros ir atliktų tyrimų analize, pastebėta, kad įgyvendinant elektroninio parašo infrastruktūrą tiek Europos tiek Lietuvos lygmeniu buvo padaryta nemažai klaidų. Įvairiose ataskaitose pabrėžiama, kad standartizacijos procesai turėjo būti atlikti daug anksčiau. Kadangi Lietuva planuoja pradėti naudoti asmens tapatybės korteles su elektroninio parašo funkcija – yra svarbu pažvelgti į kitų šalių patirtį. Darbe apžvelgti geros praktikos pavyzdžiai ir taip pat nesėkmės priežastys (pvz. Suomijoje).

Darbas gali būti naudingas visiems besidomintiems elektroninio parašo infrastruktūra. Nemažai dėmesio buvo skirta į šios technologijos principinio veikimo išaiškinimą, nes daugumą skeptikų argumentuoja, jog negali būti užtikrinamas saugumas. Atliktų Lietuvos ir Europos ataskaitų, tyrimų analizė leidžia susidaryti paskutinių metų vaizdą elektroninio parašo srityje ir įvertinti galimas prognozes. Atlikti tyrimų rezultatai parodo, jog iki pilno elektroninio parašo taikymo valstybinėse institucijose dar toli. Nors visuomenėje elektroninis parašas ir jo paslaugas teikiančios įmonės yra žinomos, tačiau realiai šia infrastruktūra naudojasi labai nedaug.

TURINYS

SANTRUMPŲ SĄRAŠAS

Santrumpa	***Paaiškinimas***	
	Lietuviškai	***Angliškai***
SSCD	Saugus Parašo Kūrimo įrenginys	Secure Signature Creation Device
ICTSB	Informacijos ir Komunikacijos Technologijų Standartų Taryba (Valdyba, Komisija)	Information & Communications Technologies Standards Board
CEN	Europos Standartizavimo Komitetas	European Committee for Standardisation
ISSS	Informacinės Visuomenės Standartizavimo Sistema	European Committee for Standardisation - Information Society Standardisation System
ETSI TC SEC/ESI	Europos Telekomunikacijos standartų Institutas	European Telecommunications Standards Institute
EESSI	Europos Elektroninių Parašų Standartizavimo Iniciatyva	European Electronic Signature Standardisation Initiative
IVPK prie LRV	Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės	
CA	Sertifikavimo tarnyba	Certification Authority
RA	Registravimo tarnyba	Registration Authority
SSC	UAB „Skaitmeninis sertifikavimo centras“	
SSCD	Saugi parašo formavimo įranga	SECURE SIGNATURE-CREATION DEVICES
SK	Sertifitseerimiskeskus	
SSGG analizė	Silpnybių, stiprybių, galimybių, grėsmių analizė	
FNMT	Sertifikavimo paslaugų teikėjas Ispanijoje	
EPPS	Elektroninio parašo priežiūros skyrius	
DVS	Dokumentų valdymo sistema	

ĮVADAS

Elektroninio parašo panaudojimo galimybės bei nauda nenuginčijami. Praėjo daugiau nei aštuoni metai nuo to kaip Europos parlamentas ir Europos Sąjungos taryba priėmė direktyvą dėl Bendrijos elektroninių parašų reguliavimo sistemos. Po šios direktyvos priėmimo tiek Lietuvoje tiek visoje Europoje sekė įstatymai, reglamentuojantys elektroninio parašo naudojimą nacionaliniame lygmenyje. Taip pat sekė standartų tvirtinimas tam, kad būtų išvengta nesuderinamumų. Darbe yra apžvelgiama dabartinė Lietuvos padėtis taikant elektroninį parašą elektroninėje valdžioje bei komercijoje, remiantis paskutiniu metu atliktais tyrimais Lietuvoje ir Europoje.

Darbas yra suskirstytas į keturias pagrindines dalis. Pirmojoje dalyje yra išanalizuoti metodai, kuriais yra remiamasi formuojant elektroninį parašą ir kaip šie metodai užtikrina, jog elektroninis parašas yra apsaugotas nuo klastojimų. Antroje dalyje apžvelgiama elektroninio parašo teisinis reglamentavimas Lietuvoje. Trečioje išanalizuojamas praktinis Lietuvos ir kelių Europos valstybių praktinis pasiruošima. Ir ketvirtoje dalyje aprašyti atlikti tyrimai. Viename iš jų įvertinama kaip Lietuvos valstybinės institucijos yra pasiruošusios priimti elektroninius dokumentus, pasirašytus e. parašu. Antrame tyrime atliktoje apklausoje yra įvertinama koks šiuo metu yra visuomenės susipažinimo lygis su elektroninio parašo infrastruktūra.

Darbo aktualumas: Šiuo metu egzistuojant elektroninio parašo infrastruktūrai, jo naudojimas yra vis dar nedidelis. Šiuo metu tik nedidelė vartotojų skaičius naudojasi šia infrastruktūra. Kritinį pradinį vartotojų skaičių būtų galima įvardinti tą, kuris yra skelbiamas ir „Elektroninio parašo proveržio programoje“, tai yra 300 000 e. parašo vartotojų. Tačiau net ir šis skaičius panašu, jog yra sunkiai pasiekiamas. Kyla klausimas kokios priemonės paskatintų didesnį e.parašo naudojimą? Kas turėtų būti pirmiau didelis elektroninės valdžios paslaugų skaičius ar kritinis elektroninio parašo vartotojų skaičius?

Tikslas: Nustatyti ir išanalizuoti priežastis, lemiančias ribotą elektroninio parašo naudojimą Lietuvoje;

Hipotezė: Lietuvos Respublikos valstybinės institucijos siunčia ir gauna elektroninius dokumentus pasirašytus elektroniniu parašu;

Pagrindiniai darbo uždaviniai:

1. Pateikti principinę elektroninio parašo formavimo technologiją bei taikomus šifravimo algoritmus
2. Apžvelgti elektroninio parašo teisinį reglamentavimą ir atitikimą elektroninio parašo direktyvai.
3. Apžvelgti bei išanalizuoti elektroninės valdžios, įskaitant ir elektroninio parašo ilgalaikę strategiją.
4. Įvertinti dabartinę asmens tapatybės kortelių (su identifikacijos ir elektroninio parašo

sertifikatais) projekto įgyvendinimo situaciją;

5. Apžvelgti Lietuvos ir kelių Europos valstybių situaciją praktiškai taikant elektroninį parašą;
6. Išnagrinėti elektroninės valdžios sistemas naudojančias elektroninį parašą;
7. Ištirti ar valdžios institucijos nagrinėja užklausimus, atsiųstus elektroniniu paštu ir pasirašytus elektroniniu parašu (Tyrimo metodas: pagrindinėms šalies institucijoms išsiunčiami elektroniniai laiškai, pasirašyti elektroniniu parašu su užklausomis. Pagal gautus atsakymus bus galima daryti išvadą ar valstybinės institucijos pasiruošusios priimti dokumentus, pasirašytus elektroniniu būdu);
8. Įvertinti dabartinį visuomenės požiūrį į elektroninio parašo infrastruktūrą (Tyrimo metodas: anketinė apklausa);
9. Identifikuoti ir išanalizuoti priežastis, lemiančias elektroninio parašo infrastruktūros Lietuvoje nepakankamą (ar pakankamą) išvystymą, patvirtinti arba paneigti darbo hipotezę.
10. Pateikti išvadas bei rekomendacijas.

1. ELEKTRONINIO PARAŠO PRINCIPINIS VEIKIMAS

Elektroninis parašas yra elektroninis ekvivalentas ranka rašytam parašui. Naudojantis elektroniniu parašu atsiranda galimybė pasirašinėti dokumentus ir užsiimti verslu elektroniniu būdu, naudojantis internetu. Yra užtikrinama (sertifikavimo teikėjų pagalba), kad elektroninio dokumento autorius yra tas, kuom dedasi esąs. Elektroninis parašas nėra ranka pasirašyto parašo paveiksliukas, kuris prisegamas prie dokumento. Pasirašymo proceso metų speciali programinė įranga suformuoja elektroninį parašą tik iš pasirašančiajam prieinamų duomenų pagal algoritmus ir standartus, kurie yra atviri. Tokia priemonė leidžia susisiekti ir keistis elektroniniais dokumentais ir elektroniniais laiškais užtikrinant siuntėjo tapatybę ir užtikrinant siunčiamo dokumento vientisumą. E. parašo patikrinimui reikalingas pasirašiusiojo sertifikatas, kuriame saugomi visi su pasirašančiuoju susiję duomenys. Vienas iš tokio sertifikato pavyzdžių pateikiamas Priede Nr. 1. Šiame skyriuje apžvelgiami pagrindiniai elektroninio parašo veikimo principai. Tam, kad elektroninis parašas neatrodytų kaip „juoda dėžė“ yra išanalizuoti principiniai šifravimo algoritmai nesigilinant į detalius matematinius skaičiavimus.

*Privalumai***.** Kiekvienai verslu užsiimančiai įmonei reikia apsikeisti informacija greitai, tiksliai ir saugiai, tiek įmonės viduje, tiek ir su kitomis įmonėmis, klientais. Keičiantis dokumentais elektroniniu būdu, o ne popieriniais suteikia vartotojams nemažai privalumų:

- Informacija pasiekia gavėją iš karto, nepriklausomai nuo atstumo;
- Vieną kartą įsigijus elektroninio parašui reikalingą įrangą daugiau nereikia papildomai investuoti (nereikia pirkti pašto ženklų, vokų, kaso aparatų, popieriaus);
- Informacija persiunčiama tiesiogiai (nėra įtraukiami pašto darbuotojai);
- Informacija visada gavėją pasiekia nepakitusi (ne taip kaip kartais tekstą iškraipantis faksas);
- Visada aktuali dokumento redakcija kompiuteriniame pavidale. Derinant dokumentus dažniausiai būna peržiūrimas kompiuterinis variantas, o pasirašomas popierinis;
- Automatiškai yra fiksuojama kada buvo išsiųstas dokumentas ir ar gavėją tikrai pasiekė;
- Elektroninių dokumentų paieška tampa daug paprastesnė ir patogesnė;

Didesnis saugumo lygis:

- Elektroniniai paršai užtikrina daug didesnį saugumo lygį nei ranką rašyti parašai.
- Naudojantis e. parašais, neįmanoma kitiems padaryti pasirašiusiojo kopijų, be to e. parašas apima iš karto visą dokumentą, o ne tik paskutinį lapą, kaip tai yra pasirašant ranka;
- Taip pat yra užtikrinama, jog dokumente niekas nebuvo pakeista;
- Persiuntimo įrodymas (laiko žyma) – sertifikavimo paslaugų teikėjai uždeda laiko žymą ant pasirašytų dokumentų tam, kad užtikrinti tikslią pasirašymo datą;

- Technologiškai galima užtikrinti, kad persiunčiamas dokumentas pasieks tik mūsų pageidaujamą gavėją;
- Taip pat elektroninio parašo pagalba yra užtikrinama, kad siuntėjas negalės paneigti, jog laiškas ar dokumentas buvo jo siųstas;

Kvalifikuoti elektroniniai parašai suteikia vartotojams realizuoti teisiškai galiojančius kontraktus su suinteresuotom šalim kai fiziškai pasirašantieji yra skirtingose vietovėse. Tačiau vartotojas yra priverstas atlikti šiuos veiksmus prie savo kompiuterio, pasinaudodamas savo parašo kortele ir kortelių skaitytuvu. Taigi, suinteresuotų šalių buvimo vieta tampa nebe problema, o vieta kurioje turi būti atliekami pasirašymo veiksmai tampa fiksuota. Gaunamas privalumas, pasirinkus elektroninį parašą, yra tas, jog atsiranda laisvė su kuo bendradarbiauti vystant verslą, atsiranda laiko nepriklausomumas ir galimybė užsiimti verslu namuose vietoj to, jog tektų vykti į specifinę susitikimo vietą, kaip tą reikėtų atlikti bendraujant su viešojo administravimo sektoriumi.

1.1 Šifravimo algoritmai – saugaus elektroninio parašo pagrindas

Skaitmeninio parašo veikimo principo įsivaizdavimui reikalingas bent minimalus šifravimo algoritmų supratimas. Apžvelgsime keletą šifravimo pavyzdžių bei jų taikymus realizuojant skaitmeninį parašą. Skaitmeninio ir elektroninio parašo sąvokos yra neretai painiojamos. Kai kalbama apie skaitmeninį parašą yra turima omenyje technologinė realizacija, o elektroninio parašo sąvoka yra globalesnė.

„Skaitmeninio parašo technologija atlieka šiuos procesus kai kažkas pasirašo dokumentą: užšifruoja duomenis ir aptinka jeigu pakeitimai buvo atlikti po pasirašymo. Tuo tarpu elektroninis parašas vizualiai atvaizduoja pasirašiusiojo ir dokumento sąryšį (panaudojant skaitmeninio parašo technologiją ar biometrinius duomenis pan.). Parašas visam laikui susiejamas su dokumentu, taip kaip pasirašant parkeriu ant popieriaus. <...> Tačiau elektroninis parašas apima ne tik vizualinį parašo atvaizdavimą, bet panaudoja skaitmeninio parašo technologiją (arba kitą technologiją), kuri patikrina duomenis ir aptinka pasikeitimus. Priedo elektroninis parašas apima keliamus teisinius reikalavimus.“ [1]

„Skaitmeniniai parašai yra naudojami viešojo rakto infrastruktūros kontekste (PKI infrastructure), kur viešasis raktas yra naudojamas parašo tikrinime ir kuris yra pririštas prie

[1] *Digital Signature vs Electronic Signature - What's the big difference?*, Silanis Technology, [žiūrėta 2008 m. gegužės 20 d.], p.2, Prieiga per internetą: <http://www.cdmspa.com/pdfs/digital%20signature%20vs%20electronic%20signature.pdf>

skaitmeninio tapatybės sertifikato išduoto sertifikavimo teikėjo, valdomo trečios šalies. PKI sistemos naudoja asimetrinio rakto kriptografiją.“ [2]

Šifravimas, tai procesas, kurio metu yra pakeičiamas žinutės turinys taip, kad tampa nebeįmanoma jo perskaityti ar suprasti, išskyrus tą asmenį, kuriam ta žinutė buvo skirta. Reikalingas specialus raktas (tam tikro ilgio kintamas simbolių rinkinys), kurį panaudojus žinutė vėl tampa skaitoma. Šifravimas yra naudojamas slaptumo užtikrinimui keičiantis informacija internete.

Elektroniniai parašai yra naudojami tam, kad patikrinti, jog žinutė ar dokumentas buvo pasirašytas konkretaus asmens ir kad žinutė nebuvo padirbta arba pakeista kito asmens.

Šifravimas ir skaitmeniniai parašai gali būti naudojami kartu arba atskirai:

- žinutė gali būti užšifruota, bet nepasirašyta skaitmeniniu būdu (tiktai asmuo su atitinkamu raktu gali perskaityti ją, tačiau gavėjas negali būti tikras siuntėjo autentiškumu (negali būti tikras, jog žmogus išsiuntęs yra tas pats žmogus, kuriuo dedasi esąs);
- žinutė gali būti skaitmeniniu būdu pasirašyta, bet neužšifruota (visi gali pasakyti kas žinutę parašė ir visi gali perskaityti ją);
- žinutė gali būti iš pradžių užšifruota ir tada skaitmeniniu būdu pasirašyta (tiktai žmogus su atitinkamu raktu gali perskaityti žinutę, bet visi gali pasakyti kas žinutę parašė);
- žinutė pirma gali būti pasirašyta skaitmeniniu būdu ir tik po to užšifruota (tiktai žmogus su atitinkamu raktu gali perskaityti žinutę ir tik tas pats žmogus gali būti tikras, siuntusiojo žmogaus autentiškumu);

Kalbant apie šifravimą svarbu išskirti dvi pagrindines šifravimo metodų grupes, tai būtų simetrinis ir asimetrinis šifravimas. Taikant simetrinį šifravimą vienas ir tas pats raktas yra naudojamas tiek žinučių užšifravimui, tiek ir jų dešifravimui. Raktas čia turima omenyje simbolių seka, kuri panaudojama taikant šifravimo algoritmą, tam kad žinutė būtų sėkmingai užšifruota. Taikant simetrinį šifravimą ta pati skaičių seka yra panaudojama ir žinutės dešifravimui. Ilgesnis raktas (ilgesnė simbolių seka) užtikrina, jog raktą bus sunkiau dešifruoti. Tarkim, jeigu turime keturių simbolių raktą (A1B2), pavertus bitais, tai būtų 36 bitų seka (4x8). Kas reikštų, jog norinčiam iššifruoti žinutę, bet nežinančiam rakto tektų patikrinti beveik 70 milijardų variantų (2^{36}). Tačiau raktai yra naudojami, kur kas didesni ir šifruojama po kelis kartus. Tokie šifravimo metodai tampa neįveikiami net šiuolaikiniams kompiuteriams net jeigu būtų bandoma iššifruoti per kelis metus.

Egzistuoja dar vienas kriptografinių sistemų tipas, kuris naudoja vieną raktą žinučių šifravimui ir kitą raktą žinučių dešifravimui. Tokia sistema yra vadinama *asimetrinė kriptografinės*

[2] *Study PKI and Certificate Usage in Europe 2006*, Fraunhofer Institute FOKUS, October 31, 2006, Editor: Petra Hoepner [žiūrėta 2008 m. gegužės 20 d.] p.7, Prieiga per internetą: <http://www.ecom.or.jp/report/Study_on_PKI_2006_in_EUROPE-FINAL.pdf>

sistema. Tokios sistemos privalumas tas, kad daug žmonių gali naudoti šifravimo raktą tam, kad užšifruoti žinutes gavėjui, bet tik gavėjas turėdamas dešifravimo raktą galės dešifruoti ir perskaityti žinutes. Kadangi šifravimo raktas yra paplatinamas visų naudojimui, tai tokia sistema dar vadinama ir *viešo rakto kriptografinė sistema,* nes vienas iš raktų yra viešas.

Viena iš labiausiai paplitusių asimetrinių kriptografinių sistemų yra pagrįsta RSA algoritmu, pavadintu pagal išradėjų inicialus (Rivest, Shamir ir Adleman).[3] Kaip ir dauguma asimetrinių algoritmų, RSA algoritmas naudoja kintamus raktų dydžius. Kaip ir visuose asimetriniuose algoritmuose, šifravimo raktas skiriasi nuo dešifravimo rakto. Viešu raktu yra užšifruojama žinutė ir tik privačiu raktu galima ją dešifruoti. Būtent šis atradimas ir sudarė pagrindą elektroninio parašo įgyvendinimui.

1.2 Elektroninio parašo mechanizmas

Šioje dalyje apžvelgiamas klasikinis Elektroninio Parašo Algoritmas (Digital Signature Algorithm - DSA), kuris leidžia vienam žmogui su **slaptu (privačiu)** raktu "pasirašyti" dokumentą, tam, kad kiti atitinkamu **viešu** raktu galėtų patikrinti (patvirtinti), kad dokumentas buvo pasirašytas ne kieno nors kito, bet slapto rakto savininko.

Elektroniniai parašai be asimetrinės kriptografijos taip pat remiasi „maišos funkcijomis" (hash functions), kurių sugeneruotas rezultatas (žinutės santrauka) yra tik vienpusis (užšifravus nebegalima iššifruoti atgal). Kitaip tariant nėra būdo gauti pradinės žinutės. Maišos funkcijų operacijos yra panašios į šifravimo operacijas, kurios naudojamos pasitelkiant simetrinį užšifravimo raktą, tačiau čia nėra dešifravimo rakto: operacija yra negrįžtama. Vienas iš tokio pobūdžio šifravimo yra „Saugios Maišos Algoritmas" (Secure Hash Algorithm (SHA).

„SHA1 yra naudojamas atvaizduoti koncentruotą santrauką tam tikro duomenų failo. Kai duomenų failui pritaikomas SHA1 algoritmas, pasekoje gaunamas 160 bitų rezultatas - vadinamas žinutės santrauka. Ši santrauka toliau gali būti naudojama taikant elektroninio parašo algoritmą (DSA), kuris skirtas patikrinti žinutės parašą. Pasirašant žinutės santrauką, o ne visą žinutė dažniausiai padidina atliekamų procesų našumą, nes santrauką dažniausiai yra gerokai mažesnė už pačią žinutę." [4]

Kad lengviau įsivaizduoti SHA veikimą kaip pavyzdys galėtų būti sakinys pateiktas 1 pavyzdį. Pirmu atveju pritaikius SHA algoritmą gauname vieną maišos rezultatą, tačiau užtenka pridėti du simbolius „ne" ir tada jau gauname visiškai kitokią reikšmę.

---

[3] Marshall D. Abrams and Harold J. Podell, *Cryptography*, [žiūrėta 2008 m. balandžio 20 d.], p.7, Prieiga per internetą: <http://www.acsac.org/secshelf/book001/15.pdf>

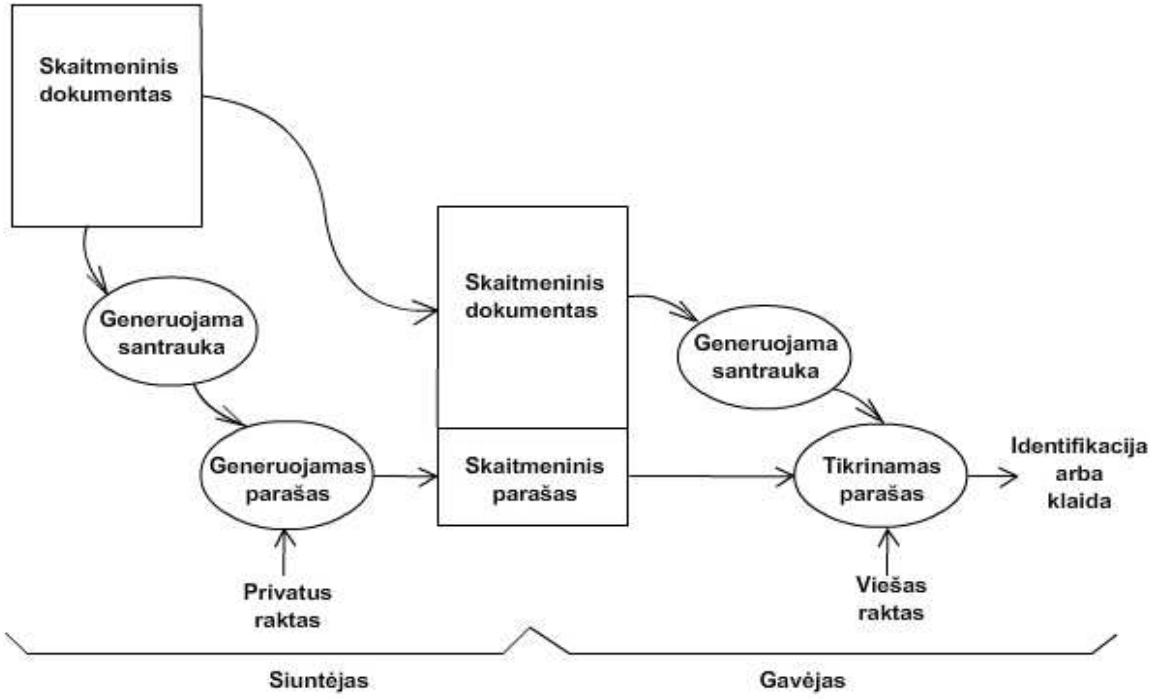
[4] *SHA1 Encryption Algorithm*, 2003 VOCAL Technologies, Ltd. Custom Product Design Division, p.1, [žiūrėta 2008 m. kovo 20 d.]. Prieiga per internetą: http://www.vocal.com/SHA1.pdf>

1 Pavyzdys. Maišos funkcijos pritaikymas.

```
SHA1(Saulė šviečia dieną)
  = 2fd5e3c6 7a2d583c ed859e31 bb765749 1b93eb35


SHA1(Saulė nešviečia dieną)
  = de9f5c9f d2559b3a f9d5e85a 09d57d9b 1005b493
```

1 paveiksliukas. Dokumento pasirašymo etapai. Sugeneravus dokumento santrauką (atspaudą), taikant SHA algoritmą, užtikrinama, jog dokumento turinys nebuvo pakeistas. [5]



1.3 Sąvokų atskyrimas: identifikacija, autentifikacija, elektroninis parašas, eID

Tam, kad nebūtų painiavos svarbu atskirti įvairius terminus. Dažnai yra painiojama elektroninis parašas su autentifikacija elektroninėje erdvėje. Tai yra du skirtingi dalykai nors technologiškai turintys nemažai panašumų. Išnagrinėjus elektroninio parašo mechanizmą, galima išskirti pagrindinius žingsnius, kurie yra atliekami formuojant, tikrinant elektroninį parašą ir identifikuojantis eID kortele. Svarbu nesumaišyti pagrindinių sąvokų:

- Identifikacija – asmens tapatybės **nustatymas**. Procesas, kurio metu yra nustatoma kito asmens tapatybė. [6] Kaip pavyzdys galėtų būti paso išdavimas. Pasas yra išduodamas tik tada kai yra nustatoma asmens tapatybė (identifikuojamas asmuo);

[5] *Authentication 101*, [žiūrėta 2008 m. kovo 20 d.]. Prieiga per internetą: <http://www.cscap.nuctrans.org/Nuc_Trans/links/dsa-disa.html>.

[6] *Alexias inc., techninis žodynas*, [žiūrėta 2008 m. kovo 20 d.]. Prieiga per internetą: <http://www.lexias.com/2.0/glossary4.html>

- Autentifikacija – asmens tapatybės **patvirtinimas**. Procesas, kurio metu yra patvirtinama tapatybė, teisė į nuosavybę arba autorizacija. [7] Kaip pavyzdys galėtų būti paso panaudojimas. Oro uoste pateikus pasą yra patvirtinama asmens tapatybė (asmuo autentifikuojamas);
- Autorizacija – asmens **teisių nustatymas**; Procesas, kurios metu yra nustatoma, kokio tipo veikla sistemoje yra leidžiama. [8]

Yra įvairių technologinių sprendimų, bet dažniausiai į asmeninius USB raktus arba lustines korteles yra įrašomi du sertifikatai iš kurių vienas yra skirtas elektroninio parašo formavimui, o kitas yra skirtas autentifikacijai elektroninėje erdvėje.

Principiniai žingsniai atliekami formuojant elektroninį parašą:

1. Elektroninis parašas gali būti formuojamas bet kokio formato elektroniniam dokumentui;
2. Įdedame USB raktą arba įstatome lustinę kortelę į skaitytuvą. Laikmena (USB raktas, lustinė kortelė ar SIM kortelė) priklauso nuo vartotojo pasirinkimo. Laikmenoje dažniausiai yra įrašyti du sertifikatai su jiems priskirtais privačiaisiais raktais. (Technologiškai yra užtikrinama, jog privatieji raktai niekada nepalieka įrenginio) Vienas sertifikatas yra skirtas elektroninio parašo formavimui, o kitas yra skirtas autentifikacijai elektroninėje erdvėje;
3. Su specialia pasirašymo programa instaliuota kompiuteryje pasirenkame dokumentą, kurį planuojame pasirašyti;
4. Programa pagal tam tikrą algoritmą suformuoja elektroninio dokumento santrauką. Šis žingsnis yra atliekamas tam, kad patikrinimo metu būtų galima nustatyti ar nebuvo pažeistas dokumento vientisumas;
5. Suformuota santrauka yra siunčiama į USB raktą, kuriame santrauka yra užšifruojama pasinaudojant privačiu raktu. Šis raktas yra skirtas elektroninio parašo formavimui, bet ne autentifikacijai elektroninėje erdvėje;
6. Užšifruota dalis ir sertifikatas yra siunčiami į kompiuterį ir su pasirašymo programa yra prikabinami prie pasirašinėjamo dokumento.

Principiniai žingsniai atliekami tikrinant elektroninį parašą:

1. Tikrinamas elektroninis dokumentas su prisegtu elektroniniu parašu, kuris susideda iš sertifikato (sertifikatas neša visa informacija apie asmenį, kuris pasirašė) ir užšifruotos santraukos dalies;
2. Speciali elektroninio parašo tikrinimo programa susisiekia su sertifikavimo teikėjo serveriu ir patikrina ar sertifikatas yra galiojantis;

---

[7] *Firewall Product Functional Summary*, Global Technology Associates, Inc, [žiūrėta 2008 m. kovo 20 d.]. P. 16, Prieiga per internetą: <http://www.gta.com/downloads/external/pdf/GTA-Functional-Summary.pdf>
[8] *Firewall Product Functional Summary*, P. 16.

3. Su viešuoju raktu iš sertifikato yra dešifruojama užšifruota santrauka;

4. Tikrinimo programa suformuoja elektroninio dokumento santrauką;

5. Sulyginama dešifruota santrauka su 4 žingsnyje suformuota santrauka. Jeigu santraukos sutampa reiškia, jog dokumento vientisumas nebuvo pažeistas;

6. Kadangi pavyksta dešifruoti su sertifikate esančiu viešuoju raktu vadinasi, užšifruoti galėjo tik privataus rakto savininkas, kuris ir nurodytas sertifikate.

Autentifikacija elektroninėje erdvėje:

1. Tarkim norime prisijungti prie banko internetinės svetainės, kurioje naudojama autentifikacija su sertifikatais;

2. Įstatome USB raktą arba lustinę kortelę į skaitytuvą (laikmenoje saugomi du sertifikatai – vienas pasirašymui, kitas – autentifikacijai);

3. Banko serveris atsiunčia informacijos tekstą į USB raktą, tai gali būti elektroninis dokumentas (turinys visiškai nesvarbu);

4. USB rakte atsiųsta informacija yra užšifruojama privačiu raktu, kuris yra susietas su autentifikacijai elektroninėje erdvėje skirtu sertifikatu.

5. Iš USB rakto yra siunčiama užšifruota informacija ir sertifikatas.

6. Banko serveris susisiekia su sertifikavimo centro serveriu ir patikrina ar sertifikatas yra galiojantis.

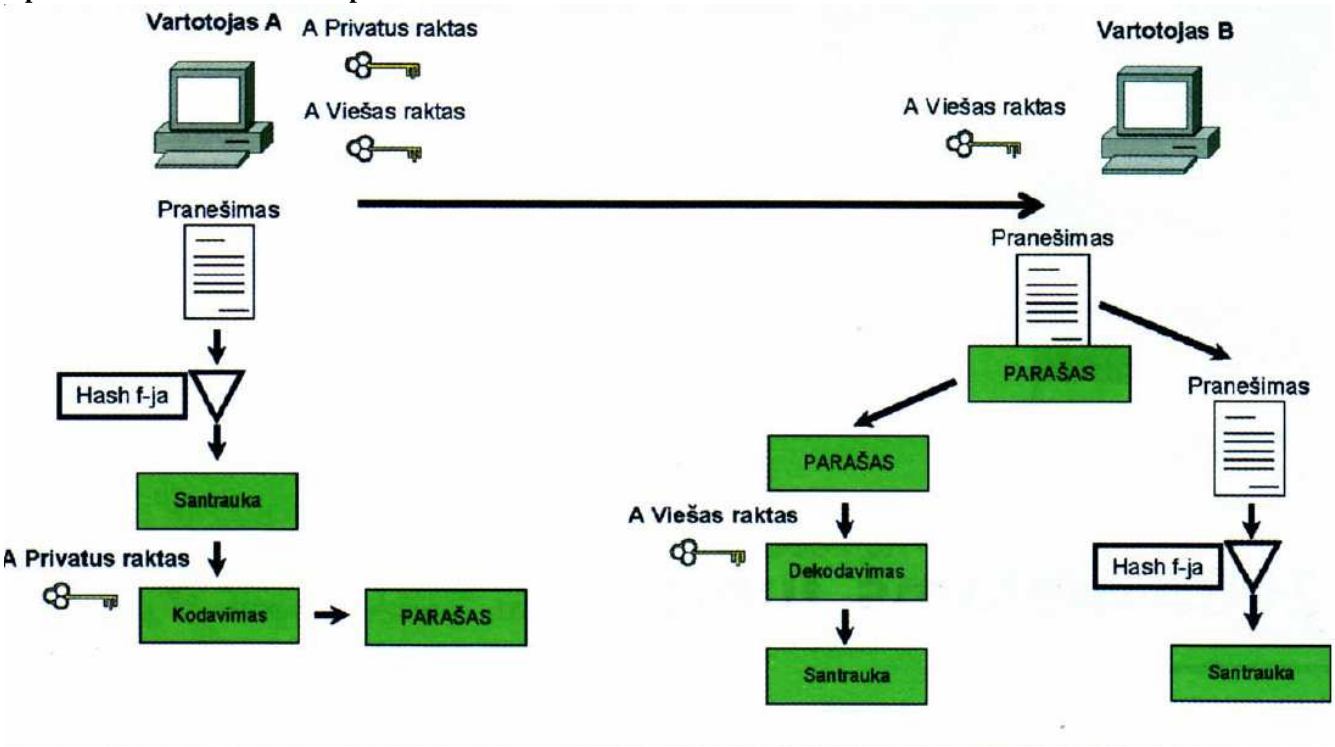
7. Jeigu sertifikatas yra galiojantis – tada su viešuoju raktu esančiu sertifikate yra dešifruojama gauta užšifruota informacija;

8. Jeigu dešifruota informacija yra identiška 3 žingsnyje vartotojui siųstai informacijai, vadinasi autentifikacija sėkminga.

Pagrindinis ir dažniausias diskusijų objektas yra sąsaja tarp elektroninio parašo ir autentifikacijos. Praktikoje neretai yra tokių situacijų kaip vartotojo yra paprašoma autentifikuotis elektroninės valdžios sistemoje ir po to vartotojas gali keistis konkrečiais dokumentais nevaržomai ir be papildomų techninių žingsnių. Šis autentifikacijos metodas (kuris yra dažnas daugelyje šalių, bet ypatingai būdingas Didžiojoje Britanijoje, **Lietuvoje**, Olandijoje ir Maltoje) dažnai yra laikomas kaip elektroninis parašas tiek ekspertų, tiek ir viešojo sektoriaus sistemų savininkų. Tačiau, tai yra ginčytinas klausimas ar toks autentifikacijos procesas gali būti laikomas elektroniniu parašu.[9]

[9] *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications*, Report, IDABC European eGovernment Services, November 2007, p.16, Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29484>.

2 paveiksliukas. Elektroninio parašo formavimo ir tikrinimo mechanizmas[10]



Šie modeliai yra supaprastinti, realiai taikomi mechanizmai yra daug sudėtingesni. Tačiau apžvelgti modeliai atsispindi esminius elektroninio parašo formavimo, tikrinimo bei identifikacijos elektroninėje erdvėje principus.

1.3.1 Slaptažodžių metodas

Beveik kiekvienas iš mūsų naudojame tiesiogiai mums priskirtus vartotojų vardus bei savo susikurtus slaptažodžius tam, kad būtume identifikuoti ir galėtume prisijungti prie įvairių sistemų. Kai kurie žmonės turi jų labai daug ir neretai juos pamiršta bei skiria nepakankamai dėmesio jų apsaugai. Šis identifikavimo būdas jau yra naudojamas dešimtmečius. Įvairios problemos susijusios su šiuo metodu yra gerai žinomos, tačiau nepaisant technologijų pažangos jos nėra išspręstos. Šios problemos išlieka viena iš didžiausių saugumo problemų, bet įvairios verslo organizacijos bei vartotojai ir toliau naudoja šį identifikavimo būdą. Vienas iš pagrindinių problemų tai vadinamasis „phishing“ metodas, kurį taikant nelegaliais būdais yra bandoma „sužvejoti“ vartotojų slaptažodžius ir prisijungimo duomenis. Vienas iš metodų nelegaliai gauti vartotojo duomenis , tai būtų sukurti identiškos išvaizdos internetinės bankininkystės puslapį ir nuorodą nusiųsti galimam realios sistemos naudotojui. Vartotojų suvesti prisijungimo duomenys tokiu būdu būtų užsaugomi visai ne banko serveryje.

Turbūt internete neįmanoma nusipirkti kokios nors prekės ar paslaugos prieš tai neprisijungus prie sistemos su savo duomenimis. Kai kurie žmonės turi daugiau nei 10 įvairių prisijungimų prie

[10] REPEČKA, Gytis. *Elektroninis parašas*, „Naujoji komunikacija“ dvisavaitinis skaitmeninio gyvenimo būdo žurnalas. 2007 m. Spalio 30d. – lapkričio 30d. , Nr. 16 (212).

pačių įvairiausių sistemų, kurios prasideda nuo internetinės bankininkystės paslaugų teikimo, aukciono svetainių, internetinių parduotuvių ir baigiant tokiom sistemom, kurios skirtos elektroninių laiškų siuntimui. Tam, kad susigaudyti tarp tiek prisijungimo duomenų, vienas iš sprendimų būtų naudoti tą patį vartotojo vardą bei slaptažodį visoms naudojamoms informacinėms sistemoms. Tačiau tai labai rizikingas būdas, nes atskleidus prisijungimo duomenis prie vienos sistemos – visos kitos sistemos taip pat taptų prieinamos. Dar vienas iš sprendimų būtų saugoti visus skirtingus prisijungimo duomenis vienoje vietoje (užrašų knygutėje ar telefone), tačiau jeigu telefonas arba piniginė būtų pavogta, tai visus prisijungimo duomenis būtų galima panaudoti tam kad pasinaudoti viena ar kita jūsų asmenine sistema. Net jeigu laikytumėte slaptažodį ir vartotojo vardą atskirai, įsilaužėlis nesunkiai galėtų atspėti vartotojo vardą, tuo labiau, kad kai kuriose sistemose vartotojo vardui prašoma priskirti elektroninio pašto adresą.

1.3.2 Kelių faktorių autentifikacija

Dabartinės autentifikacijos technologijos naudoja trijų tipų autentifikaciją:

- kažkas ką jūs žinote;
- kažkas ką jūs turite;
- arba kažkas kas jūs esate;

Kai sistema naudoja tik vieną iš šių identifikatorių, tai vadinama vieno faktoriaus identifikacija. Kaip pavyzdys tokios sistemos galėtų būti vartotojų vardų bei slaptažodžių naudojimas, ši identifikacija paremta tuo ką jūs žinote. Kai sistema naudoja du identifikatorius, tai jau dviejų faktorių identifikacija ir yra žymiai saugesnė. Kaip pavyzdys galėtų būti banko kortelių naudojimas. Naudojant šį metodą reikia kažką turėti ir kažką žinoti (PIN kodą).

Kai kurie bankai siūlo prie kortelių pridėti ir asmens naudojančio banko kortelę nuotrauką. Tai jau būtų trijų faktorių identifikacija. Pardavėjas prieš nuskaitydamas kortelę patikrina nuotrauką bei paprašo įvesti PIN kodą. Pavogta kortelė tampa bevertė jeigu nėra žinomas PIN kodas, todėl neverta niekur užsirašinėti PIN kodo. Kadangi PIN kodai yra tik keturių skaitmenų ilgio, galimų PIN kodo kombinacijų yra tik 10000. Dėl to yra leidžiamas tik fiksuotas įvedimų skaičius, dažniausiai būna trys bandymai ir po to kortelė yra užblokuojama.

Panašų į bankinių kortelių saugumo lygį užtikrina ir USB raktai, kurie yra skirti formuoti elektroninį parašą arba autentifikuotis elektroninėje erdvėje, nes čia taip pat yra taikoma dviejų faktorių autentfikacija: tai ką mes žinome (PIN kodą) ir taip ką mes turime (USB raktą).

1.4 Sertifikavimo paslaugų teikėjai

Sertifikavimo teikėjai yra atsakingi už autentiškų sertifikatų generavimą vartotojams bei sertifikatų pasirašymą. Parašai prisegti prie šių sertifikatų yra generuojami iš įstaigos (sertifikavimo teikėjo) slapto identifikavimo rakto ir visi parametrai laikomi įstaigos identifikavimo sertifikate. Sertifikavimo teikėjai gali sugeneruoti ir patys pasirašyti savo paties sertifikatą arba sertifikatas būna pasirašomas aukštesnio lygio sertifikavimo paslaugų teikėjo. Dėl ko susidaro sertifikavimo centrų hierarchija.

Sertifikavimo teikėjai su sertifikatu susietus viešuosius ir privačius raktus gali generuoti patys arba gali palikti galimybę generuoti raktus patiems vartotojams. Tarkim tam kad suteikti nepriklausomą paslaugą yra paliekama galimybė patiems vartotojams susigeneruoti viešąjį bei privatųjį raktus – tada perduoti tik viešąjį raktą sertifikavimo teikėjui. Kadangi raktų pora sugeneruota ankščiau nei sertifikatas, sertifikavimo teikėjas įterpia varotojo sugeneruotą viešąjį raktą prie visų likusiųjų sertifikato duomenų bei pasirašo jį. Lietuvoje esantis sertifikavimo centras taip pat įeina į sertifikavimo teikėjo grandinę:

3 paveiksliukas. Lietuvos sertifikavimo teikėjo padėtis Europos hierarchinėje sistemoje (http://www.europki.lt/)

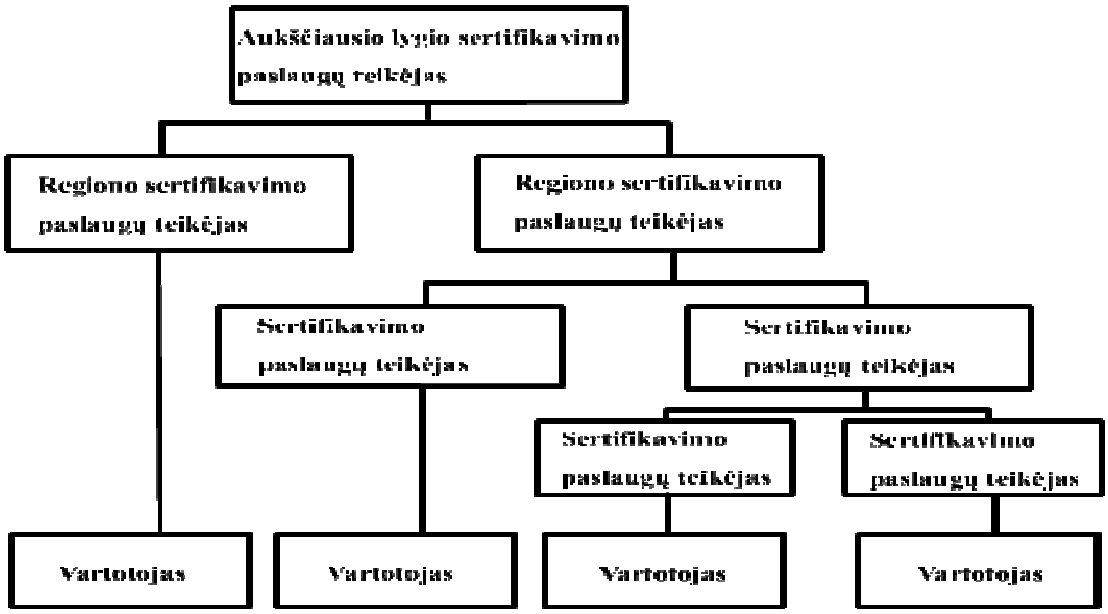
EuroPKI aukščiausio lygio sertifikavimo tarnyba (EuroPKI Top Level CA)

EuroPKI Lietuvos šakninio lygio sertifikavimo tarnyba

UAB "Skaitmeninio sertifikavimo centras" (kvalifikuotas sertifikatų tiekėjas)

Bendras sertifikavimo teikėjų modelis atsispindi šiame modelyje:

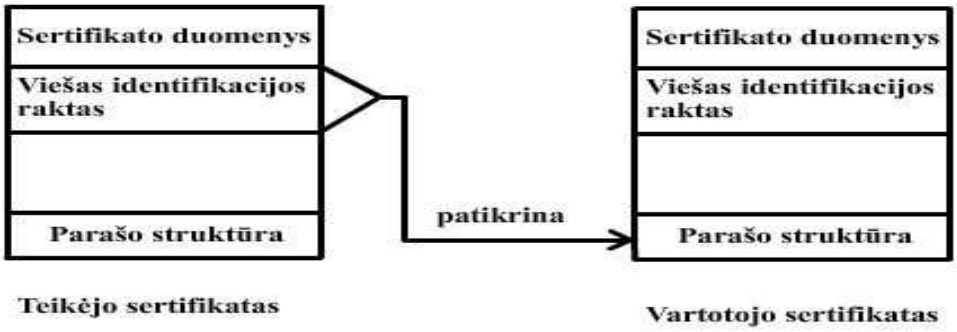
4 paveiksliukas. Hierarchiškai žemesnio sertifikavimo teikėjo sertifikatas patikrinamas pasinaudojant aukštesnio hierarchiškai sertifikavimo centro sertifikatu.



1.4.1 Sertifikato patikrinimas

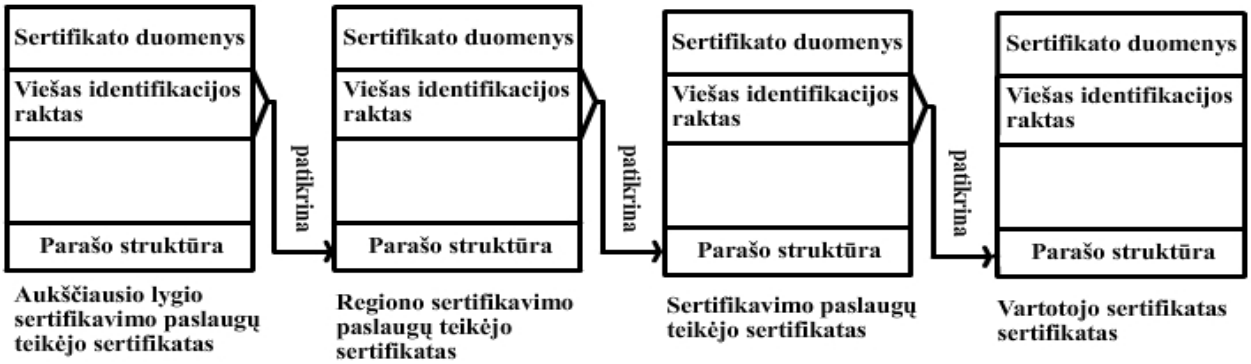
Autentifikavimo sertifikatai visų pirma turi būti sėkmingai patikrinami prieš pradedant naudoti juose esančius duomenis elektroniniam parašui patikrinti. Šie visi procesai yra atliekami pačios elektroninio parašą tikrinančios programinės įrangos ir vartotojų sertifikatai yra patikrinami pasinaudojant sertifikavimo paslaugų teikėjų sertifikatais, kurie yra suinstaliuojami kompiuteryje. Šie visi žingsniai yra automatizuoti tačiau proceso eigą svarbu žinoti tam, kad būti tikriems, jog yra užtikrinamas elektroninio parašo saugumas. Tikrinimo procesas dažniausiai susideda iš trijų etapų. Pirmame etape yra patikrinama tiesiogiai su sertifikatu susijusi informacija tokia kaip sertifikato **galiojimo laikas**. Antrajame etape yra patikrinama ar sertifikatas **nebuvo atšauktas** (pvz.: ar nebuvo paviešintas su sertifikatu susietas privatus raktas patikrinant sugeneruotą atšauktų raktų sąrašą, kurį nuolatos atnaujina sertifikavimo centras. Galutiniame etape yra patikrinama ar vartotojo sertifikatas buvo **pasirašytas atitinkamo sertifikavimo centro**.

5 paveiksliukas. Vartotojo sertifikatas yra elektroniniu būdu pasirašytas sertifikavimo centro. Parašo patikrinimui pasinaudojama paties sertifikavimo centro sertifikatu, konkrečiai sertifikate esančiu viešuoju raktu.



Šis procesas turi būti tęsiamas pradedant nuo teikėjo sertifikato, žengiant hierarchiškai iki aukščiausio lygio sertifikavimo įstaigos.

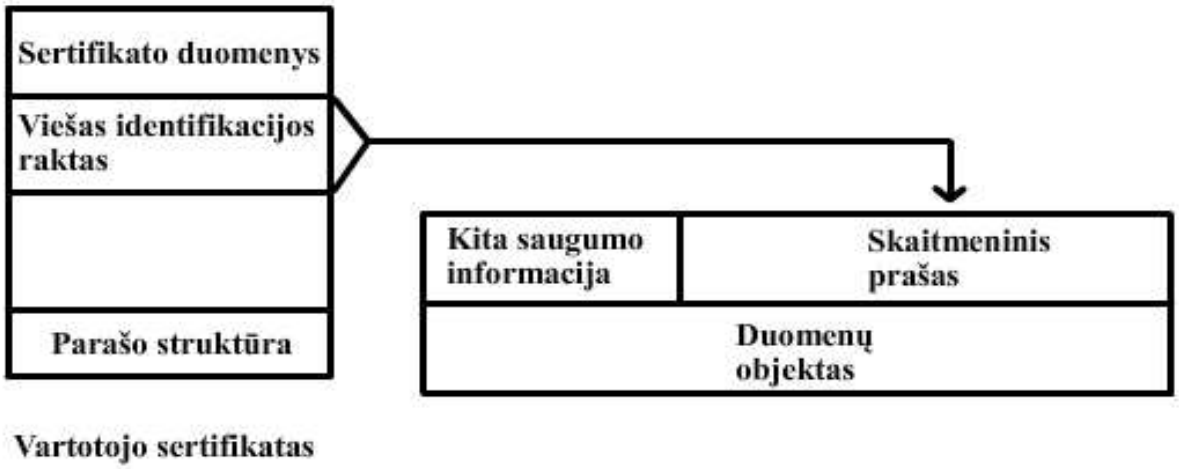
6 paveiksliukas. Hierarchiškai žemesnio sertifikavimo teikėjo sertifikatas patikrinamas pasinaudojant aukštesnio hierarchiškai sertifikavimo centro sertifikatu.



1.4.2 Vartotojo duomenų patikrinimas

Elektroniniu parašu yra pasirašomi vartotojo siunčiami duomenys tam, kad patikrinti jų vientisumą bei šaltinį. Sugeneruotas parašas yra prisegamas prie duomenų. Parašas yra patikrinamas naudojant sertifikate esančiu viešuoju raktu.

7 paveiksliukas. Vartotojo pasirašytas dokumentas patikrinamas pasinaudojant vartotojo sertifikate esančiu viešuoju raktu.



1.4.3 Sertifikavimo ir registravimo tarnybų įsipareigojimų nustatymas

Pagrindinės sertifikavimo tarnybos (certification authority) funkcijos yra tvarkyti prašymus išduoti ir atlikti naujų sertifikatų išdavimo funkcijas. Taip pat nustatyti sertifikato prašančių asmenų tapatybę galimai su atskirai paskirtų registravimo tarnybų (registration authority) pagalba. Pagal „EuroPKI sertifikavimo taisykles“ yra teigiama: „Atitinkama CA GALI pasitelkti tiek RA (Registravimo tarnybų), kiek ji nori. Jei atitinkama CA pati gali atlikti asmens identifikaciją, CA taip pat GALI atlikti RA funkcijas.“[11] Tos pačios taisykles nustato tiek sertifikavimo tarnybų, tiek registravimo tarnybų įsipareigojimus. Registravimo tarnybos įsipareigojimai yra gerokai siauresni nei sertifikavimo tarnybos:

RA TURI teikti RA paslaugas. Tai apima:

- subjekto tapatybės nustatymą
- ryšio tarp viešojo rakto ir prašymo pateikėjo, naudojant tinkamą to įrodymo būdą, patvirtinimą
- tokio ryšio patvirtinimą sertifikavimo tarnybai
- įsipareigojimą tvirtai laikytis su CA pasirašytos sutarties.

[11] *EUROPKI SERTIFIKATO TAISYKLĖS*, EuroPKI (2000-2004), 2004 m. sausis, OID: 1.3.6.1.4.1.5255.1.1.1, [žiūrėta 2008 m. kovo 20 d.], Prieiga per internetą: <http://repository.ssc.lt/get/~europki_cp>.

2. ELEKTRONINIO PARAŠO TEISINIS REGLAMENTAVIMAS

2.1 Elektroninio parašo direktyva

Pirmasis ir svarbiausias dokumentas nustatantis teisinius reikalavimus elektroniniam parašui yra Europos Sąjungos elektroninio parašo direktyva (1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos) parengta 1999 metais. Šiuo dokumentu pripažinta juridinė elektroninio parašo galia, įtvirtintos elektroninio parašo naudojimo taisyklės, įteisintas sertifikavimo paslaugų teikimas. Ši direktyva, tai pagrindas, kuriuo turėjo būti remiamasi kuriant nacionalines ES narių ir kandidačių įstatymų bazes, reglamentuojančias elektroninio parašo naudojimą.

Visos 25 Europos Sąjungos narės yra adaptavusios pagrindinius direktyvos principus. [12] Ne išimtis ir Lietuva.

2.2 Elektroninio parašo įstatymas

Šiame skyriuje apžvelgiamas Lietuvos elektroninio parašo įstatymo atitikimas direktyvai. Nagrinėjamos pagrindinės elektroninio parašo infrastruktūroje taikomos sąvokos. Taip pat apžvelgiama su kokiomis problemomis buvo susidurta taikant šį įstatymą bei kokie buvo atlikti įstatymo pakeitimai.

Įstatyme yra apibrėžiamos dvi sąvokos, tai elektroninis parašas ir saugus elektroninis parašas. Pirmojo parašo naudojimas nėra traktuojamas kaip saugaus parašo naudojimas ir jo juridinė galia yra pripažįstama tik tada jeigu naudojančios šalys susitaria dėl tokio parašo naudojimo. Vienas iš tokio parašo pavyzdžių būtų IVPK suteikti elektroniniai parašai valstybės tarnautojams. Jie yra paremti nekvalifikuotais sertifikatais. Tuo tarpu SSC suteikiami trečios klasės sertifikatai atitinka visus saugiam elektroniniam parašui keliamus reikalavimus, kurie yra tiek ES direktyvoje, tiek elektroninio parašo įstatyme:

„1) yra vienareikšmiškai susietas su pasirašančiu asmeniu (unikalumas);

2) leidžia identifikuoti pasirašantį asmenį (identifikavimas);

3) yra sukurtas priemonėmis, kurias pasirašantis asmuo gali tvarkyti tik savo valia (saugumas);

4) yra susijęs su pasirašytais duomenimis taip, kad bet koks šių duomenų pakeitimas yra pastebimas (integralumas);“ [13]

---

[12] *Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatares,* REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Prieiga per internetą: <http://ec.europa.eu/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf>

„Tačiau atkreiptinas dėmesys, kad kvalifikuotas elektroninis parašas, priešingai tarp rinkos dalyvių paplitusiam mitui, nėra vienintelis teisiškai galiojančio elektroninio parašo atitikmuo. Direktyvos 5 straipsnio 2 dalis atskleidžia elektroninio parašo kategorijos teisinį turinį, nustatydama, jog valstybės narės privalo užtikrinti, jog nebūtų panaikinta elektroninio parašo teisinė galia ir jo, kaip įrodymo, leistinumas teisme vien tik dėl to, kad jis:

- yra elektroninės formos,
- nėra paremtas kvalifikuotu sertifikatu,
- nėra paremtas akredituoto sertifikavimo paslaugų teikėjo išduotu kvalifikuotu sertifikatu,
- nėra sukurtas naudojant saugiu parašo formavimo įranga.

Paprastai tariant, ši nuostata reiškia, kad elektroninis parašas negali netekti teisinės galios ir pripažinimo kaip leistina įrodinėjimo priemonė vien tik tuo pagrindu, kad jis yra elektroninės formos ir nėra kvalifikuotas elektroninis parašas. Direktyvos 5 straipsnio 1 ir 2 dalių analizė leidžia teigti, kad vienintelis kvalifikuoto parašo elementas, iš išvardintųjų 5 straipsnio 1 dalyje, kurio neatitinkančio elektroninio parašo teisinė galia gali būti paneigta pagal šio straipsnio 2 dalį, - tai reikalavimas, kad parašas būtų patobulintas (angl. *advanced*, LR elektroninio parašo įstatyme [8] įvardijamas kaip “saugus”) elektroninis parašas. Šiame kontekste manytina, kad kvalifikuoto elektroninio parašo samprata įtvirtina sunkiai paneigiamą elektroninio parašo galiojimo prezumpciją, o kitais atvejais gali prireikti papildomų įrodymų, patvirtinančių atitikimą patobulintam (saugiam) elektroniniam parašui keliamiems reikalavimams. Manytina, kad pagal 5 straipsnio 2 dalį paneigti elektroninio parašo galią ar suvaržyti jo naudojimą galima tik tokiais pagrindais, kurie būtų nesusiję su konkrečios technologijos panaudojimu, o bet koks bandymas paneigti parašo galią ar naudojimo suvaržymas turi būti pagrįstas konkrečiais, objektyviais kriterijais, tokiais kaip technologijų patikimumo trūkumas, aplinkybių netinkamumas arba racionaliai pagrįstas konkrečios technologijos panaudojimo konkrečiu atveju įvertinimas.“ [14]

Pagal įstatymo nuostatas elektroniniam parašui suformuoti pasitelkiama parašo formavimo įranga ir panaudojami **parašo formavimo duomenys** (kurie žvelgiant iš technologinės pusės būtų - privatusis raktas, susietas su pasirašančiojo sertifikatu) ir atitinkamai tikrinant elektroninį parašą pasitelkiama parašo tikrinimo įranga ir panaudojami **parašo tikrinimo duomenys** (kurie žvelgiant iš technologinės pusės yra pasirašančiojo asmens sertifikatas su unikaliais jame saugomais duomenis). Šis bei kiti įstatymai reglamentuoja elektroninio parašo naudojimą. Sertifikavimo

[13] REPEČKA, Gytis, *Elektroninis parašas*, „Naujoji komunikacija“ dvisavaitinis skaitmeninio gyvenimo būdo žurnalas. 2007 m. Spalio 30d. – lapkričio 30d. , Nr. 16 (212).
[14] CIVILKA, Mindaugas; ir LAMANAUSKAS, Tomas. *Elektroninio parašo įteisinimas: probleminiai aspektai pagal ES ir LR teisę*, p. 7, Prieiga per Internetą: <http://www.norcous.lt/download.php/fileid/9>.

teikėjų atsakomybė už padarytą žalą sertifikatų naudotojams numatyta Lietuvos Respublikos administracinių teisės pažeidimų kodekse:

Teisės aktų, reglamentuojančių kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų veiklą, pažeidimas – užtraukia baudą kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų vadovams nuo penkių šimtų iki keturių tūkstančių litų.

Didesni nusižengimai, padarę žalos elektroninio parašo naudotojams, – „užtraukia baudą kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų vadovams nuo keturių tūkstančių iki dešimties tūkstančių litų“.[15]

Viena iš pagrindinių elektroninio parašo egzistavimo sąlygų yra patikimas elektroninių dokumentų saugojimas po pasirašymo. Tam, kad ši sąlyga būtų realizuota Lietuvos archyvų departamentas prie Lietuvos Respublikos Vyriausybės 2005 m. parengė, o 2006 m. sausio 11 d. **patvirtino elektroninių dokumentų valdymo taisykles** (Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus įsakymas Nr. V-12 „Dėl elektroninių dokumentų valdymo taisyklių patvirtinimo“ (Žin., 2006, Nr. 7-268, Nr. 6). [16] Tačiau pagal IVPK atliktos apklausos rezultatus yra teigiama, jog teisiškai ir techniškai elektroninių dokumentų saugojimui, apskaitymui siuntimui ir gavimui yra pasiruošusi tik viena institucija - IVPK.

2.3 Įstatymai susiję su elektroninio parašo naudojimu

Lietuvoje elektroninio parašo naudojimo įteisinimas prasidėjo nuo Elektroninio parašo įstatymo priėmimo. Šis įstatymas buvo priimtas 2000 m. liepos 11d. ir kuriant šį įstatymą buvo remiamasi ES elektroninio parašo direktyva. Tai pagrindinis įstatymas, kuris nustato kokiais principais turi būti remiamasi kuriant, tikrinant elektroninius parašus. Apibrėžiami sertifikavimo paslaugų teikėjų įsipareigojimai.

2002 m. birželio 6 dieną buvo priimti Elektroninio parašo įstatymo 4, 8, 14, 16 straipsnių pakeitimai ir papildymai. Vienas iš pagrindinių pakeitimų tai aštunto straipsnio papildymas 4 dalimi kuri teigia: „Juridinio asmens atstovo elektroninio parašo galia yra prilyginama juridinio asmens atstovo parašo, patvirtinto juridinio asmens antspaudu, galiai rašytiniuose dokumentuose, atsižvelgiant į elektroninio parašo galią pagal šio straipsnio 1, 2 ir 3 dalis.“ Ankstesnėje elektroninio parašo versijoje juridinio asmens pasirašymas elektroniniu būdu nebuvo reglamentuotas.

Tais pačiais 2002 metais LR Vyriausybės buvo priimti du nutarimai, kurie pastūmėjo elektroninį parašą praktinio taikymo link. Nutarimas Nr. 568 "Dėl elektroninio parašo priežiūros institucijos" priimtas balandžio 23 dieną ir juo buvo užtikrinta, jog elektroninio parašo priežiūra bus

---

[15] *Lietuvos Respublikos administracinių teisės pažeidimų kodėkas*, Lietuvos Respublikos Seimas, 214(24) straipsnis, Prieiga per Internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=312459&p_query=&p_tr2=>.

[16] „*Dėl elektroninių dokumentų valdymo taisyklių patvirtinimo*“, Lietuvos archyvų departamento įsakymas, Prieiga per Internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=269626&p_query=&p_tr2=>.

koordinuojama Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės (IVPK). Antras nutarimas[17] buvo priimtas gruodžio 31 dieną. Šiame antrajame nutarime išskirti keturi pagrindiniai skyriai, kuriuos turi atitikti sertifikavimo paslaugų teikėjai ir pagal kuriuos standartus šie atitikimai apibrėžiami:

1. Reikalavimai kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams
LST ETSI TS 101 456 „Strateginiai reikalavimai, keliami kvalifikuotus sertifikatus išduodantiems sertifikavimo paslaugų teikėjams“
2. Reikalavimai elektroninio parašo įrangai
LST CWA 14167 „Saugumo reikalavimai, keliami patikimoms elektroninių parašų sertifikatų valdymo sistemoms“
3. Kvalifikuotis sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarka
LST CWA 14168 „Saugi parašo formavimo įranga EAL 4“ ir **LST CWA 14170 „Saugumo reikalavimai, keliami taikomosioms parašo formavimo sistemoms“**
4. Elektroninio parašo priežiūros reglamentas
LST CWA 14171 „Elektroninio parašo tikrinimo procedūros“

Visi šie standartai buvo perimti iš EESSI sukurtų standartų, kurie detaliau nagrinėti sekančiame skyriuje.

2002 metais LR Vyriausybės elektroninio parašo priežiūros funkcijos buvo pavestos IVPK. Sekančiais 2003 metais IVPK direktoriaus buvo išleisti penki įstatymai iš kurių 4 buvo patvirtinti sausio 29 dieną ir dar vienas kovas 31d. :

1.„Dėl asmenų registravimo sertifikatams gauti ir konsultavimo paslaugų teikimo tvarkos patvirtinimo“;

2.„Dėl reikalavimų elektroninio parašo tikrinimo procedūrai patvirtinimo“

3.„Dėl sertifikavimo paslaugų teikėjų akreditavimo reikalavimų ir tvarkos patvirtinimo“, nustatantis sertifikavimo paslaugų teikėjų akreditacinius reikalavimus ir akreditavimo tvarką;

4.„Dėl laiko žymos formavimo paslaugų teikimo tvarkos patvirtinimo“;

5.(Kovo 31 dienos įsakymas) “Dėl minimalios draudiminės sumos kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams nustatymo”

2000 metais priimtas įstatymas ir paskui atsiradę pakeitimai, pataisymai bei vėliau sekę poįstatyminiai aktai sudarė palankias sąlygas sertifikavimo paslaugų teikėjams steigtis ir elektroninio parašo infrastruktūrai plėtotis.

[17] *„Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“*, Lietuvos Respublikos Vyriausybės nutarimas, Įsigalioja nuo 2003-01-09, Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=198003&p_query=&p_tr2=>.

2.4 Organizacijos teikiančios standartus elektroninio parašo infrastruktūrai

2.4.1 Europoje

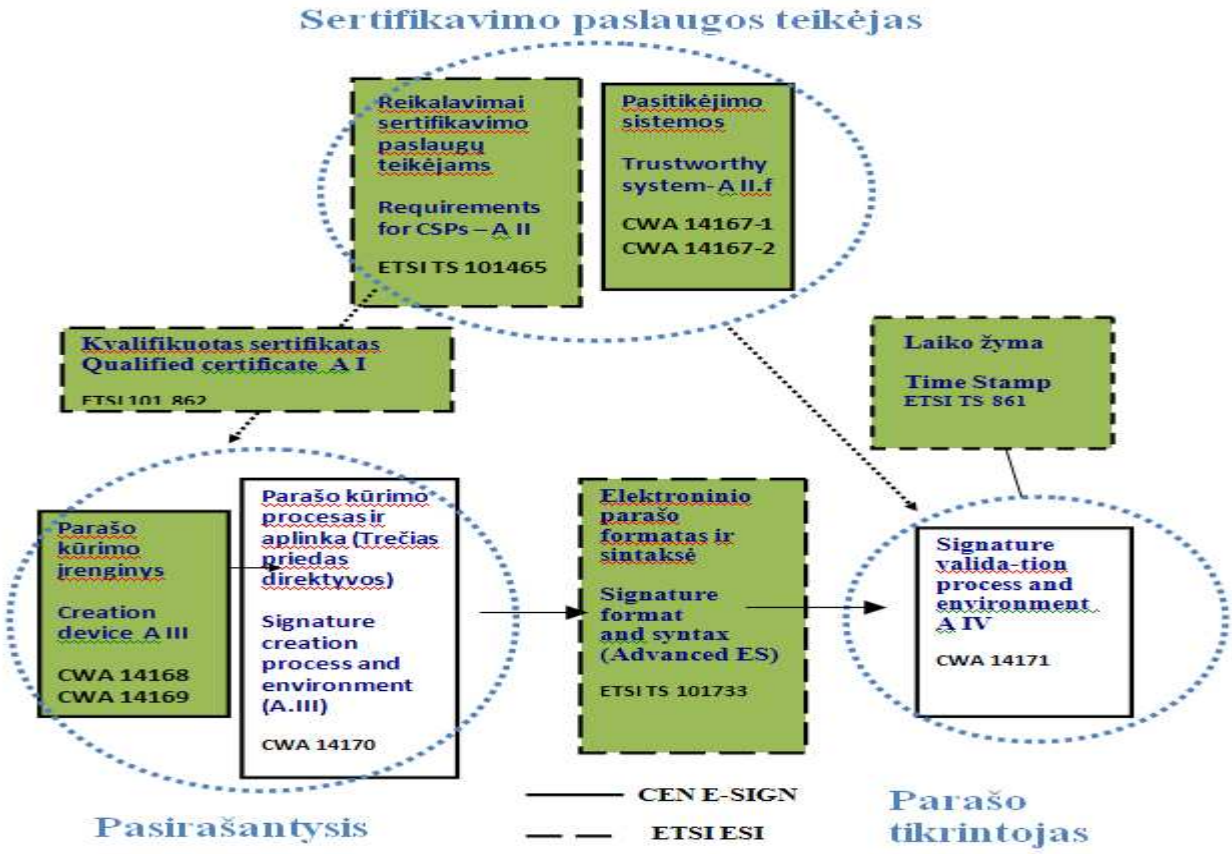
„Europos Elektroninių Parašų Standartizavimo Iniciatyva (EESSI), tai viena pagrindinių organizacijų, kuri buvo įkurta ICTSB tam kad koordinuoti elektroninio parašo direktyvos įgyvendinimą. Standartizavimo veikla buvo atliekama pasidalinus į dvi grupes. Viena iš jų tai Europos Standartizavimo Komiteto (CEN) Informacinės Visuomenės Standartizavimo Sistemos (ISSS) atlikta elektroninio parašo studija, o kita tai Europos Telekomunikacijos Standartų Instituto (ETSI) atliktas darbas.“[18] Atlikti standartizacijos procesai atsispindi 1 lentelėje. EESSI koordinuodama šių standartų išleidimą įvykdė savo darbą ir 2004 buvo uždaryta. Tačiau darbai susiję su elektroninio parašo standartais yra tęsiami ir toliau tiek CEN tiek ir ETSI. Reikia paminėti, jog šiais standartais yra vadovaujamasi ir Lietuvoje. Kaip jau ir minėta 2.3 skyriuje LR respublikos vyriausybės nutarimu buvo patvirtinti reikalavimai elektroninio parašo infrastruktūrai.

Tačiau vienoje iš pagrindinių elektroninio parašo naudojimo Europiniu lygiu ataskaitoje yra kritiškai žvelgiama į susidariusią situaciją ir nušviečiama dabartinė padėtis. „Trūkstant suderinamumo tiek valstybiniame tiek tarp valstybiniame lygmenyje atsiranda didelė kliūtis rinkos pripažinimui ir greitam šios technologijos paplitimui. Dėl ko atsiranda izoliuotų „salų“ – elektroninio parašo sistemų, kur sertifikatai tik iš vieno CA gali būti naudojami tik vienai sistemai. Kai kuriais atvejais tik sertifikatai iš kelių CA gali būti naudojami keliose sistemose. Daug daugiau turėjo būti padaryta Europos lygiu tam, kad užtikrinti suderinamumą.“ [19]

[18] *EESSI internetinis puslapis*, ICTSB, [interaktyvus], [žiūrėta 2008 m. gegužės 20 d.], Prieiga per Internetą: <http://www.ictsb.org/EESSI_home.htm>

[19] *The Legal and Market Aspects of Electronic Signatures*, Study for the European Commission – DG Information Society, Prieiga per internetą: [http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf]. Drafted by Jus Dumortier, Stefan Kelm, Hans Nilsson, Gerogira Skouma and Patrick Van Eecke.

1 lentelė. Standartų kūrimą pasidalinusios organizacijos. [20]



Egzistuoja šimtai skirtingų kriptografinių bei skaitmeninio parašo sistemų. Visos jos gali būti lyginamos šiais pagrindiniais aspektais: saugumo, skaičiavimo našumo (kiek užtrunka skaičiavimai), patogumo, pritaikomumo. Tačiau tam, kad atsirastų pasitikėjimas reikalingi bendri standartai ir naudojami algoritmai negali kelti abejonių naudojantiems kriptografines sistemas. Vienoje iš techninių specifikacijų paruoštos ETSI ESI pabrėžiama, „jog programuotojai turėtų atkreipti dėmesį į tai, jog kriptografiniai algoritmai laikui bėgant tampa vis silpnesni ir silpnesni (užšifruota informaciją galima vis lengviau dešifruoti). Kadangi vystosi naujos kriptografijos analizės technologijos ir kompiuterių skaičiavimo pajėgumai didėja, tikimybė „nulaužti“ tam tikrą algoritmą didėja. Dėl to, kriptografiniai algoritmai panaudojimas privalo būti modulinis. Tai leistų atsiradus naujiems algoritmams pakeisti senus. Programuotojai turi būti pasiruošę panaudoti sistemose panaudoti naujus algoritmus, kurie bėgant laikui keičiasi, tobulėja (tampa sunkiau nulaužiami).“[21] Pasitikėjimas sistemomis gali atsirasti tik bėgant laikui, kai jos tampa plačiai naudojamos ir atlaiko specialistų išanalizavimą. Labai sunku apibrėžti kiek laiko reikia nulaužti vieną ar kitą šifrą. Keletas iš viešai skelbiamų tokių bandymų parodo, jog ir nedideliu raktu

[20] *EESSI First Set of Deliverables*, EESSI Deliverable Description Document, 2001, [žiūrėta 2008 m. kovo 20 d.] Prieiga per Internetą: <http://www.ictsb.org/EESSI/Documents/ddd.doc>.
[21] *Electronic Signatures and Infrastructures (ESI);Electronic Signature Formats,* ***ETSI TS 101 733,*** ETSI, p. 74, [žiūrėta 2008 m. kovo 20 d.] Prieiga per Internetą: <http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_101733v010501p.pdf>.

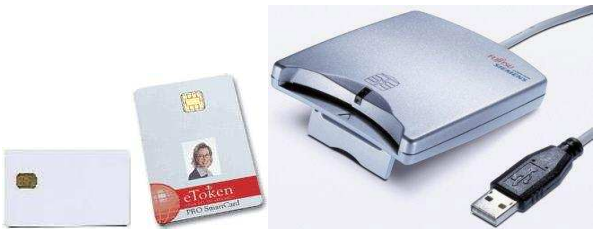
asimetriniu būdu užšifruotą žinutę sujungus tūkstančius kompiuterių tenka šifruoti keletą metų.. Sekantis svarbus kriptografinių sistemų saugumo aspektas, yra kiek šifruojami (pasirašomi) dokumentai yra svarbūs ir koks minimalus laikas, kurio pakanka tam, kad būtų užtikrinama dokumento nepažeidžiamumas. Nuo to priklauso kokie algoritmai turi būti taikomi. Tarkim yra du skirtingi dalykai ar yra pasirašoma nedidelės vertės transakcija internetė ar su darbo užmokesčiu susijusi deklaracija. Elektroniniu būdu pasirašyta deklaracija turi būti išsaugota iki deklaravęs asmuo sulauks pensinio amžiaus, o tai gali būti ir 40 metų. Tam *ETSI TS 101 733* techninėje specifikacijoje yra apibrėžti skirtingų formatų elektroninio parašo formatai tarp kurių yra: Archyvinis elektroninis parašas (Archival Electronic Signature (ES-A)). Pagal šią specifikaciją ši archyvinė forma „remiasi ES-X Long arba ES-X Long Type 1 or 2 formatais papildomai saugumo sumetimais dar pridedant vieną arba kelis archyvavimo laiko žymas. Ši forma yra skirta e. parašui saugojimui ilgą terminą. Sėkmingi laiko žymos antspaudai apsaugo duomenis nuo pažeidžiamų maišos algoritmų ar nuo kriptografinių algoritmų.“ [22]

Neabejotinai elektroninio parašo kriptografinėse sistemose yra naudojamos asimetrinė kriptografija. Simetrinė kriptografija yra neįmanoma dėl to, jog siunčiant duomenis jie gali būti perimti. Įmanoma įsilaužti tarp sertifikatų apsikeitimo ir perimti duomenų srautą ir tada apsimesti viena arba abiem pusėm. (Tai yra vadinama „vidurinio žmogaus“ ataka).

Priemonės reikalingos elektroninių parašų formavimui ir jų standartai.

Lustinės kortelės bei USB saugyklos su įrašytais sertifikatais, tai dviejų faktorių identifikacijos technologijos. Jos turi daug bendro. Abiejuose yra mikroprocesoriai, kurie palaiko tokias kriptografines operacijas kaip raktų bei maišos (hash) funkcijų generavimą. Kiekvienas iš jų turi nedidelę atmintį (dažniausiai tarp 8 ir 32 kilobaitų), tam kad būtų galima saugoti vieną ar daugiau skaitmeninius sertifikatus bei su jais susietus privačius raktus. Pagrindinis skirtumas tarp lustinių kortelių bei USB saugyklų yra tas, kad lustinių kortelių nuskaitymui reikalingas prie asmeninio kompiuterio prijungiamas arba jau integruotas skaitytuvas, o USB saugyklos jau turi USB vartotojo sąsają, kuriai pakanka vienos USB jungties, kuriuos nešiojamieji arba stacionarūs kompiuteriai dažniausiai turi.

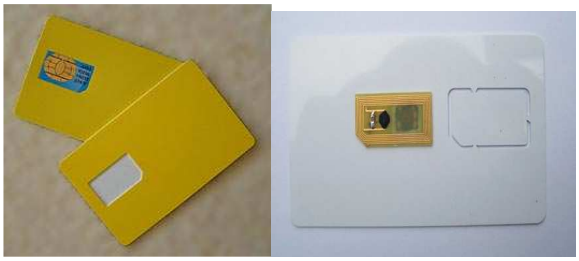
8 paveiksliukas. Lustinės kortelės bei jų nuskaitymui reikalinga įranga



[22] *Electronic Signatures and Infrastructures (ESI)*, p. 21.

9 paveiksliukas. USB saugyklos

10 paveiksliukas. Smart SIM (specialios SIM kortelės, sertifikato laikymui)



Specialūs CEN E-SIGN paruošti standartai „CWA 14168“ ir „CWA 14169“ numato kokių reikalavimus turi atitikti parašo kūrimo įrenginiai SSCD. Dokumente apibrėžiama įvairių rūšių ir skirtingos paskirties SSCD. Viena iš rūšių numato kokių saugumo reikalavimų turi būti laikomasi jeigu įrenginiu naudotųsi tik vienas žmogus: „SSCD Type2 yra personalizuotas komponentas, kas reiškia, jog gali būti naudojamas konkretaus vieno vartotojo (pvz. eID kortelė). Tam, kad užtikinti saugumą prieš naudojimą vartotojas turi būti autentifikuotas, nusiųsdamas autentifikavimo duomenis (pvz. PIN kodą) į SSCD Type2. Taip pat tarp SSCD ir parašo kūrimo aplikacijos (SCA) turi būti saugus kelias (šifruojamas kanalas). Jeigu šiame įrenginyje yra saugoma parašo tikrinimui reikalingi duomenys (SVD) ir jei jie yra eksportuojami į sertifikatų generavimo aplikaciją (CGA) tada taip pat turi būti naudojamas šifruotas kanalas.“ [23] Vien „CWA 14169“ specifikacija susideda iš daugiau nei 200 puslapių.

2.4.2 Rekomendacijos elektroninio parašo formatams Lietuvoje

Vienas pagrindinių dokumentų nustatančių kokiais standartais turi būti vadovaujamasi elektroniniu būdu keičiantis oficialiais elektroniniais dokumentais, tai IVPK prie LRV įsakymas „Dėl rekomendacijų dėl elektroninio dokumento turinio, pasirašyto elektroninio dokumento turinio ir elektroninio dokumento formatų naudojimo valstybės institucijoms ir įstaigoms elektroninėmis priemonėmis keičiantis oficialiais elektroniniais dokumentais patvirtinimo“. Šiame dokumente

[23] *Secure signature-creation devices “EAL 4+”, CWA 14169*, CEN WORKSHOP AGREEMENT, 2004 kovas, p.9, [žiūrėta 2008 m. kovo 20 d.], Prieiga per Internetą: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf>.

nustatoma kokie elektroninių dokumentų formatai yra rekomenduojami pasirašant elektroniniu būdu:

DOC, DOCX, XLS, XLSX, ODF arba PDF [24]

Tuo tarpu jau pasirašytas dokumentas (tarkim DOC formato) turi būti išsaugomas JSFC plėtiniu (naudojant XML saugaus elektroninio parašo schemą XAdES-BES). Įvairios techninės priemonės skirtos elektroninio parašo formavimui bei elektroninių oficialių dokumentų apsikeitimui yra platinamos IVPK elektroninio parašo priežiūros skriaus: http://epp.ivpk.lt/lt/edm/ . Elektroninio parašo formavimui yra rekomenduojama „Justa GE“ programinė įranga tuo tarpu duomenų apsikeitimui buvo sukurta speciali programinė įranga – Dokumentų mainų modelis „DMM“. Išanalizavus pastarąją programą akivaizdu, jog ji leidžia kontroliuoti tiek gaunamus tiek siunčiamus pasirašytus dokumentus. Pačio pasirašymo ši programa neatlieka.

Tačiau aukščiau išvardinti formatai yra tik rekomenduojami ir kol kas neprivalomi.

[24] *IVPK prie LRV įsakymas „Dėl rekomendacijų dėl elektroninio dokumento turinio. Prieiga per Internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=289137&p_query=&p_tr2=>* [žiūrėta 2008 m. sausio 12 d.].

3. ELEKTRONINIO PARAŠO PRAKTINIAI TAIKYMO ASPEKTAI

3.1 Elektroninio parašo infrastruktūra Lietuvoje

„Informacinės visuomenės plėtros komitetas, toliau IVPK, yra valstybinė institucija, kuri atsakinga už elektroninio parašo plėtojimą. Tarp įvairių funkcijų komitetas atlieka tokias funkcijas kaip valstybės strategijos įgyvendinimą, kuri susijusi su elektroniniu parašu. Taip pat organizuoja elektroninio parašo ir elektroninių dokumentų naudojimą valstybinėse institucijose. Ši institucija taip pat atlieka sertifikavimo paslaugų teikimą valstybinėms institucijoms.

2004 metais IVPK pradėjo teiti sertifikavimo paslaugas valstybinėms institucijoms dalyvaujančioms projekte „Elektroninio parašo įdiegimas valstybinėse institucijose". Tačiau IVPK teikiamos paslaugos neatitinka kvalifikuotų sertifikavimo paslaugų. Atviri elektroninio parašo standartai tokie kaip PKCS#7 buvo naudojami kartu su atvirais dokumentų standartais tokiais kaip XML, SMTP ir naudojant "E-Lock ProSigner" elektroninio parašo programine įranga."[25] Nekvalifikuoti sertifikatai buvo dalinami institucijų darbuotojams vidiniam naudojimui (rengėjo parašui, vizavimui ir panašiai. Elektroninio parašo įstatymo 8 straipsnio 3 dalis leidžia įteisinti tokių parašų juridinę galią (susitarimas gali būti įforminamas vidaus darbo reglamento pagalba). Siunčiamus dokumentų egzempliorius daugumoje atveju pasirašo tik institucijos vadovas. Dėk šios priežasties įvairioms institucijoms IVPK užsakymu iš UAB "SSC" buvo nupirkta 100 kvalifikuotų sertifikatų institucijų vadovams. [26]

„Po šio projekto, nuo 2005 metų IVPK buvo pradėtas įgyvendinti „Elektroninio parašo infrastruktūros vystymo projektas", kurio tikslas įdiegti elektroninio parašo kūrimo ir tikrinimo įrangą visose valstybinėse institucijose tam, kad valstybės tarnautojai turėtų galimybę pasirašyti dokumentus su elektroniniu parašu ir kad elektroninis parašas galėtų būti naudojamas teikiant elektroninės valdžios paslaugas. Tam tikslui SSC buvo sukurta speciali elektroninio parašo kūrimo programa „Justa GE". Norintys patikrinti elektroninius dokumentus, pasirašytus valstybės tarnautojų, gali tai padaryti pasinaudodami specialiomis programomis, kurias galima parsisiųsti adresu: http://epp.ivpk.lt/edm. IVPK kontroliuojami sertifikatai pasiekiami adresu: https://ca.ivpk.lt/." [27]

---

[25] CIVILKA, Mindaugas; MOCKAITYTĖ, Indrė; *NATIONAL PROFILE LITHUANIA*, 2007 balandis, Lietuvos ataskaita tyrimui „Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications", Skyrius 3.1 eGovernment structure, Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29088>, p.13. Trumpinimas: NPL.

[26] IVPK EPPS duomenimis.

[27] *NPL*, p. 13.

3.1.1 UAB „Skaitmeninis sertifikavimo centras“

2005 metų vasario 23 dieną Informacinės visuomenės plėtros komiteto įsakymu buvo užregistruota UAB „Skaitmeninis sertifikavimo centras“ – kvalifikuotus sertifikatus sudarantis sertifikavimo paslaugų teikėjas. Įmonė buvo įsteigta 2004 m. liepos mėnesį ir nuo to laiko teikia su elektroniniu parašu susijusias paslaugas. Įmonei įgijus sertifikavimo paslaugų teikėjos statusą, buvo suteiktos galimybes teikti elektroninio parašo paslaugas ne tik Lietuvoje, bet ir visoje ES ekonominėje erdvėje.

„Lietuvoje registruotas kvalifikuotus sertifikatus sudarantis sertifikavimo paslaugų teikėjas UAB „Skaitmeninio sertifikavimo centras“ 2005 – 2007 m. sudarė ir aptarnauja virš 5000 šiuo metu galiojančių sertifikatų, iš jų virš 500 kvalifikuotų sertifikatų.“ [28]

3.1.2 Elektroninio parašo proveržio programa ir Omnitel mobilusis parašas

2006 metų spalio 18 dieną, pasirašyta „Elektroninio parašo proveržio programa (E3P)“, kurios pagrindinis tikslas: „Pasiekti, kad per 3 metus Lietuvoje saugaus elektroninio parašo infrastruktūros naudojimas įgautų masinį pobūdį, t.y., aktyviai besinaudojančių šia infrastruktūra interneto ir mobiliųjų vartotojų skaičius siektų ne mažiau, kaip 300 000”. Šios programos nariai yra LR vyriausybė, didžiausieji Lietuvos bankai, telekomunikacijos bendrovės bei valstybinės institucijos. Taip pat „E3P nariu tapti gali bet kuri Lietuvos įmonė/organizacija, atstovaujanti savo vartotojų/klientų grupes (virš 10 000 vartotojų) ir teikianti jiems (arba numatanti teikti) elektronines paslaugas, kuriose panaudojamas saugaus elektroninio parašo funkcionalumas”.[29] E3P svetainėje (www.parasas.lt/-TOOLS/) pateikiami rekomenduojami pasirašytų dokumentų formatai, tai DigiDoc ir e-DOC. Taip pat platinama ir šio formato pasirašytam dokumentui suformuoti reikalinga įranga. Dokumentus galima pasirašinėti ir prisijungus prie specialių pasirašinėjimui skirtų portalų. Šių dviejų formatų suderinamumui užtikrinti „Baltic WPKI Forum“ rengia bendrą (suderinamą) pasirašytų e-dokumentų formatą, kurio kodinis pavadinimas „Baltic DOC“. [30]

Šios „Elektroninio parašo proveržio programos (E3P)“ iniciatyva Lietuvoje buvo pradėtas platinti Omnitel mobilusis elektroninis parašas. Ši informacija yra pateikiama ir kasmetinėje Elektroninio parašo priežiūros institucijos kasmetinėje (2007 metų) ataskaitoje: „Komiteto duomenimis, Lietuvoje jau naudojamasi ir užsienio valstybių sertifikavimo paslaugų teikėjų sudarytais kvalifikuotais sertifikatais – telekomunikacijų bendrovė UAB „Omnitel“ atlieka kvalifikuotus sertifikatus sudarančio sertifikavimo paslaugų teikėjo Estijos AS „Sertifitseerimiskeskus“ registravimo tarnybos funkcijas. Estijos sertifikavimo paslaugų teikėjo

[28] *ELEKTRONINIO PARAŠO PRIEŽIŪROS INSTITUCIJOS LIETUVOS RESPUBLIKOS ELEKTRONINIO PARAŠO ĮSTATYMO ĮGYVENDINIMO KASMETINĖ (2007 METŲ) ATASKAITA*, p. 3.
[29] *E3P svetainė*, Prieiga per internetą: <http://www.parasas.lt/> [žiūrėta 2008 m. sausio 12 d.].
[30] *E3P svetainė*, Prieiga per internetą: <http://www.parasas.lt/-TOOLS/> [žiūrėta 2008 m. sausio 12 d.].

sudarytais sertifikatais naudojasi Socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos, Valstybinis informacinės technologijos institutas ir Valstybinės kelių transporto inspekcija prie Susisiekimo ministerijos. UAB „Etnomedijos intercentras“ papildomai naudojasi ir Lenkijos sertifikavimo paslaugų teikėjo „CERTUM“ paslaugomis.“ [31]

Atliekant vieną iš šio magistrinio darbo tyrimų, kuris aprašomas kitame skyriuje, buvo įsigytas mobilusis elektroninis parašas vienoje iš Vilniuje esančių Omnitel platinimo centrų.

3.1.3 Elektroninė dokumentų pasirašymo sistema eparašas.lt

2006 metų rugsėjo mėnesį Seimui ir visuomenei buvo pristatytas eParasas.lt projektas. Norint pasirašyti dokumentus šioje sistemoje asmenys turi būti vieno iš Lietuvos bankų internetinė bankininkystės vartotojais. Ši sistema identifikacijai nenaudoja viešojo rakto infrastruktūros identifikuojant asmenis. Tačiau šios sistemos ir pasirašytų dokumentų juridinę galią užtikrinta 2002 metais priimta elektroninio parašo įstatymo 8 straipsnio priimta pataisa, kuri teigia, jog „3. Elektroninis parašas visais atvejais turi šio straipsnio 1 dalyje įtvirtintą teisinę galią, jeigu parašų naudotojai tarpusavyje dėl to susitaria.“ Kitaip tariant, šiame modelyje formuojamas elektroninis parašas turi tokia pat juridinę galią kaip ir ranką rašytas parašas, jeigu tik dėl to susitaria abi šalys. [32]

„UAB „Elektroniniai verslo projektai“ direktorius Kostas Noreika pristatė elektroninio dokumentų pasirašymo sistemos veikimo principą. PKI (private key infrastructure) technologija yra naudojama dokumentų vientisumui užtikrinti, o bankinės sistemos – naudotojų identifikacijai. Už sistemos teisinį galiojimą atsakomybę prisiėmė “Verslo ir teisės konsultacijų asociacija”. Vykstant teisminiam procesui ir kilus abejonių dėl pasirašyto dokumento tikrumo, teisme bus pateikti visi reikalingi dokumento pasirašymą įrodantys duomenys.“[33] Egzistuoja situacijų kai internetinės bankininkystės vartotojai patiki savo prisijungimo duomenis kitiems asmenims. Tam, kad išvengti įvairių teisminių ginčų sistemos kūrėjai įvedė apribojimus, kurie numato kokio pobūdžio dokumentus galima pasirašyti.

„Leistini pasirašyti dokumentai:
1. Sutartys tarp įmonių ir fizinių asmenų:
a) Autorinės sutartys
b) Ilgalaikės nuomos sutartys
c) Darbo sutartys

---

[31] *ELEKTRONINIO PARAŠO PRIEŽIŪROS INSTITUCIJOS LIETUVOS RESPUBLIKOS ELEKTRONINIO PARAŠO ĮSTATYMO ĮGYVENDINIMO KASMETINĖ (2007 METŲ) ATASKAITA*, Prieiga per internetą: <http://epp.ivpk.lt/epp/Dokumentai/2008-03-29_ataskaita.doc>.

[32] *Elektroninio parašo įstatymas*,8(3)str.Per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=169880>

[33] LIETUVOS RESPUBLIKOS SEIMO INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETAS, *POSĖDŽIO PROTOKOLAS*, 2006-09-13 Nr. 23, Vilnius, Posėdžio pirmininkė: Irena Šiaulienė Preiga per internetą: http://www3.lrs.lt/pls/inter/ivpk_print.doc_view?key=282453

d) Pensijų kaupimo sutartys
e) Draudimo polisai
f) Ilgalaikio investavimo sutartys
2. Sutartys, darbų suderinimo aktai ir visi kito dokumentai tarp juridinių asmenų

Draudžiami pasirašyti dokumentai:
1. Paskolų fiziniams asmenims išdavimo sutartys
2. Lizingo sutartys su fiziniais asmenims
3. Skolos rašteliai (Vekseliai)“ [34]

3.1.4 Elektroninės asmens tapatybės kortelės

„Šiuo metu Lietuvoje nėra naudojamos elektroninės asmens tapatybės kortelės. Dabartinės asmens tapatybės kortelės turi tik vizualinę informaciją ir neturi integruotų atminties lustų, kurie būtų skirti informacijos laikymui. VRM, Asmens dokumentų išrašymo centras prie VRM ir Klaipėdos savivaldybės administracija vykdo projektą „Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymo ir panaudojimo investicijų projekto parengimas“. Pradedant tik nuo nedidelio regiono, šio projekto tikslas yra pasiruošti ir įvertinti galimybes išduoti asmens tapatybės korteles visiems Lietuvos gyventojams, kurie dalyvautų naudojantis elektroninės valdžios paslaugomis. Yra planuojama, kad daugiafunkcinės eID kortelės galėtų būti naudojamos gauti elektroninės valdžios paslaugas tiek Lietuvoje, tiek visoje Europoje.“[35] 2006 metų rugsėjo mėnesį atliktoje investicinio projekto „Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas“ galimybių studijos SSGG analizėje įvertintos šio projekto stiprybės, silpnybės, grėsmės ir galimybės. Tarp grėsmių įvardinami tokie faktai kaip „žemas bendras IT vartojimo lygis tarp gyventojų ir verslo įmonių Lietuvoje <...> nepakankama viešųjų paslaugų pasiūla <…> Nepakankama žmonių perkamoji galia, kad galėtų įsigyti brangią kortelę;“ Tačiau įžvelgiama ir nemažai palankių galimybių tarp, kurių viena iš pagrindinių būtų galima įvardinti: „Pasiūlyti vieną daugiafunkcinę kortelę, kuri apjungtų daug atskirose kortelėse saugomų funkcijų (e.parašas, e.bilietai, e.sveikata, lojalumo programos);“ [36]

„Dabartinėje stadijoje buvo atlikta ši galimybių studija tam, kad įvertinti technines šio projekto įgyvendinimo galimybes. Ši studija numato daugiafunkcinių kortelių realizaciją panaudojant du nepriklausomus integruotus lustus (mikroprocesorius). Pirmasis – kontaktinis lustas – leistų įdiegti ir peržiūrėti keletą aplikacijų ir turėtų asmens identifikacijos elektroninėje erdvėje (elektroninės valdžios paslaugoms) ir elektroninių dokumentų pasirašymo galimybę. Antrasis – bekontaktis lustas – taip pat leistų įdiegti specialias aplikacijas. Vėliau galėtų būti pritaikomas asmens tapatybės nustatymui naujai atsirandančiose paslaugose (e. Sveikata, e. Bilietai

[34] *Elektroninė dokumentų pasirašymo sistema eParasas.lt,* Prieiga per internetą: <https://www.eparasas.lt/lit/Sistemos_naudojimo_taisykles/247>, žiūrėta [2008 04 20].
[35] *NPL,* p.18
[36] *Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas,* INVESTICINIS PROJEKTAS (GALIMYBIŲ STUDIJA), Dokumentą ruošė J. Kupinas 2006-09-18.

ir e. Lojalumo kortelės (Maxima, IKI) t.t.). Yra numatoma, kad tokios kortelės Lietuvoje pasirodys 2009-2010 metais.“ [37] Taigi pagrindinės šių lustinių kortelių funkcijos būtų:

- Elektroninė asmens identifikacija (eID kortelės turėtų ne tik vizualinę informaciją, bet taip pat informaciją apie asmenį būtų saugoma ir elektroniniu pavidalu, tai leistų sumažinti dokumentų padirbinėjimo skaičių);

- *E.parašo funkcionalumas* (kortelėje būtų saugomos dvi raktų poros: viena iš jų identifikacijai elektroninėje erdvėje, o kita elektroninių dokumentų pasirašymui);

- E.paslaugų funkcionalumas (Šis funkcionalumas suteiks galimybę užtikrinti praėjimo kontrolę (viešasis transportas, bibliotekos, sporto klubai ir t.t.). Tai būtų užtikrinama į kortelę įrašant vienokius ar kitokius su paslauga susijusius duomenis. Tokiu būdu užtikrinant kortelės funkcionalų Off-line režimu.)

Šiuo metu Lietuvoje jau atsiranda paslaugų, kurioms yra naudojamos elektroninės identifikacijos kortelės. Vienas iš pavyzdžių būtų Vilniaus miesto viešojo transporto elektroninis bilietas.

2007 gruodžio 18 buvo pateiktas naujas asmens tapatybė kortelių įstatymo projektas, nes dabartinis nenumato kortelių naudojimą elektroninėje erdvėje. Tačiau šis projektas buvo atmestas tobulinimui ir kitas jo versija pateikta 2008 balandžio 14 dieną. Šis projektas turi būti patvirtintas arba atmestas tobulinimui. Itin svarbu įvertinti kokiu principu bus platinamos kortelės. Ar jos bus privalomos ar bus galima rinktis ir seno pavyzdžio. Viename iš straipsnių pabrėžiama, jog „paliekant mokamą eID kortelę kaip galimą pasirinkimą šalia seno pavyzdžio asmens tapatybės kortelės nėra pats geriausias modelis elektroninės valdžios atžvilgiu. Dėl šios priežasties žlugo Suomijos modelis pirmaisiais įgyvendinimo metais: niekas nenorėjo brangesnių eID kortelių, nes nebuvo pakankamai elektroninės valdžios paslaugų. O paslaugų teikėjai laukė, kol padaugės kortelių naudotojų prieš pradėdami investuoti į brangias sistemas. Šio reiškinio pasekoje tik 40 000 kortelių buvo išdalinta praėjus penkiems metams. Buvo pakeista įstatyminė nuostata atmetanti seno pavyzdžio asmens tapatybės dokumentus“ [38]

3.1.5 Informacinės sistemos ir elektroninis parašas

Vienas sėkmingiausių elektroninio parašo pritaikymų sistemose atsirado šių metų pradžioje. Valstybinio socialinio draudimo fondo valdyba (Sodra) pradėjo naudoti „Elektroninę draudėjų aptarnavimo sistemą“ (toliau vadinama – EDAS). Anksčiau su darbo užmokesčiu susijusias deklaracijas darbdaviai taip pat galėdavo pateikti elektroniniu būdu, tačiau papildomai reikėdavo

[37] NPL, p. 18.
[38] DEPOORTERE, Ronny; *10 million new Belgian electronic ID cards : a success !,* Prieiga per internetą: <http://download.microsoft.com/download/4/f/d/4fd49a94-8772-4bd0-88ca-bf46e2d029fc/2_JUNE_2004/Zetes_BelgianeID_2004_Finalv.pdf>.

pateikti ir atspausdintą popierinę versiją. Sodrai pateikiami ir vėliau saugomi su darbo užmokesčiu susiję duomenys yra itin jautrūs, todėl elektroninės bankininkystės sprendimas būtų nepakankamas. Realizuota galimybė pasirašyti deklaracijas tiek su specialia programa tiek pačioje EDAS sistemoje. Iš pradžių pasirašymas buvo galimas tik su SSC platinamu elektroniniu parašu, tačiau praėjus keliems mėnesiams buvo įgyvendintas ir Omnitel mobiliojo prašo funkcionalumas.

Naudojantis mobiliuoju elektroniniu parašu buvo realizuota galimybė identifikuotis prie „Hansabanko“ internetinės bankininkystės. Valstybinėje mokesčių inspekcijoje siunčiamos deklaracijos nėra pasirašomos elektroniniu parašu, tačiau yra išsaugomi prisijungimo duomenys. Jau kurį laiką sistemoje yra realizuota galimybė identifikuotis ne tik internetinės bankininkystės pagalba, bet ir naudojantis elektroniniu prašu (eID). Sistema turėtų turėti ir deklaracijų pasirašymo galimybę.

Paminėtos didžiausią dėmesį sulaukusios informacinės sistemos, naudojančio elektroninį parašą. Tai pagrindiniai esami pavyzdžiai. Kitos institucijos taip pat yra pasirengimo etapuose prieš pradedant naudoti šią technologiją.

3.1.6 Elektroninės valdžios ir elektroninio parašo ilgalaikė strategija

Šiame skyriuje bus apžvelgtos Lietuvos bei Europos ilgalaikės strategijos susijusios su elektronine valdžia ir ypatingai bus kreipiamas dėmesys į su elektroniniu parašu susijusius dokumentus. Galima išskirti šiuos pagrindinius dokumentus, kuriuose apibrėžiamas tolesnis IT plėtros strategijos.

[ES] , [LN] , [LNI], [NS] [39]
[ES] LISABONOS STRATEGIJA (2000-2010) [ES] i-2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti (2005-2010) [LN] Nacionalinė Lisabonos strategijos įgyvendinimo programa (2005-2010) [LN] Lietuvos (ūkio) ekonomikos plėtros iki 2015 metų ilgalaikė strategija (2000-2015) [LN] Valstybės ilgalaikės raidos strategija (2002-2015) [LNI] **Viešojo administravimo plėtros iki 2010 metų strategija (2004-2010)** [NS] VAPS įgyvendinimo priemonių planas (2007-2010) [LNI] **Elektroninės valdžios koncepcija (2002-2015)** [NS] El.valdžios koncepcijos įgyvendinimo priemonių planas (2006-2010) [LNI] **Informacinės visuomenės plėtros strategija** [NS] Lietuvos informacinės visuomenės plėtros programa (2006-2008) [LNI] Prioritetinių Lietuvos mokslinių tyrimų ir eksperimentinės plėtros kryptis 2007-2010 metams (2007-2010) [LNI] Nacionalinė žmonių su negalia socialinės integracijos programa 2003-2012 metams (2003-2012) [40]

[39] [ES] Europos sąjungos informacinės visuomenės strategijos, [LN] Lietuvos nacionalinio lygio ilgalaikės raidos strategijos, [LNI] Lietuvos nacionalinės informacinės visuomenės strategijos, [NS] Nacionalinių strategijų įgyvendinimo programos.

Viešojo administravimo plėtros iki 2010 metų strategija

Šiame dokumente, patvirtintame 2004 metų balandžio 28 dieną, yra numatomos prioritetinės sritys: „šios Strategijos įgyvendinimo laikotarpiu ypač daug dėmesio bus skiriama šioms sritims:

3.1. geresniam valdymui (Better Regulation);
3.2. žmogiškųjų išteklių valdymui (Human Resource Management);
3.3. naujovėms teikiant viešąsias paslaugas (Innovative Public Services);
3.4. elektroninei valdžiai (toliau vadinama – e. valdžia) (e-Government)." [41]

Apžvelgiant šią strategiją labiausiai dėmesys bus kreipiamas į elektroninės valdžios įgyvendinimą ir elektroninio parašo naudojimą. Šioje strategijoje yra numatoma kaip valstybės ir savivaldybių institucijų viešosios paslaugos bus perkeliamos į elektroninę erdvę. Išskiriami keturi lygiai. Pirmuosiuose dviejuose lygiuose nėra interaktyvaus bendravimo su institucija. Pirmuoju lygiu yra užtikrinamas tik viešosios informacijos pateikimas internetu. Tuo tarpu antrajame lygyje vartotojams būtų pateikiamos vienokios ar kitokios dalinai paruoštos formos, kurias bereikia užpildyti ir atsispausdinti. Tačiau pateikti įstaigoms vis dėlto naudojantis internetu nebūtų galimybės. Trečiajame ir ketvirtajame lygyje reikalingas vartotojo tapatybės nustatymas. Tik identifikavimus vartotoją galima teikti vienokią ar kitokią viešąją paslaugą. Lietuvoje teikiamas viešąsias paslaugas, kurioms reikalingas asmens tapatybės nustatymas galima pasiekti internetiniu adresu: https://paslaugos.evaldzia.lt/. Vienas iš trečio lygio teikiamų paslaugų pavyzdžių butų „Teistumo (neteistumo) pažymos" užsakymas. Vartotojas užpildo prašymą pasinaudodamas Elektronine teistumo (neteistumo) pažymų užsakymo sistema, tačiau pažymą siūloma atsiimti arba pačioje įstaigoje arba ji būtų persiunčiama paštu.

Ketvirtame lygyje jau pilnai turi būti užtikrinamas interaktyvumas. Vartotojas pateikia dokumentą elektroniniu būdu ir atsakymas gaunamas taip pat elektroniniu būdu. Gautas elektroninis dokumentas turėtų būti pasirašytas elektroniniu parašu. Šiuo metu tokį interaktyvumo lygį turinčių sistemų teikiančių elektroninės valdžios paslaugas nėra.

Analogiška lygių sistema yra ir daugelyje Europos šalių. Tarkim Belgijoje taip pat yra keturių pakopų interaktyvumo lygiai (fazės):

Pirma fazė – Informacija: informacija pasiekiama internetu apie viešąsias paslaugas;
Antra fazė – Sąveika: paruoštų formų parsisiuntimas;
Trečia fazė – Dvipusė sąveika: formų apdorojimas, įskaitant asmens identifikaciją;
Ketvirta fazė – Sandoris (operacija): pilnas valdymas, priimami sprendimai ir pristatomi atsakymai;[42]

---

[40] VALSTYBINIO AUDITO ATASKAITA, *VALSTYBINIŲ INSTITUCIJŲ INFORMACINIŲ SISTEMŲ VALDYMAS ELEKTRONINĖS VALDŽIOS KONTEKSTE*, p.9, 2007 m. rugsėjo 28 d. Nr. IA-9000-4-3 Vilnius, Prieiga per internetą <http://www3.lrs.lt/docs2/HBSAPGOV.PDF>.

[41] *Dėl viešojo administravimo plėtros iki 2010 metų strategijos patvirtinimo*, LR vyriausybės nutarimas, p.1, Prieiga per internetą: <http://www.vrm.lt/uploads/media/VA_Strategija_01.doc>.

[42] *eGovernment Factsheet - Belgium - eServices for Citizens*, Prieiga per internetą: <http://www.epractice.eu/document/3288>. žiūrėta [2008 03 10].

Prisijungus prie elektroninės (2008 03 20) valdžios vartų, buvo išbandytos teikiamos elektroninės valdžios paslaugos, daugiausia teikiama tik prisijungusio vartotojo asmeninė informacija iš šių valstybinių įstaigų:

- Centrinė hipotekos įstaiga (įkeitimo, turto arešto, vedybų sutarčių, testamentų informacija);
- Gyventojų registro tarnyba (Gimimo vieta, deklaruota gyvenamoji vieta, galiojantys asmens dokumentai, šeimyninė padėtis ir kita asmeninė informacija);
- Informatikos ir ryšių departamentas (Teistumo (neteistumo) pažymų užsakymas internetu);
- Ryšių reguliavimo tarnyba (Galima elektroniniu būdu pateikti pranešimus susijusius su elektroninių ryšių veikla);
- Sodra (informacija apie valstybinį socialinį draudimą);
- Valstybinė ligonių kasa (informacija apie suteiktas medicinines paslaugas);
- Vilniaus miesto savivaldybės administracijos el. paslaugos (įvairių archyvinių pažymų pateikimas, savivaldybės veiklos, likviduotų juridinių asmenų dokumentų išrašai);

Peržiūrint įvairią asmeninę informaciją prisijungus prie šių elektroninės valdžios sistemų duomenis buvo leidžiama patikrinti tik vieną kartą. Sekantis informacijos patikrinimas po šio peržiūros nurodoma, jog bus galimas tik po vienerių metų. Gyventojų registro tarnybos už pažymą apie deklaruotą gyvenamą vietą yra taikomas 10Lt mokestis. Taip pat mokesčiai už pažymas yra taikomi ir Informatikos ir ryšių departamento už teistumo (neteistumo) pažymas. Nei vienoje iš šių sistemų nėra realizuotas ketvirto lygio interaktyvumas, kuriame būtų naudojamas elektroninis parašas.

Elektroninės valdžios koncepcija

Peržiūrint Elektroninės valdžios koncepciją, elektroninio parašo kontekste reiktų pažymėti, jog nuostatuose numatoma viena iš politinių iniciatyvų yra: „skatinti elektroninio parašo vartojimą viešajame ir privačiame sektoriuose“. Taip pat numatoma, jog nebus sudaromos kliūtys vykdant transakcijas elektroninėje erdvėje: “Kuriant naujas institucijų viešąsias paslaugas, turi būti numatytas ir jų teikimas nuotoliniais paslaugų teikimo būdais. Jokie priimami teisės aktai nesudarys kliūčių transakcijoms elektroninėje erdvėje (pvz., nebus reikalaujama fizinio parašo, kitų apribojimų).“ Kadangi elektroninio parašo infrastruktūra yra sunkiai plėtojama, strategija numato, jog „E. valdžios projektai bus kuriami ir veiks neatsižvelgiant į elektroninio parašo infrastruktūros sukūrimą Lietuvoje. Ten, kur priimtina, saugumui užtikrinti ir vartotojų tapatybei nustatyti gali būti taikomos kitos priemonės, užtikrinančios vartotojo tapatybės nustatymą ir saugų ryšį tarp vartotojo ir tarnybinės stoties.[43]

[43] D*ėl Elektroninės valdžios koncepcijos patvirtinimo*,LR Vyriausybės nutarimas,1dalis 1.3punktas,5dalis, 18punktas,9dalis 46 punktas,Prieiga per internetą:<http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=198184> žiūrėta [2008 03 20].

Informacinės visuomenės plėtros strategija

Informacinės visuomenės plėtros strategijoje taip pat keliose vietose išskiriama elektroninio parašo svarba ir susirūpinimas: “Lietuvoje elektroniniu paštu gaunami laiškai kol kas nepriskiriami oficialiai korespondencijai. Bendro sprendimo nebuvimas lemia tai, kad bendravimas elektroninėmis priemonėmis tarp viešojo administravimo institucijų ir interesantų dažniausiai nėra veiksmingas”. [44] Šioje strategijoje taip pat išsakoma, kad ”Elektroninio verslo plėtrai būtina, kad funkcionuotų elektroninio parašo infrastruktūra. Sukurta visa reikiama teisinė bazė, tačiau privatus sektorius atidėjo planus investuoti į techninės infrastruktūros plėtrą, todėl elektroninis parašas Lietuvoje dar nefunkcionuoja. Svarbus žingsnis šioje srityje bus minėtas elektroninio parašo įdiegimo valstybės institucijose bandomasis projektas, kurio metu įvertinti sprendimai padės pagrindus plėtoti elektroninį parašą ne tik valstybiniame sektoriuje”.

[44] *Dėl lietuvos informacinės visuomenės plėtros strategijos patvirtinimo,* LR Vyriausybės nutarimas, Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=257174>. žiūrėta [2008 03 10].

3.2 Elektroninio parašo infrastruktūra Europos valstybėse

3.2.1 Estijos patirtis

„Estija pradėjo platinti **nacionalines identifikavimo korteles (eID)** 2002 metų sausį. Šios kortelės atitinka reikalavimus, kurie yra keliami Estijos elektroninio parašo įstatyme. eID kortelės yra privalomos visiems Estijos piliečiams ir nuolatos gyvenantiems užsieniečiams, kurie yra vyresni nei 15 metų. Tai pagrindinis dokumentas, kuris yra skirtas piliečių ir gyventojų identifikavimui ir šios kortelės funkcijos gali būti naudojamos versle, vyriausybiniame arba privačiame komunikavime (identifikavimo dokumentas) ir taip pat kaip kelionės dokumentas (Europos Sąjungoje).“ [45]

„Estija lyginant ją su kitomis Europos valstybėmis yra pakankamai maža. Nuolatinių gyventojų yra mažiau nei 1,4 milijono iš kurių 58 procentai yra nuolatos besinaudojančių interneto paslaugomis, šie rodikliai yra vieni aukščiausių rytų Europoje.“[46] Nors Estija maža pagal savo dydį, tačiau ši šalis pasižymi inovatyvumu kai susiduriama su naujųjų technologijų produktais ir paslaugomis.

Be fizinės asmens identifikavimo paskirties šios kortelės turi ir elektronines funkcijas, kurios leidžia saugiai autentifikuotis ir pasirašinėti elektroninius dokumentus. Kortelėje integruotame luste saugomi asmens duomenys ir sertifikatas skirtas autentifikacijai (kartu su nuolatiniu elektroninio pašto adresu, kuris yra skirtas eKomunikavimui su viešuoju sektoriumi). Kortelėje taip pat saugomas atskiras sertifikatas, skirtas elektroninio parašo formavimui bei privatusis raktas, kuris nuo panaudojimo apsaugotas PIN kodu. Asmens duomenų failas saugomas kortelėje galioja tiek kiek galioja pati kortelė, taip pat ir sertifikatai, kurie turi būti atnaujinami kas penki metai. 2006 metais išdalintų kortelių skaičius viršijo vieną milijoną skaičiuojant nuo 2002 metų, kai jos buvo pradėtos dalinti. [47]

Išmoktos pamokos įgyvendinat šį projektą yra įvardintos profesoriaus Jaak Tepandi iš Talino technologijų universiteto[48]:

- Nacionalinio mąsto eID kortelių projektas yra įmanomas tik jeigu yra kruoščiai suplanuotas, inicijuojamas, vystomas ir palaikomas;
- Svarbus žingsnis yra sukurti naudingas sistemas ir skatinti žmones įsigyti įrangą, mokyti naudotis ja;

---

[45] *eGovernment Factsheet - Estonia - National Infrastructure,* 3 pastraipa, Prieiga per internetą: *<http://www.epractice.eu/document/3332>. Trumpinimas: Factsheet – Estonia.*.
[46] *Internet World Stats*, Prieiga per internetą: <http://www.internetworldstats.com/eu/ee.htm>, žiūrėta [2008 04 10]
[47] *Factsheet – Estonia*, 3 pastraipa.
[48] TEPANDI, Jaak; A Population-Wide ID card (Estonia),
Prieiga per internetą: <**http://www.epractice.eu/cases/eIDEstonia**>, Trumpinimas: APWIC.

- Estijos sukaupta patirtis įgyvendinant eID kortelių projektą gali būti panaudota kitų vyriausybių kaip geros praktikos pavyzdys;

Pasinaudojant šia identifikacijos priemone galima pasiekti daug elektroninės valdžios paslaugų, kurios pasiekiamos per specialius portalus. Estijos elektroninės valdžios portalas pradėjo veikti 2003 metų kovą. Per šį portalą yra pasiekiamos elektroninės valdžios paslaugos. Jos susideda iš dviejų grupių:

1) **Informacijos portalas (**Teabeportaal, *http://www.eesti.ee/est*), kuris suteikia praktinės informacijos apie teises ir pareigas žmonių, gyvenančių Estijoje taip pat patarimai bendraujant su Estijos valstybinėm institucijom. Portale yra pasiekiamos įvairios dokumentų formos ir internetinės paslaugos.

2) **Piliečių portalas** (Kodanikuportaal[49]) suteikia piliečiams galimybę pasitikrinti su jais susijusią informaciją daugelyje nacionalinių duomenų bazių, pildyti paraiškas, pasirašyti ir siųsti dokumentus, gauti informacija susijusią su specifinia gyvenamaja vieta. [50]

Visos šios paslaugos yra užtikrinamos naudojantis saugia autentifikacijos bei elektroninio parašo kortele. Lietuvoje prie elektroninės valdžios vartų piliečiai gali prisijungti tik tie, kurie naudojasi internetine bankininkyste arba naudojasi „Skaitmeninio sertifikavimo centro“ elektroniniu parašu. Elektronines asmens tapatybės kortelių įvedimas Lietuvoje yra dar tik planuojamas. 2007 metų gruodžio 12 dieną Seimui pateiktas LR Vidaus reikalų ministerijos asmens tapatybių kortelių įstatymo projektas buvo gražintas tobulinimui. Šiuo metu vykstant diskusijoms dėl šio didelio projekto įgyvendinimo, yra išsakomos įvairios nuomonės. Yra baiminamasi, jog „VRM elektroninio parašo išlaikymas reikalaus biudžetinių lėšų, tačiau ministerija kartu su tokios kortelės įdiegimu negali pateikti didelio elektroninių paslaugų spektro”[51]. Tačiau šis pasakymas neatitinka realybės, nes jau dabar yra teikiama nemažai elektroninės valdžios paslaugų, kur autentifikacijai yra naudojamasi internetine bankininkyste. Žvelgiant iš kitos pusės, Estijos pavyzdys parodė, jog pirmiau turi būti sukurta priemonė saugiai autentifikacijai, o sistemų pakeitimai šių kortelės naudojimui turėtų sekti iš paskos.

Viename tyrime atliktame 2006 metų spalio mėnesį, kuris yra susijęs su eID realizacija Estijoje teigiama, jog tik „2,5% eID kortelių turėtojų yra viešųjų paslaugų elektroninių funkcijų naudotojai, kur reikalinga identifikacija arba autorizacija”[52]. Kadangi Lietuvoje internetu besinaudojančių gyventojų skaičius yra dar mažesnis, tai panašu, jog besinaudojančių viešosiomis

---

[49] Estijos elektroninės valdžios portalas, Prieiga per internetą: <https://www.eesti.ee/portaal/portaal.sisene?level=30&loc=>.

[50] APWIC.

[51] PAKALKAITĖ, Vija, *Aistros ir nežinia dėl naujų asmens tapatybės kortelių,* vz.lt straipsnis, Prieiga per internetą: <http://vz.lt/Default2.aspx?ArticleID=5f6c430a-c553-44ff-9c27-0e6037de05a7>, žiūrėta [2008 03 20]

[52] *Good practice case eID in Estonia*, 2006 spalis, p. 2, 1.4.1 paragrafas, Prieiga per internetą: <http://www.egov-iop.ifib.de/downloads/Interoperability_in_eID_in_Estonia.pdf>. Trumpinimas: GP EID.

elektroninės valdžios paslaugomis bus dar mažesnis nei Estijoje. Tačiau eID kortelių naudojimas neapsiriboja vien ties elektroninė valdžios paslaugomis. Šios kortelės galėtų būti plačiai naudojamos elektroninių bilietų patikrinimui viešajame transporte. E-bilietai būtų pigesni ir tai skatintų įsigyti būtent tokius, o ne popierinius.

„Dar viena sritis, kurioje buvo panaudotos eID kortelės, tai internetinis balsavimas. Estijos savivaldybių rinkimai, kurie įvyko 2005 metų spalio mėn., buvo pirmieji pasaulyje interneto technologijų pagalba įvykdyti rinkimai. Visi Estijos rinkėjai turėjo galimybę balsuoti internetu. Apie 2 proc. balsavusiųjų pasinaudojo šia galimybe. Šie e-rinkimai parodė, jog visų socialinių sluoksnių atstovai pasinaudojo galimybe balsuoti internetu. Elektroninės balsavimo sistemos panaudojimas nepriklausė nei nuo rinkėjų amžiaus, nei nuo jų socialinės grupės, nei nuo rinkėjų išsilavinimo. Pasirinkimą naudotis elektroninio balsavimo sistema sąlygojo tik rinkėjų pasitikėjimas įdiegta elektroninio balsavimo sistema.“[53] 2007 metais vykusiuose Estijos parlameto rinkimuose Estijos piliečiai taip pat turėjo galimybe balsuoti internetu. Internetu gautų biuletenių skaičius sudarė 5,4 procentus nuo visų galiojančių biuletenių. Įdomus faktas, kad 2005 metais per Estijos savivaldybių tarybų rinkimus eID kortele identifikacijai internetinio balsavimo sistemoje *pirmą kartą* pasinaudojo 61 procentas rinkėjų nuo visų balsavusiųjų inernetu, tuo tarpu 2007 tokių rinkėjų buvo 39 procentai. Kitaip tariant likusius 61 procentą sudarė tie, kurie jau buvo panaudoję kortelę elektroninėje erdvėje (jungiantis prie elektroninės valdžios portalų, balsuojant praėjusiuose rinkimuose ir pan.). Šie duomenys paimti iš Estijos Nacionalinės Rinkimų komisijos svetainėje pateikiamos statistikos. [54]

„Iki šių dienų, elektroninių eID kortelių naudojimą kasdieninėje veikloje sunkiai įsivaizdavo tiek profesionalai tiek ir šios srities entuziastai. Ir tai pagrinde sąlygojo:

- laikas reikalingas pakeisti į požiūrį į naujas technologijas;
- per mažai taikomųjų programų (pavyzdžiui kaip nemokama internetinė telefonija);
- pirminės techninės problemos, kurios išgąsdina pirmuosius vartotojus ir dėl sumažėja staigus ID kortelių išreklamavimas;“ [55]

„Nepaisant visų sunkumų, Estijos eID kortelių platus panaudojimas yra žinomas kaip vienas sėkmingiausių Europoje. Šis projektas buvo organizuojamas bendradarbiaujant viešam ir privačiam sektoriuj ir dabar jau yra daug informacinių sistemų veikiančių naudojant šią kortelę.Vienas iš pavyzdžiui būtų šios kortelės pritaikymas viešajame transporte. Pasinaudojant eID kortele galima įsigyti e-bilietus viešajam transportui ir su ja vairuotojas gali patikrinti e-bilieto galiojimą. Piliečiai

[53] MADISE, Ülle; MARTENS, Tarvi, *E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world*. P.15,
[54] *Main Statistics of E-Voting*.Prieiga per internetą: http://www.vvk.ee/english/Ivoting%20comparison%202005_2007.pdf.
[55] *GP EID*, p.17.

gali peržiūrėti su jais susijusią informaciją gyventojų registruose, jie taip pat gali elektroniniu būdu pasirašyti dokumentus arba pastikrinti telefono sąskaitas. Ši kortelė yra taip pat naudojama atliekant bankines operacijas.“[56]

3.2.2 Ispanijos patirtis

Ispanijos eID kortelės suteikia reikalingą impulsą tam, kad elektroninis parašas būtų įtrauktas į pagrindines elektroninės valdžios paslaugas. Šių kortelių platinimas prasidėjo Burgos (Castila y Leon regione) 2006 metų kovą. 2006 metų lapkritį jau buvo išdalinta didžiojoje dalyje šiaurės Ispanijos regionų. Tuo laikotarpiu kortelės buvo platinamos 30 ofisų esančių 24 Ispanijos miestuose. 300 000 eID kortelių išdalinimas buvo numatomas iki 2006 metų pabaigos su 40 ofisų išsidėsčiusių 20 regionų. Tuo tarpu progresyvus išsiplėtimas iki pilnos Ispanijos teritorijos buvo numatomas iki 2007 metų pabaigos, kai eID kortelės turėjo apimti visą Ispanijos teritoriją. Sekančiu žingsniu planuojama išduoti 8 000 000 eID kortelių iki 2008 metų pabaigos. Kortelės išdavimo mokestis yra apie 6 eurus. [57] Šie išankstiniai Ispanijos vyriausybės planai iš dalies buvo įgyvendinti. Europos komisijos ePractice.eu portalo duomenimis paskelbtais 2007 spalio mėnesį teigiama, jog buvo peržengta vieno milijono riba: “Ispanijos nacionalinė krepšinio komanda gavo naujas eID korteles iš šalies vidaus reikalų ministro ir taip buvo pažymėta milijoninės kortelės išdavimas”.[58] Šie skaičiai palyginti nėra dideli, nes Ispanijoje yra 45 milijonų gyventojų ir iš jų 48,4 procentai besinaudojančių internetu. [59]

Nuo 2006 spalio Ispanijos piliečiai gali naudotis daugiau nei 260 elektroninių paslaugų, kurioms yra reikalingas elektroninio parašo panaudojimas. <…> Skaitmeninių sertifikatų panaudojimas labai paplito realizavus Ispanijos eID kortelių projektą ir sukūrus multiPKI Tikrinimo Platformą, kuri palaikoma MAP (Viešojo administravimo ministerijos) (http://www.dnielectronico.es/seccion_aapp/platform.html) ir kuri suteikia elektroninio parašo ir elektroninio sertifikato patikrinimo galimybę naudojantis elektroninės valdžios paslaugomis (pastaruoju metu yra apie 180 naudojančių šią platformą).[60]

Ši multiPKI Patikrinimo Platforma patikrina elektroninius sertifikatus ir elektroninius parašus, kurie buvo suteikti pagrindinio šalies sertifikavimo teikėjo taip pat ir eID kortelių sertifikavimo teikėjo bei teikia laiko žymos paslaugas.

---

[56] *GP EID*, p.18. 1.4.1 paragrafas.
[57] *NATIONAL PROFILE SPAIN*, 2007 balandis, Ispanijos ataskaita tyrimui „Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications”, Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29081>, p. 25, Trumpinimas: NPS.
[58] *ES: eID scores a million*, 2007 spalio 14, 1 pastraipa, Prieiga per internetą: <http://www.epractice.eu/document/3905>.
[59] *Internet World Stats*, Prieiga per internetą: <http://www.internetworldstats.com/eu/es.htm>.
[60] *NPS*, p. 22, paragrafas: 4.2.1. Electronic identity card (e-ID).

Speciali elektroninio parašo tikrinimo programa leidžia pasirašyti elektroninius dokumentus įvairiais elektroninio parašo standartais. Šis pasirašymas įvykdomas kompiuteryje ir tik paskui dokumentas gali būti įkeltas per internetą. Tokia paslauga yra teikiama elektroninės valdžios informacinėms sistemoms iš įvairių administravimo lygių (valstybinio, regioninio, vietinio). Ši platforma buvo sukurta kaip atviro kodo ir naudojant atvirus standartus. [61]

IDABC vykdomo tyrimo Ispanijos 2007 metų balandžio mėnesio ataskaitoje yra pateikiamos pagrindinės elektroninės valdžios teikiamos paslaugos, kurios naudoja eID kortelę identifikacijos ir elektroninio parašo tikslais. Šių paslaugų yra gerokai daugiau ir visas sąrašas naudojančių eID kortelę yra pateikiamas šiuo adresu: http://www.dnielectronico.es/servicios_disponibles/serv_disp_age.html). Šių paslaugų iš viso yra daugiau nei 260: [62]

2 lentelė. Pagrindinės informacinės sistemos, pritaikytos identifikacijai ir dokumentų pasirašymui naudojant eID, valstybiniame lygmenyje.

Institucija	**Veikla**	**Elektroninis parašas**
Mokesčių inspekcijos virtualus biuras www.aeat.es	Galimybė piliečiams ir įmonėms teikti deklaracijas internetu	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo
Virtualus kadastro biuras http://ovc.catastro.meh.es/	Konsultacijos per internetą ir kadastrinių duomenų patvirtinimas	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo
Virtualus socialinės apsaugos biuras http://www.segsocial.es/inicio/?MIval=cw_usr_view_Folder&LANG=1&ID=40033	-Visų piliečių priskirtų socialinės apsaugos filialams konsultacija internetu ir galimybė peržiūrėti su darbu susijusius duomenis - Galimybė internetu pateikti informaciją susijusią su laikinu nedarbingumu	-eID kortelė, priklausomai nuo programų, -NP skaitmeniniai sertifikatai: suteikia galimybę peržiūrėti asmeninę informaciją; -SILICON sertifikatai: skaitmeniniai sertifikatai, kurie suteikia prieigą ir konsultacijas įmonių atstovams.
Pramonės, turizmo ir prekybos ministerijos virtualus biuras http://www.mityc.es/es-ES/Servicios/OficinaVirtual	Prašymų pateikimas internetu dėl subsidijų, dotacijų, kurias skiria ministerija	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo
Bendra informacinė sistema tarp Pramonės, turizmo ir prekybos	Galimybė įmonėms gauti informaciją susijusią su pavedimais Mokesčių inspekcijai,	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo

[61] *NPS*, p. 22, paragrafas: 4.2.1. Electronic identity card (e-ID), 6 pastraipa.
[62] *NPS*, p. 55.

ministerijos ir Teisingumo ministerijos	Socialinei apsaugai, Notarų biurams.	
Viešojo administravimo ministerija www.map.es	Internetinė informacinė sistema, kuri suteikia piliečiams gauti oficialų ir saugų bendravimo kanalą iš viešojo administravimo sektoriaus per vieną elektroninio pašto adresą.	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo
Betarpiškas komunikavimas tarp valstybės tarnautojų (MUFACE) http://www.map.es/muface/oficina_virtual/	Galimybė gauti nedarbingo išrašą dėl ligos ir motinystės.	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo
Konsultavimo taryba dėl elektroninės prekybos http://catalogopatrimonio.meh.es	Sistema skirta ektroninėms varžytuvėms ir elektroninei prekybai visoms įmonėms, kurios užsiregistravusios šiame internetiniame registre.	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo
Viešas įdarbinimo biuras www.inem.es	Paslaugos dėl įdarbinimo	eID kortelė Saugus parašas suteiktas FNMT arba kito autorizuoto sertifikavimo paslaugų teikėjo

Visos išvardintos sistemos yra adaptuotos eID kortelės naudojimui tačiau didžioji dalis dar tam nėra pasiruošusios, nes ir pati kortelė dar nėra pilnai išplatinta. Nemažai sistemų atpažįsta pagrindinių Ispanijos sertifikavimo paslaugų teikėjų elektroninius parašus. Aukščiau išvardintos pagrindinės sistemos naudoja aukščiausio lygio identifikaciją. Nemažai panašių sistemų veikia ne tik valstybinių lygmeniu, bet taip pat ir regioniniu arba savivaldybių lygmeniu.

3.2.3 Belgijos patirtis

„Belgijos gyventojų skaičius viršija dešimt milijonų. Ši šalis yra dėmesio centre, nes tai pirmoji šalis, turinti gyventojų daugiau nei 10 milijonų, ir nusprendusi, kad kiekvienas pilietis turėtų eID kortelę kartu sertifikatais. Belgijos planuose yra išdalinti eID korteles visiems piliečiams vyresniems nei 12 metų iki 2009 metų, kurios pakeis senuosius popierinius dokumentus.“ [63]

„Šios kortelės buvo pradėtos dalinti 2003 metais. Galutinis planuojamas išdalintų kortelių skaičius turėtų siekti 8 milijonus. 2006 metų balandžio duomenimis apie 3,5 kortelių jau buvo

[63] Electronic Signature Dissemination WG - eID Survey Report in Bilgium, 2007 gruodžio 28 p.3, Prieiga per internetą: <http://www.ecom.jp/en/ecomnews/ecomnews_no33.pdf>. Trumpinimas: ESD.

išdalinta.[64] Elektroninės identifikacijos sistema Belgijoje apima ne tik eID korteles skirtas piliečiams, bet taip pat ir Vaikų-ID (Kids-ID) korteles kurios skirtos vaikams jaunesniems nei 12 metų (jas išpaltinti planuojama 2008 metais), taip pat yra platinamos kortelės, kurios yra skirtos nuolatos gyvenantiems užsieniečiams. Viena iš Vaikų-ID kortelių paskirčių yra apsaugoti vaikus nuo nusikalstamos veiklos. Jos yra naudojamos tam, kad įrodyti tėvų ir vaikų ryšį. Kortelės yra dalinamos pateikusiems prašymus“. [65]

IDABC vykdomo tyrimo Belgijos 2007 metų balandžio mėnesio ataskaitoje yra pateikiama didžioji dalis sistemų, kurios naudoja arba kuriose bus naudojamas elektroninis parašas. [66] Išanalizavus 17 valstybinio lygio, 5 regioninio lygio ir 5 savivaldybės lygio sistemas matoma jog didžioji dalis jau yra adaptuotos eID kortelės atpažinimui, tačiau yra išlikusios ir anksčiau naudotos atpažinimo priemonės, tai yra naudojantis komercinių sertifikavimo centrų platinamais sertifikatais.

[64] NATIONAL PROFILE BELGIUM, 2007 balandis, Belgijos ataskaita tyrimui „Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications”, Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29071>, p. 15, paragrafas: 4.2.1 Electronic identity card (e-ID), Trumpinimas: NPB.
[65] ESD, p.4.
[66] NPB, p. 15.

4. TYRIMAI IR JŲ REZULTAI SUSIJĘ SU ELEKTRONINIO PARAŠO NAUDOJIMU LIETUVOJE

4.1 Elektroninio parašo paplitimas LR institucijose

Lietuvos Respublikos viešojo administravimo įstatymo 19 straipsnyje 5 dalyje yra teigiama, jog „5. Asmenų prašymai, pateikti elektroniniu būdu, turi būti pasirašyti elektroniniu parašu. Atsakymai į šiuos prašymus pateikiami asmeniui elektroniniu paštu, o asmenų pageidavimu – siunčiami paštu prašyme nurodytu adresu arba įteikiami. Atsakymas elektroniniu paštu turi būti pasirašytas institucijos vadovo arba jo įgalioto asmens saugiu elektroniniu parašu“[67]. Remiantis šia nuostata buvo nuspręsta atlikti pagrindinių LR institucijų apklausą išsiuntinėjant anketas ir elektroniniu parašu pasirašytus prašymus elektroniniu paštu.

Prašymų pasirašymui elektroniniu būdu buvo pasirinktas mobilusis elektroninis parašas platinamas UAB „Omnitel“. Ši mobiliojo ryšio bendrovė platina estų bendrovės AS Sertifitseerimiskeskus (SK) elektroninius parašus. Kiekvienam vartotojui suteikiamas sertifikatas (elektroninio parašo liudijimas) yra susiejamas su vartotojo SIM kortele. Pagrindinė priežastis dėl ko buvo pasirinktas šis mobilusis parašas, tai yra tai, kad atliekant tyrimą jis buvo platinamas nemokamai. Antra priežastis, tai, jog SK yra akredituotas sertifikavimo paslaugų teikėjas Europos Sąjungoje. Lietuvos elektroninio parašo įstatymo 5 straipsnio 1 dalis teigia, jog “Užsienio valstybių sertifikavimo paslaugų teikėjų sudaryti kvalifikuoti sertifikatai laikomi teisiškai ekvivalenčiais Lietuvos Respublikos sertifikavimo paslaugų teikėjų sudarytiems kvalifikuotiems sertifikatams, jei:

1) yra sudaryti sertifikavimo paslaugų teikėjo, akredituoto Lietuvos Respublikoje;

2) yra sudaryti sertifikavimo paslaugų teikėjo, akredituoto Europos Sąjungos valstybėje;“ [68]. Šiuo atveju Omnitel platinimas elektroninis parašas atitinka visus kvalifikuotam parašui keliamus reikalavimus, tai patvirtino tiek IVPK EPPS atstovas tiek Omnitel atstovas.

Tyrimo tikslas: nustatyti ar LR institucijos pasiruošusios priimti ir siųsti dokumentus pasirašytus elektroniniu parašu. Išsiaiškinti kokios priežastis lemia sunkiai plintantį elektroninio parašo naudojimą.

Tyrimo uždaviniai.

1. „Omnitel“ atstovybėje įsigyti nemokamai platinamą mobilųjį elektroninį parašą;
2. Išsiaiškinti kokios institucijos dalyvavo IVPK rengtame elektroninio parašo projekte;

---

[67] *LIETUVOS RESPUBLIKOS VIEŠOJO ADMINISTRAVIMO ĮSTATYMAS*, 19 str. 5dalis, Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=257918>.

[68] *Elektroninio parašo įstatymas*,5(1)str. Per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=169880>.

3. Atlikti anketinį tyrimą, kuris padėtų išsiaiškinti kaip yra paplitęs elektroninio parašo naudojimas LR institucijose;

Tyrimo objektas – Galimybė pateikti skundus ir prašymus LR institucijoms elektroniniu būdu ir gauti atsakymus pasirašytus elektroniniu parašu.

Hipotezės.

1 hipotezė. LR institucijose yra gaunami ir siunčiami dokumentai, pasirašyti elektroniniu parašu.

2 hipotezė. Elektroninio parašo naudojimas priklauso nuo to ar įstaigoje yra naudojama dokumentų valdymo sistema;

3 hipotezė. LR institucijose yra perengtos tvarkos, kuriomis piliečiai turėtų vadovautis norėdami pateikti prašymus arba skundus elektroniniu būdu ir pasirašytus elektroniniu parašu;

4 hipotezė. LR institucijose atsakomi elektroniniu paštu atsiųsti laiškai, bet nepasirašyti elektroniniu parašu.

5 hipotezė. LR institucijoms neiškilo sunkumų patikrinti elektroninio parašo savininko tapatybę.

Klausimyno sudarymas.

Tyrimas atliktas panaudojant 10 klausimų anketa. (Priedas Nr. 3). Klausimyną sudaro aštuoni uždari klausimai ir vienas atviras klausimas, kurie susiję su elektroninio parašo naudojimu tiriamųjų institucijoje, taip pat viename klausime prašoma nurodyti kokiai institucijai pildantysis asmuo atstovauja. Klausimyno pabaigoje yra prašoma užpildytą anketą pasirašyti.

Klausimynas sudarytas laikantis klausimyno sudarymo principų. Siunčiamame laiške buvo nurodyta kokiems tikslams anketa bus naudojama. Prie siunčiamo laiško buvo prisegama ne tik pati anketa, bet ir laiško turinys pasirašytas elektroniniu parašu (DDOC formatu). Taip pat laiške buvo nurodyta kaip patikrinti elektroninį parašą. Laiško turinys pateikiamas 2 priede.

Respondentų atranka.

Respondentai atrinkti pagal EPPS svetainėje[69] platinamą informaciją apie institucijas dalyvaujančias elektroninio parašo projekte. Iš viso anketa išsiuntinėta elektroniniu paštu 61 valstybinei institucijai. Pasirinkta siųsti daugiausiai IT skyriuose dirbantiems atstovams, nes didžiausia tikimybė, jog jų žinioje yra reikalai susiję su elektroninio parašo diegimu ir naudojimu. Apklaustų institucijas galima išskirti į šias kategorijas: ministerijos, institucijos prie vyriausybės, institucijos prie ministerijų, atskiros institucijos. Taip pat anketos buvo išsiųstos ir seimo bei vyriausybės atstovams. Savivaldybių lygmeniu apklausa nebuvo atliekama.

[69] Elektroninio parašo priežiūros skyriaus svetainė, prieiga per internetą: <http://epp.ivpk.lt/lt/edm>.

Situacija prieš atliekant tyrimą ir panašūs atlikti tyrimai.

Remiantis 2008 metų ataskaita, „Komitetas nuo 2005 m. vykdo „Elektroninio parašo infrastruktūros valstybės institucijose plėtros“ projektą, kurio tikslas - sudaryti valstybės institucijoms reikiamas sąlygas naudoti elektroninį parašą pasirašant elektroninį dokumentą ir vykdant mainus tarp valstybės institucijų bei elektroniniu būdu teikti viešąsias paslaugas. Projekte dalyvaujantiems sudarytos sąlygos išbandyti ir praktiškai naudoti elektroninio parašo įrangą. Ja dalinai yra aprūpintos 67 valstybės institucijos, o Komitetas teikia sertifikavimo paslaugas (nekvalifikuotų sertifikatų) apie 1100 valstybės tarnautojų.“[70] Pagal šiuos duomenis institucijos yra pasiruošusios priimti ir siųsti elektroninius dokumentus su elektroniniu parašu. Tuo labiau, kad institucijų vadovams dar papildomai buvo nupirkta 100 kvalifikuotų sertifikatų (EPPS atstovo duomenimis).

2007 metais spalio mėnesį IVPK pateikė vyriausybei ataskaitą susijusią su valstybės institucijų apklausos rezultatais. Apklausa buvo vykdoma siekiant nustatyti kaip yra laikomasi rekomendacijos dėl DVS pertvarkymo siekiant jas pritaikyti dokumentų pasirašytų elektroniniu parašu kūrimui, saugojimui, persiuntimui. Keletas iš šio tyrimo rezultatų: „Visiškai pasirengusi (techniškai ir teisiškai) dirbti su elektroniniais dokumentais (siųsti, gauti, apskaityti, saugoti ir t.t.) yra viena institucija – Komitetas;

4.1.1 Omnitel platinamo mobilaus elektroninio parašo įsigijimas

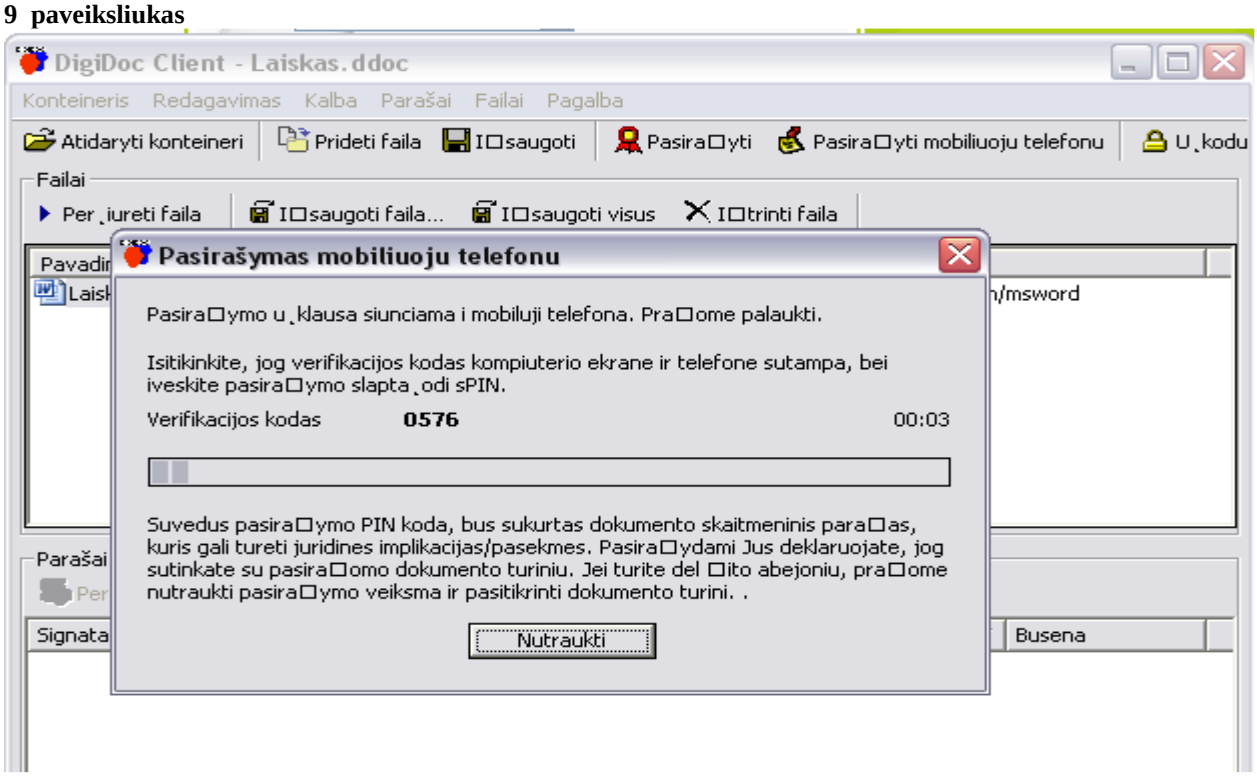
Tarp dviejų tyrimo metu buvusių sertifikavimo paslaugų teikėjų buvo pasirinktas Omnitel platinamas mobilusis parašas. Akivaizdžiai stebėtina yra tai, jog nėra propaguojama lietuviško kapitalo įmonė, t.y. SSC, kuri nėra elektroninio parašo proveržio programos narė. Apsisprendimą naudoti ne SSC parašą, o Omnitel platinamą lėmė vien tik tai, jog mobilus e. parašas buvo platinamas nemokamai. Mobilusis elektroninis parašas buvo įsigytas vienoje iš atstovybių esančios Vilniuje. Tyrimo metu parašas vis dar buvo platinamas nemokamai. Tam, kad tapti mobilaus elektroninio parašo naudotoju buvo trys sąlygos: turėti galiojanti Lietuvos Respublikos piliečio pasą, būti Omnitel abonentu (išankstinio mokėjimo kortelės netinka) ir turėti galiojančią banko kortelę, kuri reikalinga papildomam tapatybės patvirtinimui. Papildomai tapatybė yra patvirtinama įsigyjant naująją SIM kortelę ir už ją sumokant 1 centą (būtinai pasinaudojant banko kortele). Atspausdintas čekis tampa kaip papildomas įrodymas tapatybės patvirtinimui. Sekančiame žingsnyje yra pasirašoma sutartis su sertifikavimo tarnyba (CA), kuri šiuo atveju yra AB Sertiffitseerimiskeskus. Išanalizavus sutartį vienas iš punktų teigia, jog „Sertifikate pateikiami asmens duomenys (vardas, pavardė, asmens tapatybės kodas) yra traktuojami kaip vieša

[70] *ELEKTRONINIO PARAŠO PRIEŽIŪROS INSTITUCIJOS LIETUVOS RESPUBLIKOS ELEKTRONINIO PARAŠO ĮSTATYMO ĮGYVENDINIMO KASMETINĖ (2007 METŲ) ATASKAITA***,** p. 8,

informacija, pasiekiama trečiosioms šalims; [71] Šis faktas nėra priimtinas daugeliu atveju ir turės didelę įtaką vartotojų skaičiaus didėjimui, nes asmens tapatybės kodas yra itin jautrus asmens duomuo.

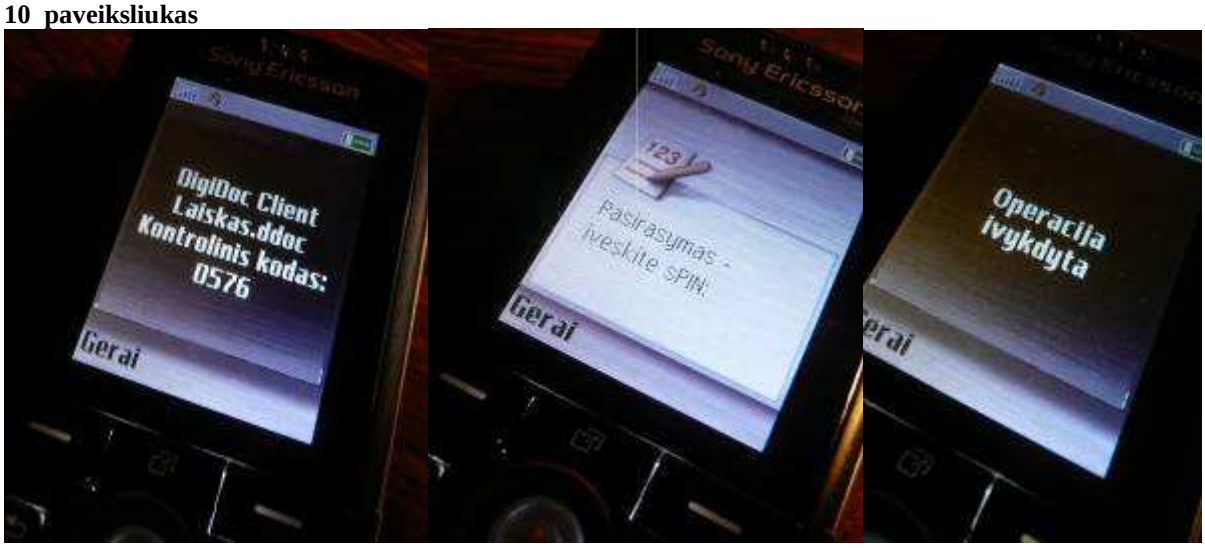
Buvo pažadėta, jog kortelė bus aktyvuota maždaug savaitės bėgyje. Kortele telefono pokalbiams buvo galima naudotis iš karto, tačiau elektroninio parašo paslauga buvo aktyvuota po kelių dienų. Programinė įranga (DigiDoc) su kuria buvo testuojamas dokumentų pasirašymas parsisiųsta ši elektroninio parašo proveržio svetainės.[72] Vienas iš pasirašymo etapų pateikiamas 9 paveiksliuke. Šiame etape programos sugeneruotas kodas yra persiunčiamas į mobilųjį telefoną. Šis kodas yra skirtas tam, kad identifikuoti konkrečią sesiją ir užtikrinti, jog yra suvokiama, jog bus pasirašinėjamas dokumentas pakrautas DigiDoc programoje. 10 paveiksliuke pateikiami sekantys etapai, kurie atliekami mobiliajame telefone. Kiti pasirašymo etapai pateikiami 4 priede. Buvo bandoma pasirašyti dokumentus naudojantis 2 skirtingais telefonų modeliais, tačiau tik su vienu iš jų pavyko tai padaryti. Su pirmuoju telefonu persiunčiant sPIN kodą įvykdavo klaida ir pasirašymas būdavo nutraukiamas. Ekrane pasirodantis klaidos pranešimas nepaaiškindavo nepasirašymo priežasties. Antruoju telefonu pasirašymas įvykdavo sėkmingai.

9 paveiksliukas



[71] *Elektroninio parašo paslaugų teikimo sutarties (su AB Sertiffitseerimiskeskus) bendrosios sąlygos*, 6.8 skyrius.
[72] *E3P svetainė*, Prieiga per internetą: <http://www.parasas.lt/-TOOLS/> [žiūrėta 2008 m. kovo 12 d.].

10 paveiksliukas



Pasirašant dokumentus taip pat buvo generuojamas pranešimas, jog dokumentų pasirašymo skaičius yra ribojamas iki 10 pasirašymų per mėnesį, o norint turėti galimybę pasirašyti dokumentus dažniau reikia kreiptis tiesiogiai į sertifikavimo paslaugos teikėją. Dokumentų pasirašymui gali naudotis anksčiau minėta DigiDoc programine įranga (taip pat ir parašo tikrinimui) arba DigiDoc portalu.[73] Bandant prisijungti prie šios portalo yra prašoma įvesti asmens kodą. Tačiau jau šiame pirmame žingsnyje nors ir suvedus kodą teisingai sistema neleido prisijungti. Elektroninio parašo patikrinimui taip pat galima naudotis šiuo portalu. Patikrinimui nereikalingos papildomos priemonės – pakanka pakrauti failą į sistemą. Šiuo portalu buvo siūloma naudotis institucijoms, kurioms buvo išsiųstas pasirašytas prašymas ir anketa.

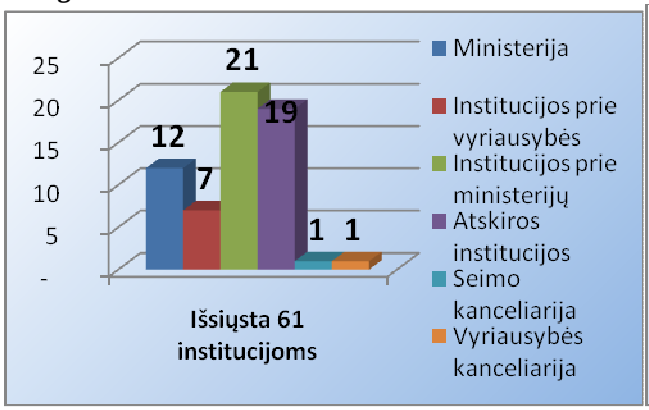
Šis mobilusis elektroninis parašas buvo pradėtas platinti 2007 metų spalio mėnesį ir kovo pabaigos duomenimis buvo apie 1000 vartotojų. Pagrindinė priežastis šio parašo naudojimo yra identifikacija prie internetinės bankininkystės sistemų. Kovo pabaigoje SODRA pritaikė savo informacinę sistemą mobilaus elektroninio parašo naudojimui. Su darbo užmokesčiu susijusius dokumentus galima teikti pasirašant arba SSC arba Omnitel platinamu parašu.

4.1.2 Tyrimo rezultatai

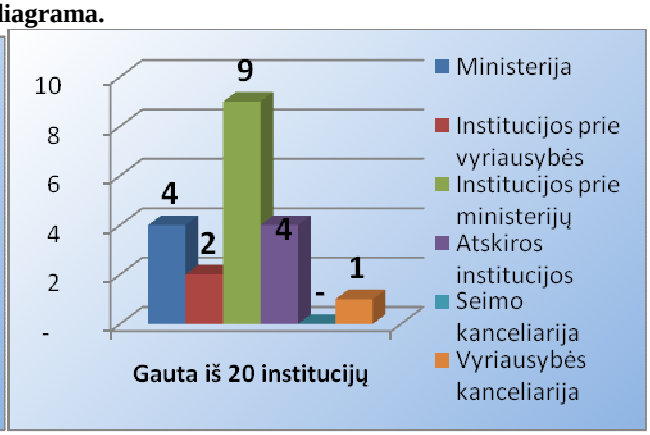
Anketos buvo išsiuntinėtos elektroniniu paštu 61 institucijai (12 ministerijų, 7 institucijom prie vyriausybės, 21 institucijai prie ministerijų, 19 atskirų institucijų ir taip pat seimo bei vyriausybės kanceliarijoms). Gauti atsakymai atitinkamai pateikiami diagramose. Iš viso gauta 20 atsakymų į anketas.

[73] *DigiDoc portalas (e. dokumentų pasirašymui ir tikrinimui)*, Prieiga per internetą: <https://digidocmid.sk.ee/?authType=mobile&f=chg_lang&lang=en>.

1 diagrama.

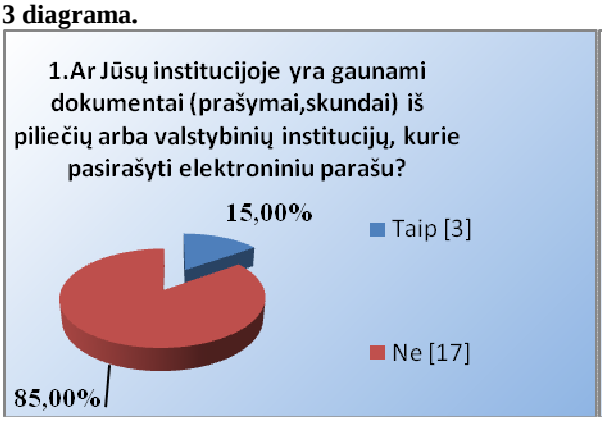


2 diagrama.

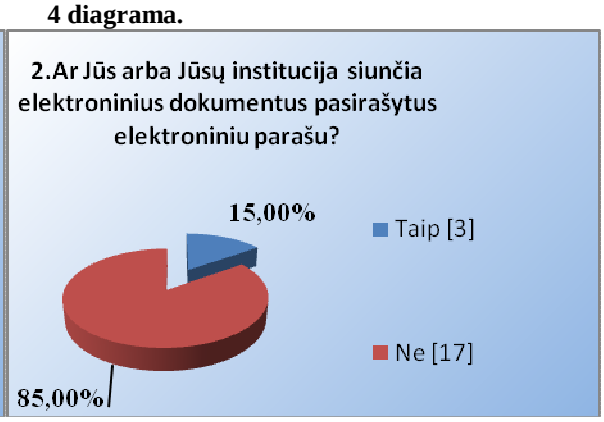


Pirmais dviem klausimais bandoma išsiaiškinti ar institucijose yra siunčiami ir gaunami dokumentai pasirašyti elektroniniu parašu. Pagal gautus rezultatus tik dvi institucijos ir siunčia ir gauna dokumentus pasirašytus elektroniniu parašu. Viena tik siunčia ir viena tik gauna. Bendri rezultatai matomi 3 ir 4 diagramose. Į klausimą kaip dažnai gaunami tokie dokumentai nurodė tik dvi institucijos Viena iš jų du kartus per mėnesį, o kitą 1 kart per mėnesį,. Kad siunčia nurodė tik viena institucija t.y. 1 kartą per du mėnesius.. Detalesnė statistika taip pat pateikiama 5 priede.

3 diagrama.



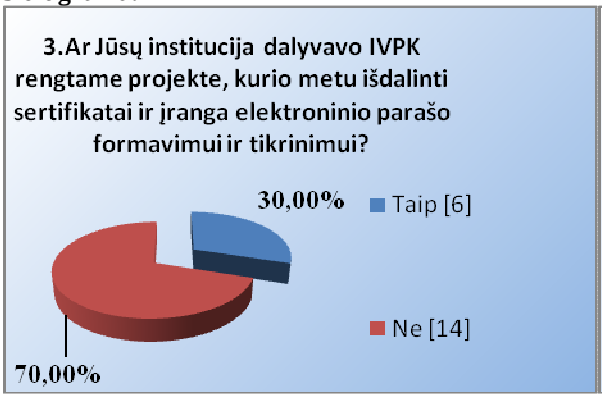
4 diagrama.



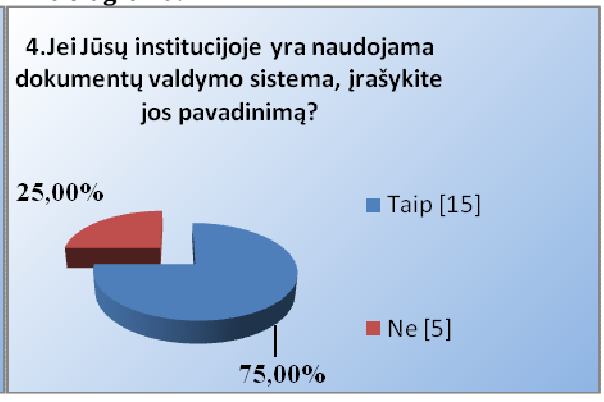
6 institucijos iš 20 teigė, jog nedalyvavo IVPK rengtame projekte, kurio metu buvo išdalintos priemonės elektroninio parašo formavimui, nors EPPS svetainėje teigiama priešingai.

Didžioji dalis institucijų naudoja DVS (75 %), o pagal EPPS ataskaitos duomenis yra tik viena institucija kuri techniškai ir teisiškai pasiruošusi elektroninių dokumentų su elektroniniu parašu tvarkymui.

5 diagrama.

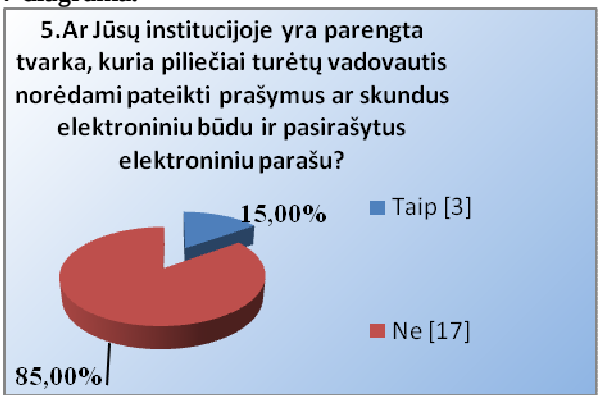


6 diagrama.



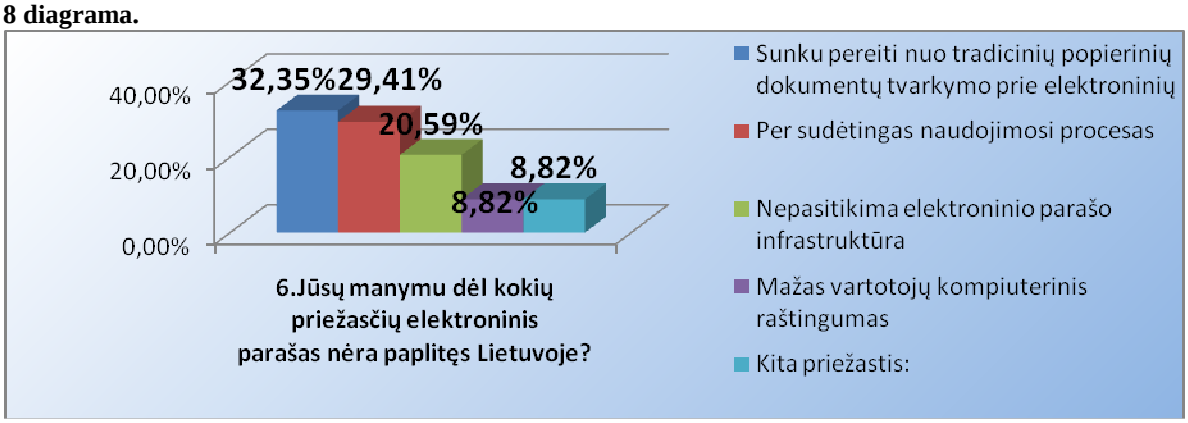
Vienas iš svarbiausių dalykų, kuris reikalingas tam, kad nekiltų nesusipratimų ir būtų naudojami vienodi standartai tai yra taisyklių nustatymas kokiu būdu piliečiai turėtų kreiptis į institucijas norėdami pateikti elektroninius dokumentus, tačiau tik 3 institucijos iš 20 turi tokias taisykles. Anketos nebuvo siuntinėjamos savivaldybių administracijoms. Tačiau pastebėta, kad kai kurios savivaldybės kitaip sprendžia dokumentų pateikimą elektroniniu būdu, t.y. nesinaudojant elektroniniu parašu. Šiaulių apskrities viršininko administracijai skundus arba prašymus galima pateikti tiesiog prisijungus prie internetinės svetainės. Tapatybės nustatymui prašoma tik teisingai nurodyti su asmens tapatybę susijusius duomenis (asmens kodas, vardas, pavardė). Pabrėžiama, jog anoniminiai skundai tiesiog nėra nagrinėjami.[74]

7 diagrama.



Pagrindinę priežastį respondentai dėl kurios elektroninis parašas nėra paplitęs nurodė, tai kad yra sunku pereiti nuo tradicinių popierinių dokumentų tvarkymo prie elektroninių. Ši priežastis buvo įvardinta kaip pagrindinė institucijų prie ministerijų ir vyriausybės, tiek pačių ministerijų. Tačiau atskirų institucijų atstovai kaip pagrindinę priežastį įvardino, tai jog yra per daug sudėtinga naudotis. Kiekvienos kategorijos atstovai vienodai sutinka, jog kompiuterinis raštingumas nėra ta priežastis, kuri būtų lemianti. Kitaip tariant manoma, jog vartotojams naudotis e-parašu nekiltų problemų. Įdomu tai, kad nei viena iš 12 institucijų prie ministerijos nepažymėjo šios priežasties.

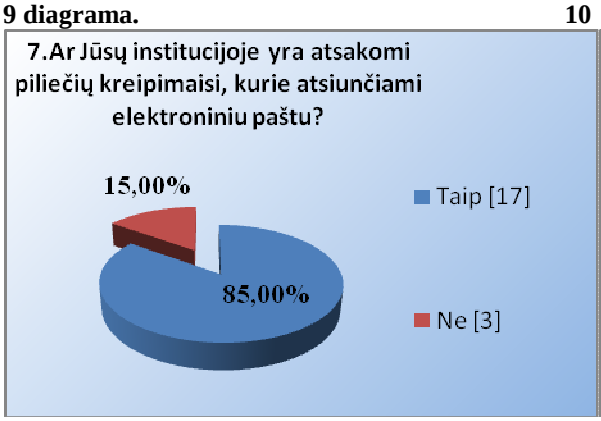
8 diagrama.



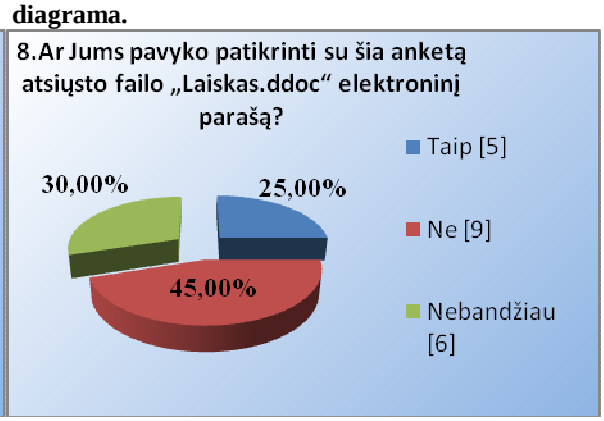
[74] *Šiaulių apskrities viršininko administracijos svetainė (elektroninių dokumentų pateikimui)*. Trumpinimas: SA. Prieiga per internetą: <http://www.siauliai.aps.lt/ava/eservices/eApplication.jsp?url=&categoryId=44&inlanguage=lt&pathId=59>.

Didžioji dalis institucijų nurodė, kad yra atsakomi laiškai siųsti elektroniniu paštu, tačiau ne visose laiškas elektroniniu paštu yra atsakomas, tuo labiau oficialiai. Valstybinėm institucijom išsiųstas prašymas buvo pasirašytas mobiliu elektroniniu parašu ir instrukcija kaip šį parašą reikia patikrinti. Tačiau pagal gautus rezultatus tik 5 institucijų atstovams iš kart pavyko patikrinti tapatybę.

9 diagrama.



10 diagrama.



4.1.3 Tyrimo išvados ir rekomendacijos

1.Valstybės tarnautojams yra išdalinta 1100 nekvalifikuotų sertifikatų, tačiau sukurta infrastruktūra praktiškai yra beveik nesinaudojama, neskaitant pavienių atvejų. Bendraujant su kai kurių institucijų atstovais buvo išreikštas pastebėjimas, jog elektroninis parašas būtų naudojamas jeigu ir kitos institucijos naudotųsi.

2.Patogiam dokumentų administravimui, saugojimui tvarkymui itin svarbų vaidmenį turi DVS. Pagal tyrimo rezultatus didžioji dalis (75%) apklaustų institucijų turi vieno ar kito gamintojo DVS. Tačiau dar nėra aiškų kiek institucijų yra pritaikiusios savo DVS dokumentų pasirašymui. SSC yra sukurtos priemonės leidžiančios atskirą modulį įdiegti į vieną ar kitą DVS tam kad būtų galimybė pasirašinėti dokumentus.

3. Didžioji dalis institucijų nėra perengusios tvarkų pagal kurias piliečiai galėtų vadovautis teikdami oficialius prašymus ar skundus. Dabar rinkoje pasirodo naujų sertifikavimo paslaugų teikėjų, o taip pat planuojama įgyvendinti naujų asmens tapatybės kortelių projektą. Jei institucijos pradėtų gauti dokumentus pasirašytus įvairiais skirtingais parašais, tai sukeltų nepatogumų. Tam, kad būtų išspręsta problema reikalinga bendra platforma, kurioje būtų galima tikrinti įvairius parašus, o ne instaliuojant kiekvieno teikėjo programinę įrangą atskirai.

Tokios panašios platformos pavyzdys yra sukurtas Ispanijos Viešojo administravimo ministerijos. Ši platforma tikrina kiekvieno akredituoto Ispanijoje sertifikavimo paslaugų teikėjo suteiktus sertifikatus. Kaip teigiama vienoje iš elektroninio parašo Ispanijoje naudojimo ataskaitų tokia platforma „multiški Validation Platform (vadinama Platform @firma v.5.0.) suteikia e.

sertifikatų ir e. parašų patikrinimą, kurie suteikti iš pagrindinių paslaugos teikėjų. Šios paslaugos suteikiamos daugeliui e. valdžios sistemų, kurios naudojamos Ispanijos viešojo administravimo sektorių (valstybinio, regioninio, vietinio (savivaldybių)). Šiuo metu ši platforma palaiko 11 sertifikavimo paslaugų teikėjų paslaugas ir 56 skirtingų sertifikatų tipų (rūšių)." [75]

Ši iniciatyva pripažinta kaip geros praktikos pavyzdys ir išskiriamas straipsnis *epractice.eu* svetainėje. [76] Panašaus pobūdžio svetainė būtų reikalinga ir įgyvendinant elektroninės valdžios projektus Lietuvoje. Egzistuojant tokiai platformai, įvairioms elektroninės valdžios sistemoms atsiradus naujam sertifikavimo paslaugos teikėjui nereikėtų atnaujinti sistemos, nes tai būtų atliekama pagrindinėj platformoj (multiPKI). Ši platforma turėtų tarnauti ir kaip pasirašytų dokumentų patikrinimo sistema, kurioje būtų atpažįstami įvairių sertifikavimo teikėjų suteikti sertifikatai.

4. LR institucijose atsakomi elektroniniu paštu atsiųsti laiškai, bet nepasirašyti elektroniniu parašu. Vis dėl to 3 institucijos iš 20 pažymėjo, jog elektroniniu paštu atsiųsti laiškai nėra atsakomi. Šame klausime nebuvo numatytas dar vienas pasirinkimas – laiškai, kuriems nereikalingas oficialus atsakymas yra atsakomi elektroniniu paštu. Institucijos, kurios pažymėjo, jog laiškai nėra atsakomi panašu, kad turėjo omenį laiškus kuriems yra reikalingas oficialus atsakymas.

5. Didžiajai daliai institucijų atstovų nepavyko arba nebuvo bandoma patikrinti pasirašyto laiško parašo savininko (45% nepavyko ir 25% nebandė). Rezultatai būtų kitokie jeigu į institucijas būtų kreipiamasi ne prašant užpildyti anketą, o klausimu, kuris yra tiesiogiai susijęs su institucijos veikla.

6. Valstybinėms institucijose sunku pereiti nuo tradicinio dokumentų administravimo metodo prie elektroninio. Nors didžioji dalis institucijų yra pasiruošę, tačiau nėra iniciatorių, kurie būti pirmieji tokių dokumentų apsikeitime. Anketos atsiliepimai praktiškai visi teigiami ir yra suprantama e. parašo nauda.

4.2 Visuomenės susipažinimo su elektroniniu parašu tyrimas

Tyrimo tikslas: Išsiaiškinti koks yra visuomenės susipažinimo lygis su elektroninio parašo infrastruktūra ir ką reikėtų keisti, kad elektroninis parašas butų naudojamas labiau.

Tyrimo uždaviniai.

1. Paruoši anketą tyrimo tikslui įgyvendinti;
2. Išanalizuoti gautus rezultatus;

---

[75] SA.

[76] ALVAREZ RODRIGUEZ, Miguel; *MultiPKI Validation Platform for eID and eSignature Services, Straipsnis: 2007 liepos 24, Redaguotas: 2008 vasario 15,* Prieiga per internetą: <http://www.epractice.eu/cases/afirma>,žiūrėta [2008 03 20].

Tyrimo objektas – internetu besinaudojančių Lietuvos piliečių žinios apie elektroninį parašą ir jų nuomonė įvairiais su tuo susijusiais klausimais.

Hipotezės.

1 hipotezė. Elektroninio parašo sąvoka ir įmonės teikiančios elektroninio parašo paslaugas yra žinomos Lietuvos piliečiams besinaudojantiems internetu.

2 hipotezė. Lietuvos piliečiai naudojasi elektroniniu parašu.

3 hipotezė. Lietuvos piliečiai mano, kad e-parašo naudojimu turi pasirūpinti patys piliečiai, o ne valstybė.

4 hipotezė. Lietuvos piliečiams svarbu, kad sertifikavimo paslaugos teikėjas būtų iš Lietuvos, o ne iš užsienio.

5 hipotezė. Lietuvos piliečiai sutinka su tuo, kad Lietuvoje nėra paplitęs elektroninis parašas dėl to, kad nėra nemokamos paslaugos (taip pat analizė ir pagal kitas priežastis).

Klausimyno sudarymas.

Tyrimas atliktas panaudojant 18 klausimų anketa.[77] Iš šių klausimų 17 yra uždari ir vienas atviras.

Tarp šių klausimų yra 5 tam, kad nustatyti respondentų socialinę-demografinę padėtį. (amžių, lyti, gyvenamą vietove, išsilavinimą ir užsiėmimą). Anketoje nurodomas tyrimo tikslas ir tai, jog anketa yra anoniminė. Kitaip tariant, kad gauti rezultatai bus nagrinėjami tik bendrai ir nesigilinant į kiekvieno respondento atsakymus.

Respondentų atranka.

Tyriamųjų grupei sudaryti buvo naudojamasi dviem metodais, tai yra „Atsitiktiniu grupių parinkimo būdu“ ir „Grupės formavimu gniūžtės principo“. Detalesnis šių būdu aprašymas pateikiamas Kęstučio Kardelio išleistoje knygoje „Mokslinių tyrimų metodologija ir metodai“. [78] Taikant atsitiktinių grupių parinkimo metodą, nuoroda į anketą buvo išplatinta asmenims esantiems arčiausiai, kitaip tariant bendradarbiams, bendramoksliams. Taip pat respondentų buvo prašoma anketos nuorodą išplatinti savame rate (Grupės formavimas gniūžtės principu). Anketų sugrįžtamumo nustatyti neįmanoma, nes anketa buvo platinama internetu, o ne siuntinėjama kiekvienam respondentu atskirai.

Populiacijos apibrėžimas.

Tyrimas orientuotas į studentus, tačiau anketa buvo užpildyta ir kitos veikla užsiimančių respondentų Kadangi anketa platinta internetu, automatiškai tiriamųjų populiacija apribota iki besinaudojančių internetu. Internetu nesinaudojančių asmenų apklausa elektroninio parašo tema

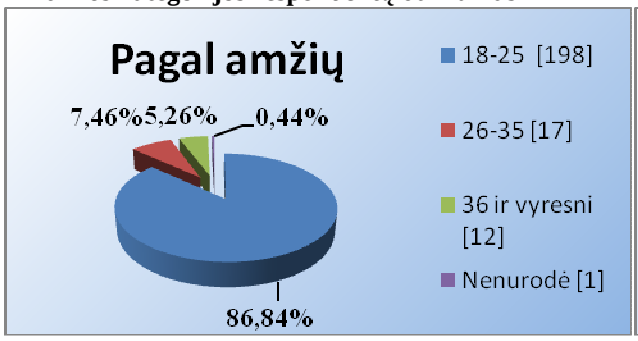
[77] *Svetainė, kurioje patalpinta anketa*, http://www.apklausa.lt/answerform.php?form=14822.
[78] KARDELIS, Kęstutis *Mokslinių tyrimų metodologija ir metodai* , p.325 ir p.326

neturėtų prasmės. Anketa orientuota į labiausiai informacines technologijas privalumais besinaudojančių grupę. T.y studentus, vadybininkus, įvairių sričių specialistus vadovus. Tyrimui nebuvo taikytas kvotų principas tam, kad atskleisti realesnę populiacijos atitiktį. Šis tyrimas neatspindi visos populiacijos (internetu besinaudojančių), tačiau situacija apklausus daugiau asmenų neturėtų kardinaliai skirtis.

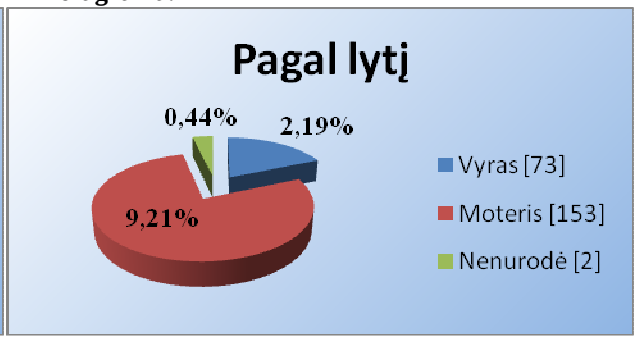
Tyrimo rezultatai.

Atliekant apklausą buvo išskirtos penkios amžiaus grupės. Daugiausia atsakymų buvo sulaukta iš 18-25 metų amžiaus grupės respondentų. Mažesnę dalį sudaro respondentai 26-35 amžiaus grupėje ir dar mažiau respondentų pateko į likusias tris amžiaus grupes. Apklausoje dalyvavo daugiau moterų nei vyrų.

1 diagrama. Laužtiniuose skliaustuose nurodytas tam tikros kategorijos respondentų dažnumas

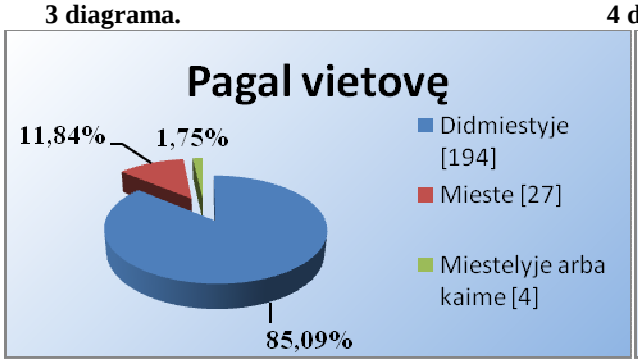


2 diagrama.

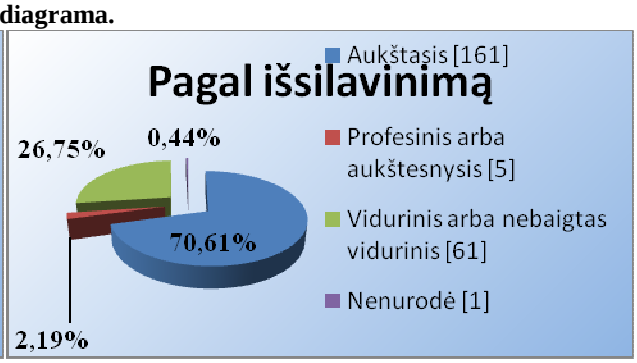


Taip pat daugiau respondentų nurodė esantys iš didmiesčio arba miesto, o iš miestelių arba kaimų respondentų kur kas mažiau. Pagal išsilavinimą daugiausia respondentų turinčių aukštąjį išsilavinimą. Toliau sekė turintys vidurinį išsilavinimą arba nebaigtą vidurinį. Galiausiai turintys profesinį arba aukštesnįjį išsilavinimą.

3 diagrama.

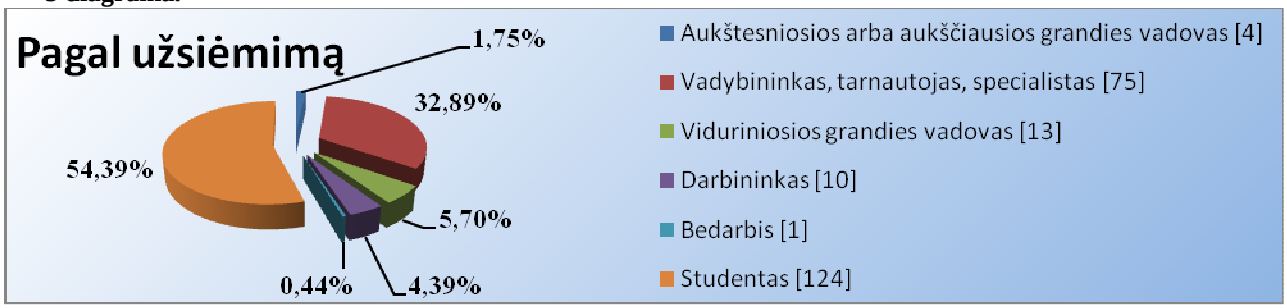


4 diagrama.



Pagal veiklą didžiąją dalį respondentų sudaro studentai, antroje vietoje valdininkai, tarnautojai ir įvairūs specialistai. Kitų veiklos kategorijų atstovai sudaro nedidelę dalį. Detalesnė informacija 5 diagramoje.

5 diagrama.

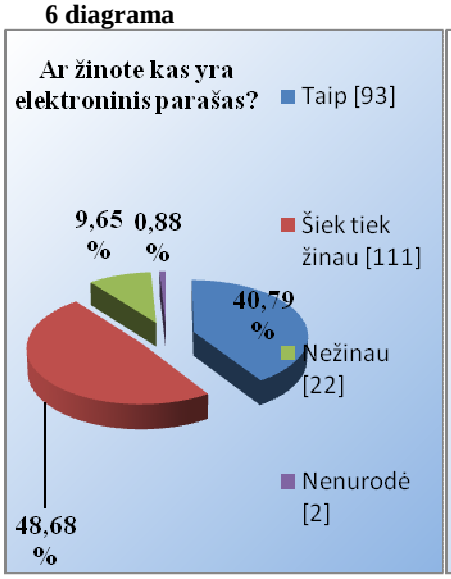


4.2.1 Tyrimo rezultatai

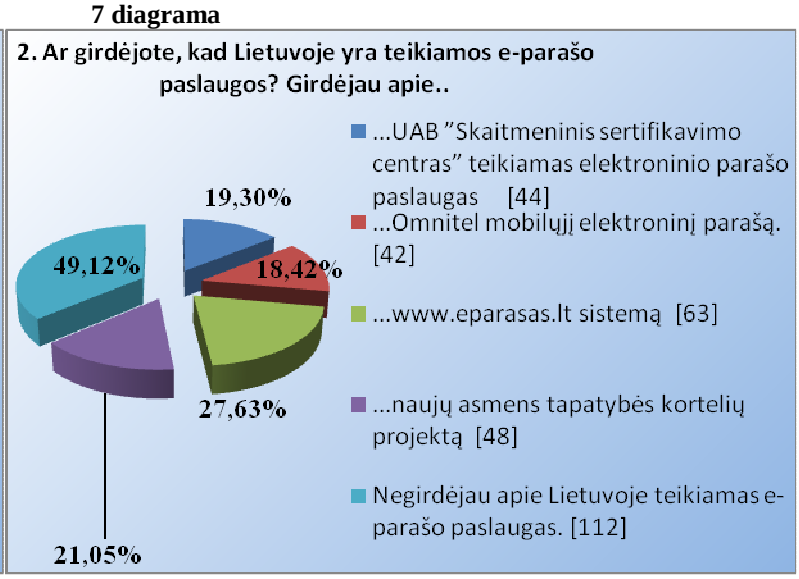
Pirmaisiais dviem klausimais buvo bandoma nustatyti kiek respondentų yra susidūrę su elektroninio parašo sąvoka ir ar apskritai yra apie jį girdėję. Klausiant apie institucijas teikiančias e-parašo paslaugas Lietuvoje tuo pačiu respondentui yra suteikiama informacija, jog pasirašinėjant dokumentus elektroniniu būdu reikalinga trečia šalis patvirtinant tapatybę. Žinančių arba šiek tiek žinančių apie elektroninį parašą pasiskirstymas pagal amžiaus grupes beveik nesiskiria. Tuo tarpu vyrai daug drąsiau tvirtino žinantys apie elektroninį parašą (vyrai-51,39%, moterys-36,6%). Nuosaikesnį atsakymai „Šiek tiek žinau“ pažymėjo daugiau moterų (50,98% ir 44,44% atitinkamai). Nežinančių (4,17% vyrų ir 12,42% moterų). Iš miestelių ir kaimo vietovių buvo sulauktą vos keli atsakymai. Dėl šios priežasties atsakymų lyginimas pagal vietovę būtų neadekvatus. Teigiančių, jog žino kas yra elektroninis parašas yra daug daugiau, kurie turi aukštąjį išsilavinimą. Tačiau nuosaikesnį atsakymą „Šiek tiek žinau“ pasirinko panašus procentas tiek turinčių aukštąjį tiek vidurinį arba nebaigtą vidurinį išsilavinimą. Profesinį arba aukštesnįjį išsilavinimą turintys respondentai į analizę neįtraukti. Studentų susipažinimas su elektroniniu parašu vienas iš žemesnių, tačiau šiek tiek žinančių apie elektroninį parašą yra daugiausia lyginat su kitos veiklos atstovais. Nežinančių apie elektroninį parašą procentas mažiausias yra „Vadybininkų, tarnautojų, specialistų“ kategorijoje (tik 2,67%). Bendras pasiskirstymas pagal e-parašą pateikiamas 6 diagramoje.

Antruoju klausimu buvo bandoma išsiaiškinti ar vartotojai yra girdėję apie įmones teikiančias elektroninio parašo paslaugas Lietuvoje (7diagrama). Šiek tiek mažiau nei pusė respondentų apskirtai nebuvo girdėję apie tokias įmones. Kiti atsakymų variantai pasiskirstė maždaug vienodai, išskyrus girdėjusių apie www.eparasas.lt sistemą buvo apie 10 procentų daugiau. Ateityje rengiant panašias apklausas reikėtų numatyti dar vieną punktą, kuriame būtų klausiame ar respondentai yra girdėję apie tokią elektroninio parašo versiją, kurioje pasinaudojama internetine bankininkyste. Yra tikimybė, kad dabartinėje anketoje dalis respondentų tokio parašo versiją klaidingai priskyrė prie www.eparasas.lt sistemos. Apskritai negirdėjusių apie tokias įmones pagal užsiėmimą pasiskirstė atitinkamai (Aukštesniosios arba aukščiausios grandies vadovas – 10%, Viduriniosios grandies vadovas – 16,67%, Vadybininkas, tarnautojas, specialistas – 22,61%, Studentas – 48.32%, Darbininkas – 80%).

6 diagrama

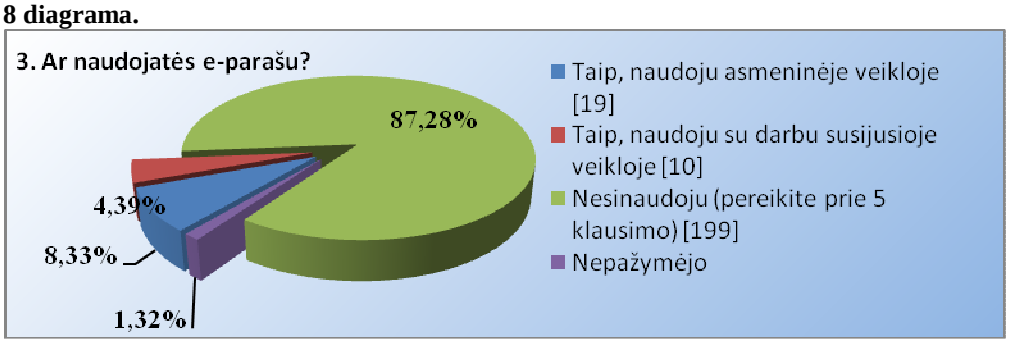


7 diagrama

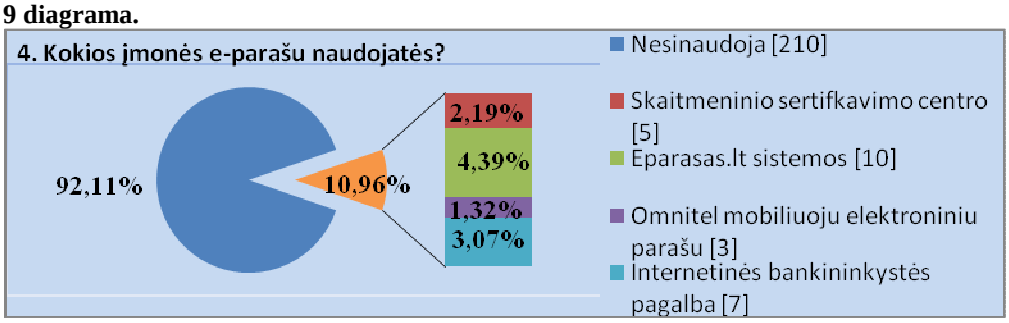


Trečias ir ketvirtas klausimai skirti tam, kad nustatyti kuri dalis respondentų naudojasi viena ar kita elektroninio parašo forma. Atliekant tyrimą labiausiai domina ta elektroninio parašo forma, kuri yra apibrėžiama elektroninio parašo įstatyme. Trečiame klausime 4 respondentai nors ir nurodė, kad naudojasi elektroniniu parašu asmeninėje arba su darbu susijusioje veikloje tačiau sekančiame klausime nedetalizavo kokios tai įmonės parašas. Asmeninėje veikloje Omnitel platinamu mobiliu parašu naudojasi du respondentai ir vienas SSC centro platinamu elektroniniu parašu. Kad asmeninėje veikloje naudojasi internetinės bankininkystės kuriamu parašu įrašė 7 respondentai. Besinaudojančių eparašas.lt pasirašytais dokumentais – 10. Su darbu susijusioje veikloje – 4 SSC parašo turėtojai, 1 Omnitel mobilaus parašo savininkas, 3 eparašas.lt sistemos naudotojas ir 1 naudojantis internetine bankininkyste. Į Omnitel arba SSC parašus naudojančių kategoriją pateko tik vadybininkų, tarnautojų ir specialistų grupė.

8 diagrama.

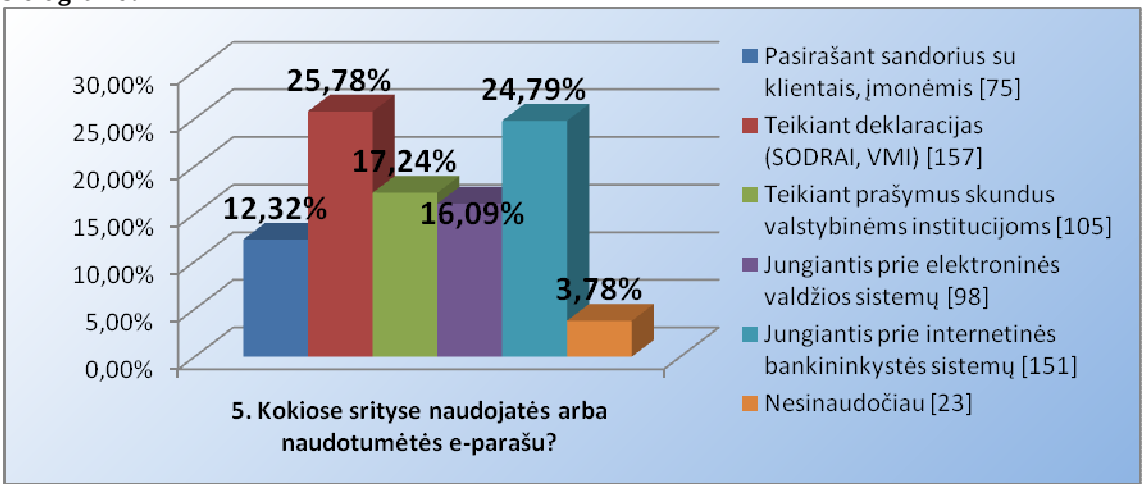


9 diagrama.



Vieną ar kitą elektroninio parašo panaudojimo sritį pasirinko didžioji dalis respondentų. Tačiau 10 procentų nesinaudoja ir nesinaudotų nei vienoje iš 10 diagramoje išvardintų elektroninio parašo panaudojimo sričių. 18-25 ir 26-35 metų kategorijose pasiskirstymas pagal e-parašo naudojimą panašus ir skiriasi tik po kelis procentus. Vyresni nei 36 metų respondentai mažiau linkę naudoti parašą įvairiose srityse, tačiau teigiančių, jog teiktų duomenis VMI arba SODRAI netgi daugiau nei jaunesnių kategorijų atstovų. Iš tų kurie nesinaudoja internetine bankininkyste, aukcionais ar parduotuvėm net 17,76% nesinaudotų ir elektroniniu parašu. Tuo tarpu, kurie jau dabar naudojasi viena iš išvardintų internetinių paslaugų tik 3,28% nesinaudotų elektroniniu parašu. Studentų pasirinkimai naudoti elektroninį parašą įvairiose srityse beveik neišsiskyrė iš kitų užsiėmimo kategorijų. Tačiau aukščiausios grandies vadovai labiau būtų linkę naudoti e-parašą išvardintose srityse. Proporcingai daugiausiai apskirtai nesinaudotų e-parašų darbininkų kategorijos atstovai.

9 diagrama.

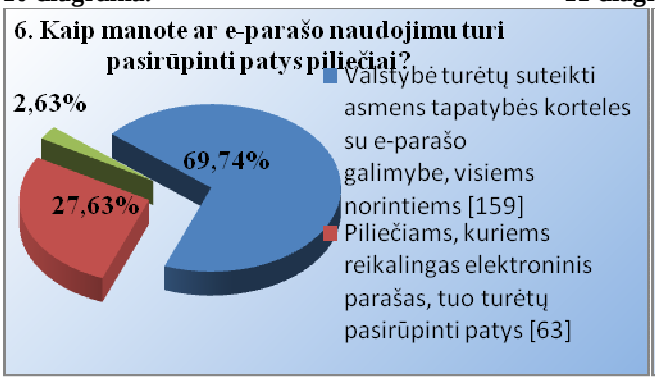


Šeštu klausimu buvo bandoma nustatyti kieno turi būti iniciatyva pradedant naudoti elektroninį parašą. Ar tuo turėtų pasirūpinti patys piliečiais? Ar valstybė turėtų suteikti asmens tapatybės korteles visiems norintiems? (10 diagrama). Beveik du trečdaliai atsakė, jog valstybė turėtų labiau imtis iniciatyvos. Tačiau beveik trečdalis atsakiusiųjų mano, jog tai pačių piliečių reikalas. Beveik 3 procentai nepasirinko nei vieno atsakymo panašu dėl labai šių kategoriškų variantų. Šioje vietoje nebuvo numatytas dar vienas švelnesnis pasirinkimas. Galbūt numatantis, jog valstybė turėtų imtis iniciatyvos, tačiau asmens tapatybės kortelės piliečiams būtų dalinamos tik už tam tikrą mokestį. Turintis profesinį arba aukštąjį išsilavinimą labiausiai linkę teigti, jog valstybė turėtų imtis iniciatyvos. Mažiau turinčių tokią nuomonę, kurie turi aukštąjį išsilavinimą ir dar mažiau turinčių vidurinį arba nebaigtą vidurinį. Tokios pat nuomonės ir 5 procentais daugiau vyrų nei moterų. Didelių skirtumų nėra ir tarp skirtingų amžiaus grupių. Tuo tarpu žvelgiant pagal užsiėmimų kategoriją, studentų skatinančių valstybę suteikti asmens tapatybės korteles visiems norintiems mažiausias iš likusių kategorijų tik 64% (aukštesniosios grandies vadovas – 100% (5/5),

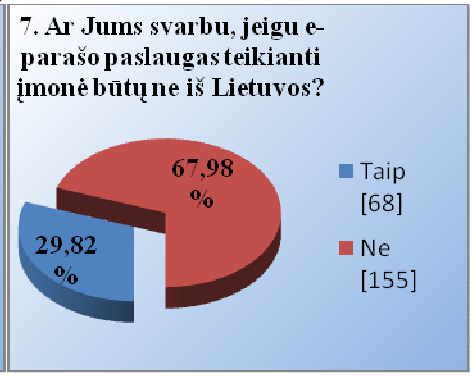
darbininkas (90%), vadybininkas, tarnautojas, specialistas (78,67%) ir viduriniosios grandies vadovas (76,92%)).

Dviems trečdaliams respondentų nėra svarbu ar elektroninio parašo paslaugas teikianti įmonė būtų iš Lietuvos ar iš užsienio. Lietuvoje jau yra platinami užsienio sertifikavimo paslaugų teikėjų sertifikatai per Omnitel atstovybes. Nors šis sertifikavimo paslaugos teikėjas yra akredituotas ES (jei tiksliau Estijoje) ir su vartotojais yra pasirašomos specialios sutartys, išlieka nemažai klausimų kaip būtų sprendžiamos įvairios iškylančias nepageidaujamos situacijos tarp sertifikavimo paslaugos teikėjo ir vartotojo. 2008 metų IVPK ataskaitoje išdėstoma į ką reiktų atkreipti dėmesį prieš pradedant naudotis užsienio sertifikavimo paslaugų teikėjų paslaugomis: „Tik šiuo atveju vartotojai, prieš sudarydami sutartis, turėtų patys išsiaiškinti, kokią atsakomybę (draudimai už galimą žalą, tolimesnis sertifikatų aptarnavimo palaikymas galiojant ir pasibaigus sutarčiai ir kiti įsipareigojimai) jiems garantuoja tokie užsienio paslaugų teikėjai, kokius įgaliojimus turi jų tarpininkai Lietuvoje. Tokia informacija turėtų būti viešai skelbiama tiekėjų Interneto svetainėse. Teisinę registraciją galima pasitikrinti ir tų šalių elektroninio parašo priežiūros įstaigoje.“ [79]

10 diagrama.



11 diagrama.



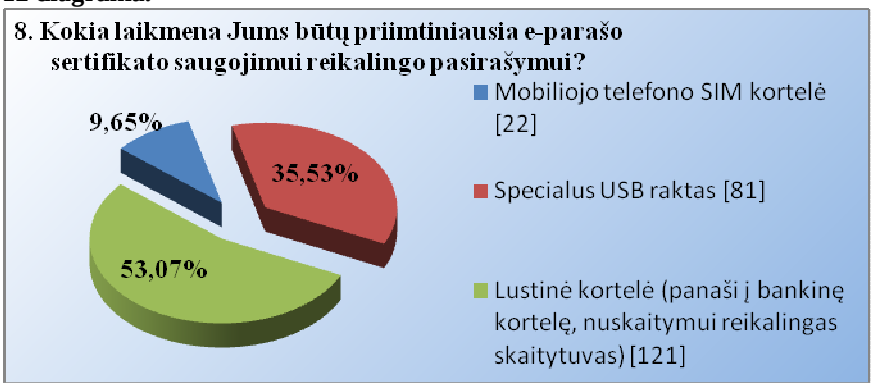
Pagal laikmenos pobūdį duomenų saugojimui reikalingų elektroninio parašo formavimui didžiausio populiarumą turi lustinės kortelės (nors jų eksploatacijai ir yra reikalingas ir nemažai kainuojantis kortelių skaitytuvas). Antroje vietoje specialūs USB raktai ir galiausiai mobiliojo telefono SIM kortelė. Praktikoje nekvalifikuoti sertifikatai dar yra įrašomi ir į kitas laikmenas (paprastus USB raktus ir pan.), tačiau aukščiausią saugumo lygį gali užtikrinti tik specialūs įrenginiai su mikroprocesoriais reikalingais duomenų šifravimui (elektroniniam pasirašymui).

Detaliau panagrinėjus pasiskirstymą pastebėta, jog panašiai tiek vyrų tiek moterų rinktųsi specialius USB raktus. Tačiau mobiliojo telefono SIM kortelei pirmenybę labiau teiktų vyrai (atitinkamai 16,44% ir 6,67%), o lustinę kortelę pasirinktų daugiau moterų (56,00% ir 49,32%). Šiuo metu SSC platina visose išvardintose laikmenose (SIM kortelė parengimo etape). Omnitel elektroninio parašo laikmena yra mobiliojo telefono SIM kortelė. Pagal užsiėmimo kategoriją

[79] *ELEKTRONINIO PARAŠO PRIEŽIŪROS INSTITUCIJOS LIETUVOS RESPUBLIKOS ELEKTRONINIO PARAŠO ĮSTATYMO ĮGYVENDINIMO KASMETINĖ (2007 METŲ) ATASKAITA*, p.4, Prieiga per internetą: <http://epp.ivpk.lt/epp/Dokumentai/2008-03-29_ataskaita.doc>.

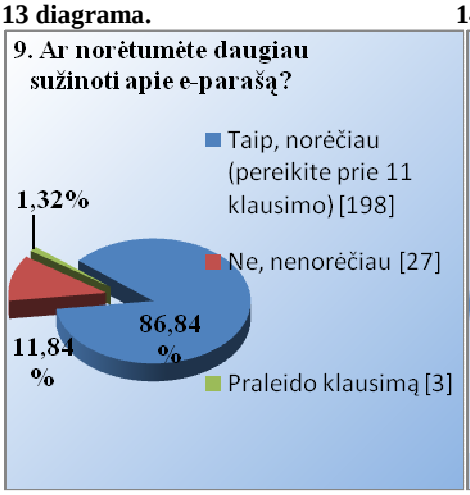
labiausiai išsiskyrė viduriniosios grandies vadovai, kurie nurodė, kad teiktų pirmenybę lustinėms kortelėms (76,92%).

12 diagrama.

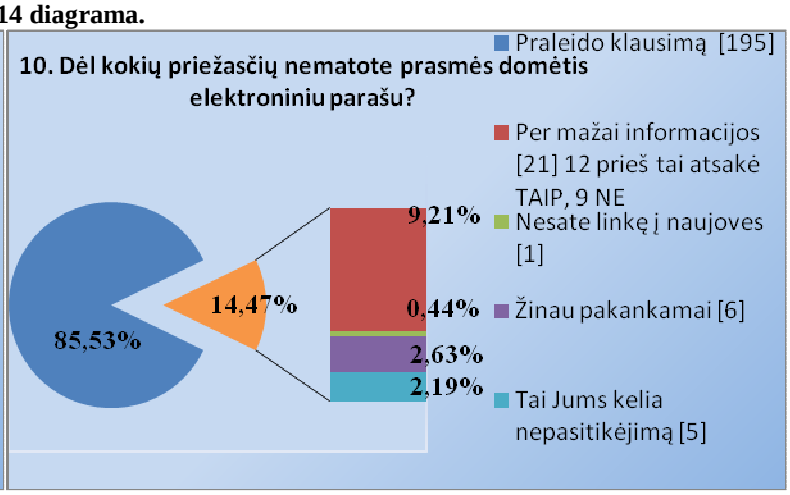


Devintu ir dešimtu klausimais klausiama ar respondentai yra linkę domėtis šia technologiją ir jeigu ne, tai dėl kokiu priežasčių. Didžioji dalis respondentų norėtų daugiau sužinoti apie elektroninį parašą (13 diagrama). Tuo tarpu iš nenorinčių daugiau sužinoti apie e-parašą priežastys atsispindi 14 diagramoje.

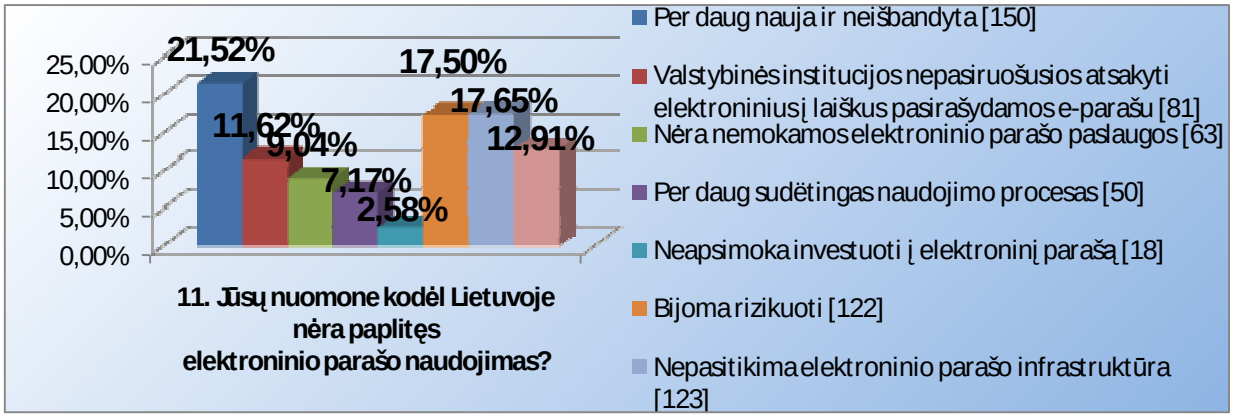
13 diagrama.



14 diagrama.



15 diagrama. Kiekvieno pasirinkimo procentas nuo visų pasirinkimų.



4.2.2 Tyrimo išvados ir rekomendacijos

1.Nors šiek tiek daugiau nei pusė apklaustųjų yra girdėję apie įmones teikiančias elektroninio parašo paslaugas, tačiau tik labai maža dalis naudojasi asmeninėje arba su darbu susijusioje veikloje. Tarp priežasčių lemiančių nedidelį elektroninio parašo naudojimą respondentai daugiausiai įvardino, tai jog tai yra per daug nauja ir neišbandyta. Tarp pagrindinių priežasčių taip pat įvardinta, jog yra nepasitikima elektroninio parašo infrastruktūra ir bijoma rizikuoti.

2.Apie trečdalis respondentų mano, kad elektroninio parašo naudojimu turi pasirūpinti pats vartotojas, o ne valstybė turėtų suteikti priemones kiekvienam norinčiam. Dabar kai bus realizuojamas projektas su naujomis asmens tapatybės kortelėmis svarbu, kad kuo daugiau šių kortelių pasiektų galutinį vartotoją tam, kad susidarytų kritinė naudojančiųjų masė.

3. Pagal gautus rezultatus trečdaliui respondentų yra svarbu, jog sertifikavimo paslaugos teikėjas būtų iš Lietuvos. Didelė dalis respondentų yra linkę domėtis e.parašo sritimi.

IŠVADOS IR REKOMENDACIJOS

1. Išanalizavus dabartinę Lietuvos elektroninio parašo teisės aktų bazę ir praktinius taikymo aspektus galima teigti, jog elektroninio parašo taikymas nors ir lėtai tačiau po truputį įsibėgėja. Kai kurie projektai tiek valstybinėse įstaigose, tiek ir privačiame sektoriuje sėkmingai veikia, nors elektroninio parašo infrastruktūra yra pakankamai sudėtinga tiek technologine, tiek ir teisine prasme.

2. Darbo pradžioje iškeltos hipotezė nebuvo patvirtinta. Priešingai nors ir nemažai institucijų dalyvavo rengtame projekte, tačiau vos kelios siunčia ar gauna pasirašytus elektroninius dokumentus.

3. Nors ir yra organizuojami įvairūs elektroninio parašo seminarai taip pat sukurta distancinio mokymo sistema (http://epm.ivpk.lt/olat/dmz/), tačiau visuomenė dar nėra pakankamai nušviesta apie elektroninio parašo naudą.

4. Atsirandantys nauji elektroninio parašo formatai iš skirtingų sertifikavimo paslaugų teikėjų sudarys keblumų pasirenkant vieną ar kitą. Skirtingos elektroninio parašo formavimo ir tikrinimo programos pritaikytos tik vienų ar kitų formatų atpažinimui. UAB „SSC“ yra paruošusi paketą skirta integravimui į dokumentų valdymo sistema, tam, kad dokumentus būtų galima pasirašyti naudojantis viena pasirinkta DVS.

5. Atsiranda elektroninio parašo sistemos, kurios naudoja elektroninę bankininkystę. (Nėra vieningos nuomonės ar dokumentus pasirašytus tokioje sistemoje galima laikyti kaip pasirašytus elektroniniu parašu)

6. Nesant centralizuotoms asmens tapatybės kortelėms, atsiranda kitos asmens identifikavimo priemonės elektroninėje erdvėje (pvz.: e-bilietai viešajame transporte). Tai sudaro papildomas išlaidas valstybei ir vartotojams.

7. Reikalinga įvertinti įvairias priemones, kuriomis sertifikavimo paslaugų centrai galėtų pritraukti daugiau vartotojų. Tam, kad padidinti kvalifikuotų elektroninių parašų gaunamą naudą, reikalinga kainos ir teikiamos naudos įvertinimas. Kainos diferencijavimas turėtų būti taikomas skirtingoms klientų grupėms. Taip pat vienas iš efektyvių metodų būtų rinkti mokestį už elektroninio parašo panaudojimą, bet sumažinti metinį mokestį. Tokią sistemą šiuo metu taiko SK platindamas mobilųjį elektroninį parašą Lietuvos vartotojams per UAB Omnitel. Dar vienas būdas pritraukti vartotojų būtų mokesčių netaikymas tada kai vartotojai atlieka įvairias operacijas elektroniniu būdu, o kreipiasi tiesiogiai į įvairias institucijas.

8. Bandyti pasiekti kritinę vartotojų masę: Tam, kad pasiekti kritinę vartotojų masę būtų naudinga naudoti minimalias sertifikatų kainas arba juos platinti nemokamai pirmose pradinėse projektų vystymosi fazėse. Naudojant ši metodą sertifikavimo paslaugų teikėją iš pradžių patirtų

nemažą nuostolį, tačiau vėliau pritaikius mokestį už elektroninio parašo panaudojimą tos investicijos sugrįžtų.

9. Supažindinti su teikiama nauda: Didelės reklaminės akcijos labai svarbios tam, kad būtų supažindinama su šia technologija. Tačiau finansavimas gultų ant pačių sertifikavimo paslaugų teikėjų. Prie reklamavimo taip pat turėtų prisidėti ir viešojo administravimo sektorius, nes grįžtamą nauda šis sektorius taip pat turėtų.

10. Sudėtingumo sumažinimas: Tam, kad sumažinti naudojimosi sudėtingumą reikia įvertinti įvairias sertifikatų saugojimo galimybes. Saugumas yra užtikrinamas vienodas tiek jeigu elektroninio prašo formavimui skirtas sertifikatas įrašomas į specialų USB raktą, ar SIM kortelę, ar į lustinę kortelę. Patogumo prasme ir išlaidų prasme SIM kortelė yra vienas iš optimaliausių sprendimų. Tačiau sertifikatų saugojimas asmens tapatybės kortelėje taip pat turi privalumų, nes tuo pačiu atstoja ir fizinę asmens identifikaciją.

11. Bandomojo laikotarpio suteikimas: daugeliui vartotojų bandomasis laikotarpis yra svarbus tam kad susipažinti su teikiama paslauga įvertinti naudojimosi patogumą ir pan.

12. Lietuva turėtų kuo aktyviau ir glaudžiau dalyvauti ir bendradarbiauti su Europos Sąjungos struktūromis, kartu su kitomis ES šalimis vykdyti bendrus projektus.

13. Viešuosiuose pirkimuose turi būti numatytos procedūros, kurios galėtų iš anksto informuoti IT visuomenę apie įstaigų ketinimus diegti vieną ar kitą technologiją, organizuoti viešas diskusijas ir pan.

14. Atsakingiems valdžios atstovams, prieš priimant sprendimus rekomenduojama organizuoti diskusijas, studijas ir pan., kad labai svarbūs Lietuvos el. parašo infrastruktūros klausimai būtų sprendžiami skaidriai, nediskriminuojant Lietuvos įmonių ir kas yra svarbiausia, išlaikant nacionalinių, o ne užsienio verslo grupių interesus.

15. Reikėtų išskirti, jog įmonės, kurios nusprendžia savo veikloje pradėti naudoti elektroninį parašą, neturėtų apsiriboti tik technologiniu įgyvendinimu. Prieš pradedant naudoti elektroninį parašą turi būti įvardijama ir apibrėžiama kokiems įmonės procesas tai bus taikoma, kokio tipo sertifikatais (saugumo lygis) bus naudojamasi. Galbūt norint užtikrinti saugų susirašinėjimą paštu ir nebūtina įsigyti kvalifikuoto sertifikato. Tačiau jeigu nusprendžiama naudoti aukščiausio lygio sertifikatus – tada įmonėje ar įstaigoje rekomenduojama, jog būtų patvirtinamos elektroninio parašo taisyklės. Dabar kai jau yra keletas elektroninio parašo paslaugas teikiančių įmonių belieka pasirinkti ir veikloje taikyti priimtiniausią sprendimą.

SANTRAUKA ANGLŲ KALBA

Electronic Signature‘s benefit is obvious. Nearly eight years have already past since European Parliament and European Commission legitimated directive on a Community framework for electronic signatures. In Lithuania and in all Europe followed legislations for electronic signature infrastructure. Also standards were created to prevent incompatibility. In this study Lithuanian situation in usage of electronic signature for electronic government, electronic commerce is reviewed. In this study review is referenced to the research that has been done lately in Europe and in Lithuania.

This study is divided into four parts. Methods that are used in creating electronic signature have been analysed in first part. Furthermore it has been analysed algorithms that are used to warrant highest security and to prevent forgery. Electronic signature legislation in Lithuania is reviewed in second part. Third part is for overlooking of practical usage aspects in Lithuania and in Europe. In fourth part two research have been made. One of them is for evaluation of preparation of main state institutions to accept and send documents signed electronically. Second research is for evaluation of society’s knowledge in electronic signature field.

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS

Teisės aktai:

1. EUROPKI SERTIFIKATO TAISYKLĖS, EuroPKI (2000-2004), 2004 m. sausis, OID: 1.3.6.1.4.1.5255.1.1.1, [žiūrėta 2008 m. kovo 20 d.], Prieiga per internetą: <http://repository.ssc.lt/get/~europki_cp>.

2. Lietuvos Respublikos administracinių teisės pažeidimų kodėkas, Lietuvos Respublikos Seimas, 214(24) straipsnis, Prieiga per Internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=312459&p_query=&p_tr2=>.

3. „Dėl elektroninių dokumentų valdymo taisyklių patvirtinimo“, Lietuvos archyvų departamento įsakymas, Prieiga per Internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=269626&p_query=&p_tr2=>.

4. „Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“, Lietuvos Respublikos Vyriausybės nutarimas, Įsigalioja nuo 2003-01-09, Prieiga per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=198003&p_query=&p_tr2=>.

5. IVPK prie LRV įsakymas „Dėl rekomendacijų dėl elektroninio dokumento turinio. Prieiga per Internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=289137&p_query=&p_tr2=> [žiūrėta 2008 m. sausio 12 d.].

6. Elektroninio parašo įstatymas,8(3)str ir 5(1)str. Per internetą: <http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=169880>.

7. LIETUVOS RESPUBLIKOS SEIMO INFORMACINĖS VISUOMENĖS PLĖTROS KOMITETAS, POSĖDŽIO PROTOKOLAS, 2006-09-13 Nr. 23, Vilnius, Posėdžio pirmininkė: Irena Šiaulienė Preiga per internetą: http://www3.lrs.lt/pls/inter/ivpk_print.doc_view?key=282453

8. Dėl viešojo administravimo plėtros iki 2010 metų strategijos patvirtinimo, LR vyriausybės nutarimas, p.1, Prieiga per internetą: <http://www.vrm.lt/uploads/media/VA_Strategija_01.doc>.

9. Dėl lietuvos informacinės visuomenės plėtros strategijos patvirtinimo, LR Vyriausybės nutarimas, Prieiga per internetą: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=257174>. žiūrėta [2008 03 10].

10. Dėl Elektroninės valdžios koncepcijos patvirtinimo,LR Vyriausybės nutarimas,1dalis 1.3punktas,5dalis, 18punktas,9dalis 46 punktas,Prieiga per internetą:<http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=198184> žiūrėta [2008 03 20].

11. LIETUVOS RESPUBLIKOS VIEŠOJO ADMINISTRAVIMO ĮSTATYMAS, 19 str. 5dalis, Prieiga per internetą: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=257918

12. Elektroninio parašo paslaugų teikimo sutarties (su AB Sertiffitseerimiskeskus) bendrosios sąlygos, 6.8 skyrius.

Šaltiniai:

Moksliniai straipsniai:

13. Digital Signature vs Electronic Signature - What's the big difference?, Silanis Technology, [žiūrėta 2008 m. gegužės 20 d.], p.2, Prieiga per internetą: <http://www.cdmspa.com/pdfs/digital%20signature%20vs%20electronic%20signature.pdf>.

14. Study PKI and Certificate Usage in Europe 2006, Fraunhofer Institute FOKUS, October 31, 2006, Editor: Petra Hoepner [žiūrėta 2008 m. gegužės 20 d.] p.7, Prieiga per internetą: <http://www.ecom.or.jp/report/Study_on_PKI_2006_in_EUROPE-FINAL.pdf>

15. SHA1 Encryption Algorithm, 2003 VOCAL Technologies, Ltd. Custom Product Design Division, p.1, [žiūrėta 2008 m. kovo 20 d.]. Prieiga per internetą: http://www.vocal.com/SHA1.pdf>.

16. Firewall Product Functional Summary, Global Technology Associates, Inc, [žiūrėta 2008 m. kovo 20 d.]. P. 16, Prieiga per internetą: http://www.gta.com/downloads/external/pdf/GTA-Functional-Summary.pdf

17. REPEČKA, Gytis. Elektroninis parašas, „Naujoji komunikacija“ dvisavaitinis skaitmeninio gyvenimo būdo žurnalas. 2007 m. Spalio 30d. – lapkričio 30d. , Nr. 16 (212).

18. CIVILKA, Mindaugas; ir LAMANAUSKAS, Tomas. Elektroninio parašo įteisinimas: probleminiai aspektai pagal ES ir LR teisę, p. 7, Prieiga per Internetą: <http://www.norcous.lt/download.php/fileid/9>.

19. MADISE, Ülle; MARTENS, Tarvi, E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world. P.15.

20. ALVAREZ RODRIGUEZ, Miguel; MultiPKI Validation Platform for eID and eSignature Services, Straipsnis: 2007 liepos 24, Redaguotas: 2008 vasario 15, Prieiga per internetą: <http://www.epractice.eu/cases/afirma>,žiūrėta [2008 03 20].

21. KARDELIS, Kęstutis Mokslinių tyrimų metodologija ir metodai , p.325 ir p.326.

22. Marshall D. Abrams and Harold J. Podell, *Cryptography*, [žiūrėta 2008 m. balandžio 20 d.], p.7, Prieiga per internetą: http://www.acsac.org/secshelf/book001/15.pdf

23. DEPOORTERE, Ronny; *10 million new Belgian electronic ID cards : a success !*, Prieiga per internetą: <http://download.microsoft.com/download/4/f/d/4fd49a94-8772-4bd0-88ca-bf46e2d029fc/2_JUNE_2004/Zetes_BelgianeID_2004_Finalv.pdf>.

Žodynai:

24. Authentication 101, [žiūrėta 2008 m. kovo 20 d.]. Prieiga per internetą: <http://www.cscap.nuctrans.org/Nuc_Trans/links/dsa-disa.html>

25. Alexias inc., techninis žodynas, [žiūrėta 2008 m. kovo 20 d.]. Prieiga per internetą: <http://www.lexias.com/2.0/glossary4.html>

Tyrimai, ataskaitos, specifikacijos:

26. Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications,

Report, IDABC European eGovernment Services, November 2007, p.16, Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29484>.

27. Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatares, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Prieiga per internetą: <http://ec.europa.eu/information_society/eeurope/i2010/docs/single_info_space/com_electronic_signatures_report_en.pdf>.

28. The Legal and Market Aspects of Electronic Signatures, Study for the European Commission – DG Information Society, Prieiga per internetą: [http://ec.europa.eu/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf] . Drafted by Jus Dumortier, Stefan Kelm, Hans Nilsson, Gerogira Skouma and Patrick Van Eecke.

29. EESSI First Set of Deliverables, EESSI Deliverable Description Document, 2001, [žiūrėta 2008 m. kovo 20 d.] Prieiga per Internetą: <http://www.ictsb.org/EESSI/Documents/ddd.doc>.

30. Electronic Signatures and Infrastructures (ESI);Electronic Signature Formats, ETSI TS 101 733, ETSI, p. 74 ir p.21, [žiūrėta 2008 m. kovo 20 d.] Prieiga per Internetą: <http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_101733v010501p.pdf>.

31. Secure signature-creation devices “EAL 4+”, CWA 14169, CEN WORKSHOP AGREEMENT, 2004 kovas, p.9, [žiūrėta 2008 m. kovo 20 d.], Prieiga per Internetą: <ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf>.

32. CIVILKA, Mindaugas; MOCKAITYTĖ, Indrė; NATIONAL PROFILE LITHUANIA, 2007 balandis, Lietuvos ataskaita tyrimui „Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications”, Skyrius 3.1 eGovernment structure, Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29088>, p.13. Trumpinimas: NPL.

33. ELEKTRONINIO PARAŠO PRIEŽIŪROS INSTITUCIJOS LIETUVOS RESPUBLIKOS ELEKTRONINIO PARAŠO ĮSTATYMO ĮGYVENDINIMO KASMETINĖ (2007 METŲ) ATASKAITA, p. 3. , Prieiga per internetą: <http://epp.ivpk.lt/epp/Dokumentai/2008-03-29_ataskaita.doc>.

34. Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas, INVESTICINIS PROJEKTAS (GALIMYBIŲ STUDIJA), Dokumentą ruošė J. Kupinas 2006-09-18.

35. VALSTYBINIO AUDITO ATASKAITA, VALSTYBINIŲ INSTITUCIJŲ INFORMACINIŲ SISTEMŲ VALDYMAS ELEKTRONINĖS VALDŽIOS KONTEKSTE, p.9, 2007 m. rugsėjo 28 d. Nr. IA-9000-4-3 Vilnius, Prieiga per internetą <http://www3.lrs.lt/docs2/HBSAPGOV.PDF>.

36. Main Statistics of E-Voting.Prieiga per internetą: http://www.vvk.ee/english/Ivoting%20comparison%202005_2007.pdf

37. NATIONAL PROFILE SPAIN, 2007 balandis, Ispanijos ataskaita tyrimui „Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications”, Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29081>, p. 25, Trumpinimas: NPS.

38. NATIONAL PROFILE BELGIUM, 2007 balandis, Belgijos ataskaita tyrimui „Preliminary

Study on Mutual Recognition of eSignatures for eGovernment applications", Prieiga per internetą: <http://ec.europa.eu/idabc/servlets/Doc?id=29071>, p. 15, paragrafas: 4.2.1 Electronic identity card (e-ID), Trumpinimas: NPB.

39. Electronic Signature Dissemination WG - eID Survey Report in Bilgium, 2007 gruodžio 28 p.3, Prieiga per internetą: <http://www.ecom.jp/en/ecomnews/ecomnews_no33.pdf>. Trumpinimas: ESD.

Informacija iš internetinių svetainių:

40. EESSI internetinis puslapis, ICTSB, [interaktyvus], [žiūrėta 2008 m. gegužės 20 d.], Prieiga per Internetą: <http://www.ictsb.org/EESSI_home.htm>.

41. E3P svetainė, Prieiga per internetą: <http://www.parasas.lt/> ir <http://www.parasas.lt/-TOOLS/> [žiūrėta 2008 m. sausio 12 d.].

42. Elektroninė dokumentų pasirašymo sistema eParasas.lt, Prieiga per internetą: <https://www.eparasas.lt/lit/Sistemos_naudojimo_taisykles/247>, žiūrėta [2008 04 20].

43. eGovernment Factsheet - Belgium - eServices for Citizens, Prieiga per internetą: <http://www.epractice.eu/document/3288>. žiūrėta [2008 03 10].

42. eGovernment Factsheet - Estonia - National Infrastructure, 3 pastraipa, Prieiga per internetą: <http://www.epractice.eu/document/3332>. Trumpinimas: Factsheet – Estonia.

43. TEPANDI, Jaak; A Population-Wide ID card (Estonia),Prieiga per internetą: <http://www.epractice.eu/cases/eIDEstonia>, Trumpinimas: APWIC.

44. Internet World Stats, Prieiga per internetą: http://www.internetworldstats.com/eu/ee.htm ir <http://www.internetworldstats.com/eu/es.htm>., žiūrėta [2008 04 10].

45. PAKALKAITĖ, Vija, Aistros ir nežinia dėl naujų asmens tapatybės kortelių, vz.lt straipsnis, Prieiga per internetą: <http://vz.lt/Default2.aspx?ArticleID=5f6c430a-c553-44ff-9c27-0e6037de05a7>, žiūrėta [2008 03 20].

46. Good practice case eID in Estonia, 2006 spalis, p. 2, 1.4.1 paragrafas, Prieiga per internetą: <http://www.egov-iop.ifib.de/downloads/Interoperability_in_eID_in_Estonia.pdf>. Trumpinimas: GP EID.

47. ES: eID scores a million, 2007 spalio 14, 1 pastraipa, Prieiga per internetą: <http://www.epractice.eu/document/3905>.

48. Elektroninio parašo priežiūros skyriaus svetainė, prieiga per internetą: <http://epp.ivpk.lt/lt/edm>.

49. DigiDoc portalas (e. dokumentų pasirašymui ir tikrinimui), Prieiga per internetą: <https://digidocmid.sk.ee/?authType=mobile&f=chg_lang&lang=en>.

50. Šiaulių apskrities viršininko administracijos svetainė (elektroninių dokumentų pateikimui). Trumpinimas: SA. Prieiga per internetą: <http://www.siauliai.aps.lt/ava/eservices/eApplication.jsp?url=&categoryId=44&inlanguage=lt&pathId=59>.

51. E3P svetainė, Prieiga per internetą: <http://www.parasas.lt/-TOOLS/> [žiūrėta 2008 m. kovo 12 d.].

PRIEDAI

1 priedas. Skaitmeninio sertifikavimo centro suteikto nemokamo sertifikato informacija

Valid Certificate

Following you can find the certificate details.

Wednesday 30 May 11:56:17 UTC

Variable	Value
Certificate Version	3 (0x2)
Serial Number	3895 (0xF37)
Common Name	Audrius Mašidlauskas
E-Mail	dr.audrius.m@gmail.com
Distinguished Name	serialNumber=3895 CN=Audrius Mašidlauskas OU=Internet O=SSC Free Certificates CA C=LT
Role	User
Fingerprint	SHA1:60:E0:6D:FC:AC:45:E9:59:4E:00:7E:A9:03:72:81:DB:AE:60:05:D1
Issued by	serialNumber=4 CN=SSC Free Certificates CA OU=Sertifikavimo Tarnyba O=Skaitmeninio Sertifikavimo Centras C=LT
Valid From	May 28 13:29:00 2007 GMT
Expiration on	Jun 27 13:29:00 2007 GMT
Current Status	Valid
Netscape CA Revocation Url	http://ra-free1.ssc.lt/pub/crl/cacrl.crl
Netscape Cert Type	SSL Client, S/MIME
Netscape Comment	Nemokamas sertifikatas nuo SSC Free Certificates CA
Netscape Revocation Url	http://ra-free1.ssc.lt/pub/crl/cacrl.crl
X509v3 Authority Key Identifier	keyid:18:80:CA:F8:35:C4:DF:9C:5B:FC:C8:83:30:4A:AC:FF:90:B4:EC:A0 DirName:/C=LT/O=EuroPKI/CN=EuroPKI Lithuanian Certification Authority serial:04
X509v3 Basic Constraints	CA:FALSE
X509v3 CRL Distribution Points	URI:http://ra-free1.ssc.lt/pub/crl/cacrl.crl
X509v3 Certificate Policies	Policy: 1.3.6.1.4.1.5255.1.1.1 CPS: http://www.europki.org/ca/root/cps/en_index.html Policy: 1.3.6.1.4.1.5255.8.1.0 CPS: http://www.europki.lt/cps Policy: 1.3.6.1.4.1.22501.1.1.0 CPS: http://www.ssc.lt/cps
X509v3 Extended Key Usage	TLS Web Client Authentication, E-mail Protection
X509v3 Issuer Alternative Name	email:pki@ssc.lt
X509v3 Key Usage	Digital Signature, Non Repudiation, Key Encipherment
X509v3 Subject Alternative Name	email:dr.audrius.m@gmail.com
X509v3 Subject Key Identifier	54:3B:50:99:10:BC:F0:4C:11:A9:D4:72:10:0A:A5:39:CF:68:19:CC

2 Priedas. Pasirašytas laiškas (prašymas) siųstas institucijoms. Laiskas.ddoc.

Laba diena,

Maloniai kviečiame prisidėti prie tyrimo apie elektroninį parašą ir atsakyti į prie šio laiško prisegtos anketos klausimus (Failas: Anketa_LR_institucijoms.doc) Šio tyrimo tikslas yra nustatyti koks yra elektroninio parašo paplitimas LR institucijose ir kas lemia nedidelį elektroninio parašo naudojimą.

Prisegtame faile Laiskas.ddoc yra šio laiško turinys, pasirašytas kvalifikuotu elektroniniu parašu, teisiškai lygiaverčiu ranka pasirašytam parašui ir vienareikšmiškai leidžiančiam nustatyti šį laišką rašiusio asmens tapatybę. Parašo galiojimą galima patikrinti prisijungus prie šios svetainės.

https://digidoccheck.sk.ee/index.php?f=upload
Informacija kaip patikrinti
http://www.parasas.lt/-TOOLS/

Iš anksto dėkui už anketos atsakymus ir sugaištą laiką.

Pagarbiai,
Audrius Mašidlauskas
Informacijos sistemų vadyba

3 Priedas. Anketa siųsta institucijoms.

VILNIAUS UNIVERSITETAS
Komunikacijos fakultetas

Elektroninio parašo paplitimas LR institucijose

Anketą rengė: Audrius Mašidlauskas

Maloniai kviečiame prisidėti prie tyrimo apie elektroninio parašo naudojimą ir atsakyti į anketos klausimus.
Prašome pažymėti Jūsų pasirinktą atsakymo variantą arba įrašyti į pilkelius laukelius.

1.Ar Jūsų institucijoje yra gaunami dokumentai (prašymai,skundai) iš piliečių arba valstybinių institucijų, kurie pasirašyti elektroniniu parašu?
- ☐ Taip
- ☐ Ne

2.Ar Jūs arba Jūsų institucija siunčia elektroninius dokumentus pasirašytus elektroniniu parašu?
- ☐ Taip
- ☐ Ne

3.Ar Jūsų institucija dalyvavo IVPK rengtame projekte, kurio metu išdalinti sertifikatai ir įranga elektroninio parašo formavimui ir tikrinimui?
- ☐ Taip
- ☐ Ne

4.Jei Jūsų institucijoje yra naudojama dokumentų valdymo sistema, įrašykite jos pavadinimą?
- ☐ Naudojama. Įrašykite sistemos pavadinimą, jei žinote:
- ☐ Nenaudojama.

5.Ar Jūsų institucijoje yra parengta tvarka, kuria piliečiai turėtų vadovautis norėdami pateikti prašymus ar skundus elektroniniu būdu ir pasirašytus elektroniniu parašu?
- ☐ Taip
- ☐ Ne

6.Jūsų manymu dėl kokių priežasčių elektroninis parašas nėra paplitęs Lietuvoje?

- ☐ Sunku pereiti nuo tradicinių popierinių dokumentų tvarkymo prie elektroninių
- ☐ Per sudėtingas naudojimosi procesas
- ☐ Nepasitikima elektroninio parašo infrastruktūra
- ☐ Mažas vartotojų kompiuterinis raštingumas

Kita priežastis:

7.Ar Jūsų institucijoje yra atsakomi piliečių kreipimaisi, kurie atsiunčiami elektroniniu paštu?
- ☐ Taip
- ☐ Ne

8.Ar Jums pavyko patikrinti su šia anketą atsiųsto failo „Laiskas.ddoc“ elektroninį parašą?
- ☐ Taip
- ☐ Ne
- ☐ Nebandžiau

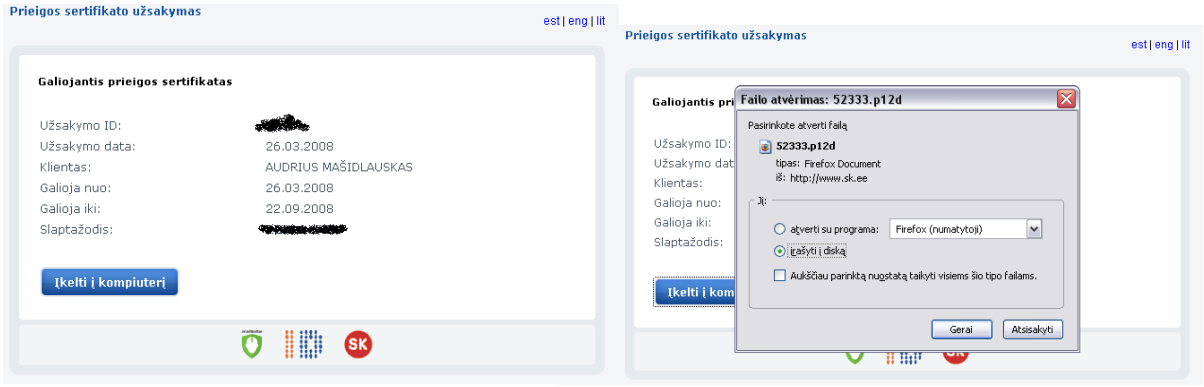
9.Ką Jūs manote apie elektroninį parašą? Įrašykite pilkame laukelyje.

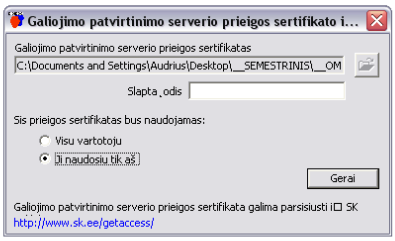
10.Kokiai atstovaujate institucijai?

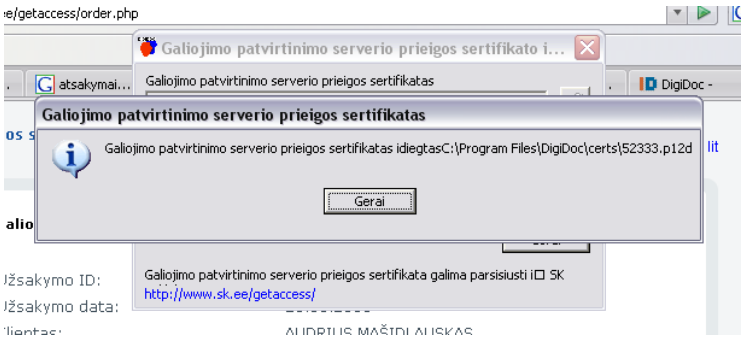
Jeigu Jūs naudojatės elektroniniu parašu, prašome pasirašyti šią užpildytą anketą ir atsiųsti elektroniniu paštu: Audrius.Masidlauskas@kf.stud.vu.lt. Iš anksto dėkui.

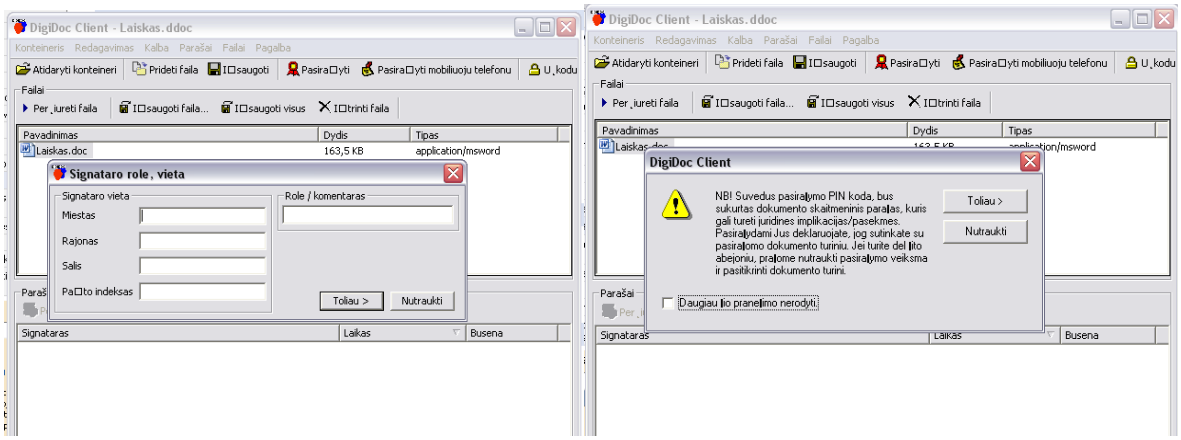
Jei Jums kiltų klausimų dėl anketos maloniai prašome kreiptis: Audrius Mašidlauskas,tel.:867347501,e.paštas: Audrius.Masidlauskas@kf.stud.vu.lt

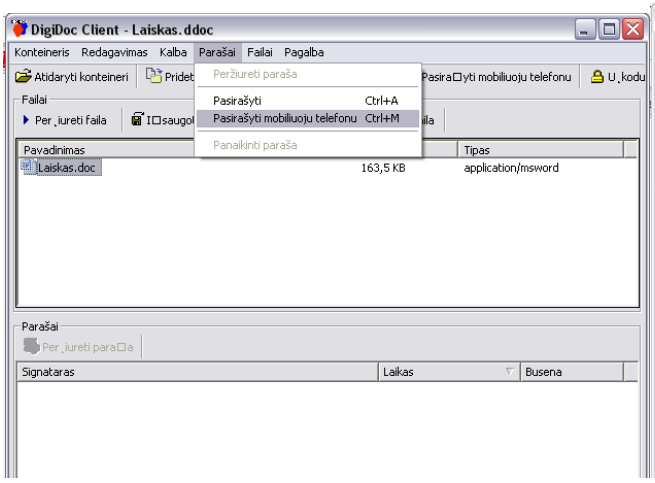
4 Priedas.

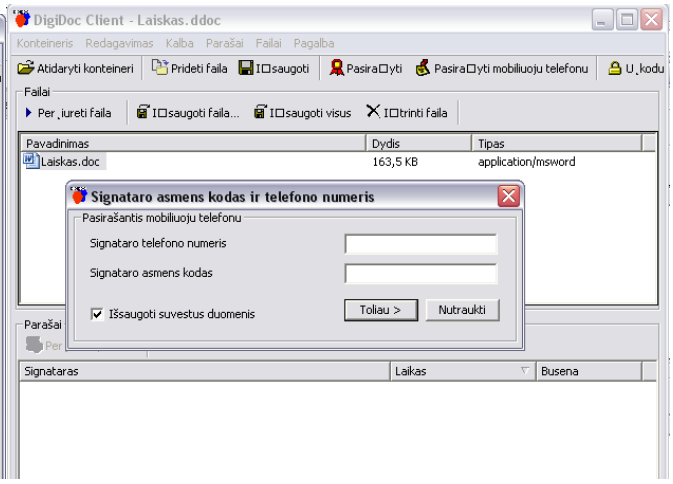

Prieigos sertifikato užsakymas
est | eng | lit
Galiojantis prieigos sertifikatas
Užsakymo ID:
Užsakymo data: 26.03.2008
Klientas: AUDRIUS MAŠIDLAUSKAS
Galioja nuo: 26.03.2008
Galioja iki: 22.09.2008
Slaptažodis:
Įkelti į kompiuterį
Failo atvėrimas: 52333.p12d
Pasirinkote atverti failą
52333.p12d
tipas: Firefox Document
iš: http://www.sk.ee
atverti su programa: Firefox (numatytoji)
Įrašyti į diską
Gerai
Atsisakyti

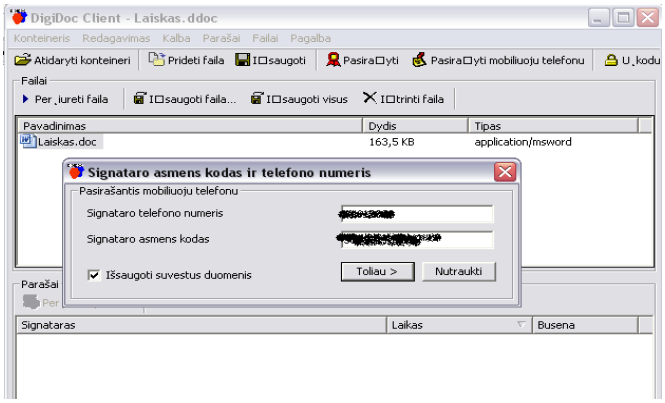

Galiojimo patvirtinimo serverio prieigos sertifikato i...
Galiojimo patvirtinimo serverio prieigos sertifikatas
Slaptažodis
Sis prieigos sertifikatas bus naudojamas:
Visu vartotoju
Gerai
Galiojimo patvirtinimo serverio prieigos sertifikata galima parsisiusti iČ SK
http://www.sk.ee/getaccess/

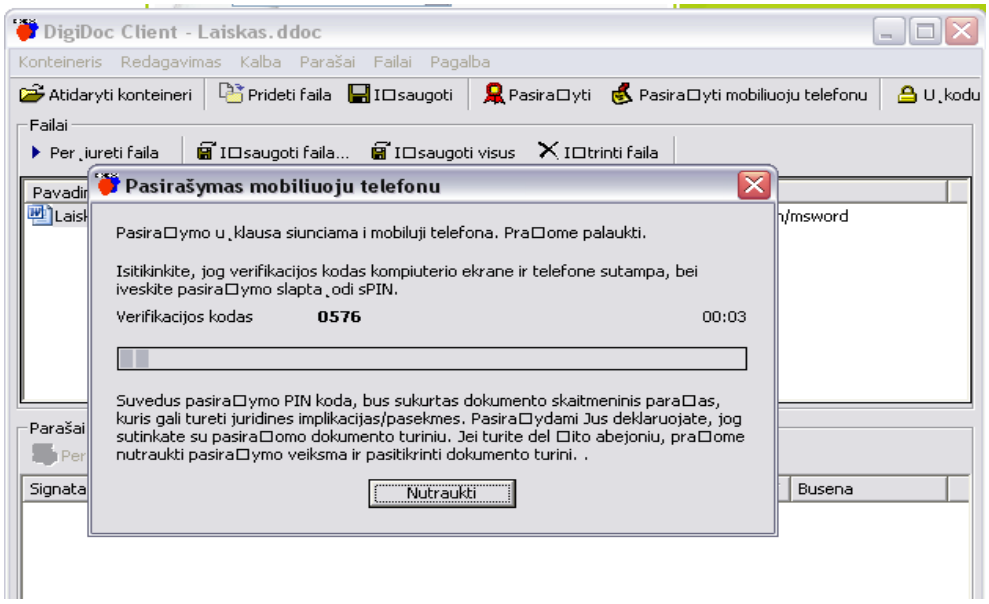

Galiojimo patvirtinimo serverio prieigos sertifikatas
Galiojimo patvirtinimo serverio prieigos sertifikatas idiegtasC:\Program Files\DigiDoc\certs\52333.p12d
Gerai
Galiojimo patvirtinimo serverio prieigos sertifikata galima parsisiusti iČ SK
http://www.sk.ee/getaccess/


DigiDoc Client - Laiskas.ddoc
Signataro role, vieta
Miestas
Rajonas
Salis
Toliau >
Nutraukti
DigiDoc Client
NB! Suvedus pasirašymo PIN kodą, bus sukurtas dokumento skaitmeninis parašas, kuris gali tureti juridines implikacijas/pasekmes. Pasirašydami Jus deklaruojate, jog sutinkate su pasirašomo dokumento turiniu. Jei turite dėl to abejonių, prašome nutraukti pasirašymo veiksmą ir pasitikrinti dokumento turinį.
Toliau >
Nutraukti
Daugiau šio pranešimo nerodyti


DigiDoc Client - Laiskas.ddoc
Konteineris Redagavimas Kalba Parašai Failai Pagalba
Peržiureti paraša
Pasirašyti Ctrl+A
Pasirašyti mobiliuoju telefonu Ctrl+M
Panaikinti paraša
Atidaryti konteineri
Failai
Pavadinimas
Tipas
Laiskas.doc
163,5 KB
application/msword
Parašai
Signataras
Laikas
Busena


DigiDoc Client - Laiskas.ddoc
Atidaryti konteineri
Failai
Pavadinimas
Dydis
Tipas
Laiskas.doc
163,5 KB
application/msword
Signataro asmens kodas ir telefono numeris
Pasirašantis mobiliuoju telefonu
Signataro telefono numeris
Signataro asmens kodas
Išsaugoti suvestus duomenis
Toliau >
Nutraukti
Parašai
Signataras
Laikas
Busena


DigiDoc Client - Laiskas.ddoc
Atidaryti konteineri
Failai
Pavadinimas
Dydis
Tipas
Laiskas.doc
163,5 KB
application/msword
Signataro asmens kodas ir telefono numeris
Pasirašantis mobiliuoju telefonu
Signataro telefono numeris
Signataro asmens kodas
Išsaugoti suvestus duomenis
Toliau >
Nutraukti
Parašai
Signataras
Laikas
Busena


DigiDoc Client - Laiskas.ddoc
Konteineris Redagavimas Kalba Parašai Failai Pagalba
Atidaryti konteineri
Prideti faila
Pasirašymas mobiliuoju telefonu
Failai
Parašai
Busena
Pasirašymas mobiliuoju telefonu
Pasirašymo užklausa siunciama i mobiluji telefona. Praðome palaukti.
Isitikinkite, jog verifikacijos kodas kompiuterio ekrane ir telefone sutampa, bei iveskite pasirašymo slaptažodi sPIN.
Verifikacijos kodas 0576 00:03
Suvedus pasirašymo PIN koda, bus sukurtas dokumento skaitmeninis parašas, kuris gali tureti juridines implikacijas/pasekmes. Pasirašydami Jus deklaruojate, jog sutinkate su pasirašomo dokumento turiniu. Jei turite del šito abejoniu, praðome nutraukti pasirašymo veiksma ir pasitikrinti dokumento turini. .
Nutraukti


DigiDoc Client
Laiskas.ddoc
Kontrolinis kodas:
0576
Operacija
ivykdyta

5 Priedas.

A	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	1.Ar Jūsų institucijoje yra gaunami dokumentai (prašymai,skundai) iš piliečių arba valstybinių institucijų, kurie pasirašyti elektroniniu parašu?			2.Ar Jūs arba Jūsų institucija siunčia elektroninius dokumentus pasirašytus elektroniniu parašu?			3.Ar Jūsų institucija dalyvavo IVPK rengtame projekte, kurio metu išdalinti sertifikatai ir įranga elektroninio parašo formavimui ir tikrinimui?		4.Jei Jūsų institucijoje yra naudojama dokumentų valdymo sistema, įrašykite jos pavadinimą?			5.Ar Jūsų institucijoje yra parengta tvarka, kuria piliečiai turėtų vadovautis norėdami pateikti		6.Jūsų manymu dėl kokių priežasčių elektroninis parašas nėra paplitęs Lietuvoje?				
	TAIP	NE	kaip dažnai per mėnesį	TAIP	NE	kaip dažnai per mėnesį	TAIP	NE	TAIP	PAVADINIMAS	NE	TAIP	NE	Sunku pereiti nuo tradicinių popierinių dokumentų tvarkymo prie elektroninių	Per sudėtingas naudojimosi procesas	Nepasitikima elektroninio parašo infrastruktūra	Mažas vartotojų kompiuterinis raštingumas	Kita priežastis:
	15,00%	85,00%	15,00%	15,00%	85,00%	2,50%	70,00%	30,00%	75,00%	0,00%	25,00%	15,00%	85,00%	55,00%	50,00%	35,00%	15,00%	
1 Institucija	1	0		1	0		1	0	1	Kontora	0	0	1	0	0	1	0	0
2 Institucija	0	1		0	1		1	0	1	Avilys	0	0	1	1	1	1	0	0
3 Institucija	0	1		0	1		0	1	0		1	0	1	1	0	0	0	0
4 Institucija	0	1		0	1		0	1	1		0	0	1	0	0	0	0	Tiesiog turėtų
5 Institucija	0	1		0	1		1	0	1	KONTOR/	0	0	1	1	0	0	1	Lietuvoje nėra
6 Institucija	0	1		0	1		1	0	1	kontora	0	1	0	1	1	1	1	0
7 Institucija	0	1		0	1		1	0	1	Avilys	0	0	1	1	1	1	0	0
8 Institucija	0	1		0	1		0	1	0		1	0	1	1	1	0	0	per mažai kom
9 Institucija	0	1		0	1		1	0	1	Testavimo bū		0	1	1	1	1	0	0
10 Institucija	0	1		0	1		1	0	1		0	0	1	0	0	1	0	0
11 Institucija	0	1		0	1		1	0	0		1	0	1	1	0	0	0	0
12 Institucija	0	1		0	1		1	0	1	Kontora		1	0	1	0	0	0	0
13 Institucija	0	1		0	1		1	0	0		1	0	1	0	1	0	0	0
14 Institucija	0	1		0	1		0	1	0		1	0	1	1	0	0	0	0
15 Institucija	0	1		0	1		0	1	1	DocLogix	0	0	1	1	0	0	0	0
16 Institucija	0	1		0	1		0	1	1	"@vilys"	0	0	1	0	1	0	0	0
17 Institucija	1	0	2	1	0	0,5	1	0	1	rasf	0	0	1	0	1	0	0	0
18 Institucija	1	0	1	0	1		1	0	1	Kontora	0	0	1	0	0	1	0	0
19 Institucija	0	1		1	0		1	0	1	Kontora	0	0	1	0	1	0	1	0
20 Institucija	0	1		0	1		1	0	1	II skynau	0	1	0	0	1	0	0	0
	3	17	3	3	17	0,5	14	6	#	0	5	3	17	11	10	7	3	3

5 Priedas (tęsinys).

A	W	X	Y	Z	AA	AD	AE	AF	AG	AH	AI	AJ
	7.Ar Jūsų institucijoje yra atsakomi piliečių kreipimaisi, kurie atsiunčiami elektroniniu paštu?		8.Ar Jums pavyko patikrinti su šia anketą atsiųsto failo „Laiskas.ddoc" elektroninį parašą?									
	TAIP	NE	TAIP	NE	NEBANDŽIAU		SEIMAS	VYRIAUSYBE	MINISTERIJA	ĮSTAIGA PRIE VYRIAUSYBĖS	ĮSTAIGA PRIE MINISTERIJOS	ATSKIRA INSTITUCIJA
	85,00%	15,00%	25,00%	45,00%	30,00%	0,00%	0,00%	5,00%	20,00%	10,00%	45,00%	20,00%
1 Institucija	1	0	1	0	0	0		1				
2 Institucija	1	0	0	0	1	0			1			
3 Institucija	0	1	0	0	1	0			1			
4 Institucija	1	0	0	1	0	0			1			
5 Institucija	e.para	1	1	0	0	0			1			
6 Institucija	1	0	0	1	0	0				1		
7 Institucija	1	0	0	0	1	0				1		
8 Institucija	1	0	0	1	0	0					1	
9 Institucija	1	0	1	0	0	0					1	
10 Institucija	1	0	0	1	0	0					1	
11 Institucija	1	0	1	0	0	0					1	
12 Institucija	1	0	1	0	0	0					1	
13 Institucija	1	0	0	1	0	0					1	
14 Institucija	1	0	0	1	0	0					1	
15 Institucija	1	0	0	1	0	0					1	
16 Institucija	1	0	0	1	0	0					1	
17 Institucija	1	0	0	0	1	0						1
18 Institucija	0	1	0	0	1	0						1
19 Institucija	1	0	0	0	1	0						1
20 Institucija	1	0	0	1	0	0						1
	17	3	5	9	6	0	0	1	4	2	9	4