MYKOLO ROMERIO UNIVERSITETAS
SOCIALINIŲ TECHNOLOGIJŲ FAKULTETAS
SKAITMENINIŲ TECHNOLOGIJŲ INSTITUTAS

OLGA KARPOVIČ

ELEKTRONINĖS ATPAŽINTIES PRIEMONĖS VIEŠAJAME SEKTORIUJE

Magistro baigiamasis darbas

Vadovė
Lekt. dr. R. Naujikienė

VILNIUS, 2014

MYKOLO ROMERIO UNIVERSITETAS
SOCIALINIŲ TECHNOLOGIJŲ FAKULTETAS
SKAITMENINIŲ TECHNOLOGIJŲ INSTITUTAS

ELEKTRONINĖS ATPAŽINTIES PRIEMONĖS VIEŠAJAME SEKTORIUJE

Elektroninio viešojo administravimo magistro baigiamasis darbas
Studijų programa 621N70005

Vadovė
Lekt. dr. R. Naujikienė
2014 ... ...

Recenzentas

2014 ... ...

Atliko
EVAmis2-01gr. stud.
O.Karpovič
2014 ... ...

Vilnius, 2014

TURINYS

ĮVADAS 9
1. ELEKTRONINIAI DOKUMENTAI IR JŲ YPATUMAI 12
1.1. Elektroninio dokumento samprata ir esminiai skirtumai 12
1.2. Elektroninių dokumentų privalomos savybės 15
2. ELEKTRONINIS PARAŠAS IR JO TAIKYMAS VIEŠOJO SEKTORIAUS VEIKLOJE 18
2.1. Elektroninio parašo samprata 18
2.2. Elektroninių parašų įvairovė: paprastas, saugus ir kvalifikuotas e. parašai 20
2.3. Grėsmės elektroninėje erdvėje – asmens tapatybės vagystė 34
3. ELEKTRONINIO PARAŠO INFRASTRUKTŪROS PLĖTRA 45
3.1. Elektroninio parašo naudojimas viešojo ir privataus sektoriaus veikloje 46
3.2. Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo prioritetinės veiklos kryptys 53
4. ELEKTRONINIO PARAŠO NAUDOJIMO VIEŠOJO SEKTORIAUS INSTITUCIJOSE VEIKLOS TYRIMAS 58
4.1. Tyrimo metodologija 58
4.2. Tyrimo duomenų analizė 61
IŠVADOS IR REKOMENDACIJOS 81
LITERATŪRA 85
ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS 95
SANTRAUKA LIETUVIŲ IR ANGLŲ KALBOMIS 97
PRIEDAI 99
1 priedas. Elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0 struktūra 99
2 priedas. Užregistruoto elektroninio dokumento, atitinkančio elektroniniu parašu pasirašyto elektroninio dokumento specifikaciją ADOC-V1.0, metaduomenys 100

3 priedas. Elektroninio parašo teisinis reglamentavimas 101
4 priedas. Biometrinių bruožų pasižymėjimo savybėmis suvestinė 102
5 priedas. Suklastoto internetinės bankininkystės tinklalapio, reikalaujančio įvesti prisijungimo slaptažodžius, fragmentas 103
6 priedas. Ekspertinio tyrimo anketos pavyzdys 104

LENTELĖS

1 lentelė. Kvalifikuoto elektroninio parašo teikėjų pasiūla viešajam sektoriui 31
2 lentelė. Mobilaus e. parašo teikėjų pasiūlos duomenys privatiems ir verslo klientams 32
3 lentelė. Pagrindiniai asmens duomenų apsaugos principai 35
4 lentelė. Tapatybės vagystės stadijų kriminalizavimas, remiantis LR baudžiamojo kodekso 166, 167, 182, 198, 198 (1), 198 (2), 207, 214, 215 ir 300 straipsniais 41
5 lentelė. Elektroninio parašo naudojimas aukščiausiuose valdžios institucijose 49
6 lentelė. E. parašo naudojimas e. dokumentų pasirašymui viešajame sektoriuje 50
7 lentelė. Elektroninio parašo naudojimas elektroninių paslaugų teikimui 50
8 lentelė. Elektroninio parašo taikymas privačiame sektoriuje 51
9 lentelė. Preliminarus tapatybės nustatymo Lietuvos e. valdžios vartų portale skirstymas, remiantis STORK klasifikacija 55
10 lentelė. Ekspertų vertinimo dėl e. parašo plėtrą skatinančių priemonių duomenys (rangai) ir grupiniai įverčiai 67
11 lentelė. Perskaičiuoti priemonių įverčiai ir jų bendroji suma 68
12 lentelė. E. parašo plėtrą skatinantys sprendimai, įverčių sumos ir reikšmingumo koeficientai pagal ekspertų vertinimus 68
13 lentelė. Ekspertų kliūčių vertinimo ir apskaičiuotų svorio k reikšmių rezultatai 78
14 lentelė. Ekspertų vertinimų apibendrintos išvados ir siūlymai 79

PAVEIKSLAI

1 pav. Įstaigos dokumentų valdymo sistema 13
2 pav. Elektroninio dokumento sandara 15
3 pav. Elektroninio dokumento savybės 16
4 pav. Elektroninio parašo rūšys ir jų teisinis reglamentavimas 21
5 pav. Elektroninių parašų įvairovė 22
6 pav. Elektroninio parašo simetrinio šifravimo sistema 23
7 pav. Reikalavimai saugiam elektroniniam parašui 24
8 pav. Informacijos siuntimo procesas, naudojant saugų elektroninį parašą 26
9 pav. Sertifikavimo centro struktūra 27
10 pav. Fiziologinių ir elgsenos asmens bruožų biometrija 28
11 pav. Sudarytų galiojančių kvalifikuotų sertifikatų skaičius 2009–2012 m. 30
12 pav. Tapatybės identifikavimas Elektroninių valdžios vartų portale 33
13 pav. Tapatybės nustatymas elektroninėje erdvėje 38
14 pav. Tapatybės vagystės trijų stadijų modelis 39
15 pav. Tapatybės vagystės stadijų kriminalizavimas konvencijoje dėl elektroninių nusikaltimų 39
16 pav. Tapatybės vagystės elektroninėje erdvėje įvykdymo būdų tendencijos 44
17 pav. 2011–2012 m. metinių pajamų deklaracijų statistika 47
18 pav. Elektroniniu parašu pasirašytų ir pateiktų elektroninių dokumentų statistika 49
19 pav. Saugaus tarpvalstybinio tapatybės nustatymo pilotinio projekto STORK veikimo schema 56
20 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus 60
21 pav. Konkordancijos koeficiento W skaičiavimas PSPP terpėje 62
22 pav. Ekspertinio vertinimo ekspertų grupės sudėtis 62
23 pav. Efektyvus e. parašo taikymo viešojo sektoriaus veikloje modelis 66
24 pav. Sprendimai dėl e. parašo plėtros 74
25 pav. Ekspertų įvertintų kliūčių dėl e. parašo plėtros eiliškumas 79

SANTRUMPOS

CK	Lietuvos Respublikos Civilinis kodeksas
CSES	Strategijos ir vertinimo paslaugų centras (angl. Centre for Strategy & Evaluation Services)
CVP IS	Centrinė viešųjų pirkimų informacinė sistema
Direktyva	Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos
DNS	Sričių vardų serveris (angl. Domain Name Server)
DVS	Dokumentų valdymo sistema
EAIS	Elektroninio archyvo informacinė sistema
EBPO	Ekonominio bendradarbiavimo ir plėtros organizacija
E. dokumentas	Elektroninis dokumentas
eID	Elektroninė atpažintis (angl. Electronic Identity)
ELPAS	Elektroninio pasirašymo sistema
E. parašas	Elektroninis parašas
E. paslauga	Elektroninė paslauga
EPĮ	Elektroninio parašo įstatymas
E. pristatymo sistema	Nacionalinė elektroninių pranešimų ir elektroninių dokumentų pristatymo fiziniams ir juridiniams asmenims informacinė sistema
ESKIS	Mokesčių mokėtojų elektroninio švietimo, konsultavimo ir informavimo paslaugų sistema
Europos Bendrijų Komisijos ataskaita	Europos Bendrijų Komisijos ataskaita „Dėl Bendrijos elektroninių parašų reguliavimo sistemos veikimo“
E. valdžia	Elektroninė valdžia
FVAS	Finansų valdymo ir apskaitos sistema
GRT prie VRM	Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos
ICA	Tarptautinė archyvų taryba (angl. International Council on Archives)
IPT	Interneto paslaugų teikėjas
IRT	Informacinės ir ryšių technologijos
IS	Informacinė sistema

ISO	Tarptautinė standartizacijos organizacija (angl. International Organization for Standartization)
IT	Informacinės technologijos
IVPK prie SM	Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos
PEPS	Bandomoji Europinė pasitikėjimo sistema (angl. Pan European Proxy System)
PKI	Viešojo rakto infrastruktūra (angl. Public Key Infrastructure)
RC	Valstybės įmonė Registrų centras
RRT	Lietuvos Respublikos ryšių reguliavimo tarnyba
SODRA	Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos
SSC	UAB „Skaitmeninio sertifikavimo centras“
STORK	Saugus tarpvalstybinis tapatybės nustatymas (angl. Secure identity across borders linked)
VAIISIS	Viešojo administravimo institucijų informacinių sistemų interoperabilumo sistema
VIISP	Valstybės informacinių išteklių sąveikumo platforma
VMI	Valstybinė mokesčių inspekcija
VPT	Viešųjų pirkimų tarnyba
VPVI	Viešosios politikos ir vadybos institutas
VSAKIS	Viešojo sektoriaus apskaitos ir ataskaitų konsolidavimo informacinė sistema

ĮVADAS

Darbo aktualumas. Siekiant užtikrinti efektyvų šiandieninės valstybės valdymą, tai įvykdyti neįmanoma be informacinių technologijų ir nuotolinio ryšio priemonių, skatinančių viešojo sektoriaus institucijas diegti naujus darbo ir valdymo metodus. Naujos technologijos iš esmės keičia valstybės ir savivaldos institucijų veiklą, sudaro sąlygas ir užtikrina geresnę viešųjų paslaugų kokybę, skaidresnę veiklą ir sumažina korupcijos atvejus viešojo sektoriaus veikloje. Siekiant užtikrinti didesnį viešojo administravimo veiksmingumą, svarbiais aspektais tampa dokumentų perkėlimas į e. erdvę, dokumentų keitimasis tarp valdžios institucijų e. forma bei e. parašo plėtra (Ožalienė, Šaparnienė, 2008, p. 199).

Sparčiai vystantis informacinėms technologijoms, vartotojai pageidauja vis daugiau viešųjų paslaugų gauti elektroniniu būdu, nepriklausomai nuo jų buvimo vietos. Tai skatina centrines, o ypač vietos valdžios institucijas įgyvendinti elektroninės valdžios projektus. Elektroninė valdžia – tai tradicinės valdžios tąsa, skirta įgyvendinti valstybės funkcijas, tame tarpe ir teikti elektroniniu būdu viešąsias paslaugas gyventojams ir verslo atstovams visuose lygiuose (Limba, 2009, p. 30).

Elektroninių dokumentų plėtrą Europoje skatina didėjantis privalomų nuostatų įgyvendinimas, kurios skirtos privataus ir viešojo sektoriaus institucijoms. Todėl vis daugiau įstaigų privalo įgyvendinti parengtas ES strategijas ir peržiūrėti ilgalaikių duomenų saugojimo būdus bei paiešką. Nacionalinėje Lisabonos strategijos įgyvendinimo programoje taip pat įtvirtinta būtinybė, naudojant informacines ir ryšių technologijas (IRT), sudaryti galimybes kelti darbuotojų kompetenciją ir socialinę sanglaudą, modernizuoti viešąjį administravimą, skatinti informacinėmis technologijomis paremtą ekonomiką. Analogiški tikslai išdėstyti ir Lietuvos informacinės visuomenės plėtros startegijoje, kurioje patvirtinama IRT teikiamių galimybių naudojimo reikšmė (Ožalienė, Šaparnienė, 2008, p. 200).

Darbo problema. Nepakankama elektroninio parašo plėtra viešajame sektoriuje daro neigiamą įtaką naujiems organizaciniams, kvalifikaciniams, technologiniams sprendimams, apsunkina inovatyvių procesų diegimą bei mažina viešojo administravimo institucijų darbo efektyvumą.

Darbo objektas ir dalykas. E. parašo naudojimo viešojo sektoriaus veikloje probleminiai aspektai ir jo taikymo kliūtys.

Darbo tikslas – nustatyti e. parašo taikymo kliūtis ir skatinamuosius veiksnius viešajame sektoriuje.

Uždaviniai. Tikslui pasiekti buvo iškelti šie uždaviniai:

1. Pateikti e. dokumento sampratą, savybes, kurios užtikrintų elektroninio dokumento lygiavertiškumą tradicinio dokumento atžvilgiu, ir esminius e. dokumentų valdymo skirtumus;

2. Išanalizuoti ir įvertinti elektroninių parašų rūšis ir jų technologiją bei naudojimo grėsmes;
3. Ištirti e. parašo taikymo viešojo sektoriaus veikloje mastą ir prioritetines veiklos kryptis;
4. Atlikti ekspertinį e. parašo taikymo viešajame sektoriuje tyrimą – remiantis tyrimo rezultatais, nustatyti skatinamuosius veiksnius ir kliūtis, darančias įtaką e. parašo naudojimui viešajame sektoriuje, pateikti veiksmingą e. parašo taikymo modelį.

Autoriai, tyrinėję darbo objektą. Elektroninio parašo taikymo problematika viešajame sektoriuje nėra plačiai išnagrinėta. Didžioji dalis informacijos yra apie elektroninius dokumentus: jų savybes, saugojimą, apie elektroninį parašą kaip svarbų elektroninio dokumento rekvizitą. Šią temą nagrinėję mokslininkai yra dr. I. Petravičiūtė ir jos disertacija „Elektroninių dokumentų Lietuvos nacionaliniame dokumentų fonde valdymas“, Audronės Ožalienės magistro darbas „Elektroninių dokumentų valdymas viešajame sektoriuje: plėtros galimybių analizė“, Mindaugo Apučio magistro darbas tema „Oficialių elektroninių dokumentų, atitinkančių ADOC specifikacijos reikalavimus, valdymas“.

Mokslo darbuose elektroninio parašo tematika daug dėmesio skiriama elektroninio parašo teisinio reglamentavimo analizei. Elektronino parašo teisinis reglamentavimas, elektroninio parašo vertė teisminiuose procesuose ir praktinio įgyvendinimo aspektai pateikiami mokslininkų doc. dr. Rimanto Garucko, prof. habil. dr. Adolfo Kaziliūno darbuose bei studentų Editos Šileikaitės, Audriaus Mašidlausko ir Luko Šidlausko magistro diplominiuose darbuose.

Šiame magistro baigiamajame darbe autorė analizuoja bei lygina mokslinėse publikacijose, mokslo darbuose ir studijuose pateiktą informaciją (mokslinių tyrimų rezultatus), bei pateikia apibendrinimus, išryškina problemines e. parašo naudojimo sritis.

Mokslinis naujumas. Moksliniuose šaltiniuose nepakankamai ištirta ir pateikta informacija apie tikslinių e. parašų rūšis bei jų ribas, nėra numatyti aiškūs kriterijai kiekvienos rūšies elektroniniam parašui. Autorė atlieka ekspertinį e. parašo taikymo viešajame sektoriuje tyrimą, turėdama tikslą išaiškinti, kodėl elektroninis parašas nėra plačiai naudojamas viešajame sektoriuje. Šio darbo mokslinis naujumas yra tai, kad literatūros analizė leido susisteminti naujausią mokslinę informaciją, o atliktas kokybinis tyrimas leido pateikti priemones, kurios skatintų e. parašo naudojimą viešojo sektoriaus institucijų darbe, siekiant ekonomiško išlaidų modelio. Darbe pateikta tyrimo rezultatais grindžiama informacija, numato kliūtis ir skatinančiuosius veiksnius e. parašo platesniam naudojimui viešojo administravimo įstaigose.

Darbo hipotezė. E. parašo naudojimas viešajame sektoriuje pagerins viešojo administravimo veiklą.

Darbo struktūra. Magistro baigiamąjį darbą sudaro keturios pagrindinės struktūrinės dalys-skyriai: 1) elektroniniai dokumentai ir jų ypatumai, kuriame aptariama e. dokumento samprata, savybės ir jų valdymas; 2) elektroninio parašo taikymo viešajame sektoriuje teoriniai aspektai ir grėsmės elektroninėje

erdvėje. Skyriuje apibrėžiama elektroninio parašo sąvoka, elektroninio parašo rūšys ir jų taikymas viešajame sektoriuje, asmens tapatybės vagystės rizika; 3) e. parašo naudojimo viešajame sektoriuje atvejai ir prioritetinės veiklos kryptys; 4) e. parašo taikymo viešojo sektoriaus veikloje empirinis tyrimas, kuriuo remiantis bus nustatytos elektroninio parašo taikymo kliūtys ir skatinamieji veiksniai.

Empirinis tyrimas

Tyrimo problema. Nepakankamai efektyvus IT panaudojimas viešojo sektoriaus darbe. Norint praplėsti e. parašo naudojimą viešajame sektoriuje, tenka nugalėti egzistuojančias kliūtis, kurios daro įtaką efektyviam viešojo administravimo institucijų darbui.

Tyrimo hipotezės:

1. Elektroninio parašo spartesnę plėtrą viešajame sektoriuje stabdo nepakankama vadovaujančių institucijų skatinimo politika taikyti e. parašą viešojo sektoriaus darbe.
2. Elektroninis parašas platesniu mastu nenaudojamas dėl valstybės tarnautojų pasipriešinimo kaitai žmogiškųjų veiksnių – informacijos, kvalifikacijos ir motyvacijos stokos.

Tyrimo objektas ir dalykas. Objektas – e. parašo taikymas Lietuvos viešajame sektoriuje esama padėtis. Tyrimo dalykas – priemonės ir būdai kaip organizuoti platesniu mastu e. parašo taikymo modelį, numatantį e. parašo plėtrą.

Tyrimo tikslas. Išplėsti elektroninio parašo naudojimą viešajame sektoriuje.

Tyrimo uždaviniai. Tikslo įgyvendinimui buvo iškelti šie uždaviniai:

1. Nustatyti ekspertų atrankos sistemą;
2. Parengti pasirinkto tyrimo metodo klausimyną;
3. Apklausti pasirinktus ekspertus;
4. Atlikti tyrimo rezultatų kokybinę ir kiekybinę analizes;
5. Išanalizavus gautus duomenis, nustatyti e. parašo taikymo viešajame sektoriuje galimybes.

Tyrimo metodai. Tyriamojo darbo problemos analizei ir sprendimui buvo pasirinkti teoriniai ir empiriniai metodai. Informacijai rinkti buvo naudojama mokslinių straipsnių, publikacijų, įstatymų, ataskaitų ir standartų analizė. Taikomi metodai – dokumentų, mokslinės literatūros ir lyginamoji analizė, apibendrinimo metodas. Darbo problemai tirti buvo pasirinktas kokybinio tyrimo metodas – ekspertų apklausa, šios apklausos informacijos analizė ir išvadų formulavimas.

Darbo praktinė reikšmė. Darbas yra naudingas šioms auditorijoms: 1) fiziniams ir juridiniams asmenims, siekiantiems ir gebantiems naudoti e. parašą darbinėje ir asmeninėje veikloje, norintiems užtikrinti didesnį e. duomenų saugumą; 2) mokslininkams, kurie tiria elektroninio parašo taikymą ir su tuo susijusias problemas viešajame sektoriuje.

1. ELEKTRONINIAI DOKUMENTAI IR JŲ YPATUMAI

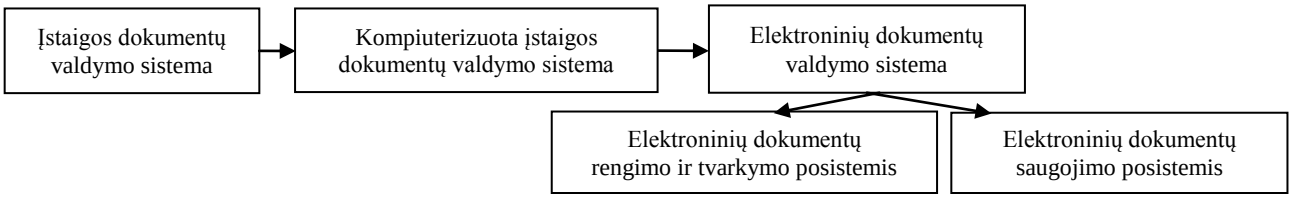
Dokumentai naudojami įvairiuose fizinio ir juridinio asmens ar organizacijų veiklos srityse. Jų dėka fiksuojama veikla, priimti sprendimai, perduodama svarbi informacija, panaudojami pagrindžiant svarbius faktus ar veiklą. Taigi, tai priemonė valstybės uždaviniams reglamentuoti ir užtikrinti visuomenės reikmes. Dokumentas visuomet buvo siejamas su laikmena ir buvo suvokiama, kad tai yra materialus, vientisas ir nedalomas objektas, kurio turinys (perduodama informacija) nėra atskiriamas nuo materialios formos laikmenos. Tačiau naujos technologijos atvėrė kelią kurti ir perduoti elektroninę informaciją e. aplinkoje, kuri panaikina materialaus objekto sampratą ir svarbiausiu dalyku tampa nebe laikmena, o dokumento turinys. E. dokumentų atsiradimas praplėtė dokumento medžiagos pateikimo būdus. Šių dokumentų turinys gali būti ne tik tekstinė, bet ir vaizdinė, garsinė medžiaga ar kt. Toks dokumentas gali būti kūriamas panaudojant kelis skirtingus įrašus. Todėl, remiantis tradicinio dokumento samprata, neapimant laikmenos, reikia iš naujo suformuoti dokumento sampratą ir savybes, kurių dėka galima būtų aiškiai nustatyti, kuri e. informacija gali būti laikoma e. dokumentu ir būti lygiavertė tradiciniam dokumentui.

1.1. Elektroninio dokumento samprata ir esminiai skirtumai

Elektroninio dokumento teisinį pripažinimą tarptautiniu mastu labiausiai skatino Jutos (1995 m., JAV) ir Vokietijos (1997 m.) elektroninio parašo įstatymas bei Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos, kurioje elektroninio dokumento forma yra prilyginama rašytiniam dokumentui (Limba, Novikovienė, 2012, p. 491). Taigi, 2001 m. Tarptautinė standartizacijos organizacija patvirtino tarptautinį dokumentų vadybos standartą ISO-15489, kuriame buvo nustatyti esminiai dokumentų rengimo principai bei reikalavimai dokumentams tokiu būdu atvėrę galimybę organizacijų veikloje naudoti ir elektroninius dokumentus. Remiantis šiuo standartu, dokumentas – tai fiksuota informacija arba objektas, kuris gali būti vertinamas kaip atskiras vienetas. Tuo tarpu oficialus dokumentas – tai organizacijos vykdomų įsipareigojimų arba juridinio asmens veiklos metu parengta, gauta ir išsaugota informacija kaip įrodymo patvirtinimas. Svarbiausia, kad dokumento struktūra išliktų nepakitusi, t.y. jo formato ir sudedamųjų dalių visuma (Petravičiūtė, 2005, p. 1). Richard'o Pearce-Moses dokumento apibrėžimas yra labai panašus ir lengvai pritaikomas elektroniniams dokumentams: dokumentas – tai informacija arba duomenys, kurie užfiksuojami bet kokioje laikmenoje,

apimantys turinį, kontekstą ir struktūrą (Kontrimavičienė, 2012, p. 143). Taigi elektroninis dokumentas – tai fizinio ar juridinio asmens veiklos metu parengta arba gauta fiksuota informacija, kurios turinys, struktūra ir kontekstas yra pakankamas veiklai įrodyti. Trumpiau tariant, elektroninis dokumentas – tai elektroninė informacija, kuri atitinka įprasto rašytinio dokumento funkcijas elektronine forma (Davidavičienė ir kt., 2009, p. 446). Dar reikėtų pabrėžti, kad toks su įstaigos veikla susijęs jos parengtas ar gautas dokumentas privalo būti rengiamas, perduodamas ir saugomas panaudojant informacines technologijos priemones, būtinai įtrauktas į įstaigos dokumentų apskaitos sistemą ir pasirašytas elektroniniu parašu (Dzemydienė, Naujikienė, 2005, p. 143). Visų šių autorių nuomones tiksliai atspindi elektroninio dokumento apibrėžimas, 2010 m. įtrauktas į LR dokumentų ir archyvų įstatymą: elektroninis dokumentas – tai fizinio ar juridinio asmens norminių teisės aktų nustatyta tvarka bei informacinių technologijų priemonių pagalba sudarytas, patvirtintas ar gautas dokumentas, kuris pasirašytas teisinę galią turinčiu elektroniniu parašu (Valstybės žinios, 2010, Nr. 79-4055). Šiuo metu jau priimti ir kiti įstatymai, reikalingi e. dokumento naudojimui užtikrinti organizacijos veikloje: 2008 m. patvirtintas elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos reikalavimų aprašas, 2011 m. įsigaliojo Dokumentų rengimo taisyklės ir Dokumentų tvarkymo ir apskaitos taisyklės, kuriuose įtvirtintas elektroninių dokumentų rengimas ir tvarkymas (IVPK, VPVI, 2012, p. 147–148), 2012 m. patvirtintos Elektroninių dokumentų valdymo taisyklės ir Dokumentų saugojimo taisyklės (reglamentuojant ir e. dokumentų saugojimą) (Lietuvos vyriausiojo archyvaro tarnyba, 2013). Pasinaudojus ES struktūrinių fondų paramos lėšomis, sukūrta elektroninio archyvo informacinė sistema (EAIS), o pagal Žmogiškųjų išteklių plėtros veiksmų programos prioritetą „Administracinių gebėjimų stiprinimas“ buvo skirtos lėšos valstybės institucijų ir įstaigų dokumentų valdymo sistemoms (IVPK, VPVI, 2012, p. 147–148).

Siekiant užtikrinti e. dokumentų apyvartą, į įstaigos dokumentų valdymo sistemą reikia įtraukti e. dokumentų valdymo sistemą (Petravičiūtė, 2005, p. 3; Valstybės žinios, 2012, Nr. 3-104) (žr. 1 pav.).



Šaltinis: sudaryta pagal Lukšaitė, Jodinskė, 2011; Valstybės žinios, 2006, Nr. 7-268.

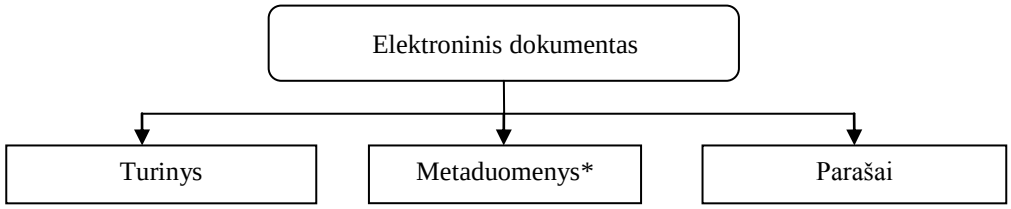
1 pav. Įstaigos dokumentų valdymo sistema

Elektroninių dokumentų valdymo sistema gali būti pripažinta efektyvia, jei užtikrina šių funkcijų veikimą (Jodinskė, 2013, p. 28–29; Valstybės žinios, 2012, Nr. 3-104):

1. Turi būti užtikrinta galimybė valdyti (t.y. rengti, tvarkyti, įtraukti į apskaitą, saugoti ar kt.) elektroninius dokumentus, atitinkančius bent vieną Lietuvos vyriausiojo archyvaro patvirtintų ar su šia įstaiga suderintų elektroninio dokumento specifikacijų;
2. Leidžiama patikrinti e. dokumento atitikimą specifikacijoje nustatytiems reikalavimams;
3. Turi būti įdiegtos e. parašo formavimo ir tikrinimo priemonės (specifikacijų ir elektroninio parašo taisyklių nustatyta tvarka), galimybė išsaugoti elektroninio parašo galiojimo įrodymus;
4. Turi būti užtikrinta, kad to pačio e. dokumento negalima būtų užregistruoti antrą kartą;
5. Turi būti suteikta galimybė atlikti paiešką visuose e. dokumentų valdymo sistemos pakopose, t.y. e. dokumentų, metaduomenų bei kt., įdiegtas vykdytos paieškos ataskaitų pateikimas;
6. Leidžiama suformuoti visų elektroninių dokumentų perkėlimo metu atliktų veiksmų sąrašą;
7. Draudžiama sunaikinti arba kitaip pašalinti e. bylas, jos tomus bei jiems priklausančius elektroninius dokumentus ir jų metaduomenys, jei elektroninės bylos, jos tomo metaduomenyse nėra įvesta informacija dėl patvirtinto elektroninių dokumentų panaikinimo akto.

Šiuo metu Lietuvoje nemažai įmonių gali pasiūlyti modernizuotas dokumentų valdymo sistemas, skirtas tvarkyti ir saugoti elektroninius dokumentus, t.y. Dovas, Smart Docs, DocLogix, Doclead, bet labai maža dalis šių sistemų atitinka visus nustatytus reikalavimus, užtikrina elektroninio parašo identifikavimo galimybes, atitinka dokumentų rengimo standartus bei kitas savybes, remiantis LR teisės aktais. Siekiant valstybinės įstaigos veikloje įgyvendinti elektroninių dokumentų valdymą ir tokiu būdu pagerinti veiklos efektyvumą, visus veiksmus reikėtų koordinuoti su kitomis institucijomis, norint užtikrinti skirtingų institucijų sistemų tarpusavio suderinamumą (Ožalienė, Šaparnienė, 2008, p. 201).

Bendruosius elektroninio dokumento struktūros reikalavimus nustato Elektroninių dokumentų specifikacijų reikalavimų aprašas, kurį įsakymu tvirtina Lietuvos vyriausiasis archyvaras (žr. 2 pav.) (Jodinskė, 2013, p. 29). Šiuo metu patvirtinta elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0, kuri plačiausiai naudojama Lietuvos viešojo sektoriaus įstaigose (žr. 1 priedą). Elektroniniai dokumentai, parengti pagal šią specifikaciją, yra prilyginami rašytiniams dokumentams. Taip pat vyksta diskusijos dėl elektroninio dokumento pdf specifikacijos ir dėl rašytiniams dokumentams neprilyginamų elektroninių dokumentų (garso, vaizdo, brėžinių) specifikacijų įteisinimo galimybių (Jodinskė, 2013, p. 21).



**Šaltinis:* *Metaduomenys* – struktūrizuoti duomenys, kurie aprašo e. dokumento sandarą, aplinką ir valdymo ypatumus visą dokumento gyvavimo laiką, tai kontekstinė informacija, pateikta atskirai nuo e. dokumento turinio (žr. 2 priedą).

Šaltinis: sudaryta pagal Valstybės žinios, 2008, Nr. 118-4488.

2 pav. Elektroninio dokumento sandara

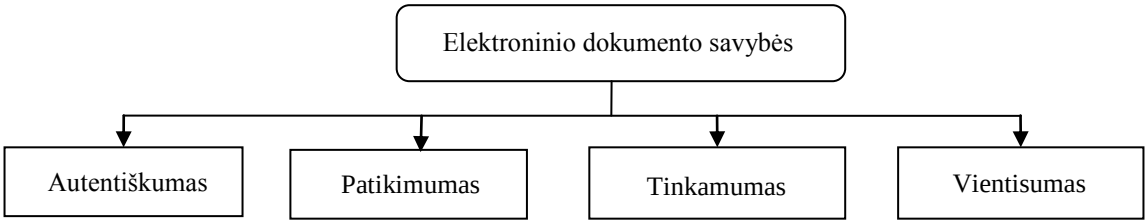
Apibendrinus pateiktą medžiagą, galima teigti, kad *elektroninis dokumentas* – fizinio ar juridinio asmens informacinių technologijų priemonių pagalba sudarytas ar gautas elektroninis dokumentas, pasirašytas teisinę galią turinčiu elektroniniu parašu, kurio turinys, struktūra ir kontekstas (metaduomenys) yra pakankami veiklai įrodyti. *Oficialus elektroninis dokumentas* – tai organizacijos vykdomų įsipareigojimų arba juridinio asmens veiklos metu informacinių technologijų pagalba parengtas arba gautas elektroninis dokumentas, kuris pasirašytas teisinę galią turinčiu elektroniniu parašu ir jo turinys, struktūra ir kontekstas (metaduomenys) yra pakankami veiklai įrodyti bei įtrauktas į įstaigos dokumentų valdymo sistemą. Elektroninių dokumentų naudojimo plėtrą užtikrina šių dokumentų valdymui įtvirtinta teisinė bazė, sukurta elektroninio archyvo informacinė sistema ir ES lėšų skirymas dokumentų valdymo sistemoms. Skirtingai nuo tradicinio dokumento, elektroninių dokumentų valdymui turi būti įrengta elektroninių dokumentų valdymo sistema, remiantis Elektroninių dokumentų valdymo taisyklėse įvardintais reikalavimais. Elektroninio dokumento sandarą reglamentuoja Elektroninių dokumentų specifikacijų reikalavimų aprašas, kurį įsakymu tvirtina Lietuvos vyriausiasis archyvaras. Dabartiniu metu patvirtinta elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0, kuri prilyginama rašytiniams dokumentams.

1.2. Elektroninių dokumentų privalomos savybės

Elektroninių dokumentų naudojimas paskatino įvertinti ir jų patikimumą. Kadangi kiekvienas dokumentas turi patvirtinti atliktą veiksmą, todėl jo struktūros ir sudedamųjų dalių visuma turi išlikti nepakitusi (Limba, Novikovienė, 2012, p. 489). Remiantis šiuo reikalavimu, privalomos elektroninio dokumento savybės, suteikiančios galimybę identifikuoti dokumentą bei užtikrinančios lygiavertiškumą tradicinio rašytinio dokumento atžvilgiu, yra autentiškumas, patikimumas, tinkamumas ir vientisumas

(Davidavičienė ir kt., 2009, p. 446; Limba, Novikovienė, 2012, p. 489; International Council on Archives (ICA), 2008, p. 13; International Organization for Standardization (ISO), 2001, p. 7) (žr. 3 pav.).

Elektroninis dokumentas, kaip ir tradicinis dokumentas, gali būti pateikiamas kaip įrodymas, faktams pagrįsti. Todėl svarbu tampa užtikrinti tokio dokumento autentiškumą (Davidavičienė ir kt., 2009, p. 447; Limba, Novikovienė, 2012, p. 489). Autentišku laikomas toks dokumentas, kuris nėra piktavališkai arba netyčia pakeistas ir turi visus būtinus atributus dokumento autoriui nustatyti (Davidavičienė ir kt., 2009, p. 447).



Šaltinis: sudaryta autorės; pagal Davidavičienė ir kt., 2009, p. 446; Limba, Novikovienė, 2012, p. 489.

3 pav. Elektroninio dokumento savybės

Remiantis ISO standartu, autentiškumo prasmė yra analogiška: autentišku yra įvardinamas dokumentas, kurį galima įrodyti, kad pradinis ir dabartinis dokumento originalas yra nepakitę bei dokumento autorius ir siuntėjas ar dokumento kūrėjas nuo dokumento gyvavimo iki atitinkamo momento yra tas pats asmuo (ISO, 2001, p. 7). Su šiuo autentiškumo apibrėžimu sutinka ir Tarptautinė archyvų taryba (ICA, 2008, p. 13). Svarbu paminėti, kad siekiant užtikrinti dokumentų autentiškumą, reikia įdiegti sistemos kontrolę, kuri užtikrintų elektroninio dokumento apyvartos fiksavimą (Limba, Novikovienė, 2012, p. 489). Tarptautinė archyvų taryba ir daugelis mokslininkų teigia, kad elektroninių dokumentų autentiškumui užtikrinti svarbu vaidmenį atlieka elektroninis parašas (Davidavičienė ir kt., 2009, p. 447; ICA, 2008, p. 16). Siekiant užtikrinti elektroninio dokumento autentiškumą, kompiuterių tinkluose vykdomas duomenų kodavimas, naudojant šifravimo sistemas ir (ar) elektroninį parašą. Elektroninis dokumentas saugomas ar perduodamas iš pradžių įvykdžius užšifravimą tam tikru raktu, o tokį dokumentą perskaityti gali atitinkamą dešifravimo raktą turintys asmuo. Tai leidžia įvykdyti atitinkamas funkcijas (Davidavičienė ir kt., 2009, p.447):

- užtikrinti reikalingą konfidencialumo lygį bei sumažinti neteisėtos prieigos prie duomenų galimybes;
- užtikrinti dokumento autentiškumą ir vientisumą;

- užtikrinti dokumento autoriaus identifikavimą;
- užtikrinti veiksmingą duomenų kodavimą, juos perduodant.

Taigi, apibendrinus mokslininkų ir tarptautinių organizacijų nuomones, galima teigti, kad elektroninio dokumento autentiškumas lemia šių elementų užtikrinimą: turinio ir dokumento autoriaus nekintamumą laiko ir erdvės atžvilgiu.

Elektroninio dokumento patikimumas prilyginamas dokumento turinio patikimumui, užtikrinant išsamius ir tikslius faktus, sandorius, veiklą, kurie gali būti panaudojami tolesnėje veikloje arba sandoriuose. Dokumentai turi būti sukurti sandorio arba įvykio metu tų asmenų, kurie turi reikalingų žinių apie vykstantį procesą (ISO, 2001, p. 7; ICA, 2008, p. 13).

Vientisumas užtikrina, kad dokumentas yra užbaigtas ir negali būti pakeistas. Taigi yra apsaugotas nuo neteisėto pakeitimo, išskyrus tuos atvejus, kai nustatyta, kokius papildymus ar pastabas leidžiama atlikti po dokumento parengimo ir asmenys, įgalioti tai įvykdyti (ISO, 2001, p. 7).

Elektroninio dokumento savybė – tinkamumas naudoti. Tinkamu naudoti gali būti įvardinamas tik toks dokumentas, kai galima nustatyti dokumento saugojimo vietą, jį rasti, pateikti tretiesiems asmenims ir suprasti visą dokumento egzistavimo laiką, ir turi būti išsaugoti visi ryšiai, susiję su veikla, iš kurios kilo pats dokumentas (ISO, 2001, p. 7).

Elektroninio dokumento patikimumas yra užtikrinamas dokumento sudarymo metu, o autentiškumas, vientisumas ir tinkamumas naudoti turi būti išsaugotas dokumento perdavimo proceso metu, įvertinus erdvės ir laiko atvejus.

Apibendrinus pateiktą medžiagą, galima išskirti vieną pagrindinę savybę iš šių keturių ir tai yra autentiškumas: ši savybė užtikrina dokumento turinio originalumą, dokumento autoriaus nekintamumą. Pasak Limbos ir Novikovienės (2012), ši savybė taip pat yra svarbiausia, nes užtikrina turinio nekeičiamumą, leidžia nustatyti autorių, tikslų dokumento sukūrimo laiką (p. 490). Elektroninio dokumento autentiškumui užtikrinti, reikia naudoti teisinę galią turinčius elektroninius parašus. Naudojant saugius elektroninius parašus, elektroninis dokumentas, siunčiamas kompiuteriniu tinklu, užšifruojamas tokiu būdu, kad neįmanoma jo atkoduoti, o pabandžius pakeisti pranešimo turinį ar parašą, šis virsta nesuprantamų simbolių virtine (Davidavičienė ir kt., 2009, p. 447).

Taigi, šiuo metu skiriamos keturios elektroninio dokumento savybės: autentiškumas, patikimumas, vientisumas ir tinkamumas naudoti. Pagrindinė iš šių savybių yra autentiškumas, nes užtikrina visų elektroninio dokumento sandaros dalių nekintamumą. Autentiškumą užtikrina teisinę galią turintys elektroniniai parašai.

2. ELEKTRONINIS PARAŠAS IR JO TAIKYMAS VIEŠOJO SEKTORIAUS VEIKLOJE

Svarbiausias dokumento rekvizitas yra parašas, kuris užtikrina jo tikrumą ir juridinę galią. Taigi, elektroninis dokumentas lygiavertis rašytiniam dokumentui yra tik tada, kai pasirašomas elektroniniu parašu, užtikrinančiu juridinę galią. Elektroninio pavidalo parašas – tai nauja galimybė viešojo sektoriaus atstovams vykdyti dokumentų mainus tarp valstybės institucijų, komunikuoti su verslo atstovais, piliečiais ir užtikrinti greitesnį bei patogesnį duomenų perdavimą.

Elektroninės priemonės vis labiau tampa priimtinesniu komunikavimo būdu, nes yra pranašesnės už tradiciniu budu perduodamą informaciją:

- vienoje erdvėje, t.y. elektroninėje, galima atlikti visus veiksmus, susijusius su dokumento kūrimu, pasirašymu bei išsiuntimu ir tomis pačiomis priemonėmis;
- duomenys galima nusiųsti iš vieno miesto ar valstybės į kitą nepaisant didelių atstumų per labai trumpą laiką ir su mažesnėmis finansinėmis sąnaudomis;
- elektroninių dokumentų kopijos – pigus ir greitas būdas gauti dokumentų originalus;
- elektroninių dokumentų saugojimui ir archyvavimui nereikia daug vietos;
- prisidedama prie gamtos saugojimo, nes ženkliai sumažėja kuro ir popieriaus poreikis: atsisakoma nereikalingų kelionių, e. dokumentų procese popierių keičia informacinės technologijos ir kt.

Taigi, šio skyriaus tikslas – išanalizuoti ir apibrėžti elektroninio parašo taikymo galimybes viešajame sektoriuje, nustatyti tinkamiausias ir saugiausias elektroninio parašo rūšis, kurios užtikrintų duomenų teisinę galią, patikimumą ir autentiškumą.

2.1. Elektroninio parašo samprata

1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvos 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos (toliau – direktyva) rengėjai Europos Parlamentas ir Europos Sąjungos Taryba vylėsi parengti ilgaamžį dokumentą, atsižvelgiant į kintančius rinkos, technologinius ir teisinius poreikius. Direktyva skirta dviejų tikslų įgyvendinimui: palengvinti elektroninių parašų naudojimą ir teisinį pripažinimą, nustato elektroninių parašų ir tam tikrų sertifikavimo paslaugų teisinio reguliavimo sistemą vidaus rinkos funkcionavimui užtikrinti (Civilka, 2013, p. 86).

Elektroninio parašo teisinį pripažinimą Lietuvoje reglamentuoja 2000 m. priimtas Elektroninio parašo įstatymas, įgyvendinant direktyvą. 2004–2011 m. buvo priimti įvairių teisės aktų ir jų nuostatų pakeitimai, atveriantys teisines prielaidas e. parašo naudojimui (žr. 3 priedą) (IVPK, 2013, p. 93).

Elektroninis parašas direktyvoje apibrėžiamas kaip duomenys, pateikti elektronine forma, kurie prijungti arba logiškai susieti su kitais elektroniniais duomenimis ir panaudojami kaip būdas patvirtinti autentiškumą (EUR–Lex, 2000, Nr. 31999L0093). Kitaip tariant, toks parašas skirtas dviejų neatskiriamų funkcijų įgyvendinimui: užtikrinti duomenų vientisumą ir identifikuoti pasirašiusį asmenį. 2006 m. direktyvos peržiūros ataskaitoje teigiama, kad tik asmens identifikavimas nėra elektroninis parašas. Panaši elektroninio parašo samprata pateikiama Tarptautinės standartų organizacijos koncepcijoje – tai duomenų siuntėjo atliekama duomenų vieneto kriptografinė transformacija, kuri leidžia duomenų vieneto gavėjui atpažinti duomenų siuntėją, užtikrinti duomenų vientisumą bei apsaugą nuo neteisėto priėjimo (Garuckas, Kaziliūnas, 2008, p. 115). Tuo tarpu LR elektroninio parašo įstatyme (toliau – EPĮ) elektroninio parašo terminas apibrėžiamas „kaip duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (**ar**) pasirašančiam asmeniui identifikuoti“ (EPĮ 2 str. 4 d.) (Valstybės žinios, 2000, Nr. 61-1827). Analogiška elektroninio parašo prasmė yra įtvirtinta ES, JAV bei kitų šalių teisinėse sistemose (Astromskis, 2011, p. 27) ir mokslininkų veikaluose (Davidavičienė ir kt., 2009, p. 442; Musteikis ir kt., 2008, p. 351). Belevičius (2008) patikslina, kad elektroninis parašas – tai atitinkama elektronine forma pateikti duomenys (p. 56).

Elektroninį parašą sudaro du elementai: materialus ir funkcinis. Materialus elementas – duomenys, kurie logiškai susieti su kitais duomenimis (t.y. informacija, kuri patvirtinama elektroniniu parašu) (Davidavičienė ir kt., 2009, p. 442–443). Pasak kitų mokslininkų, materialusis elementas – tam tikra elektronine forma pateikti duomenys, kurie prijungti arba logiškai susieti su kitais elektroniniais duomenimis. Šis elementas turi atlikti autentifikavimo arba asmens nustatymo funkciją (Belevičius, 2008, p. 56). Tokie duomenys gali būti įvairūs – piršto antspaudo elektroninis atvaizdavimas, įvairūs algoritmai, akies rainelė, balso įrašas (Davidavičienė ir kt., 2009, p. 443; Belevičius, 2008, p. 56). Svarbiausia, kad tokie duomenys būtų vieninteliai ir unikalūs (Belevičius, 2008, p. 56). Elektroninio parašo direktyva vengia griežtai reglamentuoti elektroninio parašo technologijas, remiantis nuomone, jog technologijos su laiku keisis, ir reikia reglamentuoti tik esminius dalykus (Davidavičienė ir kt., 2009, p. 443). Funkcinis elementas – tai elektroninio parašo savybė, kuri leidžia nustatyti dokumentą pasirašiusio asmens tapatybę (t.y. identifikavimo funkcija) (Davidavičienė ir kt., 2009, p. 443; Belevičius, 2008, p. 56).

Apžvelgus daugelių autorių nuomones, galima teigti, kad elektroninis parašas – tai elektronine forma pateikti duomenys, kurie prijungiami arba logiškai susiejami su kitais elektroniniais duomenimis pastarųjų autentiškumui patvirtinti ir pasirašančiam asmeniui identifikuoti.

2.2. Elektroninių parašų įvairovė: paprastas, saugus ir kvalifikuotas e. parašai

Elektroninio parašo galią patvirtina LR elektroninio parašo įstatymo 8 straipsnis, kuriame yra aiškiai išdėstyta, kad elektroninis parašas „turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme“. Į šį įstatymą yra perkeltos ir Europos Parlamento ir Tarybos direktyvos 1999/93/EB „Dėl Bendrijos elektroninių parašų reguliavimo sistemos nuostatos dėl elektroninio parašo rūšių (Astromskis, 2011, p. 26).

Direktyvoje aprašomi trijų lygių elektroniniai parašai (Graux, 2011, p. 10):

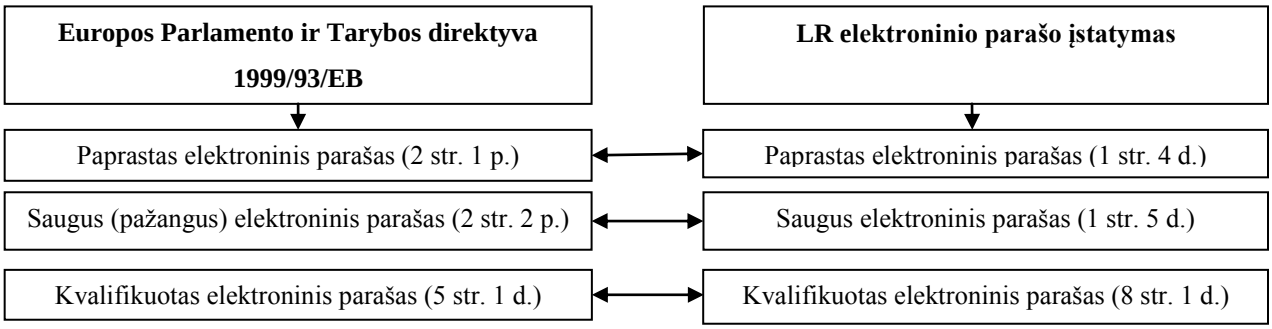
- **paprastas (klasikinis) elektroninis parašas** – elektronine forma pateikti duomenys, kurie prijungti arba logiškai susieti su kitais elektroniniais duomenimis ir panaudojami kaip autentifikavimo metodas.
- **pažangus (saugus) elektroninis parašas:**
  a) yra vienareikšmiškai susietas su pasirašančiuoju asmeniu;
  b) galima nustatyti pasirašančiojo asmens tapatybę;
  c) yra sukurtas priemonėmis, kurias pasirašantis asmuo gali kontroliuoti tik savo valia;
  d) yra susijęs su pasirašytais duomenimis tokiu būdu, kad bet koks šių duomenų pakeitimas yra aptinkamas.
- **kvalifikuotas elektroninis parašas** – pažangus elektroninis parašas, paremtas kvalifikuotu sertifikatu ir sukurtas saugia parašo formavimo įranga.

Kvalifikuotas elektroninis parašas direktyvoje nėra išskiriamas atskiru terminu, tačiau toks parašas atskiru terminu yra apibūdinamas 2006 m. Europos Komisijos ataskaitoje „Dėl Bendrijos elektroninių parašų reguliavimo sistemos veikimo“ (toliau – Europos Bendrijų Komisijos ataskaita) (Astromskis, 2011, p. 26–27): „jis susideda iš saugaus elektroninio parašo, kurio pagrindas yra kvalifikuotas sertifikatas ir kuris sukuriamas saugia parašo formavimo įranga bei atitinka I, II ir III prieduose numatytus reikalavimus“ (Europos Bendrijų Komisija, 2006, p. 4).

Petrauskas ir Vaina (2012) taip pat pabrėžia trijų lygių elektroninius parašus: paprastas, pažangus ir kvalifikuotas e. parašai. Kvalifikuotas elektroninis parašas dar turėtų būti paremtas objektyviu šalies

patvirtinimu: „kvalifikuotas elektroninis parašas – pažangus elektroninis parašas, paremtas kvalifikuotu sertifikatu ir sukurtas saugia parašo formavimo įranga (+ nešališkas šalies patvirtinimas) (p. 321).

Analogiškos e. parašo rūšys ir sampratos išdėstytos ir LR elektroninio parašo įstatyme (žr. 4 pav.).



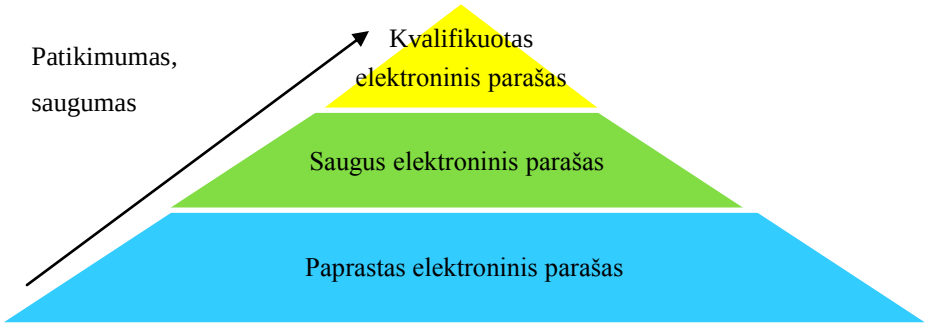
Šaltinis: sudaryta pagal Astromskis, 2011, p. 26; Graux, 2011, p. 1; Valstybės žinios, 2000, Nr. 61-1827.

4 pav. Elektroninio parašo rūšys ir jų teisinis reglamentavimas

Kiti mokslininkai išskiria tik dvi elektroninio parašo rūšis: paprastą (klasikinį) ir saugų elektroninį parašą (Davidavičienė ir kt., 2009, p. 443), paprastąjį (klasikinį) ir tobulesnį elektroninį parašą (Kiškis ir kt., 2006, p. 31). Apžvelgus mokslininkų įvardinamus reikalavimus kiekvienam elektroniniam parašui, galima teigti, kad apibrėžiami du analogiški elektroninių parašų lygiai: tobulesnis ar saugus elektroninis parašas yra ta pati elektroninio parašo rūšis.

Mokslininkai Garuckas ir Kaziliūnas (2008) pabrėžia, kad elektroninis parašas teisine galia yra pripažįstamas ir prilyginamas parašui rašytiniuose dokumentuose kaip įrodinėjimo priemonė teisme tik tuo atveju, jei jis yra saugus (EPĮ 2 str. 5 d.) (p. 115). LR elektroninio parašo įstatyme (8 str. 1 d.) aiškiai reglamentuojama, kad „saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, elektroniniams duomenims turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme” (Valstybės žinios, 2000, Nr. 61-1827). Elektroninis parašas visais atvejais turi kvalifikuotam elektroniam parašui įtvirtintą teisinę galią, jei parašų naudotojai tarpusavyje dėl to susitaria (Valstybės žinios, 2000, Nr. 61-1827).

Apibendrinus daugelių mokslininkų nuomones ir teisinius aspektus, reikėtų vadovautis trimis elektroninių parašų lygiais (rūšimis): paprastas, saugus ir kvalifikuotas elektroninis parašas. Šie parašai vienas už kitą yra labiau patikimesni (žr. 5 pav.).



Šaltinis: sudaryta autorės.

5 pav. Elektroninių parašų įvairovė

Paprastas elektroninis parašas ir jo savybės

Paprastas elektroninis parašas yra technologiškai neutralus terminas, kuris apima įvairius metodus, kuriais galima pasirašyti elektroninį įrašą. Tai reiškia, kad bet kokia pasirašymo forma, pavyzdžiui, tradicinio parašo skaitmeninis atvaizdas, asmens identifikavimo numeris arba PIN kodas, biometrinis identifikavimas kaip pirštų atspaudai ar tinklainės nuskaitymas, yra visos įmanomos ir galiojančios formos. Bet koks simbolis, kuris panaudojamas kaip elektroninis parašas, turi aiškiai užtikrinti dokumento autentiškumą ir galimybę identifikuoti pasirašiusius asmenis (Anderson, Makhdooma, 2010, p. 64.):

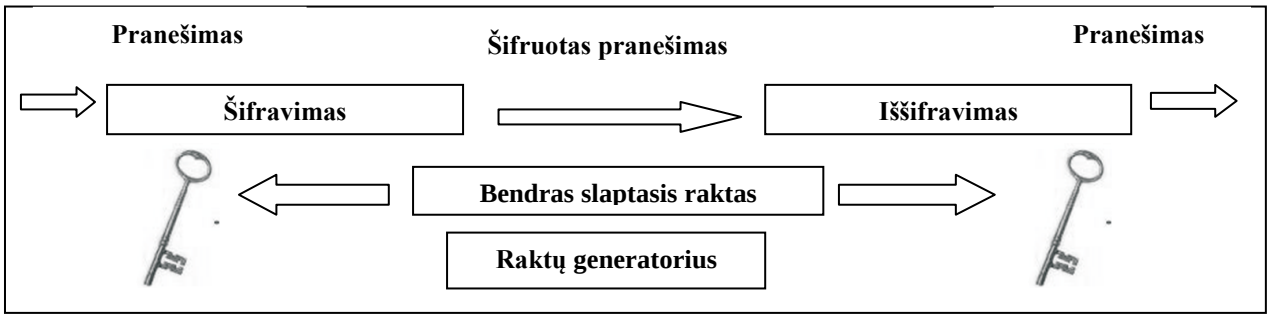
- paprasto elektroninio parašo paskirtis – padėti atpažinti duomenis bei patvirtinti jų autentiškumą (Europos Bendrijų Komisija, 2006, p. 4). Tai gali būti paprastas elektroninio laiško pasirašymas asmens vardu arba panaudojant PIN kodą (Europos Bendrijų Komisija, 2006, p. 4; Astromskis, 2011, p. 27). Autentiškumo patvirtinimas gali būti laikomas parašu, jei susietas su duomenimis, o ne tik naudojamas kaip subjekto autentiškumo patvirtinimo metodas ar technologija (Europos Bendrijų Komisija, 2006, p. 4).
- paprastas elektroninis parašas – duomenys, kuriuos įterpia, prijungia ar logiškai susieja su kitais duomenimis jų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti (Valstybės žinios, 2000, Nr. 61-1827).

Paprastas elektroninis parašas – tai technologija, kurios veikimas pagrįstas elektroninėmis priemonėmis bei kuri yra naudojama ar priimta vienos šalies, siekiančios save susieti su pasirašomu dokumentu ir (ar) tą dokumentą autentifikuoti, tokiu būdu įgyvendinus dalį ar visas funkcijas, kurias galima atlikti tradiciniu parašu. Kaip pavyzdį pateikia internetinius bankus, kurie naudoja paprastesnes technologijas, nustatant vartotoją, jo elektroninį parašą bei valią (Kiškis ir kt., 2006, p. 31). Mokslininkai Davidavičienė ir kt. (2009, p. 444) sutinka, kad tik vienoje įstaigoje, vieno banko klientai ir panašiai

patikimumui užtikrinti gali naudoti paprastas identifikavimo technologijas, pavyzdžiui, vartotojo vardas ir slaptažodis, IP adresas ir slaptažodis. Tačiau siekiant dar labiau apsisaugoti nuo galimų pavojų, naudojamos sudėtingesnės elektroninio parašo technologijos. Tai daro ir bankai, kurie savo klientams gali pasiūlyti elektroninės bankininkystės paslaugas. Sudėtingesnę technologiją sudaro:

- visų veiksmų atlikimas vykdomas per koduotą ir uždarą banko kanalą.
- kiekvieno vartotojo identifikavimui banko internetiniame puslapyje yra skirtas:
  a) asmeninis identifikacinis numeris, kurį išduoda bankas;
  b) asmeninis slaptažodis, kurį kiekvienas klientas sugalvoja asmeniškai;
  c) kiekvieną kartą, kai klientas naudojasi elektronine bankininkyste, jo paprašoma įvesti vis kitokį slaptažodį iš banko suteiktos slaptažodžių lentelės.
- dirbama on-line režimu. Jei veiksmai neatliekami ilgiau nei 10–15 min., transakcijos yra blokuojamos, prašant įvesti pakartotinį identifikavimą. Siekiant dar labiau padidinti transakcijų saugumą bei sumažinti klaidų rizikas, galima nusipirkti e. banko slaptažodžių generatorių.

Uždarose sistemose šalių tapatybė gali būti nustatoma panaudojant paprasto elektroninio parašo sprendimus, kai šalys viena kita pasitiki (Petrauskas, Vaina, 2012, p. 321; Anderson, Makhdooma, 2010, p. 64). Pasitikėjimas yra reikalingas dėl to, kad paprasto elektroninio parašo kūrimui naudojama simetrinio šifravimo sistema (žr. 6 pav.).



Šaltinis: Kiškis ir kt., 2006, p. 36.

6 pav. Elektroninio parašo simetrinio šifravimo sistema

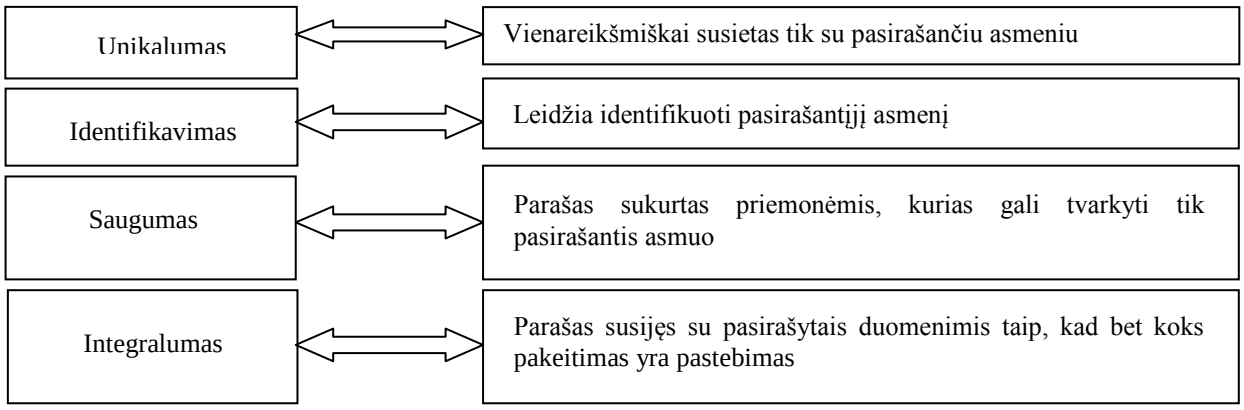
Panaudojant šią sistemą, failo užšifravimui ir iššifravimui naudojamas vienas ir tas pats raktas – slaptasis raktas. Siuntėjas, prieš siųsdamas pranešimą, jį užkoduoja naudodamas ir jam, ir gavėjui žinomą raktą bei abiem prieinamą algoritmą. Ypatybė – informaciją užkoduoti ir sugrąžinti pradinę formą galima tuo pačiu raktu. Simetrinio šifravimo sistema nelabai tinkama tose srityse, kur būtina įsitikinti duomenų siuntėjo

tapatybe, pavyzdžiui, elektronine forma keičiantis tarnybiniais dokumentais. Šiuo atveju atsiranda poreikis užtikrinti, kad dokumento autorius yra įgaliotas asmuo, turintys teisę pasirašyti tokius dokumentus. Simetrinio šifravimo sistema tinkama naudoti elektroninėje prekyboje, kai partneriai iš anksto pasitiki vienas kitu (Kiškis ir kt., 2006, p. 36–37).

Apibendrinus visas nuomones ir pateikiamas technologijas, galima teigti, kad paprasto elektroninio parašo naudojimas viešojo sektoriaus veikloje yra neįmanomas.

Saugus elektroninis parašas ir jo savybės

Daugelis mokslininkų sutinka, kad saugiu elektroniniu parašu gali būti laikomas tik toks parašas, kuris atitinka šiuos reikalavimus: 1) toks parašas vienareikšmiškai susietas tik su pasirašančiuoju fiziniu ar juridiniu asmeniu; 2) leidžia nustatyti asmenį, kuris pasirašė dokumentą; 3) parašas sukurtas priemonėmis, kurias pasirašantys asmuo gali tvarkyti tik savo valia; 4) su pasirašytais duomenimis parašas yra susijęs tokiu būdu, jog bet koks duomenų pakeitimas po pasirašymo yra pastebimas (Davidavičienė ir kt., 2009, p. 443; Krawczyk, 2010, p. 10; Limba, Novikovienė, 2012, p. 491). Kiti mokslininkai kiekvieną iš šių keturių reikalavimų įvardina tik vienu žodžiu (žr. 7 pav.).



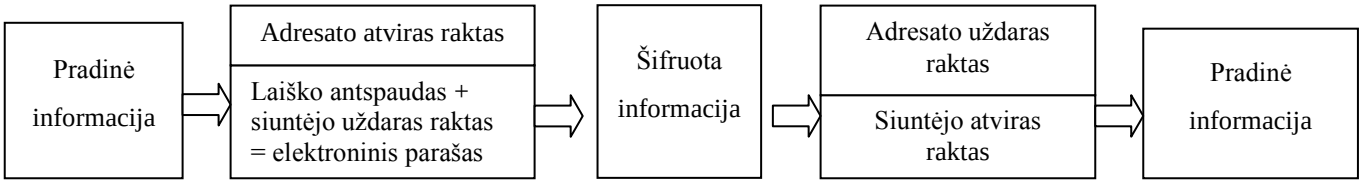
Šaltinis: sudaryta pagal Belevičius, 2008, p. 56; Musteikis ir kt., 2008, p. 353.

7 pav. Reikalavimai saugiam elektroniniam parašui

Reikėtų pabrėžti, jog nesant bent vieno iš šių elementų, elektroninis parašas yra juridiškai nepagrįstas (Garuckas, Kaziliūnas, 2008, p. 115).

Reikalavimai, kurie keliami saugiam elektroniniam parašui, susiję su LR civilinio kodekso (toliau – CK) reikalavimais teksto apsaugai ir pasirašiusio asmens identifikavimui, tik šie reikalavimai yra papildomai detaliau aprašomi, užtikrinant, kad tik pasirašantis asmuo galėtų pasirašyti elektroninę informaciją ir nei viena trečioji šalis vietoj jo šių veiksmų negalėtų įvykdyti. Taigi, EPĮ 2 str. 5 d. 1, 2, 3 reikalavimai yra CK antrojo reikalavimo – parašo identifikavimo ir pasirašiusio asmens nustatymo – detalizavimas, o 4 reikalavimas tiksliai atitinka CK įtvirtintą sutarties teksto apsaugos reikalavimą. Įvykdžius EPĮ reikalavimus, įgyvendinami ir CK reikalavimai (Čėsna, 2007, p. 95; Limba, Novikovienė, 2012, p. 491–492).

Didžiausią saugumą užtikrina dviejų raktų asimetrinio šifravimo sistemos – dar vadinama viešojo rakto infrastruktūra (toliau – PKI) – saugus elektroninis parašas (Davidavičienė ir kt., 2009, p. 444). Toks saugus elektroninis parašas, dar vadinamas skaitmeniniu parašu, pagrįstas dviejų raktų (PKI) technologija (Davidavičienė ir kt., 2009, p. 444), iš kurių vienas – vadinamas privačiu, o kitas – viešu raktu (Davidavičienė ir kt., 2009, p. 444; Garuckas, Kaziliūnas, 2008, p. 115; Limba, Novikovienė, 2012, p. 493). Ši technologija naudoja algoritmą, kuris apima du skirtingus, tačiau matematiškai susijusius raktus. Privatusis raktas skirtas kurti elektroninį parašą arba duomenis paversti užkoduotais, o viešas raktas – parašui tikrinti arba pranešimui sugrąžinti pradinę formą (Davidavičienė ir kt., 2009, p. 444). Pirmas raktas žinomas tik jo turėtojui ir yra maža tikimybė tokį raktą atspėti, nes jį sudaro skaitmenys (Garuckas, Kaziliūnas, 2008, p. 115). Toks raktas yra slaptas ir turi būti saugomas nuo trečiųjų asmenų (Limba, Novikovienė, 2012, p. 493). Viešas raktas yra prieinamas visiems, kurie keičiasi informacija (Garuckas, Kaziliūnas, 2008, p. 115): šį raktą adresatams galima perduoti elektroniniu paštu arba paskelbti internete. Turint tik viešą raktą, negalima sužinoti privataus rakto kodo. Kadangi šie raktai gali funkcionuoti, kai naudojami kartu, tokiu būdu užtikrinamas saugumas ir suteikiama galimybė patikimai identifikuoti asmenis, atliekančius elektroninius veiksmus (Limba, Novikovienė, 2012, p. 493). Kiekvienas raktas gali atlikti tik vienpusį šifravimą, t.y. užkoduoti pranešimą tokiu būdu, kad jį atkoduoti galima tik kitu tos pačios poros raktu (žr. 8 pav.). Prieš tai, kai bus išsiųstas elektroninis laiškas, jį reikia užšifruoti adresato viešuoju (atviruoju) raktu. Tokiu būdu garantuojama, jog siunčiama informacija nebus prieinama pašaliniam asmeniui. Adresatas gautą laišką iššifruoja savo privačiuoju (uždaruoju) raktu, tokiu būdu atkurdamas pradinę išsiųstą informaciją. Siuntėjo tapatybę adresatas gali patikrinti iššifravęs prie laiško „prikabintą“ kodą, kurį siuntėjas suformuoja užšifravęs unikalų elektroninio laiško antspaudą uždaruoju raktu. Toks šifras ir vadinamas elektroniniu parašu, o toks aptartų raktų porų naudojimas užtikrina, kad perduodama informacija yra saugi ir patikima (Garuckas, Kaziliūnas, 2008, p. 116):



Šaltinis: Garuckas, Kaziliūnas, 2008, p. 116.

8 pav. Informacijos siuntimo procesas, naudojant saugų elektroninį parašą

- kitas asmuo negali pasisavinti pranešimo autorystės, nes neturi slapto rakto, kuris skirtas pasirašyti;
- siuntėjas negali paneigti, kad siuntė informaciją (Kiškis ir kt., 2006, p. 33).

Problema:

- trečias asmuo gali perskaityti žinutę, panaudodamas viešąjį raktą (Kiškis ir kt., 2006, p. 33).

Taigi, galima teigti, kad dviejų raktų technologijos pagalba informacija gali būti perduodama dvejopai:

1. Jei siuntėjas dokumentą užkoduoja adresato viešuoju raktu, adresatas šį dokumentą iššifruoja savo privačiuoju raktu;
2. Jei siuntėjas dokumentą užkoduoja savo privačiuoju raktu, adresatas iššifruoja siuntėjo viešuoju raktu.

Taigi, elektroninio dokumento pasirašymo procese dalyvauja ta pati raktų pora, t.y. siuntėjo viešas ir privatus raktas arba adresato viešas ir privatus raktas.

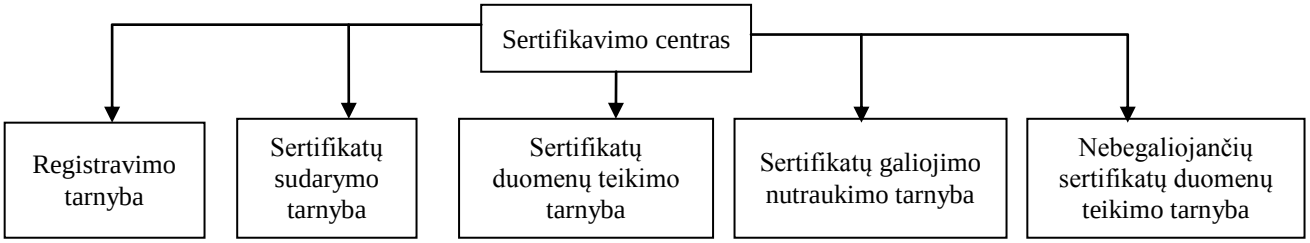
Naudojant saugius elektroninius parašus, elektroninis pranešimas, siunčiamas kompiuteriniu tinklu, yra užšifruotas tokiu būdu, kad neįmanoma jo atkoduoti, o bandant pakeisti tokio pranešimo turinį ar parašą, pranešimo tekstas virsta nesuprantamų simbolių virtine (Davidavičienė ir kt., 2009, p. 444).

Saugus elektroninis parašas yra apsaugotas nuo sukčiavimo, nes yra labai mažai tikėtina, faktiškai neįmanoma nustatyti pasirašiusio asmens privatų raktą, žinant tik viešą raktą (Blythe, 2008, p. 369).

Asmuo, siekiantis pasirašyti elektroniniu būdu, turi turėti sertifikatą (Garuckas, Kaziliūnas, 2008, p. 116). Sertifikatas – tai elektroninis liudijimas susiejantis pasirašantįjį su parašo tikrinimo duomenimis (EUR–Lex, 2000, Nr. 31999L0093; Civilka, 2013, p. 103). Kitaip tariant, tai elektroninio pavidalo liudijimas, kuris patvirtina, kad viešasis šifravimo raktas ir jį atitinkantis privatusis šifravimo raktas priklauso sertifikate nurodytam asmeniui (Garuckas, Kaziliūnas, 2008, p. 116; Davidavičienė ir kt., 2009, p. 445). Sertifikatą paprastai sudaro 5 elementai: savininko vardas, savininko viešas raktas ir jo galiojimo terminas, sertifikatą teikiančios organizacijos pavadinimas ir skaitmeninis parašas asmeniui (Garuckas, Kaziliūnas, 2008, p. 116). Kiti mokslininkai išskiria ir šeštą skaitmeninio sertifikato elementą, t.y.

skaitmeninio sertifikato serijinis numeris (Musteikis ir kt., 2008, p. 351). Pasak Civilkos (2013), skaitmeninį sertifikatą sudaro viešas raktas, informacija apie rakto turėtojo tapatybę, rakto galiojimo laikotarpis, parašo algoritmas, sertifikato numeris, sertifikavimo paslaugų teikėjo pavadinimas bei panašiai. Vis dėlto sertifikatas nesuteikia atsakymo į vieną klausimą: kokiu lygiu galima pasitikėti subjektu, išduodančiu sertifikatą (p. 103–104).

Sertifikavimo paslaugas teikia organizacijos, kurios dar vadinamos sertifikatų centrais. Šiuos centrus sudaro struktūriniai padaliniai, t.y. tarnybos (žr. 9 pav.). Sertifikavimo paslaugų teikėjais gali būti ne tik juridinis, bet ir fizinis asmuo, kuris išduoda sertifikatus arba teikia kitas paslaugas, susijusias su elektroniniais parašais (EUR–Lex, 2000, Nr. 31999L0093).



Šaltinis: Garuckas, Kaziliūnas, 2008, p. 116.

9 pav. Sertifikavimo centro struktūra

2004 m. Informacinės visuomenės plėtros komitetas teikė nekvalifikuotus sertifikatus valstybės institucijoms, dalyvaujančioms projekte „Elektroninio parašo diegimas valstybinėse institucijose“. Nekvalifikuoti sertifikatai buvo dalinami šių institucijų darbuotojams, kuriuos jie galėjo naudoti tik įstaigos viduje (supažindinimo žymai, dokumento rengėjo parašui, vizavimui ir kt.). EPĮ 8 str. 3 dalis reglamentuoja saugaus elektroninio parašo teisinę galią, tačiau abi šalys tarpusavyje turi dėl to susitarti. Susitarimas galėjo būti įteisintas vidaus darbo reglamento pagalba (Mašidlauskas, 2008, p. 29).

Dabartiniu metu nekvalifikuotus sertifikatus teikia UAB „Skaitmeninio sertifikavimo centras“ (toliau – SSC). Pirmos klasės sertifikatas identifikuoja tik pasirašiusio asmens e. pašto adresą. Sertifikato kaina metams – 62 Lt be PVM (be laikmenos ir licencijos kainos). Antros klasės nekvalifikuotas sertifikatas identifikuoja pasirašantį asmenį, kainuoja 90 Lt be PVM metams (be laikmenos ir licencijos) (SSC).

Ateityje saugus elektroninis parašas gali būti pradėtas kurti naudojant biometrinius duomenis (Kiškis ir kt., 2006, p. 32). Biometrija – automatinis žmogaus identifikavimas, remiantis fiziologinėmis

savybėmis (Davidavičienė ir kt., 2009, p. 446). Pasak Navakausko (2010), biometrija – tai mokslo sritis, apimanti metodus, kuriuos panaudojant atpažįstamas žmogus, remiantis vienu ar keliais fiziologiniais ir elgsenos bruožais (žr. 10 pav.).

Fiziologiniai biometriniai bruožai – akies rainelė, veido termograma, delno antspaudas, DNR, piršto antspaudas, akies tinklainė, ausis, delno geometrija, delno venos, veidas.
Elgsenos biometriniai bruožai – eisena, balsas, parašas, teksto rinkimas.

Šaltinis: sudaryta pagal Ivanovas, 2010, p. 24.

10 pav. Fiziologinių ir elgsenos asmens bruožų biometrija

Automatinis biometrinių duomenų atpažinimas turi būti labai greitas ir saugus. Biometrija pasižymi šiomis savybėmis: skiriantis, universalus, nuolatinis, išmatuojamas, panaudojamas, priimtinas ir nesuklastojamas. Bruožai, kurie labiausiai pasižymi šiomis savybėmis, yra tinkami naudoti automatinėse atpažinimo sistemose (žr. 4 priedą). Tiksliausi ir patikimiausi biometriniai duomenys yra akies rainelė ir piršto antspaudas (Ivanovas, 2010, p. 24). Šiuo metu dažniausiai naudojami pirštų atspaudų biometriniai duomenys. Jau yra sukurti pigūs pirštų atspaudų atpažinimo lustai, kurie ypač plačiai naudojami nešiojamų kompiuterių ar lustinių atmintinių (angl. flash) savininkams atpažinti (Davidavičienė ir kt., 2009, p. 446). Naudojant akies rainelės ir piršto antspaudo požymius sistemose, tikimybė dėl klaidingo atpažinimo yra maža (Ivanovas, 2010, p. 26).

Biometrija – techniškai pranašesnis metodas, lyginant su kitais metodais, apimant slaptažodžius, PIN kodus, elektronines identifikavimo korteles (angl. smart cards) bei kitas technologijas. Šis identifikavimo metodas nereikalauja prisiminti slaptažodžius, nešiotis papildomas korteles ar kodų generatorius. Tereikia būti identifikavimo vietoje (Davidavičienė ir kt., 2009, p. 446). Nuo 2009 m. liepos 29 d. tarnybiniame pase[1] yra talpinami biometriniai duomenys: 1) asmens veido atvaizdas, 2) asmens parašas, 3) asmens pirštų atspaudai (Valstybės žinios, 2009, Nr. 96-4078). Nuo 2009 m. sausio 1 d. išduodamos naujo pavyzdžio asmens tapatybės kortelės Lietuvos piliečiams, kuriuose fiksuojami du biometriniai duomenys: pirštų atspaudai ir veido atvaizdas (Davidavičienė ir kt., 2009, p. 446). Nuo 2009 m. lapkričio 19 d. išduodami naujo pavyzdžio valstybės tarnautojų pažymėjimai be biometrinių duomenų (Valstybės žinios, 2009, Nr. 139-6133).

[1]Tarnybinis pasas yra skirtas vykti į užsienio valstybes tarnybos tikslais.

Taigi, saugus elektroninis parašas turi teisinę galią, jei parašų naudotojai tarpusavyje dėl to susitaria, todėl šis parašas gali būti naudojamas tik viešojo sektoriaus institucijos viduje (supažindinimo žymai, dokumento rengėjo parašui, vizavimui ir kt.) bei pasirašant dokumentus, skirtus vidiniam naudojimui.

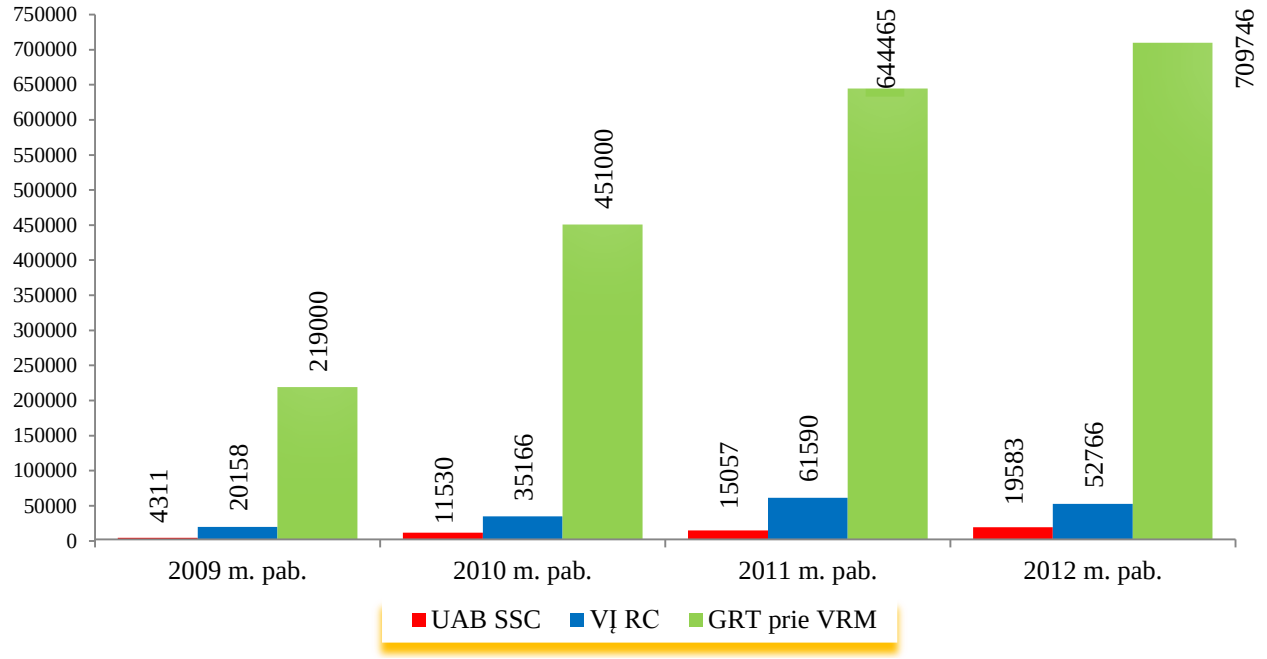
Kvalifikuotas elektroninis parašas ir jo savybės

Saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir paremtas kvalifikuotu sertifikatu, yra vadinamas kvalifikuotu elektroniniu parašu (Graux, 2011, p. 10). EPĮ 8 str. 1 d. netiesiogiai įtvirtinta platesnė kvalifikuoto elektroninio parašo samprata – „saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, elektroniniams duomenims turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme“ (Valstybės žinios, 2000, Nr. 61-1827; Česna, 2007, p. 94). Kitaip tariant, kvalifikuotas elektroninis parašas – tai tradicinio parašo atitikmuo elektroninėje erdvėje.

Elektroninis parašas, patvirtintas kvalifikuotu sertifikatu, yra patikimesnis, saugesnis dėl už jį laiduojančio trečiojo asmens, t.y. sertifikavimo paslaugų teikėjo, kuris atitinka Vyriausybės ar jos įgaliotos institucijos (Lietuvos Respublikos ryšių reguliavimo tarnybos (Valstybės žinios, 2011, Nr. 8-316)) nustatytus reikalavimus (Limba, Novikovienė, 2012, p. 492–493). Toks parašas užtikrina aukštą saugumo lygį: autentiškumą, vientisumą ir nepaneigiamumą (Krawczyk, 2010, p. 13). Kvalifikuotu sertifikatu patvirtintas e. parašas – valstybės sureguliuota saugi identifikavimo priemonė (Štitilis ir kt., 2011, p. 70).

Kvalifikuotame sertifikate yra šie duomenys: 1) užrašas, kad sertifikatas yra kvalifikuotas; 2) sertifikavimo paslaugų teikėjo tapatybė ir jo buveinės šalies identifikatorius; 3) pasirašančio asmens vardas bei pavardė arba slapyvardis; 4) pasirašančio asmens specifinis požymis, pagal poreikį, atsižvelgiant į numatomus sertifikato naudojimo tikslus; 5) parašo tikrinimo duomenys, atitinkantys parašo formavimo duomenis, kuriuos pasirašantys asmuo pats kontroliuoja; 6) sertifikato galiojimo pradžios bei pabaigos terminas; 7) sertifikato identifikacinis kodas (numeris); 8) sertifikavimo paslaugų teikėjo saugus elektroninis parašas; 9) sertifikato taikymo apribojimai, jei tokie nustatyti; 10) sandorių vertės apribojimai, kurios negalima viršyti naudojant sertifikatą, jei tai nustatyta (EUR–Lex, 2000, Nr. 31999L0093; Valstybės žinios, 2000, Nr. 61-1827). Kiti mokslininkai išskiria tik devynis elementus: neįtraukia tik sertifikato taikymo apribojimo duomenų (Dragu, 2009, p. 941). Taip pat svarbu paminėti, kad sertifikavimo paslaugų teikėjas, išduodamas arba garantuodamas kvalifikuotą sertifikatą visuomenei, turi būti atsakingas už padarytą žalą bet kuriam fiziniam ar juridiniam subjektui, kuris pagrįstai pasitiki tuo sertifikatu (EUR–Lex, 2000, Nr. 31999L0093; Valstybės žinios, 2000, Nr. 61-1827).

2012 m. kvalifikuotų sertifikatų sudarymo paslaugas teikė trys Lietuvoje įregistruoti sertifikavimo paslaugų teikėjai: UAB „Skaitmeninio sertifikavimo centras“ (toliau – SSC), valstybės įmonė Registrų centras (toliau – RC), Gyventojų registro tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – GRT prie VRM) (žr. 11 pav.) (LR Ryšių reguliavimo tarnyba (RRT), 2013).



Šaltinis: sudaryta pagal RRT, 2013, p. 4.

11 pav. Sudarytų galiojančių kvalifikuotų sertifikatų skaičius 2009–2012 m.

SSC, kaip Lietuvos kvalifikuotus sertifikatus sudarantys sertifikavimo paslaugų teikėjas, įregistruotas 2005 m. Ši institucija teikia ir laiko žymos paslaugą kaip Lenkijos sertifikavimo paslaugų teikėjo „Unizeto Technologies SA“ atstovė. Didžioji dalis išduotų kvalifikuotų sertifikatų suteikta juridiniams asmenims. RC sertifikavimo veiklą Lietuvoje pradėjo 2008 m. Ši institucija papildomai teikia ir laiko žymos formavimo paslaugą, skirtą kvalifikuotiems e. parašams. GRT prie VRM 2009 m. įregistruota kaip Lietuvos sertifikavimo paslaugų teikėja, sudaranti kvalifikuotus sertifikatus (RRT, 2012).

Užsienio valstybių sertifikavimo paslaugų teikėjų sudaryti kvalifikuoti sertifikatai taip pat pripažįstami teisiškai lygiaverčiais LR sertifikavimo paslaugų teikėjų sudarytiems kvalifikuotiems sertifikatams, jei:

1. sudaryti sertifikavimo paslaugų teikėjo, kuris akredituotas Lietuvos Respublikoje arba Europos Sąjungos valstybėje;

2. už sertifikatą laiduoja Lietuvos Respublikos ar Europos Sąjungos valstybės sertifikavimo paslaugų teikėjas, kuris atitinka LR Vyriausybės ar jos įgaliotos institucijos įtvirtintus reikalavimus kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams (Civilka, 2013, p. 88; Valstybės žinios, 2000, Nr. 61-1827).

GRT prie VRM sudaromi sertifikatai – palankiausias ir pigiausias sprendimas valstybės tarnautojams (žr. 1 lent.).

1 lentelė. Kvalifikuoto elektroninio parašo teikėjų pasiūla viešajam sektoriui

	Sertifikatų kaina*	**Galioja**	**Laikmenos tipas**	**Atnaujinimo kaina**	**Duomenų pakeitimas sertifikate**	**Pastebėjimai**
GRT	Nemokamai	3 m.	Lustinė kortelė (80 Lt)	Nemokamai	Nemokamai	Papildomai reikia įsigyti kortelių skaitytuvą (65 Lt).
SSC	342,43 Lt (su PVM)	2 m.	Nenurodytas (į kainą neįskaičiuota)	180,29 Lt (su PVM)	48 Lt (su PVM)	Didžiausia kaina lyginant su kitais sertifikavimo paslaugų teikėjais.
RC	149,63 Lt (su PVM)	2 m.	USB (įskaičiuota į sertifikato kainą)	28,42 Lt (su PVM)	9,21 Lt (su PVM)	Juridiniams asmenims neišduodami.
	100,57 Lt (su PVM)	2 m.	Lustinė kortelė (įskaičiuota į sertifikato kainą)	28,42 Lt (su PVM)	9,21 Lt (su PVM)	Komplekte yra lustinės kortelės skaitytuvas. Juridiniams asmenims neišduodami.

* asmens identifikavimo e. erdvėje sertifikatas ir kvalifikuotas elektroninio parašo sertifikatas

Šaltinis: sudaryta autorės.

GRT prie VRM sudaro sertifikatus, įrašomus į naujo pavyzdžio lustines korteles:

- nuo 2009 m. sausio 1 d. į naujas asmens tapatybės korteles įrašomi asmens atpažinimo e. erdvėje sertifikatas ir kvalifikuotas sertifikatas (Davidavičienė ir kt., 2009, p. 445). Pradinė šios kortelės kaina siekė 80 Lt (IVPK, 2013). Nuo 2011 m. sausio 1 d. ši kaina sumažinta iki 30 Lt (Valstybės žinios, 2010, Nr. 149-7640). Iki 2014 m. sausio 1 d. išrašytos 2 990 457 naujos kartos LR asmens tapatybės kortelės (Asmens dokumentų išrašymo centras prie VRM, 2014).
- 2009 m. lapkričio 26 d. įsakymu Nr. 1V-624 sudaromi naujo pavyzdžio valstybės tarnautojo pažymėjimai. Kontaktinėje elektroninėje laikmenoje įrašomi valstybės tarnautojo atpažinimo elektroninėje erdvėje sertifikatas ir e. parašo kvalifikuotas sertifkatas (Valstybės žinios, 2009, Nr. 139-6133). 2014 m. sausio 1 d. 45 973 valstybės tarnautojai (87,2 proc.) jau turi naujo pavyzdžio valstybės tarnautojo pažymėjimą (Asmens dokumentų išrašymo centras prie VRM, 2014).

2007 m. Lietuvoje startavo mobilusis elektroninis parašas. Šis parašas įgyvendinamas panaudojant mobilųjį telefoną su specialia SIM kortele, kurios dėka galima tinkamai užkoduoti siunčiamus duomenis (Davidavičienė ir kt., 2009, p. 445). SIM kortelės mikroschemoje įrašomas privatusis raktas, sertifikatas bei kita elektroniniam parašui formuoti ir tikrinti svarbi papildoma informacija (Civilka, 2013, p. 100). Šiuo metu mobilius elektroninius parašus siūlo mobiliojo ryšio operatoriai „Omnitel“, „Bitė“ ir „Tele2“ su kvalifikuotais VĮ „Registrų centro“ sertifikatais (žr. 2 lent.). UAB „Omnitel“ mobiliojo telefono SIM kortelėje įrašo ir Estijos sertifikavimo paslaugų teikėjo AS „Sertifitseerimiskeskus“ kvalifikuotus sertifikatus (Civilka, 2013, p. 88). Mobiliojo elektroninio parašo paslauga gali pasinaudoti tik privatūs ir verslo mobiliojo ryšio operatoriaus klientai: viešajam sektoriui ši paslauga neteikiama.

2 lentelė. Mobilaus e. parašo teikėjų pasiūlos duomenys privatiems ir verslo klientams

	Sertifikatų kaina*	**Galioja**	**Laikmenos tipas**	**Atnaujinimo kaina**	**Duomenų pakeitimas sertifikate**	**Pastebėjimai**
BITĖ Lietuva	15 Lt + 1 Lt/mėn.	2 m.	SIM kortelė (1 Lt)	15 Lt	– (15 Lt**)	Naudotis paslauga gali tik privatūs ir verslo Bitės klientai.
Omnitel	0,02 Lt	2/5 m.	. SIM kortelė	0 Lt	– (0,02 Lt**)	Naudotis paslauga gali tik privatūs ir verslo Omnitel klientai.
Tele2	Mėnesinio mokėjimo SIM kortelės kaina	Kol galioja sutartis	SIM kortelė	–	– (0 Lt **)	Naudotis paslauga gali tik privatūs ir verslo Tele2 klientai

* asmens identifikavimo e. erdvėje sertifikatas ir kvalifikuotas elektroninio parašo sertifikatas
** pasikeitus duomenims, reikia užsisakyti naujus sertifikatus

Šaltinis: sudaryta autorės.

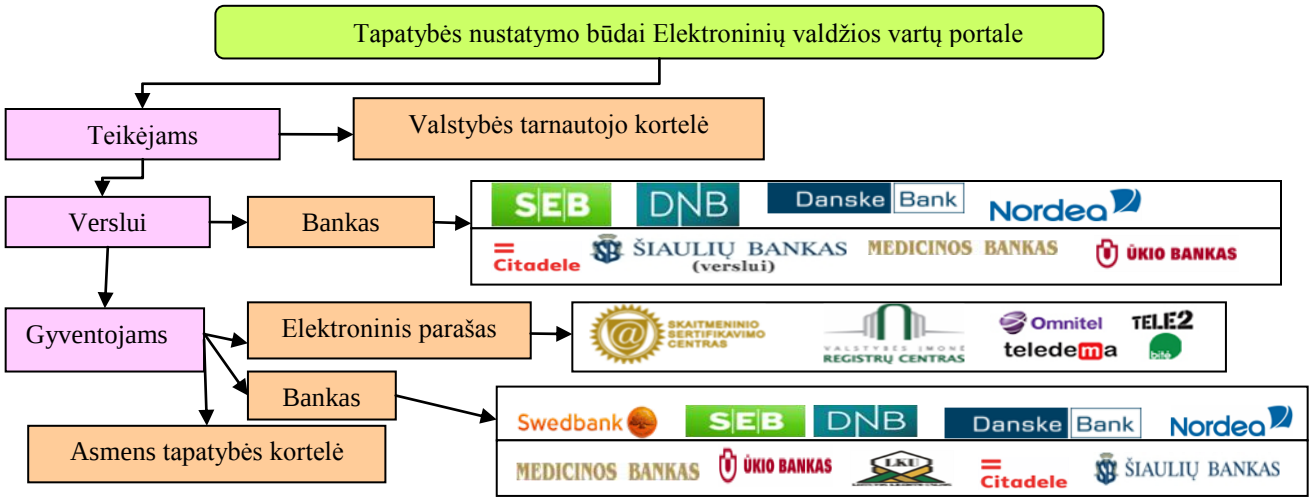
Kitas svarbus kvalifikuoto elektroninio parašo elementas – turi būti sukurtas saugia parašo formavimo įranga, kuri turi atitikti keturis reikalavimus (EUR–Lex, 2000, Nr. 31999L0093; Valstybės žinios, 2000, Nr. 61-1827):

- kiekvieną kartą yra suformuojami unikalūs ir neatkartojami elektroninio parašo formavimo duomenys ir užtikrinamas jų slaptumas;
- elektroninio parašo formavimo duomenų atkūrimas praktiškai neįmanomas, o nuo elektroninio parašo klastočių apsaugo esamos technologijos;
- parašo formavimo duomenis, kurie naudojami elektroniniam parašui sukurti, pasirašantis asmuo gali užtikrintai apsaugoti nuo kitų asmenų;

- elektroninio parašo formavimo įranga nekeičia pasirašomų duomenų ir turi užtikrinti, kad pasirašantys asmuo galėtų matyti tuos duomenis, prieš jam nusprendus pasirašyti.

Šiuo metu yra platinamos dvi nemokamos elektroninio parašo formavimo ir tikrinimo įrangos – „Justa GE“ ir „Signa 2012 (beta)“, kurias galima įsidiegti į asmeninius kompiuterius. Šių programinių įrangų autorių teises yra įsigijusi valstybė. Justa GE – pirmoji programinė įranga, skirta valstybės tarnautojams, kurti saugų elektroninį parašą ir jį tikrinti. Ši programinė įranga buvo įsigyta Informacinės visuomenės plėtros komiteto (IVPK) konkurso būdu. Tačiau IVPK kol kas nepritaikė šios programinės įrangos elektroninio dokumento ADOC specifikacijai, kurią patvirtino Lietuvos archyvų departamentas. Todėl institucijos, kurios elektroninius dokumentus kuria „Justa GE“ programinės įrangos pagalba, turės pačios investuoti į šios priemonės pritaikymą arba ją pakeisti kita programine įranga (LR Valstybės kontrolė, 2010, p. 19). Tačiau ši programa puikiai tinka kurti ir pasirašyti vaizdo ir (ar) garso dokumentus, kuriems šiuo metu nėra nustatyta specifikacija. „Signa“ – kita programinė įranga, kuri pritaikyta kurti ir pasirašyti elektroninius dokumentus, kurių formatas atitinka ADOC specifikaciją.

Šiuo metu Elektroninės valdžios vartų portale e. paslaugų teikėjai gali prisijungti tik valstybės tarnautojo kortelės dėka (žr. 12 pav.).



Šaltinis: sudaryta autorės.

12 pav. Tapatybės identifikavimas Elektroninių valdžios vartų portale

Taigi, kvalifikuotas elektroninis parašas – valstybės sureguliuota saugi identifikavimo priemonė. Toks parašas yra laikomas saugiu elektroniniu parašu, kuris turi būti sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu. Šių e. parašų saugumą užtikrina trečias asmuo,

valstybės patvirtintas kvalifikuotų sertifikatų teikėjas, todėl nereikia dviejų šalių susitarimo. Šiuo metu kvalifikuotus sertifikatus valstybės tarnautojams teikia GRT prie VRM bei Skaitmeninio sertifikavimo centras. GRT prie VRM sudaromi sertifikatai – pigiausias sprendimas valstybės tarnautojams. Kvalifikuotu elektroniniu parašu gali būti pasirašomi visi e. dokumentai nepriklausomai nuo jų paskirties ir tipo, t.y. trumpojo, ilgojo ar nuolatinio saugojimo, nes toks parašas turi neginčijamą teisinę galią.

2.3. Grėsmės elektroninėje erdvėje – asmens tapatybės vagystė

Skirtingai nei fizinėje erdvėje, kai asmens tapatybė patvirtinama asmens dokumentu, elektroninėje aplinkoje tapatybė užtikrinama panaudojant unikalų prisijungimo vardą bei slaptažodį ir visos saugumo užtikrinimo priemonės, pavyzdžiui, skaitmeniniai sertifikatai ir kt., praktiškai atitinka asmens tapatybę elektroninėje erdvėje (Štitilis, Laurinaitis, 2009, p. 241). Nepaisant visų saugumo priemonių, viena sparčiausiai plintančių XXI amžiaus nusikalstamų veikų – asmens tapatybės vagystė (Acoca, 2008).

Reikėtų pabrėžti, kad dar nėra visuotinai priimtinos ir įtvirtintos tapatybės vagystės elektroninėje erdvėje sampratos tarptautiniu mastu. Įvairiuose šalyse skirtingai įvardinama ir pati veika. ES šalyse ši veika vadinama tapatybės sukčiavmas (angl. identity fraud) arba tapatybės nusikaltimas (angl. identity crime). JAV, Kanadoje, Korėjoje naudojama tapatybės vagystės sąvoka (angl. id theft) (Ekonominio bendradarbiavimo ir plėtros organizacija (EBPO), 2008, p. 13–14). Kitose šalyse gali būti vartojamos ir kitos sampratos. Nors iš tikrųjų tapatybės vagystė ir tapatybės sukčiavimas – tai tik dvi dalys sudarančios tapatybės nusikaltimų sąrašą (Europos policijos biuras, 2011, p. 50).

Tapatybės vagystės sampratos prasmės atžvilgiu yra beveik identiškos. Pasak Europos Bendrijų Komisijos (2007), tapatybės vagystė – tai asmens tapatybę identifikuojančios informacijos panaudojimas kaip priemonė įvykdyti kitus nusikaltimus. Tapatybės vagystė įvykdoma, kai asmuo neteisėtu būdu įgyja, siunčia, valdo ar naudoja kito fizinio ar juridinio asmens privačią informaciją, ketinant įvykdyti sukčiavimą arba kitus nusikaltimus (EBPO, 2008, p. 3). Kitaip tariant, tai asmenį identifikuojančios informacijos panaudojimas be jo žinios su ketinimu įvykdyti neteisėtą veiką (Klangauskas, 2012, p. 29). Taigi, elektroninėje erdvėje siekiama išgauti informaciją apie asmens tapatybę, kad apsimesti kitu asmeniu ir jo vardu vykdyti nusikaltimus (Štitilis, Laurinaitis, 2009, p. 244). Tuo tarpu Jungtinėje Karalystėje tapatybės vagystės sąvoka sietina tik su vienu nusikaltimu – tai veika, kurios metu bet kuris asmuo gauna pakankamai informacijos apie kito asmens tapatybę, siekiant įvykdyti tapatybės sukčiavimą, nepriklausomai nuo to, ar tai gyvo, ar jau mirusio asmens duomenys (EBPO, 2008, p. 60). Taip yra dėl to, kad kol kas nėra visuotinai pripažįstamos tapatybės vagystės elektroninėjė erdvėje sampratos. Nors

vienoda samprata galėtų užtikrinti didesnį efektyvumą, kovojant su tokio pobūdžio veikomis, ypač jei kalbama apie tarptautinį tapatybės vagystės veikos pobūdį (Štitilis, Laurinaitis, 2009, p. 244).

Apibendrinus daugelių autorių nuomones, galima pateikti bendrą šios veikos apibrėžimą: tapatybės vagystė – tai neteisėtas asmens tapatybę identifikuojančių duomenų įgijimas, ketinant įvykdyti sukčiavimą arba kitą neteisėtą veiką.

Bendrieji teisės aktai dėl tapatybės vagystės elektroninėje erdvėje

Asmens tapatybės vagystė elektroninėje erdvėje yra pakankamai nauja ir pavojinga asmeniui bei visuomenei veika. Todėl svarbu tampa apžvelgti šios veikos teisinį reglamentavimą, t.y. teisus aktus kaip įrankius kovai prieš šią žalingą veiką.

Kadangi tapatybės vagystės siekiamas rezultatas yra gauti asmens duomenys ir (ar) asmeninę informaciją, kurios pagalba galima identifikuoti asmenį, todėl neišvengiamai pirmiausiai susiduriama su asmens duomenų sąvoka ir šių duomenų apsauga (Štitilis ir kt., 2011, p. 151). Pirmasis ir vienintelis tarptautinis teisės aktas dėl asmens duomenų apsaugos – 1981 m. Strasbūro konvencija „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“. Kiekviena šalis gali savanoriškai pareikšti norą laikytis šios konvencijos. Šia proga pasinaudojo ir Lietuva, kuri 2000 m. vasario 11 d. pasirašė, o 2001 m. birželio 1 d. ratifikavo Strasbūro konvenciją. Lietuvoje ši konvencija įsigaliojo nuo 2001 m. spalio 1 d. (Valstybinė duomenų apsaugos inspekcija).

Europos Sąjungos lygiu šią sritį reglamentuoja 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Lietuvoje šią direktyvą įgyvendina LR asmens duomenų teisinės apsaugos įstatymas (Petraitytė, 2011, p. 165; Štitilis ir kt., 2011, p. 63). Šis įstatymas skirtas ginti žmogaus privataus gyvenimo neliečiamumo teisę, kai tvarkomi asmens duomenys automatiniu ir neautomatiniu būdu. Šis įstatymas užtikrina pagrindinių asmens duomenų apsaugos principų įgyvendinimą (Štitilis ir kt., 2011, p. 64) (žr. 3 lent.).

3 lentelė. Pagrindiniai asmens duomenų apsaugos principai

❖ Tikslo nustatymas ❖ Teisėtumas ❖ Asmens duomenų kokybė ❖ Proporcingumas	❖ Saugumo užtikrinimas ❖ Panaudojimo apribojimas ❖ Draudimas tvarkyti ypatingus asmens duomenis ❖ Individualus dalyvavimas	❖ Atvirumas ❖ Priežiūra ❖ Sankcijos

Šaltinis: sudaryta pagal Štitilis ir kt., 2011, p. 64.

Remiantis šiuo įstatymu, vykdomas visapusiškas asmens duomenų apsaugos teisinis reglamentavimas: asmens duomenų tvarkymas, duomenų subjekto teisės, duomenų saugumas, duomenų valdytojų registravimas, asmens duomenų teikimas duomenų gavėjams, kurie yra užsienio šalyse, nurodomos valstybės institucijos, atsakingos už asmens duomenų apsaugos srityje politikos formavimą ir šio įstatymo vykdymo priežiūrą, skundų tvarka ir atsakomybė už šio įstatymo nuostatų pažeidimus. Šio įstatymo vykdymą, išskyrus 8 str., prižiūri ir kontroliuoja Valstybinė duomenų apsaugos inspekcija (Valstybės žinios, 2008, Nr. 22-804). Šios institucijos pagrindinės veiklos sritys – teisės aktų dėl asmens duomenų apsaugos rengimas ir derinimas, asmens duomenų teisėto tvarkymo užtikrinimas, duomenų valdytojų priežiūros organizavimas ir tarptautinių įsipareigojimų vykdymas asmens duomenų apsaugos srityje (Valstybinė duomenų apsaugos inspekcija). Reikėtų pabrėžti, kad pažeidus asmens duomenų teisinės apsaugos reikalavimus, taikoma administracinė atsakomybė ir sankcijos gali siekti tik iki 2000 Lt. Pavyzdžiui, JAV gali būti skiriama iki 12000 dolerių už kiekvieną pažeidimo dieną (Štitilis ir kt., 2011, p. 65).

Pastaruoju metu vis didesnis dėmesys skiriamas elektroninių duomenų arba informacijos saugai techniniu ir teisiniu požiūriu visame pasaulyje. Elektroninės informacijos sauga – tai elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimo mechanizmas (Lietuvos Respublikos Vidaus reikalų ministerija (VRM), 2013). Kitaip tariant, tai informacijos ir sistemos infrastruktūros apsauga nuo bet kokio poveikio, kuris gali padaryti žalą informacijos arba sistemos infrastruktūros savininkams ir naudotojams (Davidavičienė ir kt., 2009, p. 409–410). Reikėtų pripažinti, kad Lietuva kol kas neturi vientiso įstatymo, užtikrinančio informacijos saugą: ši sritis fragmentiškai reglamentuojama įvairiuose teisės aktuose. Iš svarbesnių reikėtų paminėti šiuos (Štitilis ir kt., 2011, p. 66–67): LR asmens duomenų teisinės apsaugos įstatymas (30 str.), LR elektroninių ryšių įstatymas (62 str.), LR elektroninio parašo įstatymas ir kt. Esančios įstatymų nuostatos dėl elektroninės informacijos saugos neįtvirtina dalį svarbių visuomeninių santykių, pavyzdžiui, ypatingos svarbos elektroninės informacijos infrastruktūros saugos (Štitilis, Klišauskas, 2012, p. 449). Taigi, šios srities reguliavimas teisiniu aspektu yra nepakankamas (Štitilis ir kt., 2011, p. 67). Toks e. informacijos ir elektroninių sistemų nenuoseklus ir paviršutiniškas reglamentavimas stabdo saugios informacinės visuomenės plėtrą ir neskatina pasitikėjimo informacine visuomene. Siekiant išspręsti šią problemą, reikėtų priimti pamatinį įstatymą, apimantį visas svarbias sritis, susijusias su elektroninės informacijos sauga (Štitilis, Klišauskas, 2012, p. 449).

Šiuo metu Lietuvoje kelios institucijos yra atsakingos už elektroninės informacijos saugą. Vidaus reikalų ministerija turi formuoti politiką valstybės informacinių išteklių saugos ir informacinių

technologijų taikymo viešojo administravimo (elektroninės valdžios) srityse (Valstybės žinios, 2011, Nr. 163-7739). Valstybinė duomenų apsaugos inspekcija privalo plėtoti duomenų apsaugą, kontroliuoti teisėtą asmens duomenų tvarkymą, kovoti su duomenų tvarkymo pažeidimais. Ryšių reguliavimo tarnyba turi užtikrinti tinkamą nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT veiklą, rengti rekomendacijas dėl galimų būdų apsisaugoti nuo elektroninės informacijos saugos pažeidimų. Taigi, šiuo metu nėra vienos institucijos, kuri būtų atsakinga už šią sritį, o išvardintų institucijų funkcijos atitinkamais atvejais dubliuojasi (Štitilis ir kt., 2011, p. 67).

Už informacijos saugos nustatytų reikalavimų nesilaikymą, kyla administracinė arba baudžiamoji atsakomybė (Štitilis ir kt., 2011, p. 68). Pavyzdžiui, LR Administracinių teisės pažeidimų kodekso 214 $^{(15)}$str. Neteisėtas valstybės informacinių sistemų duomenų tvarkymas (Valstybės žinios, 1998, Nr. 40-1065). LR Baudžiamojo kodekso XXX skyriuje įtvirtinta atsakomybė už nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui (Valstybės žinios, 2000, Nr. 89-2741).

Paskutinė svarbi sritis, siekiant tinkamai užtikrinti kiekvieno fizinio ar juridinio asmens tapatybę, tai asmens identifikavimo teisinis reguliavimas.

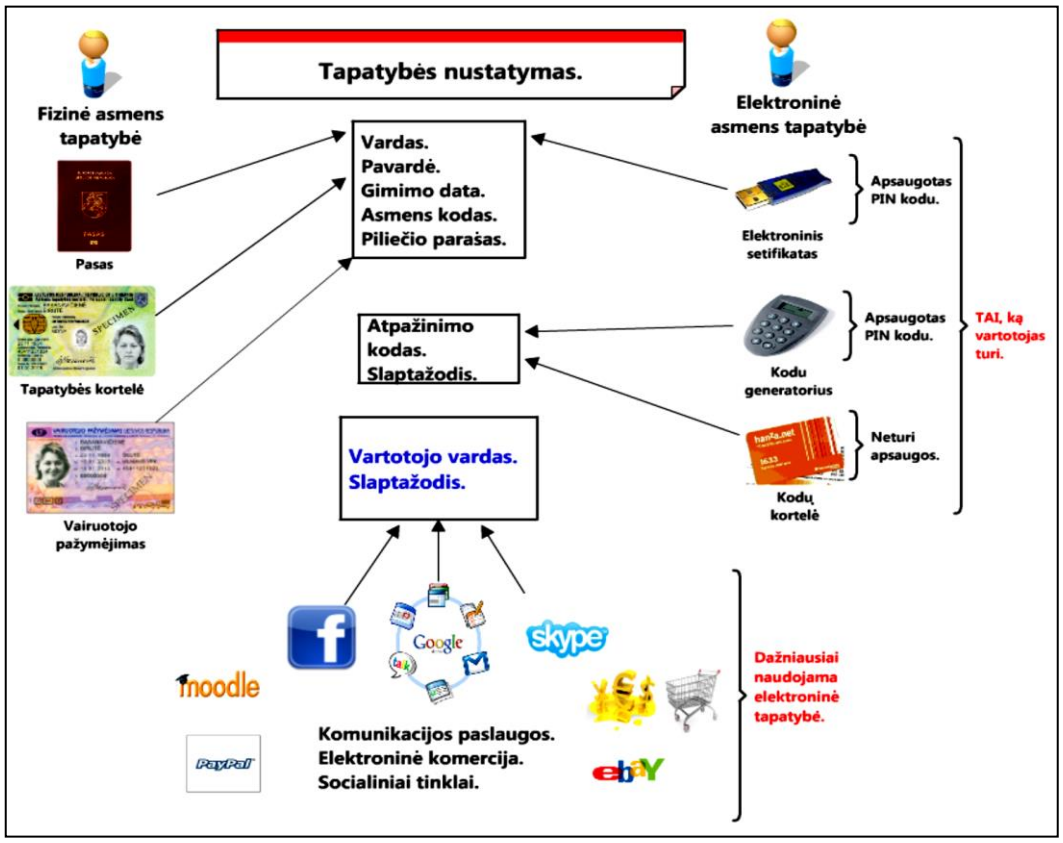
Šiuo metu jau galima išvardinti tris svarbiausius asmens identifikavimo elektroninėje erdvėje būdus:

1) identifikavimas remiantis priemonėmis, kurias turi žinoti tik vartotojas: elektroninėje erdvėje asmens tapatybė gali būti užtikrinama panaudojant unikalų vardą ir slaptažodį. Taigi, kiekvieno asmens identifikatoriai privalo būti vienetiniai ir unikalūs;
2) identifikavimas pagal vartotojo turimas priemones – tai elektroninis parašas (patvirtintas elektroniniu sertifikatu), kodų generatoriai, kodų lentelės;
3) identifikavimas pagal tai, kas yra vartotojas: tam panaudojami unikalūs bei specifiniai asmens fiziologiniai ir elgsenos biometriniai duomenys (žr. 13 pav.) (Štitilis ir kt., 2011, p. 70).

Lietuvoje, kaip ir JAV, teisiškai pripažįstamas ir reguliuojamas asmens identifikavimas elektroninėje erdvėje, panaudojant e. parašą, patvirtintą elektroniniu sertifikatu (Štitilis ir kt., 2011, p. 70).

Šiuo metu elektroninį parašą ir elektroninį sertifikatą, kaip būdą patvirtinti asmens tapatybę elektroninėje erdvėje, reglamentuoja šie pagrindiniai Lietuvos Respublikos teisės aktai:

- LR elektroninio parašo įstatymas (Valstybės žinios, 2000, Nr. 61-1827);
- LR asmens tapatybės kortelės įstatymas (Valstybės žinios, 2001, Nr. 97-3417);
- LR vidaus reikalų ministro 2002 m. liepos 11 d. įsakymas Nr. 338 „Dėl valstybės tarnautojo pažymėjimo formos ir valstybės tarnautojo pažymėjimo išdavimo taisyklių patvirtinimo“ pakeitimo (Valstybės žinios, 2009, Nr. 139-6133).



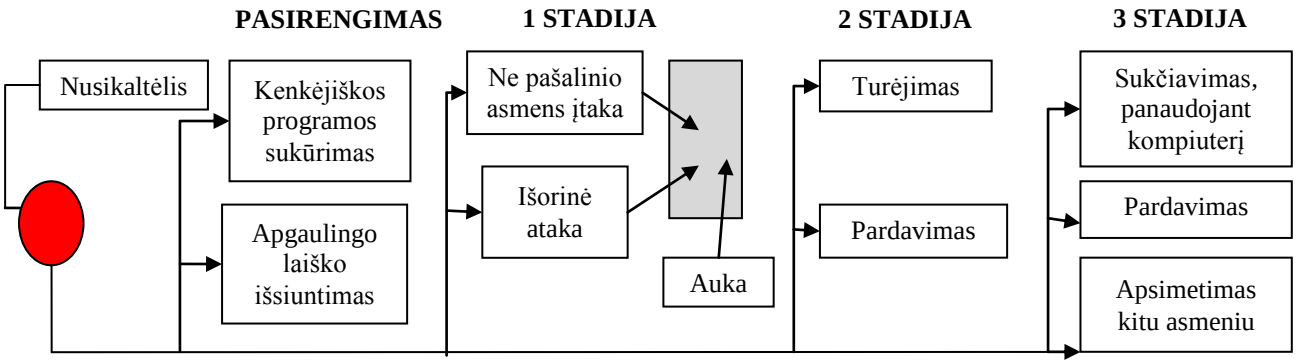
Šaltinis: Laurinaitis seminarų pranešimų medžiaga, 2012.

13 pav. Tapatybės nustatymas elektroninėje erdvėje

Apibendrinus teisinį reglamentavimą dėl tapatybės vagystės elektroninėje erdvėje, galima teigti, kad šiuo metu nuosekliai užtikrinama asmens duomenų apsauga ir elektroninio parašo taikymas praktikoje. Didžiausia kliūtis, tinkamai užtikrinti asmens tapatybės apsaugą e. erdvėje – fragmentiškas elektroninės informacijos saugos įtvirtinimas teisiniu aspektu. Šiuo atveju tinkamas sprendimas būtų priimti vientisą įstatymą, apžvelgiant visas svarbias sritis, susijusias su elektroninės informacijos sauga.

Tapatybės vagystės elektroninėje erdvėje kriminalizavimas

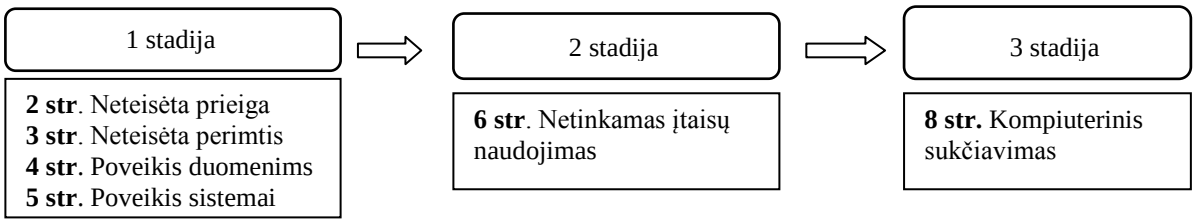
Mokslinėje literatūroje dažniausiai skiriamos tris tapatybės vagystės stadijos: 1 stadija – su tapatybe susijusios informacijos gavimas, 2 stadija – su tapatybe susijusios informacijos turėjimas, 3 stadija – su tapatybe susijusios informacijos panaudojimas, siekiant įvykdyti nusikalstamą veiką (Gercke, 2007, p. 19–20; Kalpokas, Marcinauskaitė, 2012, p. 41; Štitilis ir kt., 2011, p. 71) (žr. 14 pav.).



Šaltinis: sudaryta pagal Gercke, 2007, p. 20.

14 pav. Tapatybės vagystės trijų stadijų modelis

JAV yra viena iš pirmaujančių šalių elektroninių nusikaltimų srityje: užimą antrą vietą pasaulio mastu. Todėl ši šalis turi pakankamai patirties kovojant su šiais nusikaltimais. Ši valstybė, kaip ir Lietuva, tapo konvencijos dėl elektroninių nusikaltimų narė. JAV konvenciją ratifikavo 2006 m. rugsėjo 29 d., nuo 2007 m. sausio 1 d. ji įsigaliojo šalyje. Lietuva šią konvenciją ratifikavo 2004 m. kovo 18 d., šalyje įsigaliojo nuo 2004 m. liepos 1 d. (Štitilis ir kt., 2011, p. 72). Remiantis konvencija, 1 tapatybės vagystės stadiją kriminalizuoja 2, 3, 4 ir 5 straipsniai, 2 stadiją – 6 straipsnis, ir 3 stadiją – 8 straipsnis (Gercke, 2007, p. 22–27) (žr. 15 pav.).



Šaltinis: sudaryta pagal Gercke, 2007, p. 22–27.

15 pav. Tapatybės vagystės stadijų kriminalizavimas konvencijoje dėl elektroninių nusikaltimų

Visos trys tapatybės vagystės stadijos JAV yra kriminalizuotos: 1 stadiją įtvirtina šalies įstatymų sąvado 18 skirsnio 1 dalies 47 skyriaus 1030 straipsnis (sukčiavimas, panaudojant kompiuterį), 2 stadiją – 1002 straipsnis (suklastotų dokumentų turėjimas) ir 1028 straipsnis (baudžiamoji atsakomybė už sukčiavimą, susijusį su tapatybės nustatymo dokumentais, autentifikavimo priemonėmis, informacija

(turėjimas, perdavimas, prekyba)), 3 stadiją – 1028 straipsnis (neteisėtas dokumentų, autentifikavimo priemonių ir informacijos gaminimas, klastojimas) ir 1037 straipsnis (baudžiamoji atsakomybė už sukčiavimą, panaudojant e. paštą). 2 ir 3 tapatybės vagystės stadijos yra įtvirtintos kaip savarankiškos nusikalstamos veikos 1028 straipsnio (a) dalies (7) punkte. Pažymėtina, kad 1998 m. JAV tapatybės vagystė buvo kriminalizuota kaip savarankiška veika. Numatoma bausmė yra laisvės atėmimas iki 5 metų, o nusikaltimą įvykdžius sunkinančiomis aplinkybėmis – iki 15 metų (Štitilis ir kt., 2011, p. 72–73).

LR Baudžiamajame kodekse tapatybės vagystė kaip savarankiška nusikalstama veika nėra įtvirtinta (Valstybės žinios, 2000, Nr. 89-2741). Daugelis siūlo pasekti JAV pavyzdžiu ir kriminalizuoti tapatybės vagystę kaip atskirą nusikaltimą, nes šią veiką yra lengviau įrodyti nei sukčiavimą (Europos Bendrijų Komisija, 2007, p. 8; Štitilis, Laurinaitis, 2009, p. 246). Vietoj nusikalstamų veikų daugeto tuomet reikėtų įrodinėti tik vieną nusikalstamą veiką (Štitilis, Laurinaitis, 2009, p. 246).

1 tapatybės vagystės stadiją kriminalizuoja LR baudžiamojo kodekso 166, 167, 198, 198 $^{(1)}$ ir 214 straipsniai (Štitilis ir kt., 2011, p. 73):

- „166 straipsnis. Asmens susižinojimo neliečiamumo pažeidimas;
- 167 straipsnis. Neteisėtas informacijos apie privatų asmens gyvenimą rinkimas;
- 198 straipsnis. Neteisėtas elektroninių duomenų perėmimas ir panaudojimas;
- 198$^{(1)}$ straipsnis. Neteisėtas prisijungimas prie informacinės sistemos;
- 214 straipsnis. Netikros elektroninės mokėjimo priemonės gaminimas, tikros elektroninės mokėjimo priemonės klastojimas ar neteisėtas disponavimas elektronine mokėjimo priemone arba jos duomenimis“ (Valstybės žinios, 2000, Nr. 89-2741).

2 stadija (laikymas, perdavimas) dalinai įtvirtinama 198 ir 214 straipsniuose: su tapatybe susijusios informacijos turėjimas nėra kriminalizuotas, baudžiamoji atsakomybė taikoma tik neviešų elektroninių duomenų bei svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių laikymui. 3 tapatybės vagystės stadiją kriminalizuoja 182, 207, 215 ir 300 straipsniai (Štitilis ir kt., 2011, p. 73):

- „182 straipsnis. Sukčiavimas;
- 207 straipsnis. Kreditinis sukčiavimas;
- 215 straipsnis. Neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas;
- 300 straipsnis. Dokumento suklastojimas ar disponavimas suklastotu dokumentu” (Valstybės žinios, 2000, Nr. 89-2741).

Mokslininkai Kalpokas ir Marcinauskaitė (2012, p. 41–48) tik dalinai sutinka su šiuo tapatybės vagystės stadijų kriminalizavimo sąrašu (žr. 4 lent.). 1 tapatybės vagystės stadijai priskiria 198 $^{(2)}$ str. („neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais

duomenimis“) (Valstybės žinios, 2000, Nr. 89-2741)). Tai įvairios specialios priemonės arba įrankiai, skirti asmens tapatybei elektroninėje erdvėje liudijančios informacijos elementams gauti, sukūrti, gabenti, įgyti ir pan. Todėl sutikčiau, kad 166 str. ir 167 str. tiksliau kriminalizuotų 198 $^{(2)}$ straipsnis. Šie mokslininkai 198 $^{(1)}$ straipsnį priskiria ne pirmai, o trečiai stadijai, kuris atitinka konvencijos 2 straipsnį. Jie teigia, kad neteisėtas prisijungimas prie informacinės sistemos, pažeidžiant informacinės sistemos apsaugos priemones – tarpinis etapas sukčiavimo elektroninėje erdvėje įvykdymo schemoje. Paskutinei stadijai priskiria ir 214 straipsnyje numatytą nusikalstamą veiką, t.y. neteisėtas svetimų elektroninės mokėjimo priemonės naudotojo duomenų, patvirtinančių tapatybę, įgijimas, kurių pakanka finansinei operacijai inicijuoti. 215 str. neapima šios nusikalstamos veikos: įtvirtinamas tik neteisėtas finansinės operacijos inicijavimas, panaudojant tokius duomenis.

Išanalizavus ir apibendrinus mokslininkų nuomones, autorės sudarytas tapatybės vagystės stadijų kriminalizavimo skirstymas (žr. 4 lent.).

4 lentelė. Tapatybės vagystės stadijų kriminalizavimas, remiantis LR baudžiamojo kodekso 166, 167, 182, 198, 198 $^{(1)}$, 198 $^{(2)}$, 207, 214, 215 ir 300 straipsniais

Tapatybės vagystės stadija	1 stadija	2 stadija	3 stadija
Štitilis, Pakutinskas, Dauparaitė, Laurinaitis	166, 167, 198, 198$^{(1)}$ ir 214 straipsnis	198 ir 214 straipsnis	182, 207, 215 ir 300 straipsnis
Kalpokas, Marcinauskaitė	198 $^{(2)}$, 198, 214 straipsnis	198 $^{(2)}$, 198, 214 straipsnis	198$^{(1)}$, 215, 182, 214 straipsnis
Autorės skirstymas	198, 198$^{(1)}$, 198 $^{(2)}$, 214 straipsnis	198, 198 $^{(2)}$, 214 straipsnis	182, 207, 215 ir 300 straipsnis

Šaltinis: sudaryta autorės, pagal Kalpokas, Marcinauskaitė, 2012, p. 41–48; Štitilis ir kt., 2011, p. 73.

Baudžiamoji atsakomybė už atitinkamas pavojingas veikas, susijusias su tapatybės vagyste, Lietuvoje gali siekti iki 26 000 Lt, o laisvės atėmimas skiriamas nuo 3 iki 6 metų (Štitilis ir kt., 2011, p. 168). JAV yra taikoma tik laisvės atėmimo sankcija nuo 5 iki 15 metų (Štitilis ir kt., 2011, p. 73). Nigerijoje už šią nusikalstamą veiką gali būti baudžiama laisvės atėmimu iki gyvos galvos. Prancūzijoje bauda gali siekti iki 300 000 eurų (Štitilis ir kt., 2011, p. 248). JAV, Nigerijos ir Rusijos baudžiamuosiuose įstatymuose įtvirtintos griežčiausios sankcijos. Švelniausias sankcijas reglamentuoja Estijos ir Suomijos baudžiamasis kodeksas. Didžiausia sankcijų įvairovė dėl tapatybės vagystės elektroninėje erdvėje įtvirtinta Rusijos ir Kinijos baudžiamuosiuose įstatymuose (Štitilis ir kt., 2011).

Skirtingos sankcijos ir jų dydis skatina nusikaltimus daryti tose valstybėse, kur sankcijos už šią nusikalstamą veiką yra mažesnės (Štitilis ir kt., 2011, p. 168). Skirtingas tapatybės vagystės elektroninėje erdvėje vertinimas baudžiamuoju teisės požiūriu apsunkina šių veikų susekimą, tyrimą ir baudžiamąjį persekiojimą nacionaliniu bei tarptautiniu mastu (Štitilis ir kt., 2011).

Apibendrinant galima teigti, kad Lietuvoje asmens tapatybės vagystė nėra kriminalizuota kaip savarankiška nusikalstama veika, dėl to praktikoje yra sunkiau įrodyti. Šiuo atveju reikia pagrįsti sukčiavimo veiksmus, remiantis plačiu nusikalstamų veikų sąrašu. Sankcijos už šią neteisėtą veiką yra mažesnės lyginant su daugelių kitų šalių. Taigi, sudaromos palankesnės sąlygos vykdyti šiuos nusikaltimus būtent Lietuvoje. Skirtingas kriminalizavimas įvairiuose valstybėse atveria spragas dėl baudžiamojo persekiojimo kitose šalyse.

Tapatybės vagystės elektroninėje erdvėje įvykdymo būdai

Atsižvelgiant į tapatybės vagystės elektroninėje erdvėje įvykdymo būdus, suformuojamos tikslesnės ir efektyvesnės prevencijos priemonės, šios pavojingos veikos rizikai mažinti. Šių būdų žinojimas palengvina tokių veikų tyrimą ir užtikrina tikslesnį jų reglamentavimą bei vertinimą baudžiamosios, civilinės ar administracinės teisės pozicijose (Štitilis ir kt., 2011, p. 131).

Pasitelkiant modernias technologijas, tapatybės vagystė gali būti įvykdyta panaudojant vieną iš trijų būdų: kenkimo programinė įranga (angl. malware), slaptažodžio žvejyba (angl. phishing, pasword phishing), įsibrovimas (angl. hacking) (EBPO, 2008, p. 3).

Kenkimo programos, įdiegtos į vartotojo kompiuterį, pačios surenka reikalingus duomenis ir juos persiunčia tretiesiems asmenims (Kalpokas, Marcinauskaitė, 2012, p. 37). Tai įvairūs virusai, kirminai, Trojos arkliai, klaviatūros mygtukų paspaudimų fiksavimas, atgalinių durų virusai, šnipinėjimo programa, šakninės programos ir kt. (EBPO, 2008, p. 3). Šias programas galima aptikti ir nukenksminti, pasitelkiant antivirusinę programinę įrangą, tačiau didžiulė šių pavojingų programų įvairovė ir naujų modifikacijų plėtra lemia, kad tam tikrą laiką jos gali likti nepastebėtos. Kenkimo programinės įrangos dažniausiai platinamos interneto pagalba: vartotojui tereikia apsilankyti tam skirtose interneto svetainėse (Kalpokas, Marcinauskaitė, 2012, p. 37). Pasak daugelio mokslininkų, dažniausiai naudojamos dvi kenkėjiškos programos:

- *Trojos arklys* (angl. trojans, Trojan horse) (Klangauskas, 2012, p. 32; Štitilis ir kt., 2011, p. 130) – tai klaidinanti programa, kuri dedasi atliekanti naudingą uždavinį, tačiau iš tikrųjų pagrindinė šios programos paskirtis yra naikinti ir gadinti kompiuteryje esančius duomenis,

programas (Štitilis ir kt., 2011, p. 130). Pavojingiausios programos pasisavina informaciją ir paskui persiunčia ją tretiesiems asmenims, dažnai elektroniniu paštu arba panaudojant internetines svetaines. Naudojant šią kenkėjišką programą, gali būti įvykdytas ir elektroninių komunikacijų perėmimas (Higgins, 2010, p. 69);

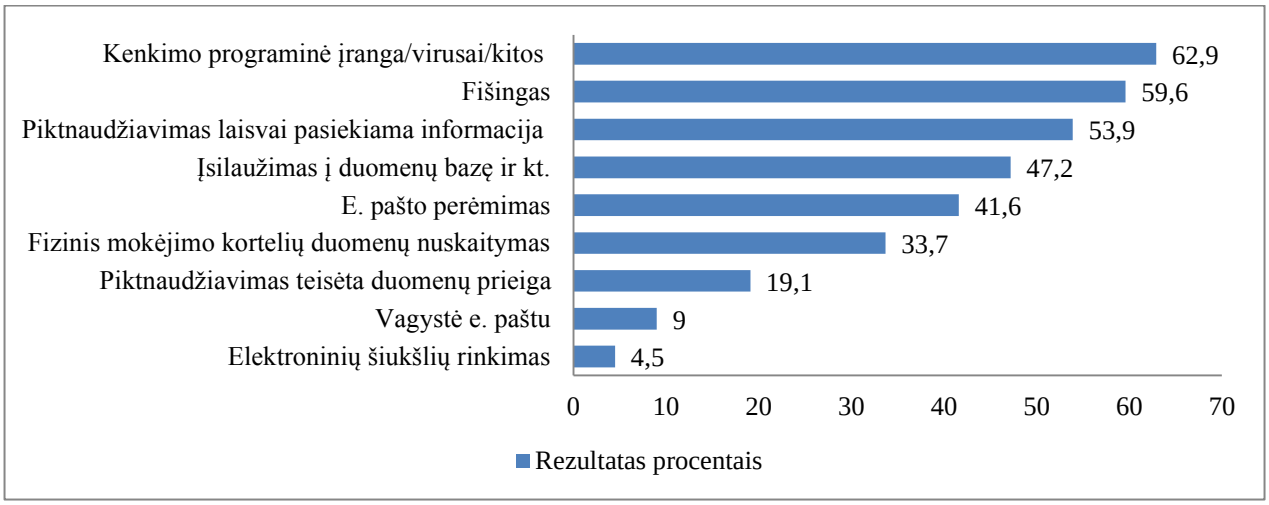
- *šnipinėjimo programinė įranga* (angl. spyware) – tai neteisėtai įdiegta programinė įranga, kurios pagalba siekiama gauti tokią svarbią informaciją kaip vartotojų vardai, slaptažodžiai, kitą saugomą informaciją arba prieigą prie finansinės informacijos. Pavogta informacija siunčiama elektroniniu būdu (Wang, Huang, 2011, p. 11; Štitilis ir kt., 2011, p. 129–130) arba nuskaitoma pažeidėjų (Wang, Huang, 2011, p. 11).

Slaptažodžio žvejyba (duomenų vagystė, fišingas) – tai metodas, kai vartotojų duomenys išgaunami prisidengiant realių finansinių arba kitų institucijų vardu. Tai gali būti vykdoma pasitelkiant suklastotus elektroninio pašto laiškus arba interneto tinklalapius (žr. 5 priedą) (EBPO, 2008, p. 3; Robinson et al., 2011, p. 128; Kalpokas, Marcinauskaitė, 2012, p. 34; Štitilis ir kt., 2011, p. 127). Modifikuotu fišingo variantu gali būti įvardinamas farmingas (apgaulinga IP taktika (Štitilis ir kt., 2011, p. 130)) (Kalpokas, Marcinauskaitė, 2012, p. 35). Šiuo atveju aukos kompiuteryje arba tarpiniuose interneto serveriuose įvykdomi atitinkami pakeitimai, t.y. pasinaudojama sričių vardų serverių (toliau – DNS) naudojimo pažeidimais, kurių dėka vartotojai nepastebimai nukreipiami į suklastotas interneto svetaines (Kalpokas, Marcinauskaitė, 2012, p. 35–36; Štitilis ir kt., 2011, p. 130). DNS serverio modifikacijos vartotojui yra nematomos, net ir antivirusinės programos tokių pakeitimų neaptinka, nes pačiuose kompiuteriuose pakeitimai nevykdomi. Tačiau nėra taip lengva modifikuoti DNS serverius, nes juos prižiūri interneto paslaugų teikėjai. Todėl gali būti panaudotas lengvesnis būdas: atakuojami tinklo maršruto parinktuvai, kurie suteikia vartotojams prieigą prie interneto. Maršruto parinktuvo konfigūracijoje yra nurodomas interneto paslaugų teikėjo (toliau – IPT) paskirtas DNS serverio adresas ir galima padaryti pokyčius, kurie leistų visoms vartotojų užklausoms keliauti ne per IPT, o suklastotą DNS serverį. Reikėtų pabrėžti, kad didesnė grėsmė kyla, kai naudojami bevielio ryšio maršruto parinktuvai, nes juos galima pasiekti iš išorės. Pakeitimai maršruto parinktuvo konfigūracijoje paprastam šio interneto savininkui yra nematomi (Kalpokas, Marcinauskaitė, 2012, p. 36–37).

Įsibrovimas – tai būdas, kai apeinamos sistemos saugumo priemonės ir sukčius gauna prieigą prie sistemos arba elektroninių ryšių tinklo. Šiuo atveju išnaudojami ir saugumo trūkumai, neapsaugoti bevieliai ir intraneto tinklai arba pasinaudojama sistemomis, kuriuose yra atjungtos apsaugos funkcijos (Štitilis ir kt., 2011, p. 125). Taikant šį būdą, pasinaudojama elektroninių sistemų arba programinės

įrangos pažeidžiamumu (EBPO, 2008, p. 3). Šiuo atveju įvykdoma neteisėta prieiga prie informacinių sistemų (Robinson et al., 2011, p. 87).

Šių tapatybės vagystės elektroninėje erdvėje metodų populiarumą patvirtina Strategijos ir vertinimo paslaugų centro (toliau – CSES) 2012 metais atlikta internetinė apklausa (žr. 16 pav.).



Šaltinis: Europos Komisija, 2012, p. 44.

16 pav. Tapatybės vagystės elektroninėje erdvėje įvykdymo būdų tendencijos

Pasaulyje egzistuoja ir kiti metodai, tačiau visų jų veikimas paremtas tinklų, sistemos saugumo ar technologinių trūkumų išnaudojimu. Svarbu tampa stebėti ir įvardinti naujus tapatybės vagystės elektroninėje erdvėje įvykdymo metodus, siekiant užtikrinti tinkamą saugumo ir duomenų perdavimo lygį.

Taigi, dažniausiai taikomi trys tapatybės vagystės elektroninėje erdvėje įvykdymo būdai: kenkimo programinė įranga (62,9 proc.), kuri dažniausiai patenka į vartotojų kompiuterį elektroninių tinklų pagalba, slaptažodžio žvejyba (59,6 proc.), prisidengiant realių institucijų vardu, įsibrovimas į duomenų bazę ir kt. (47,2 proc.), pasinaudojant sistemos saugumo ar technologinėmis spragomis.

3. ELEKTRONINIO PARAŠO INFRASTRUKTŪROS PLĖTRA

Elektroninio parašo infrastruktūra – tai priemonių visuma, kurių dėka užtikrinamas elektroninio parašo naudojimas ir keliama visuomenės kompetencija elektroninio parašo tema (RRT, 2013, p. 11). Remiantis LR Vyriausybės 2011 m. sausio 17 d. nutarimu Nr. 32, elektroninio parašo priežiūros funkcijas pavesta vykdyti Lietuvos Respublikos Ryšių reguliavimo tarnybai (Valstybės žinios, 2011, Nr. 8-316), kuri skatina elektroninio parašo infrastruktūros plėtrą, vykdydama elektroninio parašo naudotojų mokymą ir kompetencijos kėlimą (RRT, 2013, p. 11). Elektroninio parašo naudojimas skatinamas asmenis konsultuojant elektroninio parašo taikymo klausimais ir didinant pasitikėjimą sertifikavimo paslaugų teikėjais ir jų paslaugomis (RRT, 2012, p. 63). 2011 m. ši tarnyba perėmė iš Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos elektroninio parašo ir elektroninio dokumento nuotolinio mokymo sistemą ir įvykdė subdomeno įsigijimą, t. y. *elektroninisparasas.lt.* 2012 m. ši mokymo sistema buvo atnaujinta: ištaisyta pasenusi informacija, įtvirtintas greitesnis ir lengvesnis informacijos radimo procesas. Tokių veiksmų atlikimui buvo įgyvendintas projektas „Nuotolinės elektroninio parašo ir elektroninio dokumento mokymo sistemos modernizavimas“. Tai galimybė ne tik gauti reikalingas žinias, bet ir pasitikrinti jas testų pagalba bei gauti elektroninį pažymėjimą, išlaikius testą (RRT, 2013, p. 11–12).

LR Ryšių reguliavimo tarnyba 97 kartus teikė atsakymus elektroniniu paštu, telefonu arba susitikimų metu į įvairius visuomenės klausimus dėl elektroninio parašo naudojimo ir teisinio reglamentavimo. Asmenys pageidavo sužinoti apie pasirašymą planšetėse su jutikliniais ekranais, apie esamus elektroninio parašo formatus ir priemones, reikalingas elektroninio parašo kūrimui, apie laiko žymas, galimybę užsienio piliečiui gauti elektroninio parašo formavimo priemones ir kt.

2012 m. RRT atstovai aktyviai dalyvavo pasitarimuose, darbo grupėse dėl elektroninio parašo naudojimo perspektyvų ir teisinio reglamentavimo:

- bendradarbiaujant su LR vyriausiojo archyvaro tarnyba buvo sprendžiamas elektroninių dokumentų specifikacijų įteisinimas bei reikalavimai elektroninių dokumentų specifikacijoms, svarstomas elektroninio dokumento pdf specifikacijos būtinumas;
- dalyvavo LR teisingumo ministerijos surengtame pasitarime, sprendžiant elektroninio parašo taikymo galimybes teismų sistemose;
- dalyvavo LR vidaus reikalų ministerijos surengtame susitikime, siekiant nustatyti teisines galimybes, leidžiančias atidaryti banko sąskaitą nuotoliniu būdu bei kt. (RRT, 2012, p. 64).

Kartu su LR Susisiekimo ir Užsienio reikalų ministerija surengė NB8 (Nordic Baltic 8) seminarą „Practical Aspects of E-Signature and E-Documents Use in the Framework of Digital Single Market“, kuriame buvo diskutuojama dėl Europos Parlamento ir Tarybos reglamento dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje projekto bei naujovių ES valstybės narėms.

2012 m. teikė oficialias konsultacijas valstybės įstaigoms ir įmonėms, privačioms įmonėms. Pavyzdžiui, Lietuvos vyriausiojo archyvaro tarnybai buvo suteiktas paaiškinimas dėl pasirašymo planšetėse su jutikliniu ekranu, AB „SEB“ bankui išdėstė savo poziciją raštu, sprendžiant skirtingų e. parašo ir elektroninių dokumentų naudojimo galimybes, VĮ Ignalinos atominei elektrinei buvo pateiktas atsakymas dėl elektroninio parašo galiojimo tikrinimo, remiantis teisės aktais, ir kt. (RRT, 2013, p. 13).

Taigi, Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos pradėtą veiklą toliau vykdo RRT. Ši institucija 2012 m. atnaujino nuotolinio e. parašo ir e. dokumento mokymo sistemą, tęsia konsultacijų teikimą fiziniams ir juridiniams asmenims elektroninio parašo tema. Reikėtų pabrėžti, kad dažniausiai asmenys ar institucijos/įstaigos kreipiasi į RRT su prašymu dėl elektroninio parašo taikymo. Šiuo metu didelė dalis pasitarimų inicijuojama sprendžiant elektroninių dokumentų klausimus ir e. parašo taikymą teismų procese. Siekiant užtikrinti didesnes e. parašo taikymo galimybes, žengtas pirmas žingsnis diskutuojant dėl elektroninio parašo taikymo ES mastu.

3.1. Elektroninio parašo naudojimas viešojo ir privataus sektoriaus veikloje

Elektroninio parašo teisinis reglamentavimas Lietuvoje atvėrė dideles šio parašo taikymo galimybes viešojo ir privataus sektoriaus veikloje: naudoti vidaus dokumentams ir siunčiamiesiems raštams pasirašyti. Tai galimybė fiziniams ir juridiniams asmenims bendrauti su viešojo sektoriaus įstaigomis elektroniniu būdu: pateikti prašymą, skundą, paklausimą ir kt. Elektroninis parašas gali būti naudojamas ne tik elektroninių dokumentų pasirašymui, bet ir pritaikytas elektroninių paslaugų teikimui ir jų gavimui (RRT, 2013, p. 9).

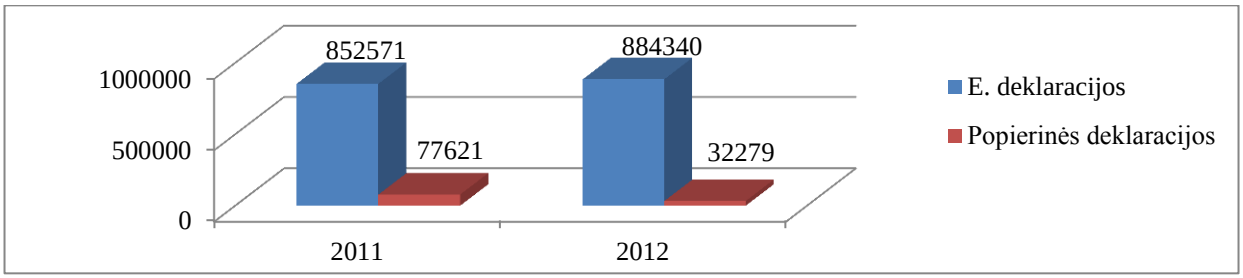
Šiuo metu Lietuvoje nėra technologinių galimybių registruoti visus elektroninio parašo naudojimo kartus, todėl siekiant išsiaiškinti šio parašo naudojimo apimtį, reikia analizuoti atskirus viešųjų elektroninių paslaugų rinkos segmentus (RRT, 2013, p. 10).

Pirmoji pagal paklausą elektroninė viešoji paslauga Lietuvoje yra mokesčių deklaravimas. Valstybinė mokesčių inspekcija (toliau – VMI) teikia skirtingas elektronines paslaugas tiek gyventojams,

tiek verslui: mokesčių deklaravimas, galimybė gauti pažymas, verslo liudijimų išdavimas. Šių paslaugų teikimas vykdomas panaudojant keturias skirtingas informacines sistemas:

- EDS sistema, skirta elektroniniam deklaravimui;
- Mano VMI – tai sistema, prie kurios prisijungus yra galimybė pratęsti arba įsigyti naują verslo liudijimą, grąžinti mokesčio permoką, sumokėti mokesčius, atlikti duomenų įvedimą/keitimą/panaikinimą ir kt.;
- Akcizų informacinė sistema atveria elektroninį sprendimą akcizo mokesčių deklaravimui ir administravimui;
- Epris sistema – tai elektroninių prašymų registravimo informacinė sistema, skirta užtikrinti PVM mokesčių administravimą ir grąžinimą.

Vienos elektroninės deklaracijos sutvarkymas kainuoja 2,5 Lt, o popierinės – apie 6 litus, todėl didėjant elektroninių deklaracijų apimčiai, užtikrinama efektyvesnė mokesčių inspekcijos veikla (UAB „Peritus sprendimai“, 2013, p. 186–187). Elektroniniu būdu pateiktų metinių pajamų deklaravimas beveik galutinai perkeltas į elektroninę erdvę (žr. 17 pav.): 2012 metais elektroniniu būdu buvo pateikta 884 340 (96,48 proc.) metinių pajamų deklaracijų (2011 – 852 571 (91,66 proc.)) (VMI, 2013).



Šaltinis: sudaryta pagal VMI, 2013.

17 pav. 2011–2012 m. metinių pajamų deklaracijų statistika

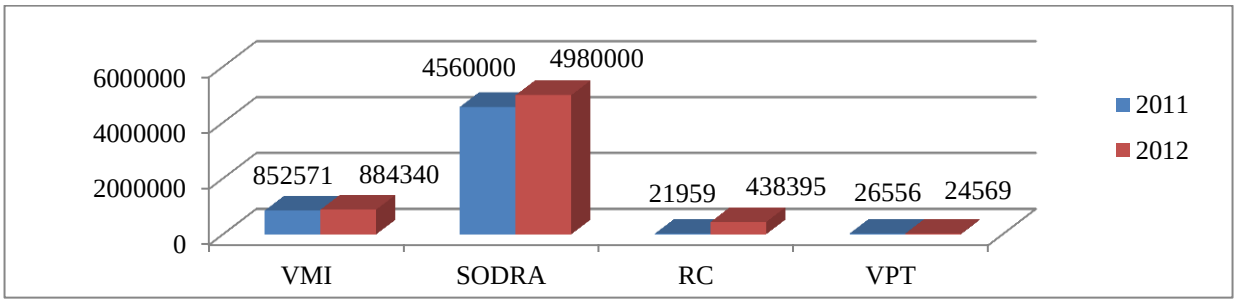
VMI elektroninį parašą artimiausiu metu plačiau planuoja naudoti sukūrus ir įdiegus Elektroninio švietimo ir konsultavimo paslaugų sistemą (ESKIS): pažymų teikimas mokesčių mokėtojams, mokestinių paskolų pasirašymas, mokesčių mokėtojams rengiamų dokumentų pasirašymas (ADOC formatu) ir kt. (RRT, 2012, p. 14). Šiuo projektu bus įgyvendintas „vieno langelio“ principas VMI paslaugų teikimui (projekto pabaiga – 2014 m. birželio mėn.) (VMI, 2013, p. 1, 3). Elektroninį parašą planuojama taikyti diegiamoje Darbo organizavimo ir dokumentų valdymo sistemoje (DODVS) vidinių bei išorinių dokumentų rengimui (RRT, 2012, p. 14–15).

Nuo 2008 m. sausio 1 d. draudėjai per Elektroninę draudėjų aptarnavimo sistemą (EDAS) SODRAI gali pateikti elektroninius socialinio draudimo pranešimus ir prašymus, pasirašytus kvalifikuotu elektroniniu parašu, gauti informaciją iš duomenų bazės (RRT, 2012, p. 14; SODRA, 2012). Nuo 2009 m. spalio 1 d. sveikatos priežiūros įstaigos šiai institucijai gali pateikti elektroninius nedarbingumo, nėštumo ir gimdymo atostogų pažymėjimus, gydytojų pasirašytus kvalifikuotu elektroniniu parašu, naudojantis elektroninių pažymėjimų tvarkymo sistema (EPTS). Nuo 2010 m. sausio 1 d. gyventojai per Elektroninę gyventojų aptarnavimo sistemą (EGAS) gali pateikti prašymus dėl išmokos, pašalpos, pensijos, kompensacijos skyrimo, teikti kvalifikuotu elektroniniu parašu pasirašytas elektronines valstybinio savanoriškojo socialinio draudimo sutartis (RRT, 2012, p. 14; UAB „Peritus sprendimai“, 2013, p. 187). Nuo 2011 m. sausio 1 d. piliečiai ir įvairių institucijų bei įmonių darbuotojai vietoj tradicinių dokumentų gali teikti elektroninius dokumentus, pasirašytus elektroniniu parašu ir atitinkančius ADOC specifikacijos reikalavimus (RRT, 2012, p. 14). SODROS teikiamų elektroninių paslaugų paklausą atspindi per šias sistemas perduotų elektroninių dokumentų, pasirašytų elektroniniu parašu, apimtis: 2012 metais buvo perduota 4,98 mln. e. dokumentų (2011 m. – 4,56 mln.). Taigi, jei vieną dokumentą sudaro du A4 formato lapai ir kiekvienas jų sveria 5 g., tai visų šių dokumentų svoris sudarytų 50 000 tonų (UAB „Peritus sprendimai“, 2013, p. 187). Bendra suma popieriui siektų apie 300 000 litų. Lėšų taupymą užtikrina ir elektroninių nedarbingumo pažymėjimų išdavimas: popieriniai pažymėjimai buvo brangūs dėl specialios formos, apsaugotos nuo padirbinėjimo (UAB „Peritus sprendimai“, 2013, p. 188).

VĮ Registrų centras užtikrina daugelių elektroninių paslaugų teikimą, kurių patvirtinimui reikalingas elektroninis parašas: elektroniniu būdu galima registruoti individualią įmonę ir uždarąją akcinę bendrovę, asociaciją ir viešąją įstaigą, juridinio asmens duomenų ir dokumentų pakeitimus (RRT, 2012, p. 15). 2012 metais RC elektroninių paslaugų sistemose elektroniniu parašu buvo pasirašyti 438 395 elektroniniai dokumentai (2011 m. – 21 959) (RRT, 2013, p. 11).

Viešųjų pirkimų tarnyba (toliau – VPT) naudodama Centrinę viešųjų pirkimų informacinę sistemą (CVP IS) užtikrina galimybę teikti elektroninius pasiūlymus, pasirašytus saugiu elektroniniu parašu (RRT, 2012, p. 15). 2012 m. elektroniniu parašu viešųjų pirkimų procedūrų metu buvo pasirašyti 24 569 pasiūlymai (2011 m. – 26 556) (RRT, 2013, p. 11).

Reikėtų pabrėžti, kad šiuo metu elektroninis parašas dažniausiai naudojamas šių keturių institucijų teikiamoms elektroninėms paslaugoms gauti (žr. 18 pav.).



Šaltinis: sudaryta pagal RRT, 2013, p. 10–11; VMI, 2013.

18 pav. Elektroniniu parašu pasirašytų ir pateiktų elektroninių dokumentų statistika

Elektroninį parašą naudoja dar keletą viešojo sektoriaus institucijų: pradedant nuo Vyriausybės ir sąrašą baigiant savivaldybių mastu. Vieną iš svarbesnių e. parašo taikymo pavyzdžių reikėtų paminėti 2011 m. Ministro Pirmininko tarnybos sprendimą visus teisės aktus bei kitus dokumentus pasirašinėti elektroniniu parašu. Tai reiškia, kad aukščiausios valdžios institucijos sutinka, kad elektroninio parašo taikymas užtikrina greitesnį procesų vykdymą, apimant ir duomenų saugumą (RRT, 2012, p. 13).

Šiuo metu elektroninį parašą savo veikloje jau naudoja ypatingai svarbios valdžios institucijos: Lietuvos Respublikos Vyriausybė ir Seimo kanceliarija, Lietuvos Respublikos generalinė prokuratūra, teismai, Lietuvos vyriausiojo archyvaro tarnyba (žr. 5 lent.).

5 lentelė. Elektroninio parašo naudojimas aukščiausiuose valdžios institucijose

Lietuvos Respublikos Seimo kanceliarija	• Priima ir tvarko e. dokumentus, pasirašytus e. parašu, iš sistemos „ELPAS“; • Planuojama kvalifikuotu e. parašu pasirašinėti Seimo kanceliarijos dokumentus, saugiu e. parašu patvirtinti asmens tapatybę, jungiantis prie Seimo kanceliarijos informacinių sistemų.
Lietuvos Respublikos Vyriausybė	• 2011 m. realizuota elektroninio pasirašymo informacinė sistema „ELPAS“; • Vyriausybės priimtų teisės aktų pasirašymui.
Ministro Pirmininko tarnyba	• Vyriausybės priimtų teisės aktų vizavimui ir pasirašymui; • Siunčiamiems raštams pasirašyti (atsakant į e. prašymą).
Teismai	• Lietuvos teismų elektroninių paslaugų portalas (e.teismas); • Fiziniai ir juridiniai asmenys e. būdu gali pateikti kvalifikuotu e. parašu pasirašytus procesinius dokumentus.
Lietuvos Respublikos generalinė prokuratūra	• Perduodant užpildytas statistines ataskaitas; • Patvirtinant duomenis, teikiamus per sistemą VSAKIS; • Teikiant duomenis į FVAS sistemą.
Lietuvos vyriausiojo archyvo tarnyba	• Viešojo sektoriaus įstaigos gali perduoti nuolat saugomus e. dokumentus per Elektroninio archyvo informacinę sistemą (EIAS).

Šaltinis: sudaryta pagal RRT, 2012, p. 13–17.

Elektroninį parašą išorinių ir/arba vidinių dokumentų pasirašymui naudoja 8 viešojo sektoriaus institucijos: Lietuvos Respublikos teisingumo ministerija, Lietuvos Respublikos susisiekimo ir sveikatos apsaugos ministerijos, Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos (toliau – IVPK prie SM), Ryšių reguliavimo tarnyba, Valstybinė vartotojų teisių apsaugos tarnyba, Biržų ir Klaipėdos rajono savivaldybės administracija (žr. 6 lent.).

6 lentelė. E. parašo naudojimas e. dokumentų pasirašymui viešajame sektoriuje

LR teisingumo ministerija	• Vidaus dokumentų pasirašymui; • Planuoja naudoti teisėkūros proceso dokumentų vizavimui ir pasirašymui.
LR susisiekimo ministerija	• Kartu su IVPK prie SM ir Valstybine kelių transporto inspekcija tarpusavyje keičiasi tik e. dokumentais, pasirašytais e. parašu.
LR sveikatos apsaugos ministerija	• Vidinių trumpai saugomų e. dokumentų pasirašymui.
IVPK prie SM	• Rengiant didžiąją dalį vidinių dokumentų, įforminant su viešaisiais pirkimais susijusius dokumentus, susirašinėjant su Susisiekimo ministerija.
Ryšių reguliavimo tarnyba	• Priima e. parašu patvirtintus e. prašymus ir skundus.
Valstybinė vartotojų teisių apsaugos tarnyba	• Galima pateikti e. skundus ir prašymus, pasirašytus kvalifikuotu e. parašu, elektroniniu paštu.
Biržų rajono savivaldybės administracija	• E. parašu pasirašo savivaldybės tarybos sprendimus, administracijos direktoriaus įsakymus dėl teritorijų planavimo, planavimo organizatorių pateiktus teritorijų planavimo dokumentus registruojant Savivaldybės teritorijų planavimo dokumentų registre.
Klaipėdos rajono savivaldybės administracija	• Nuo 2011 m. naudojasi IS „Infostatyba“, kurioje e. būdu registruojami teritorijų planavimo dokumentai, viešųjų pirkimų konkursų medžiaga, prašymai užregistruoti teritorijų planavimo dokumentus bei prašymai dėl licencijų išdavimo.

Šaltinis: sudaryta pagal RRT, 2012, p. 16, 18–20.

13 valstybės institucijų elektroninius dokumentus, pasirašomus elektroniniu parašu, jau pritaikė elektroninių paslaugų teikimui: Centrinė projektų valdymo agentūra, Muitinės ir Policijos departamentas, Valstybės tarnybos departamentas, Informatikos ir ryšių departamentas, Valstybinė kelių transporto inspekcija, Valstybinė teritorijų planavimo ir statybos inspekcija prie Aplinkos ministerijos, Anykščių rajono bei Vilniaus ir Kauno miesto savivaldybės administracija (RRT, 2012, p. 13–21) (žr. 7 lent.).

7 lentelė. Elektroninio parašo naudojimas elektroninių paslaugų teikimui

Informatikos ir ryšių departamentas	• Registro pažymoms ir išrašams pasirašyti.
Muitinės departamentas	• Nuo 2011 m. įgyvendintas elektroninių bendrųjų įvežimo deklaracijų teikimas, patvirtinant saugiu ar kvalifikuotu e. parašu.
Policijos departamentas	• Įdiegta Policijos elektroninių paslaugų sistema (ePolicija); • Dalis paslaugų yra vykdomos taikant e. parašą (pvz. e. pranešimas).
Valstybės tarnybos departamentas	• Nuo 2013 m. birželio 1 d. e. būdu galima pateikti prašymą dalyvauti konkurse valstybės tarnautojo pareigoms užimti, pateikti kitus reikalingus dokumentus ir gauti informaciją apie konkursą per Valstybės tarnybos valdymo informacinę sistemą adresu www.testavimas.vtd.lt
Centrinė projektų valdymo agentūra	• Naudotojai (tiekėjai) gali pateikti „atnaujintus“ pasiūlymus, pasirašytus kvalifikuotu

	e. parašu; • E. parašu pasirašomos viešojo pirkimo sutartys per CVP IS.
Valstybinė teritorijų planavimo ir statybos inspekcija prie Aplinkos ministerijos	• IS „Infostatyba“, Lietuvos Respublikos teritorijų planavimo dokumentų registre galima teikti elektroninius dokumentus, pasirašytus e. parašu.
Valstybinė kelių transporto inspekcija	• Galima teikti e. parašu pasirašytus dokumentus, siekiant gauti leidimą ir kt.
Anykščių rajono savivaldybės administracija	• Priima e. peticijas, skundus, pranešimus dėl įvykio rajone ir pateikia atsakymus, pasirašytus e. parašu.
Kauno miesto savivaldybės administracija	• Elektroninių paslaugų teikimas vykdomas per Elektroninių valdžios vartų portalą.
Vilniaus miesto savivaldybės administracija	• Galima teikti e. parašu pasirašytus dokumentus, siekiant gauti leidimą ar kitą užsakytą dokumentą.
Pagėgių rajono savivaldybės administracija	• Teikti nuomonę dėl Tarybos sprendimų arba balsuoti per VAIISIS sistemą.
Pasvalio rajono savivaldybės administracija	• Pateikti nuomonę dėl priimtų sprendimų ir teikti e. peticijas per VAIISIS sistemą.
Vilkaviškio rajono savivaldybės administracija	• Teikti pasiūlymus dėl teisės aktų projektų; • Planuojama vykdyti e.dokumentų apsikeitimą tarp organizacijų ir su piliečiais, plėsti e. paslaugų mastą.

Šaltinis: sudaryta pagal RRT, 2012, p. 17–20.

Privačiame sektoriuje elektroninių paslaugų plėtrą labiausiai įtakojantys bankai taip pat jau įgyvendino elektroninio parašo naudojimą elektroninių paslaugų sistemose. AB „DNB“ bankas, „Danske Bank A/S“ Lietuvos padalinys, AB „Swedbank“ ir „SEB“ bankas, UAB „Medicinos bankas“ ir „Nordea Bank Finland Plc“ Lietuvos filialas elektroninio parašo naudotojams suteikia galimybę prisijungti prie jų sistemų, taikant elektroninio parašo priemones. Keletas iš išvardintų bankų klientams leidžia elektroniniu parašu patvirtinti įvykdytas operacijas, sutartis bei kitus pakankamai svarbius dokumentus. Tokiu būdu užtikrinamas didesnis finansinių operacijų saugumas (žr. 8 lent.) (RRT, 2013, p. 9–10).

8 lentelė. Elektroninio parašo taikymas privačiame sektoriuje

„Danske bank A/S“ Lietuvos filialas	• Nuo 2012 m. I ketvirčio e. bankininkystės klientai gali prisijungti prie interneto banko ir pasirašyti įvykdytas operacijas kvalifikuotu elektroniniu parašu; • Gali būti naudojami kvalifikuoti sertifikatai įrašyti lustinėse kortelėse, USB kriptografiniuose raktuose arba mobiliojo telefono SIM kortelėse.
AB „DNB bankas“	• Banko klientai elektroninį parašą gali naudoti autentifikavimui e. bankininkystėje; • Patvirtinti e. dokumentus ir e. operacijas interneto banke, pasirašyti mokėjimo nurodymus, sutartis ir kt.; • Nuo 2011 m. dalis verslo klientams teikiamų paslaugų vykdoma e. dokumentais, tvirtinamais e. parašu; • Tvirtinant paslaugų teikimo sutartis; • Pasirašyti kaupiamosios sąskaitos sutartį, kai uždaroji akcinė bendrovė steigiama elektroniniu būdu.
AB „Swedbank“	• Teikiant internetinės ir telefoninės bankininkystės paslaugas; • Planuojama priimti e. prašymus bei kitus e. dokumentus, pasirašytus elektroniniu parašu.
AB „Ūkio bankas“	• Teikiant e. paslaugas banko klientams e. bankininkystės sistemoje.
AB „SEB bankas“	• E. parašas naudojamas elektroninės bankininkystės paslaugų teikimui; • Elektroninių dokumentų pasirašymui; • Nuo 2012 m. I ketvirčio e. bankininkystės klientai gali prisijungti prie interneto banko ir pasirašyti įvykdytas operacijas elektroniniu parašu.
UAB „Medicinos bankas“	• Saugus elektroninis parašas naudojamas tarpbankinėje veikloje ir banko vidaus poreikiams; • 2012 m. įdiegta kvalifikuoto e. parašo paslauga banko klientams e. bankinėje sistemoje (Treinis, 2012, p. 6).

Šaltinis: sudaryta pagal RRT, 2012, p. 21–22.

Elektroninio parašo skatinimą ir plėtrą gali padidinti nuo 2013 m. birželio 18 d. teikiama elektroninė paslauga „e.pristatymas“. E. pristatymo sistema atveria naujas galimybes: realizuoti saugų, patikimą ir greitą oficialių elektroninių dokumentų teikimą fiziniams ir juridiniams asmenims. Pasak Paulavičienės, elektroniniu būdu išsiųsta ir gauta korespondencija yra teisiškai lygiavertė tradicinei registruotai pašto siuntai ir turi tokią pačią įrodomąją galią. Dar svarbu pabrėžti, kad trečia šalis neturi galimybės perimti elektroninio dokumento turinio, nes siuntos yra šifruojamos (AB „Lietuvos paštas“, 2013-06-18). Tai galimybė ženkliai sutaupyti kasmet korespondencijai išleidžiamą pinigų sumą: kiekvienais metais tik valstybinės institucijos išleidžia apie 19 mln. litų registruotai pašto siuntai (IVPK, 2013). Naudojantis e. pristatymo paslauga, elektroninės dėžutės sukūrimas sistemoje ir jos naudojimas yra visiškai nemokamas. Šiuo atveju taupomi ir gamtos ištekliai: sunaudojama mažiau popieriaus, išskiriama mažiau CO_2 (AB „Lietuvos paštas“, 2013-06-18). 2013 m. gruodžio 13 d. šia paslauga jau naudojasi 51 valstybės institucija, 77 juridiniai asmenys ir 671 fiziniai asmenys (AB „Lietuvos paštas“, 2013-12-13). E. pristatymo paslaugos naudojimą valstybės institucijų mastu skatins nuo 2014 m. įsigaliosiantis Vyriausybės nutarimas, kuriuo remiantis biudžetinės įstaigos privalės vykdyti elektroninių dokumentų mainus (dienraštis „Sekundė”, 2013-06-18).

Elektroninio parašo naudojimo plėtrą viešajame sektoriuje gali užtikrinti darbuotojų, dirbančių pagal darbo sutartis, aprūpinimas elektroninio parašo priemonėmis: šie darbuotojai negali gauti naujo pavyzdžio valstybės tarnautojo pažymėjimo (RRT, 2010, p. 11).

Vadovaujantis Lietuvos vyriausiojo archyvaro tarnybos duomenimis, nuo 2014 m. sausio 1 d. elektroniniais dokumentais galėtų keistis 466 įstaigos iš 3500 apklaustųjų (RRT, 2013, p. 9).

Apibendrinus pateiktą medžiagą, galima teigti, kad elektroninis parašas viešojo sektoriaus veikloje naudojamas vangiai. Nors kasmet daugėja elektroninio parašo taikymo pavyzdžių, tačiau nėra plačiai išnaudojamos šio parašo galimybės. Šiuo metu elektroninį parašą naudoja 6 aukščiausios valdžios institucijos, 8 viešojo sektoriaus institucijos taiko išorinių ir/arba vidinių dokumentų pasirašymui, 17 valstybės institucijų elektroninius dokumentus, pasirašomus elektroniniu parašu, pritaikė elektroninių paslaugų teikimui, iš kurių 4 valstybinės institucijos yra e. parašo taikymo lyderiai, t.y. VMI, SODRA, RC ir Viešųjų pirkimų tarnyba. Reikėtų pabrėžti, kad nuo šių metų sausio 1 d. e. parašą savo veikloje galėtų naudoti tik 466 viešojo sektoriaus institucijos iš 3500 apklaustų. Elektroninio parašo plėtrą gali skatinti teikiama paslauga „e. pristatymas“ ir viešojo sektoriaus darbuotojų, dirbančių pagal darbo sutartis, aprūpinimas e. parašo priemonėmis. Šio parašo galią ir taikymo naudą jau pripažįsta ir privataus sektoriaus atstovai bankai: leidžia panaudojant elektroninį parašą prisijungti prie jų sistemų ir patvirtinti pakankamai svarbius dokumentus, t.y. operacijas, sutartis ir kt.

3.2. Elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo prioritetinės veiklos kryptys

Europos Parlamento ir Tarybos direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos neįtvirtina vientisos elektroninio parašo rinkos funkcionavimo. Toks teisinis reglamentavimas suformavo neigiamas pasekmes: rinkos fragmentaciją ir techninį nesuderinamumą nacionaliniu ir ES lygiu (UAB „Peritus sprendimai“, 2013, p. 35). Dėl šių priežasčių Europos Komisija 2012 m. birželio 4 d. paskelbė reglamento projektą „Europos Parlamento ir Tarybos reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje“. Šio pasiūlymo ataskaitoje pateikiamos dvi priežastys, stabdančios tarpvalstybinių patikimumo užtikrinimo paslaugų teikimą: rinkos fragmentacija (skirtingų valstybių paslaugų teikėjams taikomos nevienodos taisyklės) ir vartotojų pasitikėjimo trūkumas (Civilka, 2013, p. 87). Kadangi ES valstybių narių realizuotos elektroninės atpažinties (toliau – eID) sistemos skiriasi, šiame reglamente siūloma nustatyti prievolę: priimti ir pripažinti kitų ES valstybių narių teikiamas elektroninės atpažinties priemones, siekiant užtikrinti elektroninių paslaugų teikimą tarpvalstybiniu lygiu. Taigi, šiuo reglamentu siekiama užtikrinti abipusį elektroninių atpažinimo priemonių pripažinimą (EUR–Lex, 2012, Nr. 52012PC0238). Šie tikslai atspindi STORK projekto iniciatyvą.

STORK (saugaus tarpvalstybinio tapatybės nustatymo) pilotinis projektas pradėtas įgyventi 2008 m. (VĮ „Infostruktūra“, 2011). Pagrindinis tikslas – sukurti Europos eID sąveikumo platformą ir tokiu būdu užtikrinti galimybę vykdyti elektroninių paslaugų teikimą tarpvalstybiniu lygiu, panaudojant nacionalines elektroninės atpažinties priemones. „Sąveikumas – sistemų ir įrenginių gebėjimas keistis informacija, ją apdoroti ir teisingai interpretuoti. Šis uždavinys ne vien techninis, bet ir susijęs su teisiniais, organizaciniais ir semantiniais duomenų apdorojimo aspektais. Sąveikumas yra būtina išankstinė sąlyga siekiant atvirai ir lanksčiai teikti e. valdžios paslaugas ir Europoje užtikrinti administravimo institucijų bendradarbiavimą“ (Europos Komisija, 2010). Šiame projekte dalyvauja 18 šalių, tarp jų ir Lietuva, kurią atstovauja Vidaus reikalų ministerija. Šis projektas įgyvendinamas keliais etapais. 2011 m. pabaigtas įgyvendinti pirmas lygis, skirtas užtikrinti vientisą elektroninės atpažinties ir elektroninio tapatumo sistemą ES piliečiams kitose ES valstybėse (VĮ „Infostruktūra“, 2011). Šiuo metu įgyvendinamas antrasis etapas STORK 2.0, kuriame dalyvauja ir Lietuva. Šiame lygyje siekiama įgyvendinti juridinių asmenų elektroninės atpažinties taikymo galimybes. Valstybės dalyvavusios pirmame šio projekto etape ir įdiegusios demonstracinį STORK 1.0 sprendimą nacionaliniu lygiu planuoja jį įgyvendinti, kai bus pasiekti antrojo etapo rezultatai bei parengta techninė platforma, tame tarpe ir Lietuva. Šiuo metu mūsų

šalyje demonstracinė versija integruota į VIISP sistemą (Valstybės informacinių išteklių sąveikumo platforma), tapatybės nustatymui panaudojamos ES valstybių narių išduotos asmens tapatybės kortelės.

Projekto metu Lietuvoje realizuota bandomoji Europinė pasitikėjimo sistema (PEPS – Pan European Proxy System), be jokių kliūčių su 11 ES valstybėmis buvo atlikti tarpvalstybiniai asmenų identifikavimai, panaudojant eID įrašytus sertifikatus (LR vidaus reikalų ministerija, 2012, p. 11).

Remiantis STORK projektu, yra skiriamos 4 tapatybės nustatymo patikimumo lygių klasifikacijos (angl. STORK QAA) (The Standardisation Forum, 2012, p. 19):

- *1 STORK QAA lygis* – tai žemiausias patikimumo lygis. Šiuo atveju minimaliai arba visiškai neužtikrinamas asmens tapatybės autentiškumas: tapatybės rekvizitų patikrinimas nėra vykdomas. Pavyzdys, kai pareiškėjas gauna elektroninį laišką nuo institucijos su nuoroda, kurią paspaudęs gali vykdyti tam tikrus veiksmus, pavyzdžiui, atsisiųsti paraiškos dokumentus.
- *2 STORK QAA lygis* – žemas patikimumo lygis. Šiame lygmenyje patikrinamas tapatybės rekvizitų autentiškumas registracijos proceso metu. Registruojantis reikia nurodyti valstybės išduoto dokumento, pavyzdžiui, vairuotojo pažymėjimo arba paso, numerį arba pateikti šio dokumento kopiją e. būdu. Registracijos metu nereikalingas asmens fizinis dalyvavimas. Tapatybės identifikavimas užtikrinamas suteikiant unikalų vartotojo vardą ir slaptažodį arba kodą. Pavyzdys galėtų būti mokesčių deklaravimas (UAB „Peritus sprendimai“, 2013, p. 156).
- *3 STORK QAA lygis* – tai vidutinis patikimumo lygis. Šiuo atveju taikomi griežtesni tapatybės rekvizitų patikrinimo būdai. Tapatybės patikimumo užtikrinimo paslaugų teikėjas privalo būti kontroliuojamas arba akredituotas valstybės. Šiuo atveju tapatybės autentiškumas gali būti užtikrinamas panaudojant nekvalifikuotus sertifikatus arba vienkartinius slaptažodžius. Pavyzdys galėtų būti elektroninė bankininkystė.
- *4 STORK QAA lygis* – aukštas patikimumo lygis. Šiuo atveju pirminei registracijai būtinai reikalingas fizinio asmens dalyvavimas: patikrinami asmens duomenys ir jų galiojimas. Naudotojui išduodamas kvalifikuotas skaitmeninis sertifikatas, atitinkantis direktyvos I priede įvardintus reikalavimus, ir jo tikrumą garantuoja sertifikavimo paslaugų teikėjas, atitinkantis direktyvos II priede nustatytus reikalavimus. Tai maksimalus tapatybės patikimumo nustatymo lygis. Pavyzdys, kai notaras turi pateikti dokumentą į atitinkamą informacinę sistemą, pavyzdžiui, nacionalinį registrą. Šio veiksmo atlikimui reikalingas kvalifikuotas skaitmeninis sertifikatas ir elektroninis parašas. Kiekvienas notaras asmeniškai turi juos įsigyti.

Lyginant Lietuvos elektroninių parašų įvairovę ir jiems keliamus reikalavimus su STORK tapatybės nustatymo patikimumo lygių klasifikacija, galima pastebėti ryškių skirtumų. Pavyzdžiui, 1 STORK QAA

lygio elektroninio parašo taikymo pavyzdžių Lietuvos mastu nėra. Šio lygio parašo neišskiria ir mokslininkai. *3 STORK QAA lygio* e. parašą Lietuvoje gali išduoti valstybės neprižiūrimi arba neakredituoti sertfikavimo paslaugų teikėjai. STORK projekte aiškiai nurodyta, kad tokį sertifikatą gali išduoti tik valstybės kontroliuojami arba akredituoti sertifikavimo paslaugų teikėjai. Tiksliai aprašomas tik kvalifikuotas elektroninis parašas (*4 STORK QAA lygio* tapatybės nustatymo patikimumas) (žr. 9 lent.).

9 lentelė. Preliminarus tapatybės nustatymo Lietuvos e. valdžios vartų portale skirstymas, remiantis STORK klasifikacija

STORK QAA lygiai	**Atitikmenys Lietuvos mastu**	**Tapatybės nustatymo būdai, naudojami „Elektroninių valdžios vartų“ skelbiamose e. viešosiose ir administracinėse paslaugose**
1 STORK QAA lygis	–	–
2 STORK QAA lygis	Paprastas elektroninis parašas	❖ Prisijungimo vardas ir slaptažodis; ❖ E.bankininkystės sistema, kai bankas neprižiūrimas arba neakredituotas valstybės.
3 STORK QAA lygis	Saugus elektroninis parašas	❖ E.bankininkystės sistema, kai bankas prižiūrimas arba akredituotas valstybės; ❖ Sertifikavimo paslaugų teikėjo išduotas nekvalifikuotas sertifikatas (dar vadinamas kvalifikuotu sertifikatu, kai išduodamas neprižiūrimo arba neakredituoto sertifikavimo paslaugų teikėjo).
4 STORK QAA lygis	Kvalifikuotas elektroninis parašas	❖ Sertifikavimo paslaugų teikėjo išduotas kvalifikuotas sertifikatas, kai sertifikavimo paslaugų teikėjas prižiūrimas arba akredituotas valstybės; ❖ Asmens tapatybės kortelės sertifikatas; ❖ Valstybės tarnautojo pažymėjimo sertifikatas; ❖ ES valstybių narių išduotos asmens tapatybės kortelės sertifikatas.

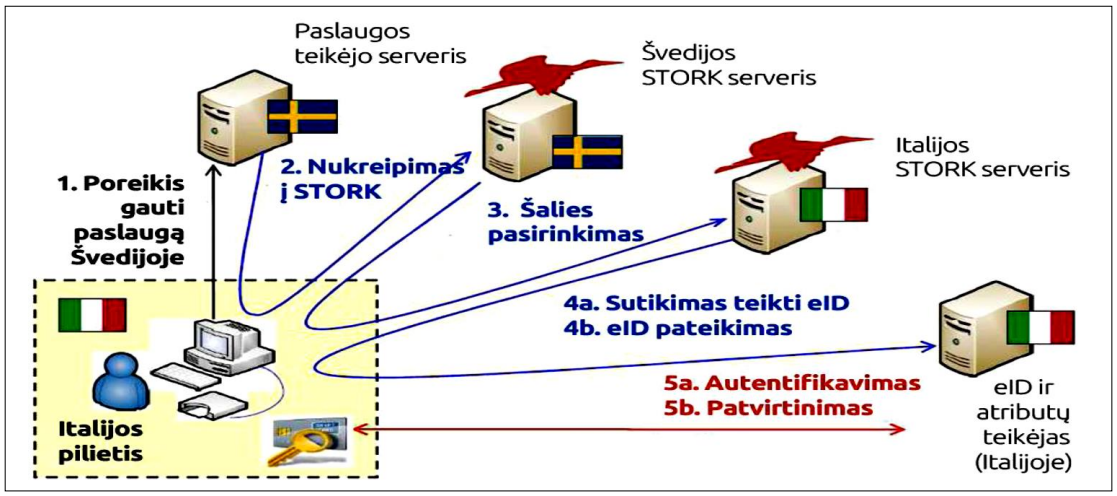
Šaltinis: adaptuota pagal UAB „Peritus sprendimai“, 2013, p. 58.

Remiantis Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (1.12), yra apibrėžtas tik saugomų duomenų pobūdis ir jų tvarkymo galima rizika, bet nėra įtvirtinta tapatybės nustatymo patikimumo lygių klasifikacija (UAB „Peritus sprendimai“, 2013, p. 57).

Galima įžvelgti ir daugiau kliūčių, kurias reikia išspręsti Lietuvoje, siekiant artimiausiu metu teikti e. paslaugas ES mastu. Kai kuriose valstybėse fizinių asmenų identifikavimui nėra naudojamas asmens kodas: nėra vieningos nuomonės dėl asmens kodo naudojimo ES mastu (UAB „Peritus sprendimai“, 2013, p. 60). Tuo tarpu Lietuvoje tik Registrų centro ir GRT išduodami kvalifikuoti sertifikatai apima unikalų asmens kodą, o SSC išduodamuose sertifikatuose tokie duomenys neįrašomi (SSC, 2013-10-03). Elektroninių duomenų, kurie buvo pasirašyti SSC e. parašu, gavėjas negali tiksliai jų susieti su konkrečiu fiziniu ar juridiniu asmeniu: reikia siųsti paklausimą į SSC (UAB „Peritus sprendimai“, 2013, p. 44). ES valstybių asmenys prisijungdami prie Lietuvos informacinių sistemų, naudojant savo šalies elektroninės atpažinties priemones be unikalaus asmens identifikatoriaus, gali turėti keletą atpažinties priemonių ir manipuliuoti savo tapatybe. Jei vieno žmogaus valdomos kelios elektroninės atpažinties priemonės yra su

skirtingais identifikaciniais duomenimis, tuomet informacinėje sistemoje tas pats asmuo nebus siejamas (UAB „Peritus sprendimai“, 2013, p. 44–45).

STORK efektyvumas ir funkcionalumas aiškiai suprantamas remiantis žemiau pateikta schema (žr. 19 pav.).



Šaltinis: UAB „Peritus sprendimai“, 2013, p. 160.

19 pav. Saugaus tarpvalstybinio tapatybės nustatymo pilotinio projekto STORK veikimo schema

Svarbu tampa plačiau apžvelgti ir paaiškinti penktą žingsnį. Šiame etape naudotojas gali sužinoti, kokie asmens duomenys reikalingi Švedijos paslaugų teikėjui ir patvirtinti šių duomenų perdavimą iš savo šalies Italijos tapatybės arba atributų teikėjų. Tuomet įvyksta autentifikavimo procesas ir patvirtinimas bei naudotojo asmens duomenų perdavimas Švedijos paslaugų teikėjui. Identifikavus naudotoją, gali būti teikiama elektroninė paslauga (UAB „Peritus sprendimai“, 2013, p. 160).

Apžvelgus ateities perspektyvas Lietuvos ir ES mastu, galima pateikti prioritetines veiklos kryptis Lietuvai, kurias reikia įgyvendinti, siekiant plačiau taikyti elektroninį parašą. Pirmiausia reikėtų dar kartą paminėti, kad elektroninis parašas viešojo sektoriaus veikloje dar nėra ypač plačiai naudojamas, nors taikymo pavyzdžių kasmet vis daugėja. Šiuo metu labiau taikomos pasyvios elektroninio parašo skatinimo priemonės: nuotolinio mokymo sistema, RRT konsultacijos. Todėl reikėtų suformuoti informacinę kompaniją, kuri būtų kompetentinga elektroninio parašo srityje ir galėtų aiškiai ir aktyviai skleisti informaciją apie elektroninio parašo taikymą viešajame sektoriuje, apimant visas svarbias temas: elektroninių parašų įvairovė ir jų patikimumas, taikymo galimybės, privatumas, rizika ir asmens duomenų apsauga elektroninėje erdvėje, galimybė gauti paramą bei kt. Kita svarbi sritis – parengti tinkamą

priemonių sąrašą viešojo sektoriaus darbuotojų mokymui, siekiant užtikrinti valstybės tarnautojų kompetenciją, taikant naujas technologijas. Taip pat reikėtų užtikrinti dažnai naudojamų viešųjų paslaugų spartesnį perkėlimą į e. erdvę. Prioritetinių veiklos krypčių sąrašą reikėtų papildyti dar šiais veiksmais:

1. 2014–2016 m. valstybiniu lygiu suderinti viešojo sektoriaus institucijų dokumentų valdymo sistemas (toliau – DVS), e. archyvo sistemos diegimo ir atnaujinimo darbus, siekiant sudaryti sąlygas viešojo sektoriaus institucijoms ir įstaigoms vykdyti elektroninių dokumentų mainus;
2. 2014–2016 m. įtvirtinti bendrus reikalavimus viešojo sektoriaus institucijų ir įstaigų DVS, skatinti viešojo sektoriaus institucijas rengti bendras DVS pavaldžioms įstaigoms bei organizacijoms (IVPK, Viešosios politikos ir vadybos institutas (VPVI), 2012 p. 281);
3. 2014–2022 m. įtvirtinti e. sąskaitų faktūrų naudojimą viešajame sektoriuje, kurios automatiškai patenka į organizacijos finansų valdymo sistemą. Pavyzdžiui, nuo 2010 m. šią naujovę taiko Estijos viešasis sektorius. Tokiu būdu taupomas viešojo ir privataus sektoriaus laikas bei lėšos;
4. Tęsti dalyvavimą STORK bei kituose ateities projektuose, kurie užtikrintų eID kortelės taikymo galimybes gauti e. viešąsias bei administacines paslaugas ES valstybėse ir skatintų viešojo sektoriaus institucijas įgyvendinti inovatyvias technologijas, t.y. taikyti elektroninį parašą (IVPK, VPVI, 2012, p. 292); parengti tapatybės nustatymo patikimumo lygių klasifikaciją.

Taigi, artimiausiu metu reikėtų suformuoti kompetentingų asmenų kompaniją, kuri aktyviai teiktų išsamią informaciją dėl e. parašo taikymo galimybių viešajame sektoriuje: nustatytų kliūtis ir pateiktų jų sprendimo būdus, patartų, rengiant planą dėl organizacinių, techninių, teisinių sprendimų e. parašo taikymui įgyvendinti, bendradrabiautų su valdžios institucijomis, atsakingomis už e. parašo infrastruktūrą, informacinės visuomenės plėtrą ir kt. Kitas svarbus žingsnis – parengti ir įgyvendinti teisinių, organizacinių ir techninių veiksmų planą dėl bendrųjų reikalavimų viešojo sektoriaus institucijų ir joms pavaldžių įstaigų, ir organizacijų dokumentų valdymo sistemoms. Trečias žingsnis – suderinti e. archyvo sistemos diegimo ir atnaujinimo veiksmus. Ketvirta – didinti e. paslaugų pasiūlą fiziniams bei juridiniams asmenims, pavyzdžiui, e. sąskaitų faktūrų naudojimas viešajame sektoriuje. Penktas svarbus žingsnis – toliau dalyvauti STORK bei panašiuose projektuose, kurie suteiktų galimybę plačiau taikyti e. atpažinties priemones ne tik Lietuvos, bet ir ES mastu, teikiant ir gaunant e. viešąsias ir administracines paslaugas. Šiuo metu yra pateiktas Europos Komisijos 2012 m. birželio 4 d. parengtas reglamento projektas „Europos Parlamento ir Tarybos reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje“, kuris artimiausiu metu gali pakeisti direktyvą. Paskutinis etapas – priimti teisės aktą dėl tapatybės nustatymo patikimumo lygių klasifikacijos, kuris užtikrintų aiškų kiekvieno elektroninio parašo patikimumą ir įtvirtintų keliamus reikalavimus.

4. ELEKTRONINIO PARAŠO NAUDOJIMO VIEŠOJO SEKTORIAUS INSTITUCIJOSE VEIKLOS TYRIMAS

4.1. Tyrimo metodologija

Tyrimo problema. Nepakankamai efektyvus IT panaudojimas viešojo sektoriaus darbe. Norint praplėsti e. parašo naudojimą viešajame sektoriuje, tenka nugalėti egzistuojančias kliūtis, kurios daro įtaką efektyviam viešojo administravimo institucijų darbui.

Tyrimo objektas ir dalykas. Objektas – e. parašo taikymas Lietuvos viešajame sektoriuje esama padėtis. Tyrimo dalykas – priemonės ir būdai kaip organizuoti platesniu mastu e. parašo taikymo modelį, numatantį e. parašo plėtrą.

Tyrimo tikslas. Išplėsti elektroninio parašo naudojimą viešajame sektoriuje.

Tyrimo uždaviniai. Tikslo įgyvendinimui buvo iškelti šie uždaviniai:

1. Nustatyti ekspertų atrankos sistemą;
2. Parengti pasirinkto tyrimo metodo klausimyną;
3. Apklausti pasirinktus ekspertus;
4. Atlikti tyrimo rezultatų kokybinę ir kiekybinę analizes;
5. Išanalizavus gautus duomenis, nustatyti elektroninio parašo taikymo viešajame sektoriuje galimybes.

Tyrimo hipotezės:

1. Elektroninio parašo spartesnę plėtrą viešajame sektoriuje stabdo nepakankama vadovaujančių institucijų skatinimo politika taikyti e. parašą viešojo sektoriaus darbe;
2. Elektroninis parašas platesniu mastu nenaudojamas dėl valstybės tarnautojų pasipriešinimo kaitai žmogiškųjų veiksnių – informacijos, kvalifikacijos ir motyvacijos stokos.

Tyrimo metodas – ekspertų apklausa. Ekspertinis vertinimas dažniausiai naudojamas siekiant ištirti problemą, reiškinį ar procesą, kai reikalingos specialios žinios. Ekspertinis vertinimas – tai apibendrinta atitinkamo masto ekspertų grupės nuomonė, kuri formuojama remiantis ekspertų kompetencija (Augustinaitis ir kt., 2009, p. 174). Pasirinktas tyrimo metodas priskiriamas kokybinių tyrimų grupei, nes siekiama sistemingai įvertinti atvejį (Žukauskienė R., 2008). Svarbu pabrėžti, kad tam tikro dydžio ekspertų grupės nuomonė neženkliai skiriasi nuo realiojo problemos sprendinio. Šis tyrimo metodas leidžia įvykdyti šias svarbias funkcijas:

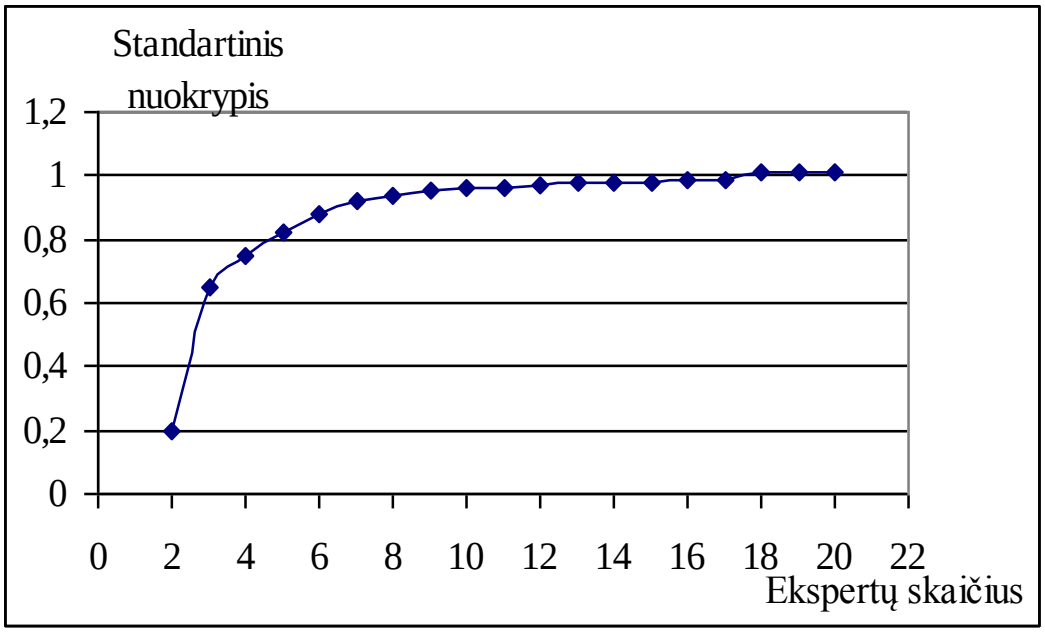
- įvertinti objekto, proceso ar reiškinio esamą būklę;
- pateikti rekomendacijas sprendimų priėmėjams dėl planuojamų rezultatų gavimo (Augustinaitis ir kt., 2009, p. 176–177).

Dabartiniu metu dažniausiai vertinami individualūs ekspertinio vertinimo metodai: pašaliniai asmenys dažnai trikdo tinkamai atlikti užduotis (Augustinaitis ir kt., 2009, p. 187–188). Labiausiai taikomas tikimybinis metodas – apklausa anketavimo būdu. Anketą sudaro atitinkamos srities klausimai, į kuriuos siekiama gauti respondentų atsakymus. Reikėtų pabrėžti, kad palankiau vertinamas anketos pildymo būdas, kai su anketa supažindintas ekspertas gali savarankiškai pildyti anketą: šiuo atveju gali tinkamai apmąstyti savo atsakymus (Augustinaitis ir kt., 2009, p. 191–192). Remiantis šiais mokslo teiginiais, nuspręsta pasirinkti individualų ekspertinio vertinimo metodą – apklausą anketavimo būdu.

Tyrimo imtis – ekspertinė imtis, kuri suformuojama atsižvelgiant į ekspertų nuomonę. Ekspertų imtis sudaroma remiantis netikimybinės atrankos būdais (Rudzkienė V., 2005, p. 28). Pasak Kardelio (2005), kokybinių tyrimų reprezentatyvumą užtikrina ne atsitiktiniai tiriamųjų parinkimo būdai, o pakankamai lankstūs vieni ar kiti teoriniai aspektai (p. 273). Tokiu būdu siekiama atrinkti ekspertus, kurie turi pakankamai kompetencijos tyriamajai problemai ar uždaviniui išspręsti (Kardelis, 2005, p. 325–326). Todėl tyrėjas nusprendė į formuojamą grupę įtraukti asmenis, kurie, jo nuomone, yra tinkamiausi tiriamojo požymio atžvilgiu. Toks pasirinktas netikimybinis tiriamųjų grupių parinkimo būdas įvardinamas kaip tikslinių grupių formavimas (Kardelis, 2005, p. 325–326). Remiantis pateikta moksline medžiaga, tyrėjas nusprendė suformuoti 7 ekspertų tikslinę grupę.

Tyrimo patikimumas. Ekspertinio vertinimo patikimumas gali būti įvertintas remiantis apklausos rezultatais. Patikimumui įtakos turi pasirinktas ekspertų skaičius, jų sudėtis pagal specialybes ir ekspertų kompetencija (Augustinaitis ir kt., 2009, p. 199). Siekiant pasirinkti tinkamą ekspertų skaičių, reikia vadovautis metodologinėmis prielaidomis, kurios suformuotos klasikinėje testų teorijoje. Remiantis teorija, galima teigti, kad agreguotų sprendimų patikimumą ir priimančiųjų sprendimą (šiuo atveju ekspertų) skaičių sieja sparčiai nykstantis netiesinis ryšys (žr. 20 pav.). Jau yra įrodyta, kad agreguotų ekspertinių vertinimų moduliuose nedidelių ekspertų grupių su vienodais svoriais priimtų sprendimų ir vertinimų tikslumas nenusileidžia tiems sprendimams ir vertinimams, kurios priėmė didelės ekspertų grupės. Didžiausias gautų įverčių tikslumas yra tuomet, kai ekspertų grupę sudaro 5–9 ekspertai. Jei 5–9 ekspertų grupės vertinimo tikslumas nėra pakankamas, reikia didinti ne ekspertų grupę, bet kelti kompetencijos reikalavimus ekspertams (Augustinaitis ir kt., 2009, p. 202). Sprendimų ir vertinimų tikslumas yra pakankamai aukštas, kai ekspertų grupę sudaro 7 ekspertai (žr. 20 pav.). Suformavus

didesnę ekspertų grupę, šis tikslumas nežymiai kyla aukštyn. Remiantis šia moksline informacija, buvo nuspręsta, kad 7 ekspertų grupė gali užtikrinti aukštą tyrimo duomenų patikimumą.



Šaltinis: Libby, Blashfield, 1978, p. 125.

20 pav. Ekspertų vertinimų standartinio nuokrypio priklausomybė nuo ekspertų skaičiaus

Ekspertinis vertinimas remiasi prielaida, kad tinkamą sprendimą gali užtikrinti ekspertų nuomonių suderinamumas. Kadangi tyrime dalyvauja 7 ekspertų grupė, todėl jų nuomonių suderinamumas tikrinamas remiantis Kendallo konkordancijos koeficientu W, kuris kinta nuo 0 iki 1. Šiuo atveju 0 reiškia visišką ekspertų nuomonių nesuderinamumą, o 1 – visišką suderinamumą. Siekiant apskaičiuoti konkordancijos koeficientą, reikią ranguoti ekspertų vertinimus (Augustinaitis ir kt., 2009, p. 204–206). Reikėtų pabrėžti, kad apskaičiavus šį koeficientą, neįmanoma nustatytų ekspertų, kurių nuomonė ryškiai išsiskiria iš kitų. Siekiant nustatyti tokius ekspertus, reikia įvertinti ekspertų kompetenciją. Ekspertų kompetencijos koeficientas yra apskaičiuojamas pagal alternatyvų įvertinimo rezultatus. Remiantis šiais rezultatais, iš ekspertų grupės pašalinami ekspertai, kurių nuomonės vienareikšmiškai išsiskiria iš kitų grupės narių (Augustinaitis ir kt., 2009, p. 210). Tokiu būdu atmetamos nekvalifikuotos ir originalios ekspertų nuomonės. Ekspertinis vertinimas laikomas patikimu ir tuo atveju, jei susidaro kelios nuomonių grupės. Tai reiškia, kad bendros nuomonės dėl tyriamojo reiškinio nėra (Augustinaitis ir kt., 2009, p. 204).

Tyrimo duomenys. Tyrimo duomenis galima suskirstyti į tris grupes, t.y. kiekybiniai (skaitmeniniai duomenys), kokybiniai (duomenys, pateikti ne skaičiais) ir nominaliniai (vardiniai). Pirmajai grupei priklauso duomenys, kuriuos galima įvertinti, remiantis matematiniais skaičiavimais, t.y. e. parašo plėtrai viešajame sektoriuje taikomų priemonių pakankamumas, remiantis 10 balų skale, bei kliūčių išdėstymas pagal svarbą dėl nepakankamo e. parašo naudojimo viešojo sektoriaus veikloje, suteikiant skirtingus reitingus nuo 1 iki 10. Kokybinių duomenų grupę sudaro visi kiti gauti tyrimo rezultatai, nes pagrindinis tyrimo tikslas – gauti ekspertų atsakymus į klausimus, kurie nėra pateikiami mokslinėje literatūroje. Nominaliniai duomenys – tai respondento darbovietės pavadinimas ir pareigos, kuriuos jis pateikia anketos įvadinėje dalyje.

Tyrimo organizavimas. Visiems ekspertams anketos buvo išsiųstos elektroniniu paštu. Respondentų buvo prašoma užpildytas anketas pateikti tokiu pačiu būdu, kurį naudojo ir anketos siuntėjas. Respondentų apklausa buvo vykdoma nuo 2014-01-30 iki 2014-03-02 d. Tolesniame tyrimo etape buvo atrinkti ekspertų duomenys, kurie beveik arba visiškai sutampa su daugelio ekspertų nuomonėmis. Apibendrinus ekspertų sprendimus ir vertinimus, pateiktos tyrimo išvados ir siūlymai. Ekspertai, kurių duomenys buvo pasirinkti tyrimui atlikti, toliau įvardinami 1EK, 2EK, 3EK, 4EK, 5EK, 6EK, 7EK.

4.2. Tyrimo duomenų analizė

Atliekant tikrinimą dėl ekspertų vertinimų tarpusavio suderinamumo, suformuluojamos dvi hipotezės:

H_0 – ekspertų vertinimai dėl e. parašo plėtrą skatinančių priemonių yra prieštaringi (t.y. konkordancijos koeficientas lygus nuliui);

H_1 – ekspertų vertinimai dėl e. parašo plėtrą skatinančių priemonių yra panašūs (t.y. konkordancijos koeficientas nėra lygus nuliui).

Kadangi ekspertų vertinimuose yra sutampančių rangų (žr. 10 lent.), PSPP terpėje tyrimo autorius formavo dialogo langą *kriterijai kelioms priklausomoms (porinėms) imtims*, remiantis šių komandų seka – analizuoti, neparametrinė statistika, K priklausomų imčių. Apskaičiuotas Kendallo konkordancijos koeficientas W = 0,69 rodo, kad ekspertų nuomonės yra pakankamai suderinamos (žr. 21 pav.). Asimetrinė p-reikšmė = 0,00 < α = 0,05, todėl patvirtinta hipotezė H_1, konkordancijos koeficientas yra reikšmingas.

NPAR TESTS
NPAR TEST /KENDALL = Kint0001 Kint0002 Kint0003 Kint0004 Kint0005 Kint0006 Kint0007.

Rangai	Vidutinis rangas
Kint0001	4.1
Kint0002	2.3
Kint0003	2.8
Kint0004	5.8
Kint0005	2.2
Kint0006	5.4
Kint0007	5.4

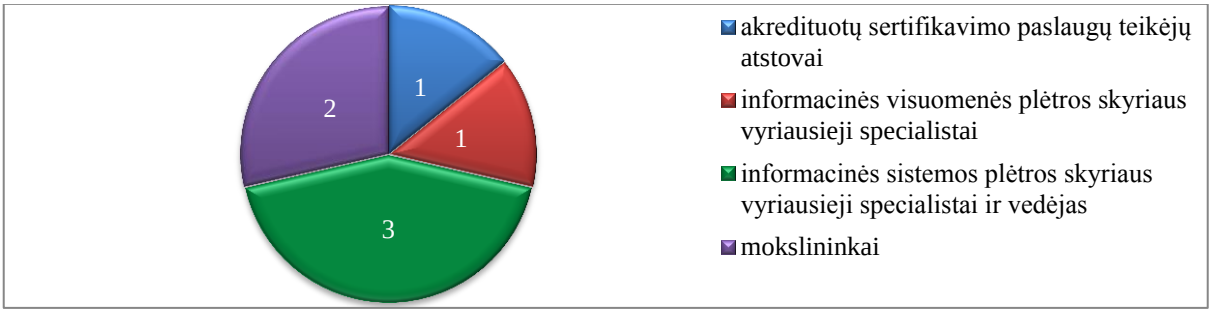
Kriterijaus statistika

N	5
Kendalo W	0.69
Chi kvadratas	20.76
skirt.	6
Asimt. p-reikšmė	0

Šaltinis: sudaryta autorės.

21 pav. Konkordancijos koeficiento W skaičiavimas PSPP terpėje

Ekspertinio vertinimo grupę sudarė keturių skirtingų sričių ekspertai – tai viešojo sektoriaus institucijų informacinės visuomenės plėtros skyriaus ir informacinės sistemos plėtros skyriaus vyriausieji specialistai ir vedėjai, mokslininkai ir akredituotų sertifikavimo paslaugų teikėjų atstovai (žr. 22 pav.).



Šaltinis: sudaryta autorės.

22 pav. Ekspertinio vertinimo ekspertų grupės sudėtis

Remiantis autorės darbe pateikta moksline teorine analize, tik dalinai galima suformuoti tikslų e. parašo taikymo vientisą ir palankų sprendimą viešajam sektoriui. Pagrindinis ir aiškiai neišspręstas klausimas yra dėl e. parašo suteikimo darbuotojams, dirbantiems pagal darbo sutartį, viešajame sektoriuje. Dažniausiai siūlomas e. parašo sprendimas valstybės tarnautojams – valstybės tarnautojo pažymėjimas. Taigi, e. parašo ir laikmenos pasirinkimo įvairovė – menka, dažniausiai siūloma stacionari e. parašo įranga. Siekiant išsiaiškinti visas esamas e. parašo alternatyvas, pirmas klausimas buvo susijęs su šių parašų pasiūla viešajam sektoriui, t.y. galimybę taikyti įstaigos viduje, siunčiamų e. dokumentų pasirašymui ir jungiantis prie išorinių informacinių sistemų. Taigi, buvo suformuotas ir pateiktas toks

klausimas: „*Kokį elektroninio parašo modelį siūloma taikyti viešojo sektoriaus veikloje*?“ Ekspertai turėjo pateikti e. parašo pasiūlymus, naudotis išoriniame ir vidiniame lygmenyje. Išoriniam naudojimui ekspertai pateikė dalinai vienodus e. parašo sprendimus.

1 EK pasiūlė naudoti „kvalifikuotus e. parašus, kuriuos teikia akredituotos valstybinės įmonės“.

2 EK taip pat sutinka, kad „geriausia naudoti kvalifikuotą sertifikatą. Šis sertifikatas užtikrina, kad visi dalyviai remsis vienu pagrindiniu modeliu“.

3 EK teigia, kad „kvalifikuotas e. parašas – tinkamiausias pasirinkimas viešajame sektoriuje, t.y. siunčiamų elektroninių dokumentų pasirašymui, jungiantis prie išorinių informacinių sistemų ir kitais atvejais. Toks parašas yra lygiavertis tradiciniam parašui, nes automatiškai užtikrina teisinę galią. Išoriniam naudojimui siūlau kelis kvalifikuoto e. parašo sprendimus – tai valstybės tarnautojo pažymėjimas (lustinė kortelė), SSC išduodami kvalifikuoti sertifikatai valstybiniam sektoriui lustinėje kortelėje arba USB laikmenoje, tačiau šių sertifikatų įsigijimo ir pratęsimo kaina yra nepalanki”.

4 EK dalinai sutinka su pirmo eksperto nuomone. Šis ekspertas mano, kad „reikėtų pasirinkti kvalifikuoto elektroninio parašo variantą, kuriuos šiuo metu gali pasiūlyti trys Lietuvoje akredituoti sertifikavimo paslaugų teikėjai: Skaitmeninio sertifikavimo centras, Registrų centras ir Gyventojų registro tarnyba. Paskutinio sertifikavimo centro siūlomų sertifikatų įsigijimo ir pratęsimo kaina yra mažiausia. Šie sertifikatai įrašomi į naujo pavyzdžio valstybės tarnautojo pažymėjimą (lustinė kortelė)“.

5 EK taip pat teigia, kad „nors yra kelios elektroninio parašo rūšys, tačiau kvalifikuotas elektroninis parašas yra geriausias pasirinkimas. Šiuo metu jau yra vienas tinkamas sprendimas – tai valstybės tarnautojo pažymėjimas, kuriame integruotas kvalifikuoto elektroninio parašo sertifikatas, ir jokių kitų variantų nereikėtų ieškoti”.

6 ekspertas taip pat mano, kad „reikėtų naudoti tik kvalifikuotus elektroninius parašus. Pavyzdžiui, viešojo sektoriaus darbo veikloje aš naudoju naujo pavyzdžio valstybės tarnautojo pažymėjimą. Tačiau šio e. parašo stacionari įranga nėra patogi kaip, pavyzdžiui, naudojantis e. banko sistema arba mobilia e. parašo formavimo įranga”.

7 EK teigia, kad „šiuo metu Lietuvoje yra patvirtintas e. dokumento ADOC formatas, todėl išoriniam lygmeniui siūlau taikyti kvalifikuotą elektroninį parašą”.

Apibendrinus pateiktus duomenis, galima teigti, kad visi ekspertai vienbalsiai sutinka, kad tik kvalifikuotas e. parašas gali būti naudojamas išoriniam lygmeniui. Dauguma ekspertų (4 respondentai) tvirtina, kad šiuo metu palankiausias ir pigiausias kvalifikuoto e. parašo sprendimas – naujo pavyzdžio valstybės tarnautojo pažymėjimas, kuriame įrašomas e. parašo kvalifikuotas sertifikatas (lustinė kortelė).

Pateikiant sprendimus dėl elektroninio parašo naudojimo vidiniame lygmenyje, daugelių ekspertų nuomonės taip pat sutampa.

1 EK teigia, kad „jei organizacija turi savo dokumentų valdymo sistemą (DVS), kuri apima galimybę naudoti saugius elektroninių parašų sertifikatus, tada tikrai užtektų tokio parašo pasirinkimo, bet manau, kad geriau naudoti kvalifikuotus sertifikatus: projektuojant DVS sistemas galima remtis vienu standartu ir procesais, svarbu ir tai, kad šiuo atveju pačiai organizacijai nereikia rūpintis sertifikatų galiojimu ir apsauga“.

2 EK mano, kad „vadovai, pavaduotojai ir skyrių vedėjai turėtų naudoti valstybės tarnautojo kortelėje (VTK) esamus kvalifikuotus sertifikatus. Kitų tarnautojų atveju (pvz. vizuojant) reikėtų naudoti autentifikavimo duomenų prijungimą prie metaduomenų“.

3 EK tvirtina, kad „asmenys, neturintys valstybės tarnautojo pažymėjimo, vidiniam naudojimui galėtų taikyti kelis kvalifikuoto e. parašo sprendimus – mobilus e. parašas arba naujo pavyzdžio asmens tapatybės kortelė. Šiuo atveju reikėtų atitinkamo viešojo sektoriaus institucijos vidaus teisinio sprendimo“.

4 EK teigia, kad „šiuo metu palankiausi e. parašo sprendimai yra dėl kvalifikuoto elektroninio parašo. Todėl toks parašas turėtų būti naudojamas ir įstaigos viduje“.

5 EK tvirtina, kad „valstybės tarnautojai turėtų taikyti kvalifikuotą e. parašą, integruotą į valstybės tarnautojo pažymėjimą. Dėl kitų asmenų reikia tinkamo sprendimo – darbuotojai, dirbantys pagal darbo sutartį, negauna panašių pažymėjimų. Šiuo atveju yra puikūs kvalifikuoto e. parašo pasirinkimai – tai mobilus e. parašas (SIM kortelė), asmens tapatybės kortelė. Reikėtų apžvelgti ir įvertinti taikymo galimybes. Esant poreikiui suteikti valstybės darbuotojo pažymėjimą su kontaktine elektronine laikmena, kurioje būtų asmens identifikavimo e. erdvėje ir kvalifikuoto e. parašo sertifikatas”.

6 EK mano, kad „šiai dienai nėra vieningo sprendimo. Aišku, kad asmenys, kurie kvalifikuotą e. parašą taiko išoriniam naudojimui (valstybės tarnautojų pažymėjimai), būtų logiška ir pigiau, jei taikytų ir vidiniam naudojimui. Dėl viešojo sektoriaus darbuotojų, kurie neturi tokių pažymėjimų, siūlyčiau esant poreikiui priimti atitinkamą sprendimą. Manyčiau, kad galėtų taikyti ir asmens tapatybės kortelę arba mobilų e. parašą. Tokiu atveju reikėtų vadovybės pritarimo ir sprendimo“.

7 EK teigia, kad „kiekviena organizacija pati sprendžia ir pasirenka tinkamus sprendimus. Tai priklauso nuo to, ar organizacija viduje toliau vykdo ADOC formato e. dokumentų pasirašymą, ar užtenka tik identifikacijos ir dokumentų valdymo sistemos priemonėmis užtikrinamas išsaugojimas. Pavyzdžiui, jei e. dokumentas turi būti saugomas ne ilgiau kaip 5 metus, tuomet užtektų identifikacijos priemonių, o dokumentų valdymo sistemos priemonėmis užtikrinamas išsaugojimas. Tuo tarpu, jei e. dokumentas turi būti saugomas ilgiau kaip 10 metų, tuomet reikėtų taikyti tik kvalifikuotą elektroninį parašą“.

Taigi, vidiniam naudojimui 5 iš 7 ekspertų siūlo naudoti taip pat kvalifikuotą elektroninį parašą. Tik keli ekspertai nurodo kvalifikuoto e. parašo pasirinkimus. Valstybės tarnautojų atžvilgiu tinkamas sprendimas – valstybės tarnautojo pažymėjimas (4 respondentai). Kitų viešojo sektoriaus darbuotojų atveju siūlomi keli sprendimai – tai mobilus e. parašas (3 respondentai), asmens tapatybės kortelė (3 respondentai) arba valstybės darbuotojo pažymėjimas (su kvalifikuotais sertifikatais) (1 respondentas).

Mokslinėje literatūroje dažniausiai aprašomas e. parašo poreikis ir sprendimai yra susiję su valstybės tarnautojais. Todėl buvo remtasi prielaida, kad ir ekspertai gali pateikti pasiūlymus tik šiai viešojo sektoriaus darbuotojų grupei. Dėl to tyrimo autorius pateikė sekantį kreipimąsį: „*Kaip sprendžiamas klausimas dėl e. parašo suteikimo darbuotojams, dirbantiems pagal darbo sutartį, viešajame sektoriuje*?“

1 EK teigia, kad niekaip nesupranta, „kam reikia tarnautojų pažymėjimų su sertifikatais, kurie patvirtina asmens tapatybę, juk tą patį užtikrina tapatybės kortelėje esantis sertifikatas. Manau, tikslinga numatyti, kad valstybės tarnautojai turėtų tapatybės korteles, o jau DVS galima žymėti specifinius atributus (pareigos ir t.t.). Kai asmuo pasirašo kaip vadovas ar kaip fizinis asmuo, jo parašai nesiskiria, skiriasi tik dokumentas ir asmens pozicija. Visą tai galima sudėti į DVS atributus ir naudoti tą patį asmens sertifikatą ir tarnyboje, ir asmeniniame gyvenime. Taip išspręstume problemą, kai asmeniui netekus darbo arba pakeitus darbo vietą, privalo būti panaikinti sertifikatai ir išduodami nauji“.

2 EK tvirtina, kad „viešojo sektoriaus institucijoje, kurioje aš dirbu, e. parašo nereikėjo pagal darbo sutartis dirbantiems viešojo sektoriaus darbuotojams. Pasiūlymai yra tokie:

- gauti mobilaus operatoriaus SIM kortelę. Šiuo metu du operatoriai jas teikia nemokamai;
- Valstybės tarnybos departamentas esant reikalui galėtų išdavinėti korteles su kvalifikuotais sertifikatais, t.y. analogiškai kaip valstybės tarnautojo kortelės su kvalifikuotais sertifikatais“.

3 EK teigia, kad „mano viešojo sektoriaus darbovietėje parašo teisę turi valstybės tarnautojai. Darbuotojams, dirbantiems pagal darbo sutartį, nėra poreikio pasirašinėti dokumentų e. parašu”.

4 EK mano, kad „šių darbuotojų atžvilgiu yra du galimi sprendimai – tai asmens tapatybės kortelė arba SIM kortelė (mobilus e. parašas)“.

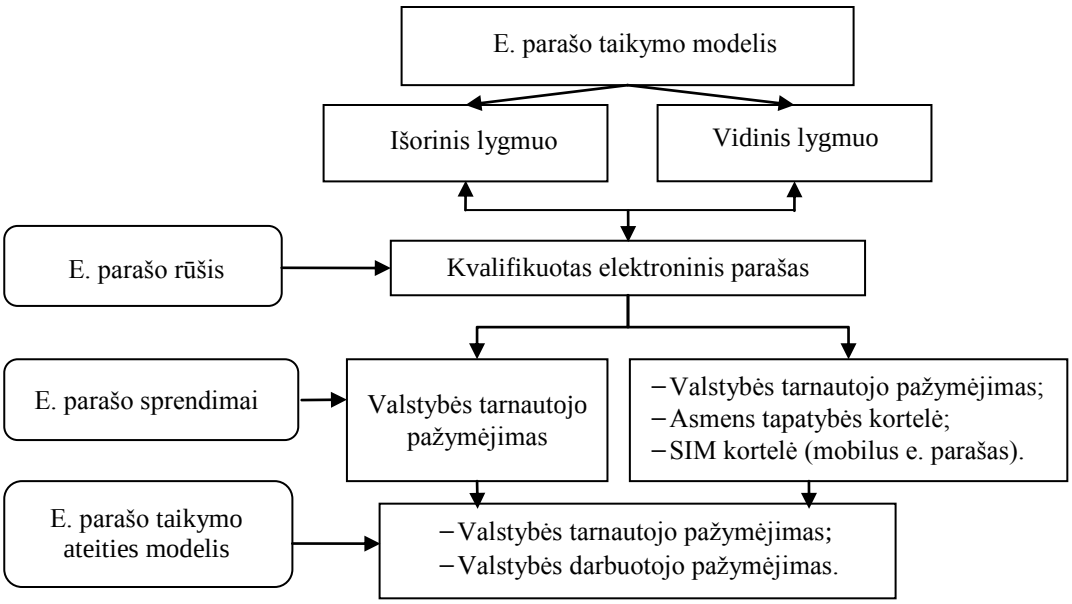
5 EK nuomone „esamos alternatyvos – mobilus e. parašas (SIM kortelė), asmens tapatybės kortelė. Reikėtų apžvelgti ir įvertinti šias taikymo galimybes. Esant poreikiui suteikti valstybės darbuotojo pažymėjimą su kontaktine elektronine laikmena, kurioje būtų asmens identifikavimo e. erdvėje ir kvalifikuoto e. parašo sertifikatas”.

6 EK mano, kad „galima taikyti ir asmens tapatybės kortelę arba mobilų e. parašą. Tokiu atveju reikėtų vadovybės pritarimo ir sprendimo“.

7 EK tvirtina, kad „tik politikai neturi specialių pažymėjimų. Valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartį, turi valstybės tarnautojo arba valstybės darbuotojo pažymėjimą. Politikai turėtų naudoti asmens tapatybės kortelę arba RC siūlomus e. parašus. Darbuotojų, dirbančių pagal darbo sutartį, atveju reikėtų įvertinti ir DVS priemones. Šiuo metu yra parengtas nutarimo projektas dėl pažymėjimų išdavimo politikams, kurie būtų analogiški valstybės tarnautojo pažymėjimui“.

Taigi, šiuo metu galimi du kvalifikuoto e. parašo sprendimai dėl viešojo sektoriaus darbuotojų, dirbančių pagal darbo sutartį – tai asmens tapatybės kortelė (5 respondentai), mobilaus operatoriaus SIM kortelė (5 respondentai). Esant poreikiui Valstybės tarnybos departamentas galėtų teikti valstybės darbuotojo pažymėjimus su kvalifikuotais sertifikatais (3 respondentai).

Apibendrinus dviejų klausimų rezultatus, nuspręsta pateikti veiksmingą e. parašo taikymo viešojo sektoriaus veikloje modelį (žr. 23 pav.).



Šaltinis: sudaryta autorės.

23 pav. Efektyvus e. parašo taikymo viešojo sektoriaus veikloje modelis

Remiantis išanalizuota moksline literatūra, darbo autorius negali įvertinti e. parašo plėtrą užtikrinančių sprendimų lygio. Todėl ekspertams buvo pateikta užduotis: „Įvertinkite priemones (politiniai, ekonominiai, socialiniai, organizaciniai ir technologiniai sprendimai), taikomas e. parašo plėtrai užtikrinti viešajame sektoriuje”. Šių priemonių pakankamumą reikėjo įvertinti 10 balų skalėje (1 – žemiausias, o 10 – aukščiausias įvertinimas). Gautus įvertinimus tyrimo autorius nusprendė suranguoti ir

apskaičiuoti reikšmingumo koeficientus. Duomenys buvo apdorojami, naudojant Microsoft Office Excel 2007 programą.

Pirmiausia visoms alternatyvoms buvo suteiktas vienodas svorio koeficientas (žr. (1) formulę).

$$k = \frac{1}{n}; \qquad (1)$$

Čia: k – svorio koeficientas;

n – ekspertizės objektų skaičius.

Antrame etape – nustatyti grupiniai (ekspertų vertinimų) įverčiai (žr. 10 lent.), t.y. suma kiekvieno vertinusio eksperto penkių alternatyvų rangų padauginta iš svorio koeficiento kvadratu (žr. (2) formulę).

$$c_{ij} = k^2 \times x_{ij}; \qquad (2)$$

Čia: c_{ij} – grupinis įvertis;

k – svorio koeficientas;

x_{ij} – pradinių įverčių suma.

10 lentelė. Ekspertų vertinimo dėl e. parašo plėtrą skatinančių priemonių duomenys (rangai) ir grupiniai įverčiai

Sprendimai	**1 EK**	**2 EK**	**3 EK**	**4 EK**	**5 EK**	**6 EK**	**7 EK**
Politiniai	8	7	7	8	7	8	8
Ekonominiai	8	6	8	8	7	8	8
Socialiniai	5	6	5	7	5	6	6
Organizaciniai	8	8	8	9	8	9	9
Technologiniai	10	8	9	10	9	10	10
Pradinių įverčių suma	39	35	37	42	36	41	41
Grupiniai įverčiai	1.56	1.4	1.48	1.68	1.44	1.64	1.64

Šaltinis: sudaryta autorės.

Tolesniame etape kiekviena i-ojo eksperto alternatyva (stulpelis) buvo dauginama iš grupinio įverčio ir apskaičiuojama elementų suma (žr. 11 lent.).

11 lentelė. Perskaičiuoti priemonių įverčiai ir jų bendroji suma

Sprendimai	**1 EK**	**2 EK**	**3 EK**	**4 EK**	**5 EK**	**6 EK**	**7 EK**
Politiniai	12.48	9.8	10.36	13.44	10.08	13.12	13.12
Ekonominiai	12.48	8.4	11.84	13.44	10.08	13.12	13.12
Socialiniai	7.8	8.4	7.4	11.76	7.2	9.84	9.84
Organizaciniai	12.48	11.2	11.84	15.12	11.52	14.76	14.76
Technologiniai	15.6	11.2	13.32	16.8	12.96	16.4	16.4
Perskaičiuotų įverčių suma	60.84	49	54.76	70.56	51.84	67.24	67.24
Suma	**421.48**						

Šaltinis: sudaryta autorės.

Paskutiniu žingsniu grupiniai įverčiai dauginami iš pradinės matricos eilučių ir susumuojami. Gautas sumas padalinus iš prieš tai gautos elementų sumos gaunamas reikšmingumo koeficientas (žr. 12 lent.)

12 lentelė. E. parašo plėtrą skatinantys sprendimai, įverčių sumos ir reikšmingumo koeficientai pagal ekspertų vertinimus

Sprendimai	**Įverčių sumos**	**Reikšmingumo koeficientas**
Politiniai	82.4	0.195501566
Ekonominiai	82.48	0.195691373
Socialiniai	62.24	0.147670115
Organizaciniai	91.68	0.217519218
Technologiniai	102.68	0.243617728
	421.48	1

Šaltinis: sudaryta autorės.

Reikšmingumo koeficientai leidžia nustatyti aiškius prioritetus dėl e. parašo skatinimo priemonių. Remiantis šiais duomenimis, galime teigti, kad įgyvendinti technologiniai sprendimai užtikrina galimybę modernizuoti viešojo sektoriaus darbą. Reikėtų pabrėžti, kad ši pažanga yra svarbiausia dalis visame e.

parašo procese. Taigi, valstybinėms institucijoms, savivaldybėms ir kitiems viešojo sektoriaus subjektams tik reikia išsirinkti tinkamas priemones ir jas pritaikyti visuomenės gerovei. Reikšmingumo koeficientas dėl organizacinių sprendimų parodo, kad valstybiniu mastu yra realizuotas elektroninio valdymo modelis, tačiau esamų sprendimų dar trūksta žemiausiame viešojo sektoriaus lygmenyje. Politiniai ir ekonominiai sprendimai yra vertinami beveik vienodai. Galima numatyti dvi priežastis: dėl lėšų trūkumo nėra įgyvendinami politiniai sprendimai, nors teisės aktuose ir yra įtvirtinti, arba finansinių išteklių stoka neskatina reglamentuoti svarbių politinių nuostatų. Reikėtų pabrėžti, kad šio parašo taikymo plėtrai didinti ypač nepakanka socialinių sprendimų. Tai reiškia, kad atsakingos valstybinės institucijos dar nesuformavo palankios aplinkos visuomenei, plačiai taikyti e. parašą.

E. parašas – svarbus pasiekimas ne tik e. dokumentų valdymo procese, bet ir nuotoliniu būdu teikiant e. paslaugas. Todėl svarbu nustatyti e. parašų naudojimo galimybes e. viešųjų paslaugų portale LR valstybės tarnautojams, viešojo sektoriaus darbuotojams, gyventojams ir verslo atstovams. Todėl ir buvo pateiktas sekantis klausimas: „*Kaip vertinate esamas e. parašo taikymo galimybes viešojo sektoriaus e. paslaugų teikėjams/naudotojams Elektroninių valdžios vartų portale*?“

1 EK teigia, kad „esami identifikavimo būdai ir priemonės pilnai tenkina vartotojų poreikius. Esamas paslaugų spektras, kuriame taikomas kvalifikuotas sertifikatas, maksimaliai priartintas prie asmeninių poreikių.“

2 EK tvirtina, kad šiuo metu yra „pakankamos priemonės naudotis autentifikavimo paslauga vienoje vietoje“.

3 EK teigia, kad „e. parašas, kalbant apie viešąsias paslaugas, labiau naudojamas kaip autorizavimo priemonė. Pavyzdžiui, mano darbovietės internetinėje svetainėje realizuota galimybė užsakant paslaugą pasirašyti e. parašu. Tačiau interesantai dažniausiai identifikuoja savo tapatybę pasinaudojus internetinės bankininkystės sistema, užsako paslaugas savo paskyroje be papildomo pasirašymo”.

4 EK nuomone „e. parašų taikymo įvairovė yra pakankamai didelė, identifikuojantis e. viešųjų paslaugų portale, todėl neapribojama vartotojų pasirinkimo teisė. Apžvelgus identifikavimo būdus valstybės tarnautojams ir viešojo sektoriaus darbuotojams, šiuo atveju galimas tik vienas pasirinkimas – valstybės tarnautojo pažymėjimas. Kadangi darbuotojai neturi galimybių prisijungti prie šios sistemos, todėl reikėtų peržvelgti ir įvertinti e. parašo taikymo poreikį bei realizuoti atitinkamus sprendimus”.

5 EK teigia, kad šiuo metu „e. identifikavimo priemonių pasirinkimą galima įvertinti 9 balais (10 balų skalėje) – galbūt reikėtų realizuoti identifikavimo sprendimus viešojo sektoriaus darbuotojams. Šiuo atveju reikėtų tinkamo vertinimo ir sprendimo“.

6 EK tvirtina, kad „viename portale integruotas platus e. parašų kaip identifikavimo priemonių pasirinkimas. Svarbus klausimas yra dėl e. parašo taikymo e. viešųjų paslaugų teikėjams. Nors vidiniam naudojimui siūliau, kad viešojo sektoriaus darbuotojai taikytų mobilų e. parašą arba asmens tapatybės kortelę, tai jungiantis prie išorinių sistemų tokio pasiūlymo negaliu pateikti“.

7 EK teigia, kad „užtenka jau dabar esamų integruotų e. parašo sprendimų valstybės tarnautojams e. viešųjų paslaugų svetainėje“. Šis sprendimas – valstybės tarnautojo pažymėjimas, kuriame integruotas kvalifikuoto e. parašo ir asmens identifikavimo e. erdvėje sertifikatas. Tokiu būdu užtikrinama, kad e. paslaugas teikia asmuo, kuris tuo metu dirba viešajame sektoriuje ir yra valstybės tarnautojas. Jei kalbėtume apie e. parašo sprendimus dėl viešojo sektoriaus darbuotojų, dirbančių pagal darbo sutartis, tai negalime kalbėti apie asmens tapatybės kortelės taikymą ar panašių fiziniems asmenims teikiamų e. parašų pritaikymą, teikiant e. paslaugas. Šiuo atveju realizuojamas asmens identifikavimas, bet nepatvirtinamos jo, kaip viešojo sektoriaus darbuotojo, pareigos“.

Taigi, galime teigti, kad e. parašų taikymo pasirinkimas e. valdžios vartų portale yra pakankamas gyventojams ir verslo subjektams – šiuo metu identifikuotis sistemoje negali viešojo sektoriaus darbuotojai, neturintys valstybės tarnautojo statuso. Todėl siūloma apsvarstyti ir esant poreikiui realizuoti tokią galimybę.

Siekiant plačiai taikyti e. parašą viešojo sektoriaus darbo veikloje ir visuomenės asmeniniame gyvenime, svarbu įvertinti e. parašo saugumą. Remiantis išanalizuota moksline literatūra, asmens tapatybę identifikuojančių duomenų vagystė – labiausiai plintanti XXI a. nusikaltimų rūšis. Todėl ekspertams buvo pateiktas sekantis klausimas – „*Kokias e. parašo saugumo problemas įžvelgiate*?“ Kiekvienas ekspertas turėjo įvardinti saugumo problemas e. parašo diegimo etape, e. parašu pasirašytų dokumentų perdavimo etape ir e. dokumentų saugojimo etape. Pirmiausiai buvo aprašomos aktualios problemos diegiant e. parašą.

1 EK teigia, kad „kalbant apie stacionarias e. parašų priemones, tai įžvelgiu tik vartotojų riziką. Vartotojai turėtų suvokti, kad personalizuoti saugumo duomenys yra riboto naudojimo ir turi būti ypatingai saugomi“.

2 EK tvirtina, kad „programinės priemonės, skirtos pasinaudoti stacionaria e. parašo generavimo įranga (pvz. asmens tapatybės kortele), parsisiunčiant iš paslaugų portalų, turi būti pasirašytos sertifikatu, išduotu tiekėjo, kurio pagrindinis (angl. ROOT) sertifikatas yra išplatintas pasaulyje dažniausiai naudojamose operacinėse sistemose“.

3 EK teigia, kad „e. parašo privatus raktas turėtų būti ypač gerai saugomas. Jokiu būdu nereikėtų saugoti šio rakto kompiuteryje. Šiai dienai ypač populiarios kenkėjiškos programos, kurios gali pasisavinti šiuos duomenis“.

4 EK tvirtina, kad „jei e. parašo naudotojai laikysis visų saugumo priemonių, jokių problemų neturėtų kilti“.

5 EK nuomone „naudojant saugius ar kvalifikuotus e. parašus, yra maža tikimybė prarasti asmens tapatybės duomenis, nes šių parašų veikimas paremtas dviejų raktų technologija. Šiai dienai lengviausiai prarandami asmens duomenys, kai asmuo jungiasi per internetinę bankininkystę, nes toks parašas paremtas vieno rakto technologija“.

6 EK teigia, kad „siekiant užtikrinti e. parašo saugumą, didžiausia kliūtis gali būti atsiųsta ir įdiegta nesaugi e. parašo formavimo programinė įranga”.

7 EK mano, kad „nebent programinė įranga bus suprojektuota nesaugiai ir galimybė bus įterpti virusą“.

Apibendrinus visų ekspertų nuomones, galima teigti, kad pagrindinė e. parašo saugumo rizika – vartotojai. Nesilaikydami saugumo priemonių ar dėl kompetencijos trūkumo, gali patys atskleisti šiuos duomenis.

Kita svarbi sritis – įvardinti e. parašo saugumą, perduodant e. parašu pasirašytą dokumentą.

1 EK teigia, kad „esanti nauja e. paslauga https://epristatymas.post.lt/ žengia pirmuosius žingsnius, kuri tikrai pagerins e. dokumentų pristatymo problemą (registruotų siuntų ir t.t.). Tik reikia ryžtingo sprendimo, kad bent jau viešosios organizacijos privalomai naudotų panašias paslaugas“.

2 EK tvirtina, kad „elektroniniai dokumentai negali būti perduodami viešaisiais interneto tinklais, pavyzdžiui, neapsaugotu e. paštu. Todėl siunčiant e. dokumentus, reikia pasirinkti saugius būdus (kanalus)“.

3 EK taip pat mano, kad „tik saugus e. dokumentų perdavimo būdas gali užtikrinti perduodamų e. dokumentų saugumą. Reikėtų paminėti, kad šiuo metu yra naujas sprendimas, kuris atvėrė galimybę saugiai pristatyti e. dokumentus fiziniams ir juridiniams asmenims bei viešojo sektoriaus institucijoms – tai e. pristatymo paslauga. Šiuo atveju reikėtų, kad abi šalys naudotusi šia paslauga. Galima drąsiai teigti, kad šis sprendimas – tradicinio pašto technologinis sprendimas“.

4 EK teigia, kad „šiandien labai mažai valstybinių institucijų teikia e. paslaugas, todėl nevisuomet galima saugiai keistis e. dokumentais. Tik praeitais metais buvo pristatyta nauja e. paslauga https://epristatymas.post.lt/, kuri gali paskatinti vykdyti e. dokumentų mainus. Tai saugus e. duomenų perdavimo kanalas“.

5 EK tvirtina, kad „e. pristatymo paslauga užtikrina, kad e. dokumentas bus užregistruotas ir perduotas tik adresatui. Dar svarbu pabrėžti, kad e. dokumentų turinys nėra prieinamas trečiosioms šalims, nes siuntos yra šifruojamos. Reikėtų akcentuoti, kad tai yra efektyvesnis sprendimas, nes ne visos viešojo sektoriaus institucijos dar teikia e. paslaugas, todėl fiziniams ir juridiniams asmenims bei valstybinėms institucijoms bus saugu keistis e. dokumentais. Labai svarbu paminėti, kad ypač fiziniai asmenys dažniausiai siųsdavo paklausimus viešojo sektoriaus institucijoms e. paštu, taip pat dažnai nurodydavo svarbius duomenis“.

6 EK patvirtina, kad „jei ankščiau ir buvo saugumo spragų, perduodant e. dokumentus, tai dabar jų nėra. Viešojo sektoriaus institucijos gali perduoti e. dokumentus per https://www.epaslaugos.lt/portal/, naudojantis e. pristatymo paslauga. Taip pat e. dokumentus galima teikti per e. valdžios vartų portalą ar savitarną“.

7 EK teigia, kad „e. dokumentai neturėtų būti siunčiami e. paštu, o perduodami per sistemą, kuri yra saugi. Šiuo metu e. dokumento pateikimas įmanomas per e.paslaugos.lt portalą, per savitarną, pavyzdžiui, SODRA turi savo savitarną, kurioje vienareikšmiškai identifikuojamasi ir pateikimas vykdomas koduotu kanalu, t.y. saugiu protokolu. Tai reiškia, kad siuntimo metu nepavogs duomenų, nes kanalas yra užkoduotas. Jei siųstume e. paštu, tai galimos dvi problemos: gali būti perimtas e. dokumentas arba nepasiekti adresato. E-delivery paslauga skirta saugiai pristatyti e. dokumentus“.

Taigi, visi ekspertai vienbalsiai sutinka, kad šiai dienai nėra jokių e. dokumento perdavimo saugumo kliūčių. Saugus e. parašu pasirašytų e. dokumentų perdavimas įmanomas naudojantis e. pristatymo paslauga. Šią paslaugą ypač teigiamai vertina net 6 ekspertai. Jų nuomone, tai geriausias ir tinkamiausias sprendimas – tai tradicinio pašto alternatyva.

Paskutinė šio klausimo dalis – e. parašo saugumas e. dokumentų saugojimo etape.

1 EK teigia, kad „esanti e. dokumentų saugojimo galimybė Lietuvos archyvų sistemoje išsprendė saugojimo problemas, tačiau organizacijų IS dar tik pradeda tinkamai veikti“.

2 EK mano, kad „turėtų būti ribojama pašalinių asmenų prieiga prie pasirašytų e. dokumentų“.

3 EK teigia, kad „dauguma viešojo sektoriaus institucijų dar nėra pasirengusios e. dokumentų saugojimui. Kiekviena organizacija turi priimti svarbius organizacinius ir technologinius sprendimus, tinkamam e. dokumentų saugojimui užtikrinti, pavyzdžiui, e. dokumentų saugojimo planas, išteklių planas ir atsakingų asmenų sąrašas. Svarbiausia sritis – technologiniai sprendimai, kurie užtikrintų e. dokumentų tinkamumą naudoti atitinkamam laikotarpiui“.

4 EK teigia, kad „e. parašo saugumas priklauso nuo e. dokumento saugumo. Todėl reikia kas kelis metus atnaujinti e. dokumentų saugojimo programinę įrangą, laikmenas, paskirti atsakingus asmenis, kurie visą tai tikrintų ir atnaujintų".

5 EK tvirtina, kad „technologijos sparčiai žengia į priekį, todėl svarbu per tam tikrą laikotarpį atnaujinti esamas programas, perkelti saugomus e. dokumentus iš vienų įtaisų į kitus".

6 EK teigia, kad „e. parašo saugumą lemia e. dokumentų saugojimo programinės įrangos ir laikmenų atnaujinimas. Dar svarbu, kad prieigą prie e. dokumentų turėtų tik paskirti asmenys".

7 EK mano, kad „egzistuoja problema, nes siekiant tinkamai išsaugoti ADOC e. dokumentus, reikia visų pirma per 1–3 d. paruošti e. dokumentą trumpalaikiam saugojimui, o ilgalaikiam saugojimui užtikrinti – kas 3–5 m. reguliariai uždėti laiko žymą".

Apibendrinus nuomones, galima teigti, kad siekiant užtikrinti e. parašo saugumą e. dokumentų saugojimo etape, reikia nuolat atnaujinti programinę įrangą ir laikmenas bei apriboti fizinių asmenų prieigą prie e. dokumentų.

Analizuojant mokslinę literatūrą, darbo autorius pastebėjo, kad e. parašas nėra plačiai taikomas viešojo sektoriaus veikloje. Dėl to buvo pateiktas sekantis klausimas – „*Kokie sprendimai galėtų padidinti e. parašo taikymo mastą viešajame sektoriuje?*"

1 EK teigia, kad „visos priemonės jau yra, reikia ryžtingų sprendimų:

1. trumpesni apdorojimo terminai pateiktiems e. dokumentams, pasirašytiems e. parašu. Tai paskatintų vartotojus su viešojo sektoriaus institucijomis komunikuoti e. būdu.
2. grąžinti įstatymiškai nuostatą dėl asmens tapatybės kortelės privalomumo – dauguma asmenų, kurie turi pasus, tapatybės kortelių neužsako, todėl automatiškai neturi elektroninių sertifikatų.
3. valstybė turi užsiimti socialine rinkodara".

2 EK tvirtina, kad „e. parašo plėtrą gali padidinti valstybės mastu įsigyta Lietuvoje platinamų sertifikatų OCSP tikrinimo paslauga bei laiko žymų tarnybos paslauga, skirta viešajam sektoriui".

3 EK mano, kad „turėtų būti griežtesnis teisinis reglamentavimas. Pavyzdys galėtų būti teisės aktų registras (TAR). Į šį registrą galima patalpinti tik e. dokumentą, pasirašytą kvalifikuotu e. parašu".

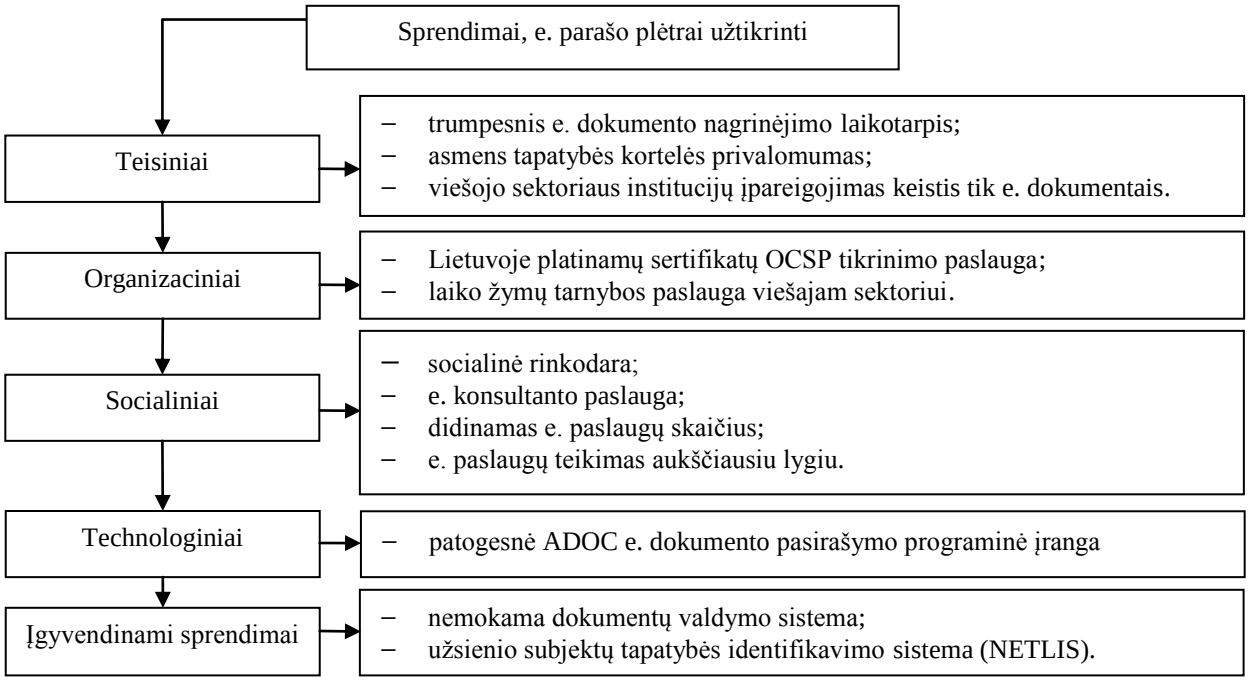
4 EK siūlo „pasekti verslo pavyzdžiu ir įgyvendinti e. konsultanto paslaugą. Šią paslaugą galėtų teikti, pavyzdžiui, RRT, kuri yra atsakinga už e. parašo infrastruktūrą. E. konsultantas praverstų ir naudojantis e. paslaugomis. Kitas pasiūlymas – aktyviai skatinti piliečius taikyti e. parašą, pavyzdžiui, bankai kiekvieną klientą informuoja apie e. bankininkystės privalumus. Manyčiau, kad reikėtų teisiškai reglamentuoti ir trumpesnį e. prašymų, skundų bei pranešimų nagrinėjimo laikotarpį".

5 EK tvirtina, kad „reikėtų didinti e. paslaugų skaičių ir e. paslaugas teikti aukščiausiu lygiu, taip pat priimti teisinę nuostatą dėl trumpesnio e. dokumento nagrinėjimo laikotarpio“.

6 EK mano, kad „valstybė turėtų priimti vientisą sprendimą dėl laiko žymų pirkimo viešajam sektoriui”.

7 EK teigia, kad „šiuo metu kuriama nemokama dokumentų valdymo sistema (DVS), kuria galės naudotis mažesnės viešojo sektoriaus institucijos, kurios neturi nuosavos. Tai planuojama įgyvendinti 2014–2015 m. Iki 2015 m. birželio mėnesio bus realizuotas ir užsienio subjektų tapatybės liudijimas, naudojantis Nacionaline elektroninės tapatybės liudijimo sistema (NETLIS). Galėčiau pasiūlyti du sprendimus, kurie, mano muomone, galėtų padidinti e. parašo naudojimo lygį. Pirmiausia reikėtų akcentuoti, kad ADOC e. dokumento pasirašymas yra ilgas ir sudėtingas procesas. Todėl galima padaryti įrankius (tools), kurie užtikrintų patogesnį naudojimą. Tai yra reikėtų atrasti kaip galima būtų paprasčiau pasirašyti ADOC e. dokumentą, pavyzdžiui, pažymėti varnele vieną iš kelių siūlomų variantų ir pasirašymo procesas įvykdytas. Tai yra ADOC e. dokumento pasirašymo procesas turi būti paremtas vartotojams draugiškais įrankiais. Kitas pasiūlymas – kelti e. paslaugų teikimo lygį“.

Apibendrinus nuomones, galima teigti, kad dauguma pasiūlymų yra susiję su piliečiais. (žr. 24 pav.).



Šaltinis: sudaryta autorės.

24 pav. Sprendimai dėl e. parašo plėtros

E. parašo platesnį naudojimą gali lemti ir Lietuvos e. atpažinties priemonių pripažinimas ES valstybėse. Todėl buvo pateiktas sekantis klausimas – „*Ar Lietuvoje taikomi reikalavimai elektroninės atpažinties priemonėms yra tapatūs su ES reikalavimais. Ar jų pripažinimas įmanomas kitose ES valstybėse narėse?* Šį dvigubą klausimą sudarė tris dalys: *reikalavimai sertifikavimo paslaugų teikėjams, sertifikatuose įrašomų asmens duomenų elementai, pripažinimas tarpvalstybiniu lygiu.* Taigi, pirmiausiai buvo pateikiami respondentų atsakymai dėl reikalavimų sertifikavimo paslaugų teikėjams.

1 EK teigia, kad „galioja e. parašo direktyva, įstatymas atitinka ją. Mūsų kvalifikuotų e. sertifikatų leidėjai yra pripažistami ES, toks direktyvos reikalavimas. Jie akreditavosi ir veikia tinkamai“.

2 EK tvirtina, kad „yra ES direktyva, todėl yra tapatūs. Pripažinimas yra įmanomas visoje ES“.

3 EK taip pat sutinka kad, „e. parašą reglamentuojanti teisinė bazė buvo rengiama suderinus su Europos Sąjungos reikalavimais. E. parašo direktyvoje yra griežtai įtvirtinti reikalavimai kvalifikuotų sertifikatų teikėjams“. Todėl saugūs e. parašai, paremti kvalifikuotu sertifikatu ir išduoti akredituotų sertifikavimo paslaugų teikėjų, yra pripažįstami ne tik Lietuvoje, bet ir visoje ES“.

4 EK taip pat teigia, kad „e. parašo įstatymas buvo parengtas remiantis ES e. parašo direktyva, todėl ir reikalavimai sertifikavimo paslaugų teikėjams, išduodantiems kvalifikuotus sertifikatus, yra vienodi. Taigi, jų pripažinimas yra privalomas visose ES valstybėse“.

5 EK taip pat tvirtina, kad „e. parašo įstatymas tinkamai reglamentuoja ES direktyvą dėl Bendrijos elektroninių parašų reguliavimo sistemos, todėl ir reikalavimai kvalifikuotų sertifikatų teikėjams yra analogiški”.

6 EK visiškai palaiko kitų ekspertų nuomonę. Šiuo metu „yra ES e. parašo direktyva ir buvo nustatyta, kad ji tinkamai buvo perkelta į Lietuvos teisinę bazę, t.y. LR elektroninio parašo įstatymą. Todėl jokių abejonių dėl reikalavimų sertifikavimo paslaugų teikėjams, išduodantiems kvalifikuotus sertifikatus, skirtumų Lietuvoje ir ES šalyse negali būti net kalbos“.

7 EK teigia, kad „jei kalbama apie kvalifikuotą e. parašą, tai galioja visose ES valstybėse. Kvalifikuotų sertifikatų teikėjai yra suskaičiuoti visoje ES ir valstybės keičiasi tarpusavyje informacija, kuris teikėjas yra kvalifikuotas, o kuris nekvalifikuotas. Jei Ispanijoje įsigijau kvalifikuotą sertifikatą, tai galiu naudoti ir Lietuvoje bei atvirkščiai”.

Kita svarbi šio klausimo dalis – sertifikatuose įrašomų asmens duomenų elementų suderinamumas ES mastu.

1 EK teigia, kad „remiantis ES STORK projektu, mūsų tapatybės kortelės su sertifikatais yra unifikuotos ES lygiu. Registrų centro išduoti sertifikatai ir teismo sprendimas uždraudęs juose nurodyti asmens kodą tik patvirtina, kad Lietuvoje nėra vieningos e. parašo plėtros strategijos“.

2 EK tvirtina, kad „yra ES direktyva, todėl yra tapatūs. Tačiau išlieka klausimas, kaip vienareikšmiškai nustatyti, kad kitos šalies pilietis yra tas pats asmuo sertifikate ir asmens dokumente. Pagal Lietuvoje išduotą sertifikatą, asmuo vienareikšmiškai nustatomas lyginant jo vardą, pavardę ir asmens kodą“.

3 EK tvirtina, kad „visuose sertifikatuose įrašomas asmens vardas ir pavardė. Tačiau nėra vieningo sprendimo dėl asmens kodo ES lygiu“.

4 EK tvirtina, kad „dar ir šiandien galima susidurti dėl skirtingų asmens duomenų pateikimo sertifikatuose. Reikėtų prisiminti nepalankų teismo sprendimą dėl asmens kodo. 2012 m. Lietuvos vyriausiasis administracinis teismas priėmė galutinį sprendimą, kuriuo patvirtino Valstybinės duomenų apsaugos inspekcijos draudimą į kvalifikuotus sertifikatus įrašyti asmens kodą. Šiuo metu Lietuvoje išduota dešimtys tūkstančių sertifikatų su asmens kodu. Tačiau išlieka neišspręstas klausimas – kaip tinkamai identifikuoti asmenį tik pagal vardą ir pavardę“.

5 EK teigia, kad „teismo sprendimu buvo nustatyta, kad Registrų centro išduoti sertifikatai su asmens kodais prieštarauja įstatymui. Todėl, remiantis tokiu sprendimu, galima teigti, kad nėra aiškaus reglamentavimo, t.y. spragos, kurios leidžia skirtingai traktuoti įstatymą. Nemanau, kad tik asmens vardas ir pavardė gali būti baigtiniai asmens duomenys: sunku būtų susieti tą patį asmenį, jei jis naudotų kelis sertifikatus. Taigi, neaiškumų šiuo klausimu vis dar yra“.

6 EK taip pat tvirtina, kad „šiuo metu sertifikatuose yra privalomas tik asmens vardas ir pavardė. Remiantis įstatymu, gali būti panaudoti ir kiti asmenį labiau identifikuojantys duomenys. Tačiau asmens kodas tikrai ne, nors kai kurie sertifikavimo paslaugų teikėjai įrašo tokius duomenis. Taigi, kokie tai galėtų būti duomenys, kurie leistų tiksliau identifikuoti asmenį, yra nežinia“.

7 EK teigia, kad „vardas ir pavardė – vienareikšmiškai privalomi, o asmens kodas – kiekvienos šalies reikalas. Pavyzdžiui, dėl Registrų centro išduotų sertifikatų su įrašytu asmens kodu teismas priėmė nepalankų sprendimą“.

Svarbiausias klausimas – dėl e. atpažinties priemonių pripažinimo tarpvalstybiniu lygiu.

1 EK teigia, kad „ES lygiu viskas išspręsta minėtame STORK projekto rėmuose. Tačiau Lietuvos situacijos pakomentuoti neturiu galimybės“.

2 EK tvirtina, kad „teisiškai yra įmanoma, nes atitinka ES direktyvą. Šiuo metu praktinis pripažinimas yra tik bandomojoje stadijoje“.

3 EK teigia, kad „šiuo metu yra vykdomas STORK pilotinis projektas. Šiame projekte dalyvauja ir Lietuva. Pagrindinis šio projekto tikslas yra sukurti Europos eID sąveikumo platformą. VIISP sistemoje esanti STORK versija yra tik parodomoji. Kai bus įgyvendintas STORK 2.0 etapas, planuojama

įgyvendinti pirmąjį ir antrąjį STORK lygius. Tai reiškia, kad visi veiksmai dėl pripažinimo ES lygiu yra vykdomi“.

4 EK sutinka, kad „artimiausiu metu bus galima praktiškai taikyti Lietuvos e. atpažinties priemones visose ES šalyse. Pavyzdys yra STORK projektas“.

5 EK tik patvirtina kitų ekspertų nuomones. „Nereikia abejoti, tikrai visi e. parašai bus pripažįstami ES šalyse. Dėl to ir buvo priimta direktyva, kad lengviau būtų suderinti visas e. atpažinties priemones, jų naudojimą ne tik vienos šalies lygiu“.

6 EK mano, kad „kiekvienas LR pilietis galės taikyti nacionalines e. parašo priemones net ir būdamas kitoje šalyje. Aišku, šiandien tokio sprendimo dar nėra – turime STORK projektą, bet viskas tik išbandoma ir dar derinama“.

7 EK tvirtina, kad „pripažinimas yra įteisintas ES ribose. Lietuva artimiausiu metu (1,5 m. laikotarpyje) užtikrins galimybę užsienio subjektams identifikuoti tapatybę, naudojant savo nacionalines elektroninės atpažinties priemones“.

Taigi, visi ekspertai yra vieningos nuomonės, kad Lietuvoje taikomi reikalavimai sertifikavimo paslaugų teikėjams, išduodantiems kvalifikuotus sertifikatus, yra vienodi ES mastu ir jų pripažinimas yra privalomas – LR elektroninio parašo įstatymas atitinka ES direktyvą „Dėl Bendrijos elektroninių parašų reguliavimo sistemos”. Šiai dienai nėra vieningo sprendimo dėl asmens kodo įrašymo kvalifikuotuose sertifikatuose – asmens duomenys kaip vardas ir pavardė yra privalomi, tuo tarpu asmens kodas – kiekvienos šalies reikalas. Pavyzdžiui, Lietuvos teismai priima nepalankius sprendimus dėl asmens kodo įrašymo sertifikatuose. Kalbant apie pripažinimą tarpvalstybiniu lygiu, teisiškai yra įmanoma, o praktiškai – dar įgyvendinamas STORK pilotinis projektas.

Analizuojant mokslinę literatūrą, darbo autorius pastebėjo, kad elektroninio parašo plėtra vyksta labai lėtai. Todėl reikėtų nustatyti svarbiausias ir menkiausias kliūtis, turinčias įtakos elektroninio parašo taikymui viešajame sektoriuje. Šie argumentai paskatino pateikti sekantį klausimą – „*Kokios yra pagrindinės kliūtys pagal jų svarbą dėl nepakankamo elektroninio parašo naudojimo viešojo sektoriaus veikloje?*“ Ekspertinio vertinimo anketoje buvo pateikta 10 kliūčių (žr. 6 priedo 8 klausimą). Visas kliūtis kiekvienas ekspertas turėjo išdėstyti eiliškumo tvarka. Ekspertų įvertintų kliūčių elementų svarbumas buvo išreikštas santykiu (žr. (3) formulę), kuris parodo, kiek kartų atskiras elementas buvo paminėtas ir kokį vidutinį balų skaičių jis surinko (žr. 13 lent. ir 6 priedo 8 klausimą). Kuo vidutinis balas yra žemesnis, tuo elemento vieta – aukštesnė reitingų eilėje (Augustinaitis ir kt., 2009, p. 272). Duomenys buvo apdorojami, naudojant Microsoft Office Excel 2007 programą.

$$k = \frac{m^2}{\sum_{i=1}^{m} x_i}; \qquad (3)$$

Čia: m – suminis skaičius, kuris parodo, kiek kartų visi ekspertai paminėjo kliūties elementą;

x_i – elementui suteiktas rangas, i = 1, 2, ..., m.

13 lentelė. Ekspertų kliūčių vertinimo ir apskaičiuotų svorio k reikšmių rezultatai

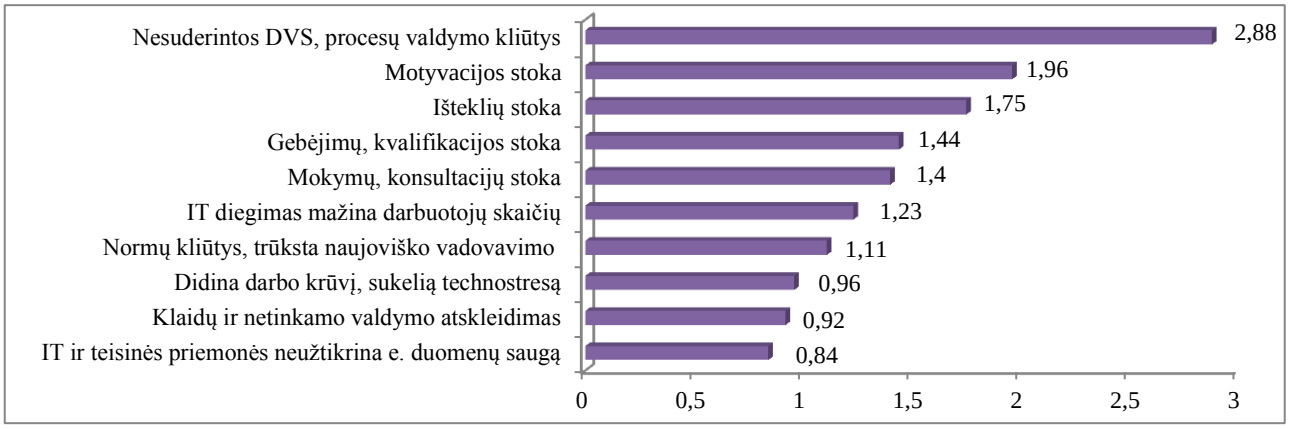
Ekspertas	*Kliūčių elementai (alternatyvos)*									
	1 kliūtis	2 kliūtis	3 kliūtis	4 kliūtis	5 kliūtis	6 kliūtis	7 kliūtis	8 kliūtis	9 kliūtis	10 kliūtis
1 EK	7	8	10	9	5	1	2	3	6	4
2 EK	2	7	1	6	5	10	3	8	9	4
3 EK	10	5	9	8	3	2	1	6	4	7
4 EK	9	8	10	7	4	1	2	6	5	3
5 EK	8	7	10	9	1	2	3	5	4	6
6 EK	7	8	9	5	4	1	2	10	3	6
7 EK	10	1	9	7	6	8	4	2	3	5
Rangų suma	*53*	*44*	*58*	*51*	*28*	*25*	*17*	*40*	*34*	*35*
Svorio k reikšmės	*0.92*	*1.11*	*0.84*	*0.96*	*1.75*	*1.96*	*2.88*	*1.23*	*1.44*	*1.40*

Šaltinis: sudaryta autorės.

Atsižvelgiant į kliūčių svorius, galima teigti, kad svarbiausi trūkumai yra susiję su e. parašo plėtrai vadovaujančiomis institucijomis (žr. 25 pav.). Pirma, šiai dienai dar nėra suderintos e. dokumentų valdymo sistemos Lietuvos mastu: nėra parengtas tinkamas e. dokumentų sistemų suderinimo modelis, apimantis tinkamus teisinius, organizacinius ir technologinius sprendimus. Dėl šios priežasties e. dokumentų mainai tarp viešojo sektoriaus institucijų nėra plačiai vykdomi. Antra, atsakingos institucijos silpnai motyvuoja viešąjį sektorių taikyti e. parašą. Šiuo atveju galima išskirti dvi priežastis: arba taikomos priemonės yra neveiksmingos, arba jų nepilnai pakanka. Antrą priežastį patvirtina trečia kliūtis: valstybė neskiria lėšų e. parašo diegimui viešajame sektoriuje. Ketvirta kliūtis – gebėjimų kliūtys ir kvalifikacijos stoka. Tai reiškia, kad valstybės tarnautojų ir viešojo sektoriaus darbuotojų turimo išsilavinimo nepakanka, dėl to nežinoma kaip tiksliai įgyvendinti e. dokumentų pasirašymo ir valdymo procesą. Šią situaciją dar labiau sutvirtina penkta kliūtis – trūksta mokymų ir konsultacijų dėl e. parašo ir

e. dokumento procedūrų. Taigi, galima tik patvirtinti, kad atsakingos valstybinės institucijos nerealizavo ypač svarbių sprendimų, kurie šiai dienai yra įvertinami kaip didžiausios kliūtys. Tai leidžia patvirtinti visas tyrimo hipotezes:

1. Elektroninio parašo spartesnę plėtrą viešajame sektoriuje stabdo nepakankama vadovaujančių institucijų skatinimo politika taikyti e. parašą viešojo sektoriaus darbe;
2. Elektroninis parašas platesniu mastu nenaudojamas dėl valstybės tarnautojų pasipriešinimo kaitai žmogiškųjų veiksnių – informacijos, kvalifikacijos ir motyvacijos stokos.



Šaltinis: sudaryta autorės.

25 pav. Ekspertų įvertintų kliūčių dėl e. parašo plėtros eiliškumas

Išanalizavus visus tyrimo klausimus ir apibendrinus atsakymus, tyrimo autorius nusprendė pateikti ekspertų atsakymų į tyrimo klausimus esminių išvadų ir siūlymų lentelę (žr. 14 lent.).

14 lentelė. Ekspertų vertinimų apibendrintos išvados ir siūlymai

Klausimas	Išvados	Siūlymai
1. Kokį e. parašo modelį siūloma taikyti viešojo sektoriaus veikloje? **1.1. Išorinis lygmuo** **1.2. Vidinis lygmuo**	1.1. Kvalifikuotas e. parašas. E. parašo priemonės – valstybės tarnautojo pažymėjimas. 1.2. Kvalifikuotas e. parašas. E. parašo priemonės – valstybės tarnautojo pažymėjimas, SIM kortelė, asmens tapatybės kortelė.	Kvalifikuotas e. parašas. E. parašo sprendimai: – valstybės tarnautojo pažymėjimas; – valstybės darbuotojo pažymėjimas.
2. Kaip sprendžiamas klausimas dėl e. parašo suteikimo darbuotojams, dirbantiems pagal darbo sutartį, viešajame sektoriuje?	Vidiniam naudojimui – asmens tapatybė kortelė, SIM kortelė.	Išoriniam naudojimui Valstybės tarnybos departamentas turėtų teikti valstybės darbuotojo pažymėjimus su kvalifikuotais sertifikatais.

Klausimas	Išvados	Siūlymai
3. Įvertinkite žemiau pateiktas priemones (politiniai, ekonominiai, socialiniai, organizaciniai ir technologiniai sprendimai), taikomas e. parašo plėtrai užtikrinti viešajame sektoriuje.	– technologiniai sprendimai užtikrina galimybę modernizuoti viešojo sektoriaus darbą; – organizacinių sprendimų dar trūksta žemiausiame viešojo sektoriaus lygmenyje; – politinių priemonių trūkumą lėmė finansavimo stoka; – labiausiai trūksta socialinių sprendimų – atsakingos valstybinės institucijos dar nesuformavo palankios aplinkos visuomenei, plačiai taikyti e. parašą.	Skirti pakankamą finansavimą, e. parašo plėtrai užtikrinti, įgyvendinti daugiau socialinių sprendimų.
4. Kaip vertinate esamas e. parašo taikymo galimybes viešojo sektoriaus e. paslaugų teikėjams/ naudotojams e. valdžios vartų portale?	E. parašų taikymo pasirinkimas yra pakankamas gyventojams ir verslo subjektams – šiuo metu identifikuotis sistemoje negali viešojo sektoriaus darbuotojai, neturintys valstybės tarnautojo statuso.	Valstybės tarnybos departamentas esant poreikiui turėtų teikti valstybės darbuotojo pažymėjimus su kvalifikuotais sertifikatais.
5. Kokias e. parašo saugumo problemas įžvelgiate? **5.1. E. parašo diegimo etape** **5.2. E. parašu pasirašytų dokumentų perdavimo etape** **5.3. E. dokumentų saugojimo etape**	5.1. E. parašo saugumo rizika – vartotojai. 5.2. Nėra e. dokumento perdavimo saugumo kliūčių: saugus e. dokumentų perdavimas įmanomas, naudojantis e. pristatymo paslauga. 5.3. Reikia nuolat atnaujinti programinę įrangą ir laikmenas bei apriboti fizinių asmenų prieigą prie e. dokumentų.	5.1. E. parašo nuotolinio mokymo sistema. 5.3. Periodiškas programinės įrangos ir laikmenų tikrinimas bei atnaujinimas.
6. Kokie sprendimai galėtų padidinti e. parašo taikymo mastą viešajame sektoriuje?	6.1. **Teisiniai** – trumpesnis e. dokumento nagrinėjimo laikotarpis, asmens tapatybės kortelės privalomumas, viešojo sektoriaus institucijų įpareigojimas keistis tik e. dokumentais. 6.2. **Organizaciniai** – Lietuvoje platinamų sertifikatų OCSP tikrinimo paslauga, laiko žymų tarnybos paslauga viešajam sektoriui. 6.3. **Socialiniai** – socialinė rinkodara, e. konsultanto paslauga, didinamas e. paslaugų skaičius, e. paslaugų teikimas aukščiausiu lygiu. 6.4. **Technologiniai** – patogesnė ADOC e. dokumento pasirašymo programinė įranga. 6.5. **Įgyvendinami sprendimai** – nemokama dokumentų valdymo sistema, užsienio subjektų tapatybės identifikavimo sistema (NETLIS).	Įgyvendinti pateiktus sprendimus.
7. Ar Lietuvoje taikomi reikalavimai e. atpažinties priemonėms yra tapatūs su ES reikalavimais. Ar jų pripažinimas įmanomas kitose ES valstybėse narėse?	**7.1. Reikalavimai sertifikavimo paslaugų teikėjams** Reikalavimai sertifikavimo paslaugų teikėjams, išduodantiems kvalifikuotus sertifikatus, yra vienodi, nes LR elektroninio parašo įstatymas atitinka ES direktyvą „Dėl Bendrijos elektroninių parašų reguliavimo sistemos". **7.2. Sertifikatuose įrašomų asmens duomenų elementai** Vardas ir pavardė yra privalomi, o asmens kodas – kiekvienos šalies reikalas. Pavyzdžiui, Lietuvos teismai yra prieš asmens kodo įrašymą sertifikatuose. **7.3. Pripažinimas tarpvalstybiniu lygiu** Teisiškai yra įmanoma, o praktiškai – dar įgyvendinamas STORK pilotinis projektas.	Tęsti dalyvavimą STORK ir kituose ateities tarpvalstybinio e. atpažinties pripažinimo projektuose.
8. Kokios yra pagrindinės kliūtys pagal jų svarbą dėl nepakankamo e. parašo naudojimo viešojo sektoriaus veikloje?	1. Nesuderintos DVS, procesų valdymo kliūtys; 2. Motyvacijos stoka; 3. Išteklių trūkumas; 4. Gebėjimų, kvalifikacijos stoka; 5. Mokymų, konsultacijų trūkumas.	Pašalinti kliūtis.

Šaltinis: sudaryta autorės.

IŠVADOS IR REKOMENDACIJOS

Išvados

1. Išanalizavus mokslinę literatūrą, suformuota oficialaus e. dokumento samprata, įvardintos pagrindinės e. dokumento savybės ir esminiai e. dokumentų valdymo skirtumai:
   1.1. Oficialus e. dokumentas – tai organizacijos vykdomų įsipareigojimų arba juridinio asmens veiklos metu informacinių technologijų pagalba parengtas arba gautas e. dokumentas, kuris pasirašytas teisinę galią turinčiu e. parašu ir jo turinys, struktūra ir kontekstas (metaduomenys) yra pakankami veiklai įrodyti bei įtrauktas į įstaigos dokumentų valdymo sistemą.
   1.2. Pagrindinė e. dokumento savybė yra autentiškumas, nes užtikrina visų e. dokumento sandaros dalių nekintamumą. Autentiškumą užtikrina teisinę galią turintys elektroniniai parašai.
   1.3. Elektroninių dokumentų naudojimo plėtrą užtikrina šių dokumentų valdymui įtvirtinta teisinė bazė, sukurta elektroninio archyvo informacinė sistema. Viešojo sektoriaus institucijos turi įrengti elektroninių dokumentų valdymo sistemą, remiantis Elektroninių dokumentų valdymo taisyklėse įvardintais reikalavimais. Elektroninio dokumento sandarą reglamentuoja Elektroninių dokumentų specifikacijų reikalavimų aprašas, kurį įsakymu tvirtina Lietuvos vyriausiasis archyvaras. Dabartiniu metu patvirtinta elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0, kuri prilyginama rašytiniams dokumentams.
2. Apžvelgus mokslinę literatūrą, įvardintos e. parašo rūšys ir jų taikymas viešojo sektoriaus veikloje:
   2.1. Elektroninis parašas – tai elektronine forma pateikti duomenys, kurie prijungiami arba logiškai susiejami su kitais elektroniniais duomenimis, pastarųjų autentiškumui patvirtinti ir pasirašančiam asmeniui identifikuoti.
   2.2. Paprasto elektroninio parašo kūrimui naudojama simetrinio šifravimo sistema – failo užšifravimui ir iššifravimui naudojamas vienas ir tas pats raktas, t.y. slaptasis raktas. Simetrinio šifravimo sistema nelabai tinkama tose srityse, kur būtina įsitikinti duomenų siuntėjo tapatybe. Taigi, viešojo sektoriaus darbo veikloje paprasto e. parašo naudojimas yra nerekomenduojamas.
   2.3. Saugus e. parašas pagrįstas dviejų raktų asimetrinio šifravimo sistema (PKI). Privatusis raktas skirtas kurti e. parašą arba duomenis paversti užkoduotais, o viešas raktas – parašui tikrinti arba pranešimui sugrąžinti pradinę formą. Saugus e. parašas yra apsaugotas nuo sukčiavimo. Toks parašas turi teisinę galią, jei parašų naudotojai tarpusavyje dėl to susitaria. Šį parašą saugu

naudoti viešojo sektoriaus institucijos viduje (dokumento rengėjo parašui, vizavimui ir kt.) bei pasirašant dokumentus, skirtus vidiniam naudojimui.

2.4. Kvalifikuotas e. parašas – tai valstybės sureguliuota saugi identifikavimo priemonė. Toks parašas įvardinamas kaip saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu. Šių e. parašų saugumą užtikrina trečias asmuo, valstybės patvirtintas kvalifikuotų sertifikatų teikėjas, todėl nereikia dviejų šalių susitarimo. Kvalifikuotu e. parašu pasirašomi e. dokumentai yra saugūs.

3. Atlikus e. parašo naudojimo analizę, nustatytas e. parašo taikymo viešojo sektoriaus veikloje mastas bei prioritetinės veiklos kryptys:

3.1. E. parašas viešojo sektoriaus veikloje naudojamas vangiai – naują parašo technologiją naudoja tik 6 aukščiausios valdžios institucijos, 8 viešojo sektoriaus institucijos taiko išorinių ir/arba vidinių e. dokumentų pasirašymui, 17 valstybės institucijų teikia e. paslaugas.

3.2. Prioritetinės veiklos kryptys – toliau dalyvauti STORK ir kituose projektuose dėl e. atpažinties priemonių taikymo ES mastu.

4. Remiantis ekspertinio tyrimo dėl e. parašo taikymo viešojo sektoriaus veikloje rezultatais, nustatyti skatinamieji veiksniai ir kliūtys, įtakojantys e. parašo naudojimą, bei parengtas veiksmingas e. parašo taikymo modelis:

4.1. E. parašo plėtrą skatinantys veiksniai – technologiniai sprendimai užtikrina galimybę modernizuoti viešojo sektoriaus darbą, valstybiniu mastu yra realizuotas e. valdymo modelis.

4.2. E. parašo naudojimo plėtrą stabdo nesuderintos e. dokumentų valdymo sistemos Lietuvos mastu ir šių procesų valdymo kliūtys, motyvacijos naudoti e. parašą stoka, finansinės paramos trūkumas, gebėjimų kliūtys ir kvalifikacijos stoka, mokymų ir konsultacijų dėl e. parašo ir e. dokumento procedūrų trūkumas. E. parašo plėtrai kliudo nepakankama vadovaujančių institucijų skatinimo politika ir kvalifikacijos, motyvacijos bei informacijos trūkumas.

4.3. Veiksmingas ir užtikrinantis e. dokumentų saugumą e. parašo taikymo modelis viešajame sektoriuje išoriniame lygmenyje turėtų būti kvalifikuotas e. parašas, integruotas į valstybės tarnautojo pažymėjimą, o vidiniame lygmenyje kvalifikuotas e. parašas, pasirenkant valstybės tarnautojo pažymėjimą, SIM kortelę arba asmens tapatybės kortelę.

Rekomendacijos

1. Įgyvendinti veiksmingą e. parašo taikymo viešojo sektoriaus veikloje ateities modelį, pagal kurį išoriniame ir vidiniame lygmenyje reikėtų naudoti kvalifikuotą e. parašą. E. parašo priemonės – valstybės tarnautojo ir valstybės darbuotojo pažymėjimas su kvalifikuotais sertifikatais.
2. Aprūpinti viešojo sektoriaus darbuotojus, dirbančius pagal darbo sutartis, e. parašo priemonėmis – įgalioti Valstybės tarnybos departamentą teikti valstybės darbuotojo pažymėjimus su kvalifikuotais sertifikatais.
3. Reglamentuoti teisinius sprendimus:
    3.1. Priimti teisės aktą dėl tapatybės nustatymo patikimumo lygių klasifikacijos;
    3.2. Patvirtinti e. dokumento pdf specifikaciją (trumpai saugomiems e. dokumentams) ir rašytiniams dokumentams nepriskiriamų e. dokumentų specifikacijas;
    3.3. Įpareigoti viešojo sektoriaus institucijas tarpusavyje keistis tik e. dokumentais;
    3.4. Reglamentuoti bendrus reikalavimus viešojo sektoriaus institucijų ir įstaigų DVS;
    3.5. Parengti technologinių sprendimų specifikacijas dėl e. dokumentų valdymo sistemų suderinimo Lietuvos mastu;
    3.6. Teisiškai reglamentuoti elektroninės informacijos saugą, detalizuojant galimus saugos pažeidimus;
    3.7. Kriminalizuoti tapatybės vagystę kaip atskirą nusikaltimą, taikant sankcijas už šią neteisėtą veiką, pasinaudojant šalių gerosios praktikos pavyzdžiais.
4. Įvykdyti organizacinius sprendimus, užtikrinančius e. dokumentų saugumą:
    4.1. Lietuvoje platinamų sertifikatų OCSP tikrinimo paslaugą;
    4.2. Laiko žymų tarnybos paslaugą viešajam sektoriui;
    4.3. Parengti efektyvų e. dokumentų valdymo sistemų suderinimo modelį, apimant teisinius, organizacinius ir technologinius sprendimus;
    4.4. Valstybiniu lygiu suderinti viešojo sektoriaus institucijų DVS, elektroninio archyvo sistemos diegimo ir atnaujinimo darbus;
    4.5. Periodiškai tikrinti ir atnaujinti e. dokumentų saugojimo programinę įrangą ir laikmenas.
5. Įgyvendinti socialines priemones, skatinančias naudotis viešosiomis e. paslaugomis:
    5.1. Plėsti socialinę rinkodarą;
    5.2. Teikti e. konsultanto paslaugas;
    5.3. Didinti e. viešųjų paslaugų pasiūlą fiziniams ir juridiniams asmenims bei teikti auščiausiu lygiu.

6. Tobulinti technologinius įrankius – patogesnė ADOC e. dokumento pasirašymo programinė įranga.
7. Parengti tinkamą skatinimo politiką dėl e. parašo naudojimo viešajame sektoriuje: skirti finansavimą e. parašo diegimui viešajame sektoriuje, kelti valstybės tarnautojų ir darbuotojų kvalifikaciją, vykdyti nuolatinius mokymus ir konsultacijas dėl e. parašo ir e. dokumento procedūrų, suformuoti palankesnę aplinką visuomenei plačiai taikyti e. parašą.
8. Plėtoti dalyvavimą STORK ir kituose ateities tarpvalstybinio e. atpažinties projektuose, supažindinant visuomenę su šiais sprendimais ir jų teikiama nauda.

Atliko
EVAmis2-01gr. stud.
O.Karpovič
2014 ... ...

LITERATŪRA

Teisės aktai

1. Europos Parlamento ir Tarybos 1999 m. gruodžio 13 d. direktyva 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos. EUR–Lex, 2000, Nr. 31999L0093
2. Komisijos komunikatas Europos parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui 2011–2015 m. Europos e. valdžios veiksmų planas IRT naudojimas siekiant pažangios, darnios ir novatoriškos valdžios SEK(2010) 1539 galutinis. EUR–Lex, 2010, Nr. 52010DC0743
3. Pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje. EUR–Lex, 2012, Nr. 52012PC0238
4. Lietuvos Respublikos Seimo 1998 m. balandžio 7 d. įstatymas Nr. VIII-687 Administracinių teisės pažeidimų kodekso papildymo $214^{(14)}$, $214^{(15)}$, $214^{(16)}$, $214^{(17)}$ straipsniais ir 224, $259^{(1)}$ straipsnių papildymo įstatymas. Valstybės žinios, 1998, Nr. 40-1065
5. Lietuvos Respublikos Seimo 1996 m. birželio 11 d. įstatymas Nr. I-1374 Asmens duomenų teisinės apsaugos įstatymas. Valstybės žinios, 2008, Nr. 22-804
6. Lietuvos Respublikos Seimo 2001 m. lapkričio 6 d. įstatymas Nr. IX-577 Asmens tapatybės kortelės įstatymas. Valstybės žinios, 2001, Nr. 97-3417
7. Lietuvos Respublikos Seimo 2000 m. rugsėjo 26 d. įstatymas Nr. VIII-1968 Baudžiamojo kodekso patvirtinimo ir įsigaliojimo įstatymas. Valstybės žinios, 2000, Nr. 89-2741
8. Lietuvos Respublikos Seimo 2010 m. birželio 18 d. įstatymas Nr. XI-917 Dokumentų ir archyvų įstatymo 1, 2, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16, 18 straipsnių, antrojo skirsnio pavadinimo pakeitimo, 9 straipsnio pripažinimo netekusiu galios ir įstatymo priedo papildymo įstatymas. Valstybės žinios, 2010, Nr. 79-4055
9. Lietuvos Respublikos Seimo 2000 m. liepos 11 d. įstatymas Nr. VIII-1822 Elektroninio parašo įstatymas. Valstybės žinios, 2000, Nr. 61-1827
10. Lietuvos Respublikos Seimo 2011 m. gruodžio 15 d. įstatymas Nr. XI-1807 Valstybės informacinių išteklių valdymo įstatymas. Valstybės žinios, 2011, Nr. 163-7739
11. Lietuvos Respublikos Vyriausybės 2011 m. sausio 17 d. nutarimas Nr. 32 Dėl elektroninio parašo priežiūros institucijos. Valstybės žinios, 2011, Nr. 8-316

12. Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimas Nr. 716 Dėl bendrųjų elektroninės informacijos saugos reikalavimų aprašo, saugos dokumentų turinio gairių aprašo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo. Valstybės žinios, 2013, Nr. 86-4310
13. Lietuvos Respublikos Vyriausybės 2010 m. gruodžio 15 d. nutarimas Nr. 1780 Dėl Lietuvos Respublikos Vyriausybės 2000 m. gruodžio 15 d. nutarimo Nr. 1458 „Dėl konkrečių valstybės rinkliavos dydžių ir šios rinkliavos mokėjimo ir grąžinimo taisyklių patvirtinimo“ pakeitimo. Valstybės žinios, 2010, Nr. 149-7640
14. Lietuvos Respublikos Vidaus reikalų ministro 2009 m. liepos 29 d. įsakymas Nr. 1V-427 Dėl Lietuvos Respublikos vidaus reikalų ministro 2003 m. rugpjūčio 29 d. įsakymo Nr. 1V-311 „Dėl tarnybinio paso išdavimo, keitimo, grąžinimo, paskelbimo negaliojančiu ir sunaikinimo tvarkos patvirtinimo“ pakeitimo. Valstybės žinios, 2009, Nr. 96-4078
15. Lietuvos Respublikos Vidaus reikalų ministro 2009 m. lapkričio 19 d. įsakymas Nr. 1V-624 „Dėl valstybės tarnautojo pažymėjimo formos ir valstybės tarnautojo pažymėjimo išdavimo taisyklių patvirtinimo“ pakeitimo. Valstybės žinios, 2009, Nr. 139-6133
16. Lietuvos archyvų departamento 2006 m. sausio 11 d. įsakymas Nr. V-12 Dėl elektroninių dokumentų valdymo taisyklių patvirtinimo. Valstybės žinios, 2006, Nr. 7-268
17. Lietuvos archyvų departamento 2008 m. spalio 9 d. įsakymas Nr. V-119 Dėl elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos reikalavimų aprašo patvirtinimo. Valstybės žinios, 2008, Nr. 118-4488
18. Lietuvos archyvų departamento 2009 m. rugsėjo 7 d. įsakymas Nr. V-60 Dėl elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos ADOC-V1.0 patvirtinimo. Valstybės žinios, 2009, Nr. 108-4574
19. Lietuvos vyriausiojo archyvaro tarnybos 2011 m. gruodžio 29 d. įsakymas Nr. V-158 Dėl Elektroninių dokumentų valdymo taisyklių patvirtinimo. Valstybės žinios, 2012, Nr. 3-104

Moksliniai straipsniai

20. Anderson W. L., Makhdoom S. Electronic Contracts and Valid Signatures // Journal of International Diversity. – Franklin: Franklin Publishing Company, 2010, Issue 4, p. 62–66. – ISSN 2152-6486

21. Astromskis P. E-vekselis // Teisės apžvalga. – Kaunas: Vytauto Didžiojo universitetas, 2011, Nr. 1(7), p. 13–32. – ISSN 2029-4239
22. Belevičius L. Duomenų perdavimo elektroninių ryšių tinklais galimybės baudžiamojoje procesinėje veikloje // Jurisprudencija: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2008, Nr. 6(108), p. 54–59. – ISSN 1392-6195
23. Blythe S. E. Bulgaria' s Electronic Document and Electronic Signature Law: Enhancing E-Commerce with Secure Cyber-Transactions // Transnational Law & Contemporary Problems. – Iowa City (USA): The University of Iowa College of Law, 2008, Vol. 17, No 2, p. 363–392. – ISSN 1058-1006
24. Civilka M. Elektroninio parašo naudojimo vidaus rinkoje problemos // Teisė: mokslo darbai. – Vilnius: Vilniaus universitetas, 2013, Nr. 87, p. 86–111. – ISSN 1392-1274
25. Česna R. Kai kurie elektroninių įrodymų panaudojimo civiliniame procese aspektai // Jurisprudencija: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2007, Nr. 10(100), p. 92–98. – ISSN 1392-6195
26. Dragu G. The electronic signature // Economic Science. – Oradea: Annals of the University of Oradea, 2009, Vol. 18, Issue 4, p. 940–942. – ISSN 1582-5450
27. Dzemydienė D., Naujikienė R. Situacijų nustatymo ir sprendimų priėmimo komponentės elektroninių dokumentų valdymo sistemoje // Informacijos mokslai: mokslo darbai. – Vilnius: Vilniaus universitetas, 2005, Nr. 34, p. 142–148. – ISSN 1392-0561
28. Garuckas R., Kaziliūnas A. Elektroninio parašo teisinis reglamentavimas ir jo įgyvendinimo ypatumai Lietuvoje // Viešoji politika ir administravimas: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2008, Nr. 24, p. 114–123. – ISSN 1648-2603
29. Graux H. Rethinking the e-signature directive: on laws, trust services, and the digital single market // Digital Evidence & Electronic Signature Law Review. – London: Institute of Advanced Legal Studies, 2011, Vol. 8, p. 9–24. – ISSN 1756-4611
30. Ivanovas E. Biometriniai požymiai asmens atpažinimo sistemose // Mokslas – Lietuvos ateitis = Science – future of Lithuania: Elektronika ir elektrotechnika = Electronics and electrical engineering. – Vilnius: Technika, 2010, T. 2, Nr. 1, p. 23–26. – ISSN 2029-2341
31. Kalpokas V., Marcinauskaitė R. Tapatybės vagystė elektroninėje erdvėje: technologiniai aspektai ir baudžiamasis teisinis vertinimas // Teisės problemos. – Vilnius: Lietuvos teisės institutas, 2012, Nr. 3 (77), p. 30–52. – ISSN 1392-1592

32. Kontrimavičienė D. Prieiga prie dokumentų valstybės archyvuose: teoriniai aspektai // Knygotyra. – Vilnius: Vilniaus universitetas, 2012, Nr. 58, p. 136–159. – ISSN 0204-2061
33. Krawczyk P. When the EU qualified electronic signature becomes an information services preventer // Digital Evidence & Electronic Signature Law Review. – London: Institute of Advanced Legal Studies 2010, Vol. 7, p. 7–18. – ISSN 1756-4611
34. Libby R., Blashfield R. K. Performance of a composite as a function of a number of judges // Organizational Behavior and Human Performance, 1978, Vol. 21, Issue 2, p. 121–129. – ISSN 0030-5073
35. Limba T. Elektroninės valdžios paslaugų pakopų modeliai: jų lyginamoji analizė // Informacijos mokslai: mokslo darbai. – Vilnius: Vilniaus universitetas, 2009, Nr. 50, p. 30–39. – ISSN 1392-0561
36. Limba T., Novikovienė L. Elektroninio parašo ir laiko žymos įtaka elektroninių sutarčių apsaugai // Socialinės technologijos = Social technologies: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2012, Nr. 2(2), p. 483–501. – ISSN 2029-7564
37. Musteikis Š. ir kt. Elektroninis parašas ir jo pritaikymas Lietuvoje // 11-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis“ teminės konferencijos INFORMATIKA (2008 m. balandžio 9–11 d.) straipsnių rinkinys. – Vilnius: Technika, 2008, p. 351–357. – ISBN 978-9955-28-302-7
38. Ožalienė A., Šaparnienė D. Elektroninių dokumentų valdymas viešajame sektoriuje: plėtros galimybių analizė // Ekonomika ir vadyba: aktualijos ir perspektyvos. – Šiauliai: Šiaulių universitetas, 2008, Nr. 3(12), p. 199–205. – ISSN 1648-9098
39. Petraitytė I. Asmens duomenų apsauga ir teisė į privatų gyvenimą // Teisė: mokslo darbai. – Vilnius: Vilniaus universitetas, 2011, Nr. 80, p. 163–174. – ISSN 1392-1274
40. Petrauskas R., Vaina P. Development of electronic identification measures in the public sector in Lithuania: reality, demand and the future // Socialinės technologijos = Social technologies: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2012, Nr. 2(2), p. 319–334. – ISSN 2029-7564
41. Štitilis D., Klišauskas V. Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai // Socialinės technologijos = Social technologies: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2012, Nr. 2(2), p. 441–455. – ISSN 2029-7564

42. Štitilis D., Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje // Informacijos mokslai: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2009, Nr. 87, p. 240–247. – ISSN 1392-0561
43. Štitilis D. ir kt. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai // Socialinių mokslų studijos = Societal studies: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2011, Nr. 3(1), p. 153–171. – ISSN 2029-2244
44. Štitilis D. ir kt. Teisinė aplinka siekiant išvengti tapatybės vagystės elektroninėje erdvėje: JAV ir Lietuvos teisės aktų lyginamoji analizė // Socialinės technologijos = Social technologies: mokslo darbai. – Vilnius: Mykolo Romerio universitetas, 2011, Nr. 1(1), p. 61–80. – ISSN 2029-7564
45. Wang S.Y.K., Huang W. The Evolutional View of the Types of Identity Thefts and Online Frauds in the Era of the Internet // Internet Journal of Criminology, 2011, p. 1–21. – ISSN 2045-6743

Mokomieji leidiniai

46. Davidavičienė V. ir kt. Elektroninis verslas: vadovėlis. – Vilnius: Technika, 2009. – 468 p. – ISBN 978-9955-28-513-7
47. Kardelis K. Mokslinių tyrimų metodologija ir metodai: vadovėlis. – Šiauliai: Lucilijus, 2005. – 398 p. – ISBN 9955-655-35-6
48. Kiškis M. ir kt. Teisės informatika ir informatikos teisė: vadovėlis. – Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006. – 268 p. – ISBN 9955-19-048-5
49. Rudzkienė V. Socialinė statistika: vadovėlis. – Vilnius: Mykolo Romerio universiteto Leidybos centras, 2005. – 260 p. – ISBN 9955-19-002-7

Monografijos ir magistro baigiamieji darbai

50. Augustinatis A. ir kt. Lietuvos e. valdžios gairės: ateities įžvalgų tyrimas: kolektyvinė monografija. – Vilnius: Mykolo Romerio universiteto Leidybos centras, 2009. – 352 p. – ISBN 978-9955-19-160-5
51. Klangauskas A. Identity Theft in Electronic Environment: Does the current approach to the penal legislation of European Union and Lithuania adequate for combating cybercrime?: master thesis. – Oslo: University of Oslo, 2012. – 63 p. – URL: https://www.duo.uio.no/bitstream/handle/10852/34432/174180.pdf?sequence=1

52. Mašidlauskas A. Elektroninis parašas: teisinis reglamentavimas ir praktiniai įgyvendinimo aspektai Lietuvoje: magistro darbas: 06H – Komunikacija ir informacija. – Vilnius: Vilniaus universitetas, 2008. – 75 p. – URL: http://vddb.laba.lt/fedora/get/LT-eLABa-0001:E.02~2008~D_20090908_201746-12407/DS.005.1.01.ETD
53. Štitilis D. ir kt. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai: kolektyvinė mokslo monografija. – Vilnius: Mykolo Romerio universitetas, 2011. – 508 p. – ISBN 978-9955-19-374-6

Ataskaitos

54. Robinson N. et al. Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report. – United Kingdom: RAND Europe, 2011, 618 p. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf [žiūrėta 2013 12 09]
55. Direktyvos 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos veikimo ataskaita. – Briuselis: Europos Bendrijų Komisija, 2006. http://eurlex.europa.eu/Notice.do?mode=dbl&lang=lt&ihmlang=lt&lng1=lt,fi&lng2=cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,sk,sl,sv,&val=423632:cs [žiūrėta 2013 12 05]
56. Europos veiklos apžvalga. Bendroji Europolo veiklos ataskaita // Europos policijos biuras. – Liuksemburgas: Europos Sąjungos leidinių biuras, 2011, 60 p. – ISSN 1681-1550. – URL: https://www.europol.europa.eu/sites/default/files/publications/lt_europolreview.pdf
57. Lietuvos informacinės visuomenės plėtros tendencijų ir prioritetų 2014–2020 metais vertinimas: svarbiausi rezultatai ir įžvalgos. – Vilnius: IVPK, 2013, 44 p. – ISBN 978-609-95343-2-9
58. Lietuvos informacinės visuomenės plėtros tendencijų ir prioritetų 2014–2020 metais vertinimas. Vertinimo ataskaita. – Vilnius: IVPK, VPVI, 2012, 327 p. http://www.ivpk.lt/uploads/Tendencijos%20ir%20prioritetai/atnaujinti/Informacines%20visuomenes%20vertinimas%20-%20%20tekstas%202012-04-26%20VPVI.pdf [žiūrėta 2014 01 02]
59. Lietuvos Respublikos elektroninio parašo įstatymo įgyvendinimo 2010 metų ataskaita. – Vilnius: Lietuvos Respublikos ryšių reguliavimo tarnyba, 14 p. http://www.google.lt/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCcQFjAA&url=http%3A%2F%2Fwww.rrt.lt%2Fdownload%2F14499%2F2010%2520epi%2520ataskaita.doc&ei=09zFUvnNPKKzywPHrYKYCQ&usg=AFQjCNHEHPQQ_BYcRcKII0IvfbetbRQ5BQ [žiūrėta 2013 12 17]

60. Lietuvos Respublikos elektroninio parašo įstatymo įgyvendinimo 2011 metų ataskaita. – Vilnius: Lietuvos Respublikos ryšių reguliavimo tarnyba, 2012, 27 p. http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroninio-paraso-istatymo-1b73.html [žiūrėta 2013 12 05]
61. Lietuvos Respublikos elektroninio parašo įstatymo įgyvendinimo 2012 metų ataskaita. – Vilnius: Lietuvos Respublikos ryšių reguliavimo tarnyba, 2013, 15 p. http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/elektroninio-paraso-istatymo-1b73.html [žiūrėta 2013 12 05]
62. Lietuvos Respublikos ryšių reguliavimo tarnybos 2012 metų veiklos ataskaita. – Vilnius: Lietuvos Respublikos ryšių reguliavimo tarnyba, 2013, 117 p. http://www.rrt.lt/lt/apzvalgos-ir-ataskaitos/veiklos-ataskaitos/2011-metu-veiklos-ataskaita.html [žiūrėta 2013 12 21]
63. „Reglamento dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje poveikis Lietuvos teisinei bazei, valstybės informacinėms sistemoms ir registrams, valstybės bei verslo sprendimams, priemonėms ir paslaugoms, jų kūrėjams, teikėjams ir vartotojams“ tyrimas. – Vilnius: UAB „Peritus sprendimai“, 2013, 281 p. http://www.lrv.lt/bylos/LESSED%20projektas/Dokumentai/galutine_ataskaita_galutine%20atsizvelgta%20i%202013-12-09%20sumin%20susitikimo%20komentarus.pdf [žiūrėta 2013 12 21]
64. Scoping Paper on Online Identity Theft. OECD, Ministerial Background Report, 2008, 69 p. http://www.oecd.org/sti/40644196.pdf [žiūrėta 2013 12 18]
65. Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft. European Commission, 2012, 177 p. http://ec.europa.eu/dgs/home-affairs/elibrary/documents/policies/organized-crime-and-human trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf [žiūrėta 2013 12 05]
66. 2010 m. gruodžio 31 d. valstybinio audito ataskaita valstybės tarnautojų pažymėjimų panaudojimas elektroninėje erdvėje. – Vilnius: LR valstybės kontrolė, 2010, 61 p. http://www.google.lt/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CDEQFjAB&url=http%3A%2F%2Fwww.vkontrole.lt%2Ffailas.aspx%3Fid%3D2286&ei=J6isUt2lAqb9ygP7gYHYAQ&usg=AFQjCNGGh4O8gayIU1GDe3SG88Oa478DHg [žiūrėta 2013 12 05]
67. Viešasis administravimas Lietuvoje: 2012 metų apžvalga. – Vilnius: Lietuvos Respublikos vidaus reikalų ministerija, 2012, 82 p. http://www.google.lt/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCcQFjAA&url=http%3A%2F%2Fvakokybe.vrm.lt%2Fget.php%3Ff.660&ei=pzvMUqXpF6HpywPgyYCgCA&usg=AFQjCNERGiFrTM4vJ-ie5GMZqMg8fd3gHQ [žiūrėta 2014 01 02]

Knygos

68. Higgins G. Cybercrime: An Introduction to an Emerging Phenomenon. – New York: McGraw-Hill Publishing, 2012. – 192 p. – ISBN-10: 0073401552

Publikacijos

69. Petravičiūtė I. Elektroniniai dokumentai organizacijos veikloje. http://www.archyvai.lt/lt/profesine-informacija_52/publikacijos.html [žiūrėta 2013 12 10]
70. Jodinskė A. Elektroninio dokumento metaduomenys // Biuro administravimas, 2013, Nr. 4, p. 25–28
71. Jodinskė A. Elektroninis dokumentas: įstaigos veiklos įrodymas // Biuro administravimas, 2013, Nr. 3, p. 19–22
72. Jodinskė A. Elektroninių dokumentų valdymo esminiai aspektai // Biuro administravimas, 2013, Nr. 7–8, p. 28–34
73. Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems. International Council on Archives, 2008, 69 p. – ISBN 978-2-918004-01-1
74. ISO 15489-1. Information and documentation – Records management – Part1. International Organization for Standartization, 2001, 26 p. http://www.clio.uni-sofia.bg/itarch/iso_15489.pdf [žiūrėta 2013 12 21]

Elektroniniai šaltiniai

75. Acoca B. Online identity theft. OECD Observer No. 268 (2008). http://www.oecdobserver.org/news/archivestory.php/aid/2662/Online_identity_theft.html [žiūrėta 2013 12 28]
76. Gercke M. Internet-related identity theft. Project on cybercrime. Germany, 2007, 32 p. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/documents/reports-presentations/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf [žiūrėta 2013 12 15]
77. Laurinaitis M. Asmens tapatybė elektroninėje erdvėje. – Vilnius: Mykolo Romerio universitetas, 2012. http://www.vartotojai.lt/get.php?f.1828 [žiūrėta 2013 12 12]
78. Lukšaitė D., Jodinskė A. Elektroninių dokumentų valdymas viešajame sektoriuje. – Vilnius: Lietuvos vyriausiojo archyvaro tarnyba, 2011-03-01.

http://www.google.lt/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCwQFjAA&url=http%3A%2F%2Fw.verslovartai.lt%2Fdownloads%2Fdokumentai%2Fseminaras1%2Fel_dok_vald_arch.ppt&ei=Tu7aUu7vHLPdygPrr4DICQ&usg=AFQjCNH2UScSfIqe7fh-FtjgWMw8do4RIw&sig2=sy_FRgcy0ccNRZcqGy0-Ew [žiūrėta 2013 12 11]

79. Navakauskas D. Biometrija. http://vkd.vgtu.lt/ziniasklaidai/pranesimai-ziniasklaidai/vgtu-kuria-naujausias-patikimas-ir-patogias-vartotojui-duomenu-apsaugo/ [žiūrėta 2013 12 10]
80. Šliavas G. Valstybės informacinės sistemos ir asmens duomenys „debesyje“ – ką apie saugumą kalba teisės aktai? http://xn--debesis-9eb.lt/valstybes-informacines-sistemos-ir-asmens-duomenys-debesyje-ka-apie-sauga-kalba-teises-aktai [žiūrėta 2013 12 17]
81. Štitilis D. ir kt. Pasisavino jūsų asmens duomenis: kuo tai gresia jums? http://www.elektronika.lt/straipsniai/kompiuterija/32006/pasisavino-jusu-asmens-duomenis-kuo-tai-gresia-jums/ [žiūrėta 2013 12 20]
82. Zilnys A. Elektroninių dokumentų reguliavimo srities teisės aktai. – Vilnius: Lietuvos vyriausiojo archyvaro tarnyba, 2013-04-18. http://www.archyvai.lt/lt/teisine-informacija_51/teisesaktai/aktualiosredakcijos.html [žiūrėta 2013 12 10]
83. Žukauskienė R. Kokybiniai ir kiekybiniai metodai. http://www.google.lt/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCcQFjAA&url=http%3A%2F%2Frzukausk.home.mruni.eu%2Fwp-content%2Fuploads%2Fkokybiniai-ir-kiekybiniai-tyrimai1.ppt&ei=IuzwUrSwB8Wv4ASW-4DACg&usg=AFQjCNF_UcrUmfmBwFbKjZeh6bRcih0Ugw [žiūrėta 2014 01 30]
84. Assurance levels for authentication for electronic government services. The Standardisation Forum, 2012, 17 p. http://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_EN_WEB.pdf [žiūrėta 2014 01 01]
85. Asmens kodo įrašymas kvalifikuotose sertifikatuose. – Vilnius: SSC, 2013-10-03. https://www.asmenskodas.lt/oficialus-dokumentai/4.htm [žiūrėta 2014 01 01]
86. Elektroninės informacijos sauga. – Vilnius: Lietuvos Respublikos vidaus reikalų ministerija, 2013. http://www.vrm.lt/e-sauga [žiūrėta 2013 12 15]
87. Elektroninė draudėjų aptarnavimo sistema EDAS. – Vilnius: Valstybinio socialinio draudimo fondo valdyba, 2012. http://www.sodra.lt/index.php?cid=2696 [žiūrėta 2013 12 19]

88. „E. pristatymas“ – alternatyva susirašinėjimui paštu. – Vilnius: IVPK, 2013-07-31. http://www.ivpk.lt/news/1882/21/E-pristatymas-alternatyva-susirasinejimui-pastu [žiūrėta 2013 12 19]
89. E-pristatymo sistemos naudotojai. – Vilnius: AB „Lietuvos paštas“, 2013-12-13. https://epristatymas.post.lt/naujienos/-/news/show/26798 [žiūrėta 2013 12 21]
90. 2011–2012 m. metinių pajamų deklaracijų statistika. – Vilnius: Valstybinė mokesčių inspekcija, 2013. http://www.vmi.lt/cms/deklaravimu-statistika [žiūrėta 2013 12 19]
91. Komisijos komunikatas Europos parlamentui, tarybai ir Europos regionų komitetui. – Briuselis: Europos Bendrijų Komisija, 2007, 11 p. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:LT:PDF [žiūrėta 2013 12 19]
92. Naujos kartos Lietuvos Respublikos asmens dokumentų išdavimo bendra statistika. – Vilnius: Asmens dokumentų išrašymo centras prie VRM, 2013-12-01. http://www.dokumentai.lt/viewpage.php?page_id=41 [žiūrėta 2013 12 14]
93. Nuo šiol visus oficialius dokumentus galima siųsti ir gauti internetu. – Vilnius: AB „Lietuvos paštas“, 2013-06-18. http://www.post.lt/lt/apie-mus/naujienos/item/pasto-naujienos/nuo-siol-visus-oficialius-dokumentus-galima-siusti-ir-gauti-internetu [žiūrėta 2013 12 21]
94. Pradėjo veikti elektroninė pašto korespondencijos pristatymo sistema // Sekundė, 2013, birželio 18 d. http://www.sekunde.lt/pinigai/pradejo-veikti-elektronine-pasto-korespondencijos-pristatymo-sistema/ [žiūrėta 2013 12 21]
95. Projektas „Elektroninių paslaugų mokesčių mokėtojams vystymas plėtojant mokesčių mokėtojo registro, apskaitos ir tarptautinių mainų pridėtinės vertės mokesčio srityje informacines sistemas“. – Vilnius: Valstybinė mokesčių inspekcija, 2013, 3 p. https://www.vmi.lt/cms/documents/10162/12287/Proj007_2013-10-03.pdf/f8a8cde2-d7b1-4827-8c20-35146e0b5acc [žiūrėta 2013 12 21]
96. Saugus tarpvalstybinis tapatybės nustatymas. – Vilnius: VĮ „Infostruktūra“, 2011. https://www.eid-stork.eu/pilots/pilot1_LT_more.htm [žiūrėta 2014 01 02]
97. Skaitmeninio sertifikavimo centro skaitmeniniai sertifikatai. – Vilnius: SSC. http://www.ssc.lt/?name=cert&act=main&L=lt&ct=personal&ssc_m=3,24&method=buy [žiūrėta 2013 12 14]
98. Valstybinės duomenų apsaugos inspekcijos veiklos sritys. – Vilnius: Valstybinė duomenų apsaugos inspekcija. https://www.ada.lt/go.php/lit/Veiklos-sritys/399 [žiūrėta 2013 12 14]

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Karpovič O. Elektroninės atpažinties priemonės viešajame sektoriuje / Elektroninio viešojo administravimo magistro baigiamasis darbas. Vadovas lekt. dr. R. Naujikienė. – Vilnius: Mykolo Romerio universitetas, Socialinių technologijų fakultetas, Skaitmeninių technologijų institutas, 2014. – 106 p.

ANOTACIJA

Aktualiausia problema modernizuojant viešojo sektoriaus veiklą valstybiniu ir ES lygiu – nepakankamai sparti e. parašo plėtra Lietuvos viešajame sektoriuje. Mokslinio tyrimo objektas – e. parašo taikymas Lietuvos viešajame sektoriuje esama padėtis. Tyrimo dalykas – priemonės ir būdai kaip organizuoti platesniu mastu e. parašo taikymo modelį, numatantį e. parašo plėtrą.

Šiame darbe nustatomos e. parašo sampratos ir rūšių pagrindinės charakteristikos, įvertinamas e. parašo saugumas elektroninėje erdvėje, apžvelgiami e. dokumentų ypatumai, pateikiami efektyvaus e. parašo taikymo pavyzdžiai viešojo ir privataus sektoriaus veikloje, įvertinamos prioritetinės veiklos kryptys dėl šio parašo taikymo ES lygiu. Elektroninių atpažinties priemonių sistema yra nagrinėjama kaip neatsiejama nacionalinės inovacijų sistemos dalis, veikianti kaip jungiamoji grandis ES politiniuose, ekonominiuose ir socialiniuose-kultūriniuose kontekstuose. Suformuotas veiksmingas e. parašo taikymo viešojo sektoriaus veikloje modelis, apimantis naujus, kituose mokslo darbuose dar nenagrinėtus sprendimus. Susisteminti duomenys leido nustatyti skatinamuosius veiksnius, naujų prioritetinių kliūčių eiliškumą ir pateikti kompetentingus sprendimus, sparčiai e. parašo plėtrai užtikrinti valstybiniu lygiu, bei įvertinti taikymo mastą ES lygiu.

Pagrindiniai žodžiai: elektroninis parašas, elektroninis dokumentas, duomenų saugumas, viešosios e. paslaugos.

Karpovič O. Electronic identification measures in the public sector / Master's thesis in electronic public administration. Supervisor lect. Dr. R. Naujikienė. – Vilnius: Mykolas Romeris University, Faculty of Social Technologies, Institute of Digital Technologies, 2014. – 106 p.

ANOTATION

The most pressing issue in modernizing public sector activities on the national and the EU levels – the lack of rapid development of e-signature in Lithuanian public sector. Research object – current situation of the application of e-signature in Lithuanian public sector. Research subject matter – means and methods to expand the organization of an e-signature application model designed for the development of e-signature.

This paper sets out key characteristics of the e-signature concept and types, evaluates the e-signature security in the cyberspace, provides an overview of the peculiarities of e-documents, presents examples for effective application of e-signature in private and public sector activities, and evaluates priority directions of activity in respect of the application of e-signature on the EU level. A system of electronic identification measures is analyses as an integral part to the national innovation system, acting as a bridge between ES political, economic and social-cultural contexts. An effective model for the application of e-signature in public sector activities has been designed, which includes new, previously unstudied solutions. Systematized data allowed to identify motivators and the order of new priority challenges, provide competent solutions for ensuring rapid development of e-signature on the national level, and evaluate the scope of e-signature on the EU level.

Keywords: electronic signature, electronic document, document security, public e-services.

SANTRAUKA LIETUVIŲ IR ANGLŲ KALBOMIS

Karpovič O. Elektroninės atpažinties priemonės viešajame sektoriuje / Elektroninio viešojo administravimo magistro baigiamasis darbas. Vadovas lekt. dr. R. Naujikienė. – Vilnius: Mykolo Romerio universitetas, Socialinių technologijų fakultetas, Skaitmeninių technologijų institutas, 2014. – 106 p.

SANTRAUKA

Informacinių technologijų ir nuotolinio ryšio priemonių plėtra verčia vykdyti pokyčius viešojo sektoriaus darbo veikloje bei pertvarkyti valdymo procesus. Technologijų inovacijos atveria naujus bendravimo su visuomene ir kitais subjektais būdus bei užtikrina didesnį skaidrumą. Siekiant užtikrinti efektyvią viešojo administravimo veiklą, reikia įgyvendinti atitinkamus sprendimus dėl e. dokumentų valdymo ir mainų bei vykdyti e. parašo plėtrą.

Darbo objektas ir dalykas – e. parašo naudojimo viešojo sektoriaus veikloje probleminiai aspektai ir jo taikymo kliūtys. Darbo tikslas – nustatyti elektroninio parašo taikymo kliūtis ir skatinamuosius veiksnius viešajame sektoriuje.

Darbą sudaro keturios pagrindinės dalys. Pirmoje dalyje pateikiama mokslinių šaltinių apžvalga dėl e. dokumento sampratos, savybių ir esminiai valdymo skirtumai. Antroje dalyje vykdoma mokslinių šaltinių analizė e. parašo sampratos tema, įvertinamos e. parašo rūšys (jų privalumai ir trūkumai) bei grėsmės e. erdvėje. Trečioje dalyje pateikiami efektyvaus e. parašo taikymo pavyzdžiai viešojo ir privataus sektoriaus veikloje, įvertinamos prioritetinės veiklos kryptys dėl e. parašo taikymo ES lygiu. Ketvirtoje dalyje pateikiami e. parašo naudojimo viešojo sektoriaus institucijose tyrimo rezultatai. Apibendrinus atlikto tyrimo rezultatus, nustatyta, kad e. parašo naudojimo plėtrą stabdo nesuderintos e. dokumentų valdymo sistemos Lietuvos mastu ir šių procesų valdymo kliūtys, motyvacijos stoka, finansinės paramos trūkumas, gebėjimų kliūtys ir kvalifikacijos stoka, mokymų ir konsultacijų dėl e. parašo ir e. dokumento procedūrų trūkumas. E. parašo spartesnei plėtrai kliudo nepakankama vadovaujančių institucijų skatinimo politika ir kvalifikacijos, motyvacijos bei informacijos trūkumas. Susisteminti duomenys leido nustatyti skatinamuosius veiksnius, naujų prioritetinių kliūčių eiliškumą ir pateikti kompetentingus sprendimus, sparčiai e. parašo plėtrai užtikrinti valstybiniu lygiu, bei įvertinti taikymo mastą ES lygiu.

E. parašo plėtra užtikrintų administracinės naštos mažinimą bei efektyvesnius ir saugius keitimosi dokumentais būdus visuomenei, verslui ir viešojo sektoriaus darbuotojams.

Karpovič O. Electronic identification measures in the public sector / Master's thesis in electronic public administration. Supervisor lect. Dr. R. Naujikienė. – Vilnius: Mykolas Romeris University, Faculty of Social Technologies, Institute of Digital Technologies, 2014. – 106 p.

SUMMARY

The development of information technologies and means of distance communication forces us to change public sector activities and rearrange management processes. Technology innovations open new ways of communicating with the public and other subjects, and ensures improved transparency. In order to ensure effective public administration activities, relevant solutions in respect of e-document management and exchange, and development of e-signature need to be implemented.

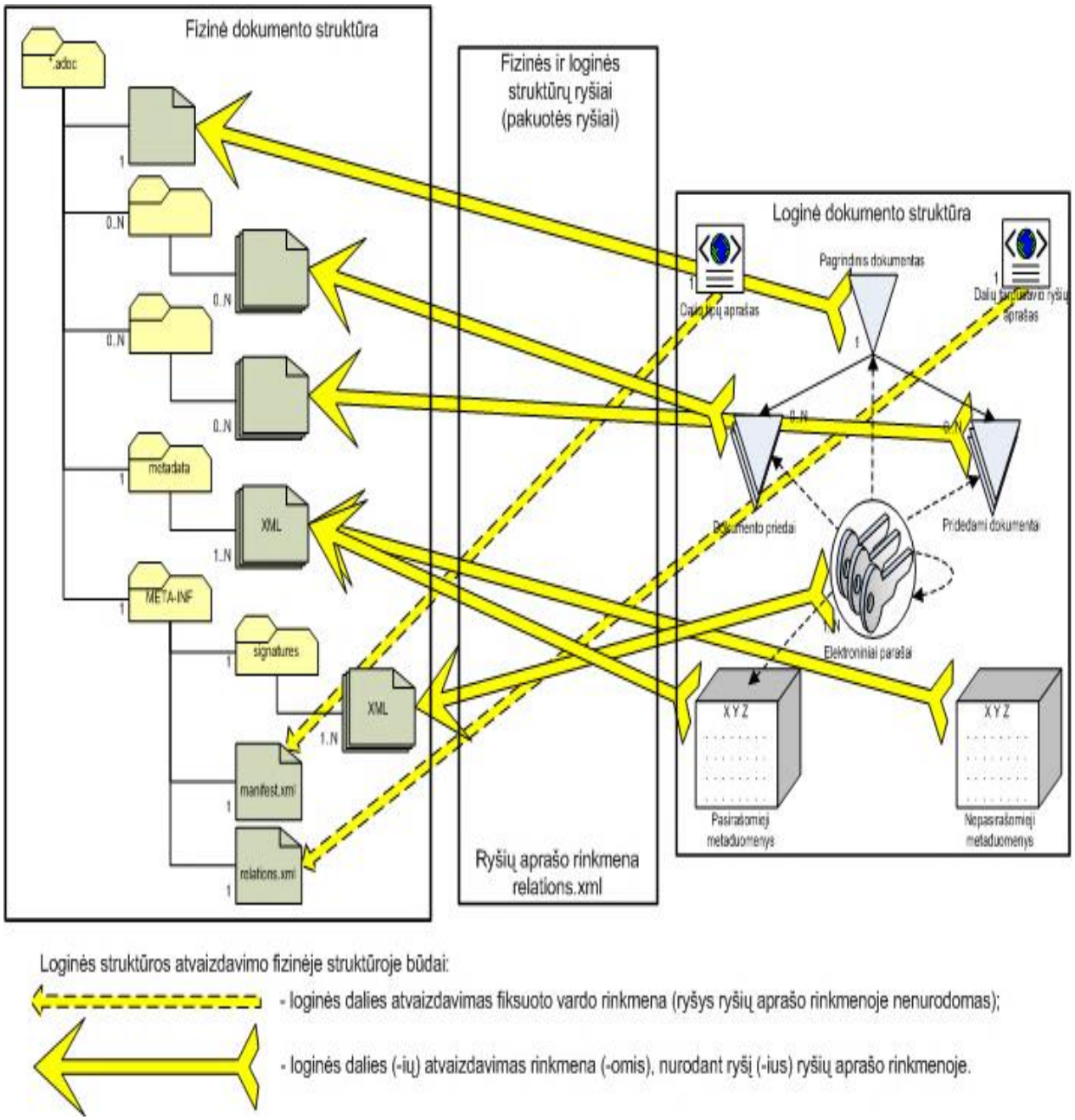
Object and subject matter of the paper – problematic aspects of the use of e-signature in public sector activities and challenges for its application. Purpose of the paper – to identify challenges and motivators for the application of e-signature in the public sector.

The paper consists of four key sections. The first one provides a literature review in terms of e-document concept and characteristics, and presents essential differences in management. The second section contains an analysis of scientific sources on the concept of e-signature and assesses e-signature types (their pros and cons) and threats in the cyberspace. The third section presents examples for effective application of e-signature in public and private sector activities, and evaluates priority directions of activity in respect of the application of e-signature on the EU level. The fourth section provides the results of the study on the use of e-signature in public sector institutions. In summarizing the results of the study, it was found that the development of the use of e-signature is inhibited by uncoordinated e-document management systems on the nationwide level and obstacles to the management of these processes, the lack of motivation, the lack of financial support, capacity challenges and the lack of qualifications, and insufficient amount of trainings and consultations regarding e-signature and e-document procedures. More rapid development of e-signature is hindered by an insufficient promotion policy and qualifications of managing authorities, the lack of motivation and information. Systematized data allowed to identify motivators and the order of new priority challenges, provide competent solutions for ensuring rapid development of e-signature on the national level, and evaluate the scope of e-signature on the EU level.

The development of e-signature would allow to reduce the administrative burden and ensure more effective and secure document exchange methods for the public, business and public sector employees.

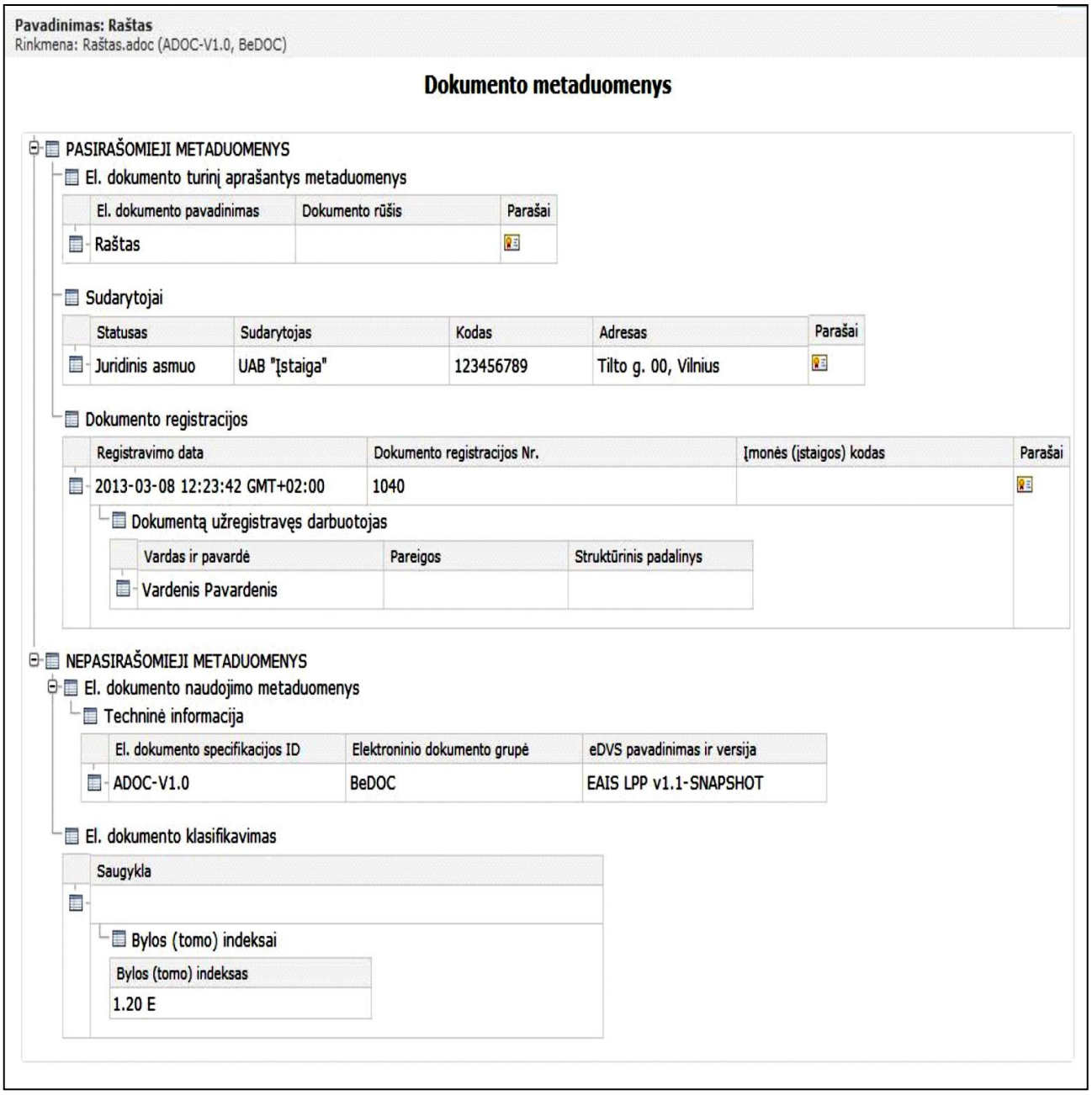
PRIEDAI

1 PRIEDAS. ELEKTRONINIU PARAŠU PASIRAŠYTO ELEKTRONINIO DOKUMENTO SPECIFIKACIJOS ADOC-V1.0 STRUKTŪRA



Šaltinis: Valstybės žinios, 2009, Nr. 108-4574.

2 PRIEDAS. UŽREGISTRUOTO ELEKTRONINIO DOKUMENTO, ATITINKANČIO ELEKTRONINIU PARAŠU PASIRAŠYTO ELEKTRONINIO DOKUMENTO SPECIFIKACIJĄ ADOC-V1.0, METADUOMENYS



Pavadinimas: Raštas
Rinkmena: Raštas.adoc (ADOC-V1.0, BeDOC)

Dokumento metaduomenys

PASIRAŠOMIEJI METADUOMENYS

El. dokumento turinį aprašantys metaduomenys

El. dokumento pavadinimas	Dokumento rūšis	Parašai
Raštas		

Sudarytojai

Statusas	Sudarytojas	Kodas	Adresas	Parašai
Juridinis asmuo	UAB "Įstaiga"	123456789	Tilto g. 00, Vilnius	

Dokumento registracijos

Registravimo data	Dokumento registracijos Nr.	Įmonės (įstaigos) kodas	Parašai
2013-03-08 12:23:42 GMT+02:00	1040		

Dokumentą užregistravęs darbuotojas

Vardas ir pavardė	Pareigos	Struktūrinis padalinys
Vardenis Pavardenis		

NEPASIRAŠOMIEJI METADUOMENYS

El. dokumento naudojimo metaduomenys

Techninė informacija

El. dokumento specifikacijos ID	Elektroninio dokumento grupė	eDVS pavadinimas ir versija
ADOC-V1.0	BeDOC	EAIS LPP v1.1-SNAPSHOT

El. dokumento klasifikavimas

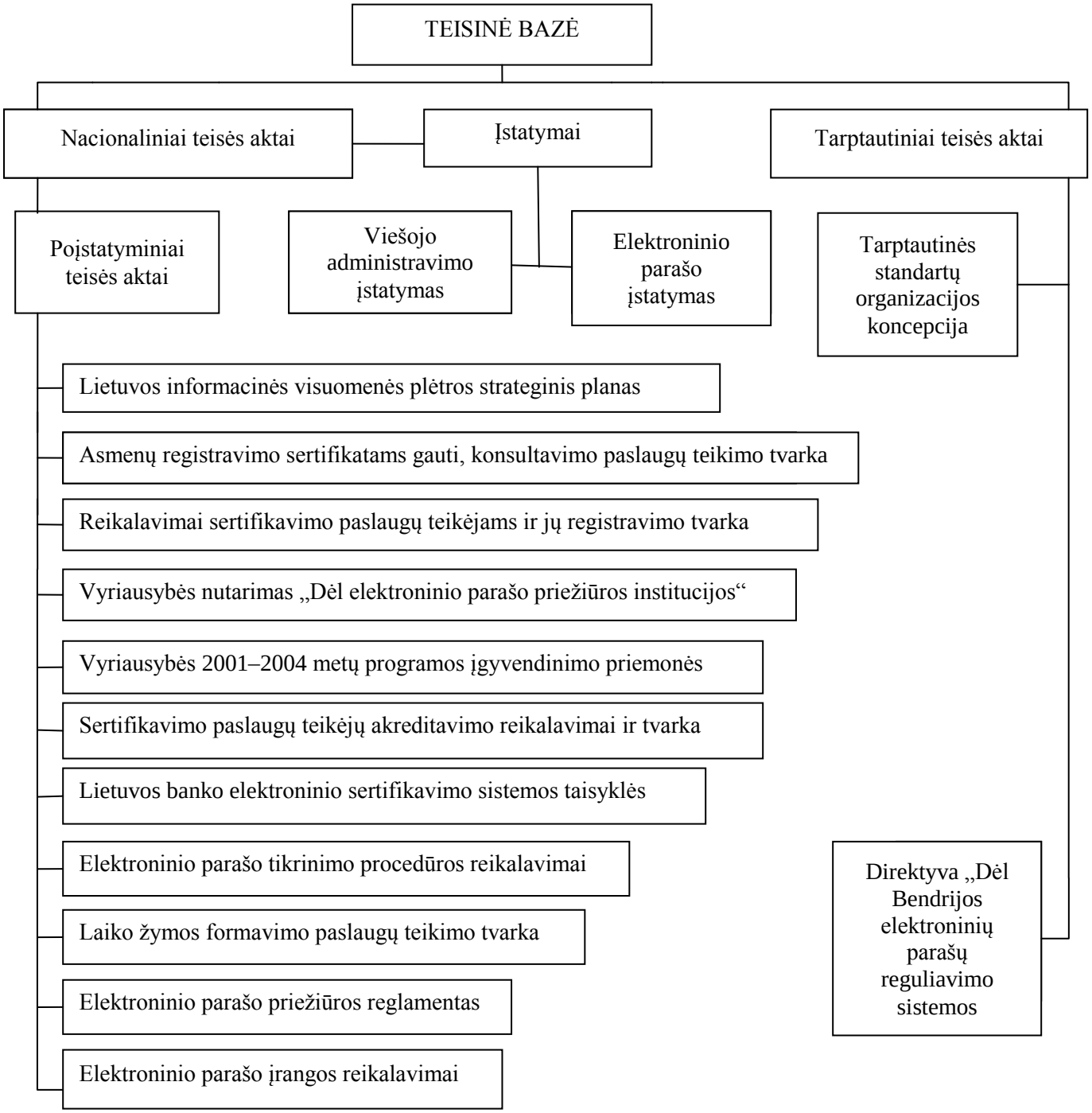
Saugykla

Bylos (tomo) indeksai

Bylos (tomo) indeksas
1.20 E

Šaltinis: Jodinskė, 2013, p. 26.

3 PRIEDAS. ELEKTRONINIO PARAŠO TEISINIS REGLAMENTAVIMAS



Šaltinis: Garuckas, Kaziliūnas, 2008, p. 117.

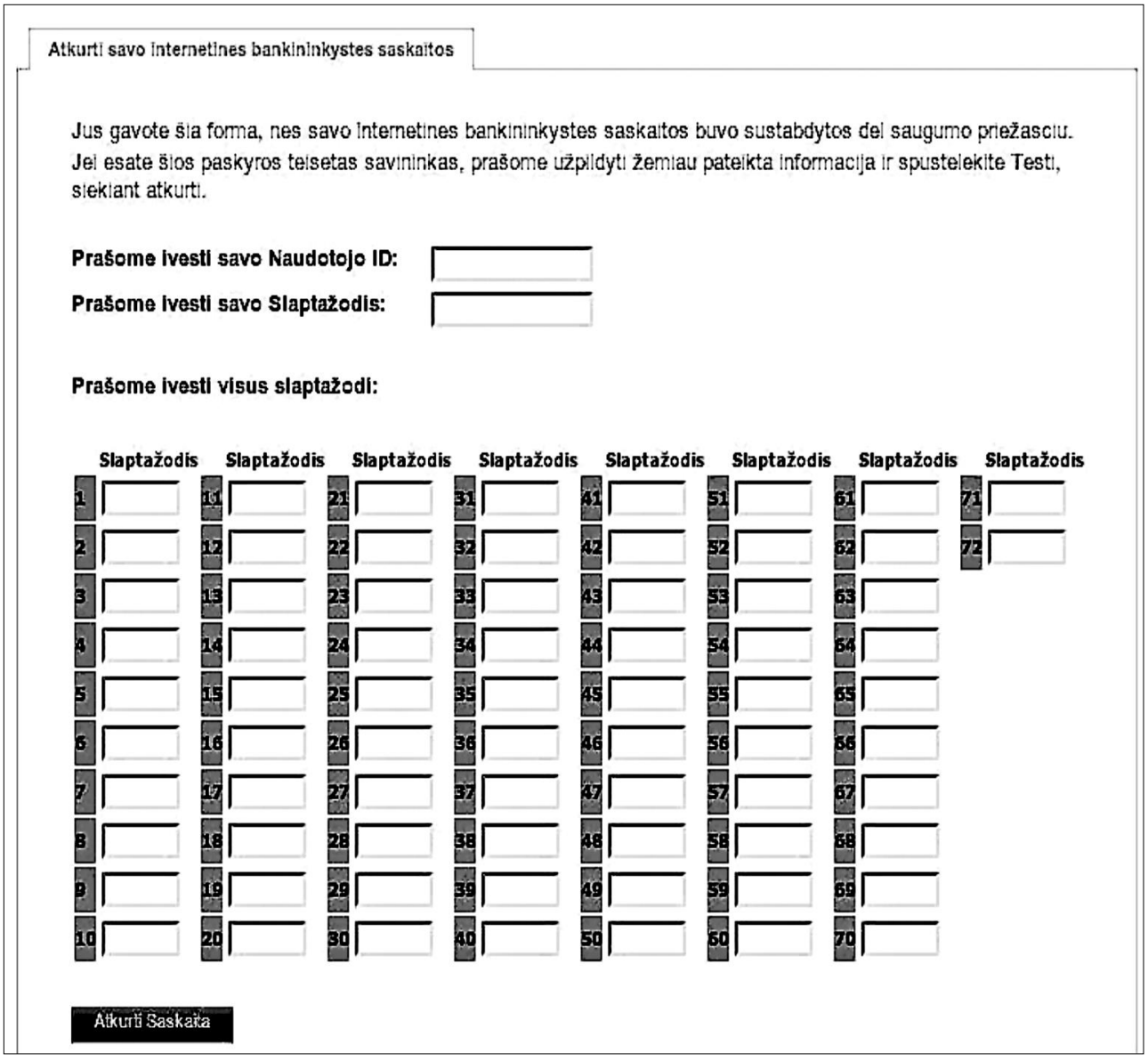
4 PRIEDAS. BIOMETRINIŲ BRUOŽŲ PASIŽYMĖJIMO SAVYBĖMIS SUVESTINĖ

Žmogaus biometrinis bruožas	**Bruožo savybės** (Jain et al. 2004)							**Bendras bruožo pažymėjimas savybėmis**	**Publikacijų skaičius**
	Universalus	**Skiriantis**	**Nuolatinis**	**Išmatuojamas**	**Panaudojamas**	**Priimtinas**	**Nesuklastojamas**		
Fiziologiniai biometriniai bruožai									
Akies rainelė	+++	+++	+++	++	+++	+	+++	18	433
Veido termograma	+++	+++	+	+++	++	+++	+++	18	46
Delno antspaudas	++	+++	+++	++	+++	+++	++	17	137
DNR	+++	+++	+++	+	+++	+	+++	17	13
Piršto antspaudas	++	+++	+++	++	+++	++	++	17	680
Akies tinklainė	+++	+++	++	+	+++	+	+++	16	18
Ausis	++	++	+++	++	++	+++	++	16	76
Delno geometrija	++	++	++	+++	++	++	++	15	120
Delno venos	++	++	++	++	++	++	+++	15	9
Veidas	+++	+	++	+++	+	+++	+	14	1310
Elgsenos biometriniai bruožai									
Eisena	++	+	+	+++	+	+++	++	13	216
Balsas	++	+	+	++	+	+++	+	11	252
Parašas	+	+	+	+++	+	+++	+	11	299
Teksto rinkimas	+	+	+	++	+	++	++	10	46

Ženklai „+”, „++” ir „+++” rodo požymio savybės išreikštumą: atitinkamai silpną, vidutinišką ir smarkų.

Šaltinis: adaptuota pagal Ivanovas, 2010, p. 24.

5 PRIEDAS. SUKLASTOTO INTERNETINĖS BANKININKYSTĖS TINKLALAPIO, REIKALAUJANČIO ĮVESTI PRISIJUNGIMO SLAPTAŽODŽIUS, FRAGMENTAS



Šaltinis: Kalpokas, Marcinauskaitė, 2012, p. 34.

6 PRIEDAS. EKSPERTINIO TYRIMO ANKETOS PAVYZDYS

EKSPERTŲ APKLAUSA

Data:
Magistro darbo tema: Elektroninės atpažinties priemonės viešajame sektoriuje
Respondentas: darbovietės pavadinimas, pareigos
Apklausos rengėjas: Mykolo Romerio universiteto Socialinių technologijų fakulteto Elektroninio viešojo administravimo magistrantūros studijų programos II kurso studentė Olga Karpovič.
Apklausos klausimai – 6 atviri ir 2 uždari.
Tyrimo problema – nepakankamai efektyvus IT panaudojimas viešojo sektoriaus darbo veikloje. Norint išplėsti e. parašo naudojimą viešajame sektoriuje, tenka nugalėti egzistuojančias kliūtis, kuriuos daro įtaką efektyviam viešojo administravimo institucijų darbui.
Tyrimo tikslas – praplėsti e. parašo naudojimą viešojo sektoriaus veikloje.

1. **Kokį elektroninio parašo modelį siūloma taikyti viešojo sektoriaus veikloje?**

   1) Išorinis lygmuo[2]

   2) Vidinis lygmuo[3]

2. **Kaip sprendžiamas klausimas dėl elektroninio parašo suteikimo darbuotojams, dirbantiems pagal darbo sutartį, viešajame sektoriuje?**

3. **Įvertinkite žemiau pateiktas priemones, taikomas e. parašo plėtrai užtikrinti viešajame sektoriuje. Šių priemonių taikymo pakankamumą vertinkite 10 balų skalėje (1 – žemiausias, 10 – aukščiausias įvertinimas).**

Nr.	Priemonės	Vertinimas
1)	Politiniai sprendimai	
2)	Ekonominiai sprendimai	
3)	Socialiniai sprendimai	
4)	Organizaciniai sprendimai	
5)	Technologiniai sprendimai	

[2]Siunčiamų e. dokumentų pasirašymui, jungiantis prie informacinių išorinių sistemų, pavyzdžiui, IS „INFOSTATYBA".
[3]Vidaus e. dokumentų pasirašymas – įsakymai, protokolai, aktai, tarnybiniai pranešimai, kurie sudaryti įstaigoje ir skirti tik jos reikalams. Įstaigos parengtų ir gautų e. dokumentų registravimui ir tvarkymui, panaudojant supažindinimo žymai, dokumento rengėjo parašui, vizavimui ir kt., jungiantis prie institucijos vidinių informacinių sistemų, pavyzdžiui, finansų valdymo sistemos, dokumentų valdymo sistemos.

4. **Kaip vertinate esamas e. parašo taikymo galimybes viešojo sektoriaus e. paslaugų teikėjams/naudotojams Elektroninių valdžios vartų portale?**

5. **Kokias e. parašo saugumo problemas įžvelgiate?**

   1) E. parašo diegimo etape

   2) E. parašu pasirašytų dokumentų perdavimo etape

   3) E. dokumentų saugojimo etape

6. **Kokie sprendimai galėtų padidinti e. parašo taikymo mastą viešajame sektoriuje?**

7. **Ar Lietuvoje taikomi reikalavimai elektroninės atpažinties priemonėms yra tapatūs su ES reikalavimais. Ar jų pripažinimas įmanomas kitose ES valstybėse narėse? Atsakymą pagrįskite.**

   1) Reikalavimai sertifikavimo paslaugų teikėjams

   2) Sertifikatuose įrašomų asmens duomenų elementai

   3) Pripažinimas tarpvalstybiniu lygiu

8. Kokios yra pagrindinės kliūtys pagal jų svarbą dėl nepakankamo e. parašo naudojimo viešojo sektoriaus veikloje? Įvertinkite lentelėje pateiktas kliūtis (jų pateikta 10) pagal svarbą (reitinguodami), nuo 1 iki 10 (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) (1 – didžiausia kliūtis, 10 – menkiausia kliūtis). Pastaba – kliūtims negali būti suteiktas tas pats reitingo numeris.

Nr.	E. parašo plėtrą viešojo sektoriaus veikloje stabdo:	Reitingas
1.	E. parašo naudojimas gali neleisti nuslėpti neigiamų valdymo padarinių, daromų klaidų ir pan.	
2.	Normų kliūtys, nusistovėjusios viešųjų institucijų griežto reglamentavimo taisyklės, trūksta naujoviškos vadovavimo sampratos	
3.	Asmens tapatybės apsaugos e. erdvėje problema – nepakankamas e. duomenų saugos teisinis ir techninis reglamentavimas	
4.	Sparti informacinių technologijų plėtra viešojo sektoriaus darbuotojams didina darbo krūvį, sukelia technostresą*	
5.	Išteklių stoka. Didelė elektroninio parašo infrastruktūros diegimo kaina, viešajame sektoriuje nėra tam numatytų lėšų	
6.	Motyvacijos naudoti e. parašą stoka. (Reikėtų keisti vertybines nuostatas, taikyti tinkamas paskatas)	
7.	Viešojo sektoriaus institucijų e. dokumentų valdymo sistemos nėra suderintos valstybiniu lygiu, trūksta teisinio reglamentavimo ir šių procesų tinkamo valdymo modelio	
8.	Darbuotojų įsitikinimas, kad naujų technologijų diegimas mažina darbo vietų skaičių	
9.	Gebėjimų kliūtys, kvalifikacijos stoka. Nepakanka žinių pereiti nuo tradiciniu būdu prie e. parašu pasirašomų dokumentų	
10.	Mokymų, konsultacijų dėl procedūrų pažinimo, e. parašo ir e. dokumentų naudojimo stoka	

*__Technostresas –__ tai informacinių komunikacinių technologijų keliamas stresas.

DĖKOJU UŽ JŪSŲ ATSAKYMUS!