MYKOLO ROMERIO UNIVERSITETO
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETO
INFORMATIKOS IR STATISTIKOS KATEDRA

AGNĖS TRAKŠELYTĖS
(ELEKTRONINĖS VALDŽIOS ADMINISTRAVIMAS,
MAGISTRANTŪROS NEAKIVAIZDINĖS STUDIJOS, EVAmn6-02)

VIEŠOSIOS ELEKTRONINĖS PASLAUGOS: ASMENS IDENTIFIKAVIMO PROBLEMOS

Magistro baigiamasis darbas

Darbo vadovas –
Prof. dr. Rimantas Petrauskas

Vilnius, 2007

TURINYS

SUTRUMPINIMŲ SĄRAŠAS

DEP - Dokumento Elektroninio Pasirašymo paslauga

e.parašas – elektroninis parašas

e.terpė – elektroninė terpė

e.valdžia – elektroninė valdžia

EER – angl. Equal Error Rate

EIK - Elektroninės Identifikavimo Kortelės

EP - Elektroninis Parašas

ES – Europos Sąjunga

FAR – angl. False Acceptance Rate

FRR – angl. False Rejection Rate

GPRS – angl. General Packet Radio Service

GSM – angl. Global System for Mobile communications

ID – angl.Identification

IVPK - Informacinės Visuomenės Plėtros Komitetas

LRV - Lietuvos Respublikos Vyriausybė

NEM – angl. the Networked and Electronic Media

NESSI – angl.the Networked European Software and Services Initiative

PDV - Pasirašyto Dokumento Validavimo/perskaitymo paslauga

PKI – angl. Public Key Infrastructure

SIM – angl. Subscriber Identity Module

SSC - Skaitmeninio Sertifikavimo Centras

USB – angl. Universal Serial Bus

VEP – Viešosios Elektroninės Paslaugos

ĮVADAS

Darbo aktualumas. Informacinių technologijų pasiekimų pritaikymas valstybės valdymui atveria naujas didžiules galimybes gyventojų bendradarbiavimui su valdžios institucijomis, skaidresniam valdymui, aiškesniam sprendimų priėmimui [10]. Jis sudaro gyventojui visiškai naujas galimybes bendrauti ir dirbti su viešojo administravimo institucijomis sau patogiu laiku, bet kurioje vietoje ir įvairiais būdais [17, 35].

Elektroninės valdžios koncepcijoje buvo numatytas svarbiausias uždavinys – pasiekti, kad nuo 2005 metų viešosios paslaugos Lietuvos Respublikos gyventojams ir verslo subjektams būtų teikiamos panaudojant skaitmenines technologijas (internetą, mobiliuosius telefonus ir kt.) [22, 24, 34]. Pagal Europos Bendrijos Komisijos komunikatą i2010 [18], taip pat buvo iškeltas siekis, kad Europos piliečiai ir verslo įmonės galėtų pasinaudoti vietos, regiono ar šalies lygiu teikiamomis saugiomis ir patogiomis elektroninėmis paslaugomis. Tam, kad tai įvyktų, buvo reikalinga įdiegti tam tikras priemones, ypač siekiant, kad plataus poveikio paslaugos būtų veiksmingos [15, 16, 46, 58].

Daugelio priemonių, kurios buvo numatytos ir e.valdžios koncepcijoje, ir komunikate [18, 19, 20], Lietuvoje įgyvendinti nepavyko. Nors tai ir leistų kasmet tiesiogiai ir netiesiogiai sutaupyti milijonines lėšas, viešųjų paslaugų perkėlimas į elektroninę erdvę valstybės valdyme stringa (priedas Nr.12) [6, 9, 26, 37].

Kai paslaugos pradėtos perkelti į elektroninę erdvę [8], iškilo svarbus klausimas: kaip atpažinti asmenį prieš suteikiant jam informaciją? Prieš pateikiant duomenis informacijos tiekėjas turi įsitikinti, kad perduoda duomenis būtent tam asmeniui, kuris padarė užklausą. Atitinkamai užklausą padaręs asmuo turi autentifikuoti save, arba kitaip sakant įrodyti savo tapatybę. E-valdžios koncepcijoje taip pat buvo planuota sukurti asmens identifikavimo sistemą, atitinkančią Europos Sąjungos reikalavimus. Ji turėtų neklystamai identifikuoti asmenį ir informacinių technologijų pagalba bendrauti su viešojo administravimo institucijomis [54]. Tokia sistema numatyta, tačiau iki šiol nesukurta.

Informacinės visuomenės plėtros komiteto užsakymu sukurta informacinė sistema „Valdžios elektroniniai vartai“ [43]. Dabartinė e. valdžios portalo paskirtis - bendra interneto prieiga prie valstybės institucijų teikiamos informacijos ir viešųjų paslaugų. E. valdžios portale saugomas ir kaupiamas nuorodų sąrašas į Viešųjų įstaigų ar Valstybinių institucijų svetaines, kuriose yra patalpintos elektroninės viešosios paslaugos ar tam tikra vartotojams aktuali informacija [41].

„Elektroninės valdžios vartų“ portale teikiamomis elektroninėmis paslaugomis gali naudotis tik Lietuvos Respublikos piliečiai, sėkmingai atlikę asmens tapatybės nustatymo procedūrą (identifikavimą) portale.

Problema. Vartotojai, norėdami atlikti asmens tapatybės nustatymo procedūrą (identifikuotis) portale, turi turėti 2 ar 3 klasės asmeninį skaitmeninį sertifikatą, išduotą kvalifikuoto elektroninio parašo paslaugų teikėjo arba būti vieno iš komercinių bankų internetinės bankininkystės sistemos vartotoju. Asmeninis skaitmeninis sertifikatas yra pakankamai brangu (kaina metams 90 Lt - 149 Lt) [39], o asmens identifikavimas pasinaudojant bankų internetinės bankininkystės sistema - paremtas pasitikėjimu banku, ir tarp banko ir kliento. Nors bankai prognozuoja [23], kad 2007 metų pabaigoje jie turėtų turėti 1,72 mln. šių paslaugų vartotojų, šis būdas nėra pats saugiausias. Todėl privaloma ieškoti alternatyvių būdų, kaip būtų galima būtų identifikuoti asmenį elektroninėje erdvėje.

Tyrimo objektas – asmens identifikavimo elektroninėje erdvėje būdai ir jų patikimumo aspektai, galimybės.

Darbo tikslas – įvertinti galimus ir perspektyvius asmens identifikavimo būdus; išanalizuoti jų patikimumo, saugumo ir sąveikumo aspektus; pateikti numatomų priemonių rekomendacijas.

Uždaviniai:

1. išnagrinėti esamus bei alternatyvius asmens identifikavimo elektroninėje erdvėje būdus;
2. apžvelgti naujausių technologijų siūlomus asmens identifikavimo būdus;
3. išanalizuoti geriausius asmens identifikavimo pavyzdžius Europos Sąjungoje bei kitose užsienio šalyse;
4. atlikus tyrimą įvertinti asmens identifikavimo problemas Lietuvoje, pasiūlyti sprendimo būdus.

Metodai. Darbe taikyti mokslinės literatūros, teisinių dokumentų analizės ir sintezės, indukcijos, dedukcijos, kiekybinio tyrimo metodai. Duomenų apdorojimo metodas – matematinė statistika. Šis darbas rengtas panaudojus teisinius dokumentus, surinkti ir išanalizuoti antrinės ir pirminės informacijos šaltinių duomenys.

Atliekant tyrimą taip pat buvo naudojama žvalgomojo tyrimo metodika.

Darbo struktūra. Darbą sudaro įžanga, 4 skyriai, išvados, naudotos literatūros sąrašas, priedai. Bibliografinį aprašą sudaro 61 šaltinis.

Teorinę darbo dalį sudaro pirmieji trys skyriai. Pirmajame skyriuje nagrinėjami esami bei alternatyvūs asmens identifikavimo elektroninėje erdvėje būdai: elektroninis parašas, mobilus elektroninis parašas, asmens identifikavimas per bankų sistemas, apžvelgiamas investicinis projektas (galimybių studija) “Daugiafunkcinių mikroprocesorinių asmens

dokumentų išrašymas ir panaudojimas” [4]. Antrajame skyriuje apžvelgiamas naujausių technologijų taikymas sprendžiant asmens identifikavimo problemas. Trečiajame skyriuje analizuojami geriausios praktikos pavyzdžiai pasaulyje, priemonės Europos Sąjungoje.

Praktinė dalis – ketvirtasis skyrius, atliktas gyventojų naudojamų būdų identifikuotis elektroninėje erdvėje tyrimas. Tai nedidelės apimties preliminarus tyrimas, kurio tikslas yra ištirti, kokias būdais respondentai dažniausiai naudojasi identifikuojant save elektroninėje erdvėje, kokiomis viešosiomis paslaugomis naudojasi.

1. ASMENS IDENTIFIKAVIMO ELEKTRONINĖJE ERDVĖJE BŪDAI, JŲ ANALIZĖ

Šiame skyriuje nagrinėjami esami bei alternatyvūs asmens identifikavimo elektroninėje erdvėje būdai: elektroninis parašas, mobilus elektroninis parašas, asmens identifikavimas per bankų sistemas, apžvelgiamas investicinis projektas (galimybių studija) "Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas".

1.1. Elektroninis parašas

Elektroninio parašo įstatymas įsigaliojo dar 2002 metais [32], o 2005 metų pradžioje savo veiklą pradėjo pirmasis skaitmeninius kvalifikuotus sertifikatus sudarantis sertifikavimo paslaugų teikėjas. Tai reiškia, kad Lietuvoje elektroninis parašas jau turi tokią pačią juridinę galią, kaip ir tradicinis, ranka pasirašytas [31]. Kol kas elektroniniu parašu daugiausia naudojasi (eksperimentuoja) tik keletas valstybinių įmonių bei pavieniai technologijų entuziastai [14].

Elektroninis parašas - duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti [7]. Tai yra popierinio parašo atitikmuo elektroninėje erdvėje, naudojamas vartotojo identifikavimui ir dokumentų pasirašymui, tam tikrų duomenų unikalus rinkinys kuris tarnauja kaip elektroninė tapatybė kurią galima patikrinti elektroninėje erdvėje [12]. Saugus elektroninis parašas - elektroninis parašas, kuris atitinka visus šioje dalyje nurodytus reikalavimus [27]:

1) yra vienareikšmiškai susietas su pasirašančiu asmeniu;

2) leidžia identifikuoti pasirašantį asmenį;

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

4) yra susijęs su pasirašytais duomenimis taip, kad bet koks šių duomenų pakeitimas yra pastebimas.

Pasirašyti duomenys - duomenys, į kuriuos yra įterptas, prie kurių prijungtas ar su kuriais logiškai susietas elektroninis parašas [21].

UAB "Skaitmeninio sertifikavimo centras" (SSC) [39] vienintelis Lietuvoje išduoda kvalifikuotą elektroninį parašą. UAB – pirmas elektroninio parašo paslaugų teikėjas Lietuvoje, įkurta 2004 m. liepos 1 d. ir yra EuroPKI sertifikavimo infrastruktūros narys.

2005 m. sausio 27 d. bendrovė pateikė Informacinės Visuomenės Plėtros Komitetui prie Lietuvos Respublikos Vyriausybės (toliau tekste (IVPK prie LRV) paraišką, įregistruoti įmonę sertifikavimo paslaugų teikėju, sudarančiu kvalifikuotus sertifikatus. Po išsamaus įmonės patikrinimo, 2005 m. kovo 1 d. IVPK prie LRV įregistravo SSC sertifikavimo paslaugų teikėju sudarančiu kvalifikuotus sertifikatus.

Įgytas statusas suteikė bendrovei puikią galimybę teikti e-parašo paslaugas ne tik Lietuvoje, bet ir visoje ES ekonominėje erdvėje. Pagal ES ir Lietuvos teisinius aktus skaitmeninio sertifikavimo paslaugas gali teikti kiekvienas, tačiau kvalifikuotus (patikimus) sertifikatus išduoda tik įmonė, turinti kvalifikuoto paslaugų teikėjo statusą. Pasinaudodama naujo verslo galimybėmis, bendrovė aktyviai plečia savo verslą. 2005-2006 metais SSC kartu su partneriais laimėjo e-parašo valstybės institucijoms techninės dokumentacijos, e-parašo programinės įrangos ir nuotolinio mokymo sistemos konkursus. Visi laimėti konkursai sėkmingai užbaigti.

Nuo 2005 m. gruodžio mėn. įmonė teikia kvalifikuotus sertifikatus aukšto lygio valstybės tarnautojams įskaitant Lietuvos Respublikos ministrus.

Suprasdama e-parašo technologijų sudėtingumą ir kompleksiškumą, ir savo misiją, kaip kol kas vienintelio šalyje sertifikavimo paslaugų teikėjo, bendrovė padeda Lietuvos įmonėms diegti modernias dokumentų pasirašymo, asmens autentifikavimo technologijas. SSC yra pirma ir kol kas vienintelė įmonė Lietuvoje teikiančia saugius dvejų faktorių autentifikavimo sprendimus (Lietuvos vartotojai gali nemokamai autentifikuotis tokiuose portaluose kaip http://www.evaldzia.lt, www.registrucentras.lt, www.vilnius.lt ir www.vmi.lt). Bendrovės pagalbos tarnyba nemokamai konsultuoja Lietuvos piliečius, valstybinio sektoriaus ir verslo įmonių atstovus šių modernių technologijų diegimo ir naudojimo klausimais (pagalbos tarnybos adresas: www.ssc.lt/support) ir nemokamai išduoda testinius skaitmeninius sertifikatus šalies įmonėms bei piliečiams.

SSC yra viena iš dinamiškai augančių įmonių, aktyviai dalyvaujančių tarptautiniuose renginiuose bei forumuose: Porvoo group, OpenDocument Foundation Alliance, NESSI (the Networked European Software and Services Initiative) bei NEM (the Networked and Electronic Media) Initiative SEC klasterio narė. Nuo bendrovės steigimo pradžios bendrovė nuolat dalyvauja viename iš svarbiausių kasmetinių renginių e-saugumo srityje – RSA konferencijose (San Francisco, JAV).

E.parašą galima įsigyti įvairiose laikmenose: lustinėje kortelėje, USB laikmenoje ar SIM kortelėje(1 pav.) [55].

1 pav. Specialios laikmenos: lustinės kortelės, USB saugyklos, SIM kortelės

Norint įsigyti kvalifikuotą e.parašą būtina asmens identifikacija vienoje iš SSC Registravimo Tarnybų.

E.parašu pasirašantis asmuo turi turėti sertifikatą. Sertifikatas – tai elektroninio pavidalo liudijimas, patvirtinantis, kad šifravimo raktų pora priklauso sertifikate nurodytam asmeniui.

Skaitmeninis sertifikatas - tai elektroninis paso, vairuotojo pažymėjimo arba nario kortelės atitikmuo, kurio pagalba galima įrodyti savo asmens tapatybę arba teisę prieiti prie reikalingos informacijos internete. Skaitmeninių sertifikatų veikimas yra paremtas šifravimo viešųjų raktų technologijomis, kai naudojama vienas kitą papildančių raktų pora - asmeninis ir viešasis. Naudojant skaitmeninį sertifikatą galima patikrinti vartotojo teises į konkretų raktą - tai užkerta kelią neteisėtam asmeninio rakto naudojimui. Taigi, skaitmeniniai sertifikatai specialaus šifravimo dėka suteikia saugumą ir garantuoja visų elektroninių veiksmų dalyvių tapatybę.

SSC, kaip kvalifikuota sertifikavimo tarnyba sudaro ir pasirašo sertifikatus savo privačiu raktu, ir teikia sertifikatų duomenis parašo naudotojams elektroniniams parašams tikrinti.

Paprastai skaitmeninis sertifikatas susideda iš:

- savininko viešo rakto;
- savininko vardo;
- viešo rakto galiojimo termino;
- skaitmeninį sertifikatą teikiančios organizacijos (CA) pavadinimo;
- skaitmeninio sertifikato serijinio numerio;
- sertifikatą teikiančios organizacijos skaitmeninio parašo.

Asmens sertifikatai, išduodami skaitmeninių sertifikatų centre, tampa elektroniniu užantspauduoto dokumento pakaitalu. Saugiai įdiegtas naršyklėje arba elektroninio pašto siuntimo programinėje įrangoje, asmeninis skaitmeninis sertifikatas suteikia galimybę skaitmeniniu būdu pasirašyti ir užkoduoti dokumentus bei siunčiamus elektroninius pranešimus. Asmeniniai sertifikatai specialiose elektroninėse laikmenose (USB raktai, lustinės kortelės ir pan.) aprūpina aukščiausio lygio duomenų apsaugą.

Vienas iš pagrindinių pliusų, kad vartotojui nereikia naudoti ir prisiminti daug slaptažodžių jungiantis prie kiekvieno portalo. Vienas sertifikatas - kelias prie visų viešųjų paslaugų. Tyrimai parodo, kad vartotojo slaptažodžių skaičius pastoviai auga, tampa sunku juos prisiminti, ir tie slaptažodžiai užrašomi į mobiliuosius telefonus, užrašų knygeles, kitur. Tokiu būdu didinama rizika gauti slaptažodį tretiems asmenims, ir juo pasinaudoti. Jeigu institucija teikia elektronines viešąsias paslaugas ir yra prijungta prie Skaitmeninio sertifikavimo centro

autentifikavimo sistemos tuomet asmeniui suteikiama galimybė prisijungti prie sistemos skaitmeninio sertifikato pagalba ir pasinaudoti viešosiomis paslaugomis, gauti reikalingą informaciją.

1 lentelė. Sertifikatų aprašymas pagal klases

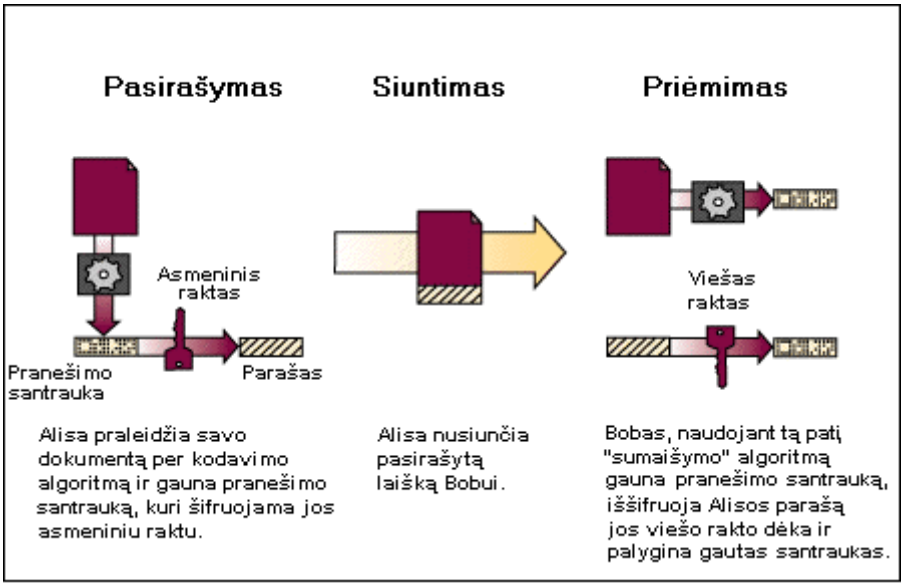
Klasė	Aprašymas
	Šis kvalifikuotas sertifikatas vienareikšmiškai identifikuoja pasirašantį asmenį ir yra kvalifikuotas. Sertifikato įsigijimui yra būtinas sertifikato užsakovo tapatybės nustatymas vienoje iš SSC Registravimo Tarnybų. Kaina metams - 149 Lt be PVM (be laikmenos ir jos licencijos kainos).
	Šis sertifikatas vienareikšmiškai identifikuoja pasirašantį asmenį. Sertifikato įsigijimui yra būtinas sertifikato užsakovo tapatybės nustatymas vienoje iš SSC Registravimo Tarnybų. Kaina metams - 90 Lt be PVM (be laikmenos ir jos licencijos kainos).
	Šis sertifikatas identifikuoja tik pasirašančio asmens el. pašto adresą. Sertifikato įsigijimui nėra būtinas sertifikato užsakovo tapatybės nustatymas su atvykimu į SSC Registravimo Tarnybą. Kaina metams - 62 Lt be PVM (be laikmenos ir jos licencijos kainos)

Asmuo, norintis gauti viešąsias paslaugas apsilanko įstaigos internetiniame puslapyje. Pasirenkama, kad autentifikavimas bus vykdomas naudojant skaitmeninį sertifikatą. Jeigu sertifikatas saugomas laikmenoje, sistema paprašys įvesti laikmenos slaptažodį ir pasirinkti sertifikatą, o jeigu kompiuteryje reikės pasirinkti sertifikatą iš esamų kompiuteryje. Kai asmuo bus atpažintas, iš pateikto sąrašo reikia pasirinkti paslaugą, kuria norima pasinaudoti. Asmuo turi sutikti, kad nurodyti asmens duomenys iš skaitmeninio sertifikavimo centro bus perduoti tos įstaigos, iš kurios norima gauti informaciją, informacinei sistemai. Sutikus, asmuo matys duomenis, kuriuos buvo užklausęs.

Asmuo, užsakydamas asmeninį skaitmeninį sertifikatą pildo prašymą ir nurodo savo asmens duomenis, kurie saugomi sertifikavimo centre. Kai asmuo autentifikuojasi prie viešųjų paslaugų portalo, jis pateikia savo sertifikatą. Portalas susijungia su sertifikavimo centru, ir tikrina ar toks sertifikatas yra išduotas ir yra galiojantis. Jeigu sertifikatas galioja, sertifikato turėtojo asmens duomenys saugiu būdu perduodami portalui. Tokiu būdu viešųjų paslaugų tiekėjas atpažįsta asmenį, ir suteikia jam reikalingą informaciją. Kadangi prieš išduodant skaitmeninį sertifikatą asmuo pateikia asmens dokumentus sertifikavimo centrui, pastarasis gali užtikrinti, kad tas sertifikatas priklauso būtent tam asmeniui ir autentifikuoja asmenį.

Skaitmeniniai sertifikatai gali būti panaudoti įvairioms elektroninėms operacijoms, susijusioms su svarbių duomenų perdavimu internetu. Tai gali būti elektroninio pašto laiškų siuntimas, elektroninė komercija, o taip pat elektroninės finansinės operacijos. Skaitmeniniai sertifikatai elektroniniu būdu patikrina asmens tapatybę. Naudojami perduodamos informacijos kodavimu, skaitmeniniai sertifikatai tuo pačiu užtikrina būtiną saugumą bei visų asmenų, dalyvaujančių duomenų apsikeitime, tapatybės nustatymą.

Skaitmeninių sertifikatų veikimas yra pagrįstas kodavimo viešuoju raktu technologija, veikiančia naudojant porą tarpusavyje "surištų" raktų - privatų ir viešą [3]. Viešasis raktas turi būti žinomas visiems, kas nori susisiekti su raktų poros savininku. Jis gali būti panaudotas pranešimo, pasirašyto privačiuoju raktu, patikrinimui arba pranešimo, kuris galės būti iššifruotas tik privačiuoju raktu, kodavimui. Tokiu būdu užšifruotų pranešimų saugumas yra pagrįstas privataus rakto saugumu, kuris turi būti gerai apsaugotas nuo neteisėto priėjimo.



2 pav. Skaitmeninio sertifikato veikimas

Šį būdą išrado JAV Masačiusetso Technologijos Instituto profesoriai R. Rivest, A. Shamir, ir L.Adleman.(RSA). Nors viešasis ir asmeninis raktai yra skirtingi, tačiau jie gali atlikti tiktai vienpusį kodavimą - užkoduoti pranešimą taip, kad jį atkoduotų tik kitas tos pačios poros raktas. RSA viešasis raktas perduodamas asmenims, su kuriais kontaktuojama, o asmeninis raktas turi būti gerai apsaugotas. Asmeninio rakto pagalba siuntėjas siunčiamą žinutę užkoduoja. Tokiu būdu ši užkoduota žinutė gali būti atkoduota tik su žinutės gavėjo viešuoju raktu. Ir atvirkščiai, siunčiamas pranešimas, kuris užkoduojamas viešuoju raktu, gali būti atkoduotas tik su asmeniniu raktu. Kitaip tariant raktai koduoja "priešingomis kryptimis". Ši technologija sukuria pagrindą elektroninio parašo atsiradimui. Jei gavėjas gali atkoduoti pranešimą viešojo rakto pagalba, tai ši žinutė yra užkoduota siuntėjo asmenino rakto pagalba. Kadangi asmeninis

raktas yra tik vienas ir yra gerai apsaugotas, tai jis tampa tam tikru elektroniniu parašu - dokumentu, kurio niekas kitas negali sukurti.

Skaitmeninių sertifikatų sudėtyje yra informacija apie savininką: vardas, pavardė, darbovietė, elektroninio pašto adresas ir kt. Įdiegtas interneto naršyklėje, toks sertifikatas gali būti naudojamas kaip elektroninis asmens pažymėjimas, kurį WEB serveriai gali patikrinti. Tai padeda išvengti slaptažodžio įvedimo ir tikrinimo tais atvejais, kai yra reikalingas narystės patikrinimas.

Tam, kad patikrinti gautos žinutės vientisumą, sukuriamos papildomos žinutės vientisumą patikrinančios santraukos (toliau santraukos). Santraukos yra užkoduojamos naudojant siuntėjo asmeninį raktą ir tokiu būdu suformuojamas elektroninis parašas. Šis parašas gali būti atkoduotas tik viešuoju tos pačios raktų poros raktu. Gavėjas iššifruoja žinutės elektroninį parašą ir tada pagal gautą pranešimą sukuria savo santrauką. Ši nauja santrauka palyginama su iš skaitmeninio parašo gauta santraukos reikšme. Jeigu abidvi reikšmės sutampa, galima daryti išvadą, kad žinutė nebuvo pakeista. Kadangi pranešimas yra iššifruojamas viešuoju raktu, galima teigti, kad pranešimas buvo užkoduotas atitinkamu asmeniniu raktu, kurį gali žinoti tiktai siuntėjas. Šis autentifikavimo procesas yra integruotas į bet kurią naudojamą saugumo programą, į kurią yra įtraukta saugumą užtikrinanti funkcija.

Kai gaunamas pranešimas, pasirašytas skaitmeniniu būdu, galima patikrinti, ar skaitmeninis sertifikatas nėra suklastotas, ar jo galiojimo terminas dar nėra pasibaigęs. Kai siunčiamas pranešimas, galima jį pasirašyti ir tai įtikins gavėją, kad laiškas tikrai yra nuo siuntėjo.

Yra dar vienas skaitmeninio sertifikato panaudojimo būdas - asmens tapatybės nustatymas WEB serveriuose. Tuomet nereikia įvedinėti jokių slaptažodžių, serveris automatiškai nuskaitys sertifikatą, ir jeigu asmuo yra registruotas narys, bus leista dirbti toliau. Tereikia įdiegti skaitmeninį sertifikatą ir nustatyti savo interneto naršyklę ir elektroninio pašto programą, taip jos galėtų automatiškai juo naudotis.

1.2. Mobiliojo e. parašo infrastruktūra ir standartai

Vartotojams, kurie nori suteikti juridinę galią elektroniniams dokumentams naudojant mobiliojo e. parašo technologiją, nereikia keisti telefono, įsigyti papildomos techninės ar programinės įrangos. Užtenka pasikeisti telefono SIM kortelę, kuri mobiliojo e. parašo infrastruktūroje atlieka SMART kortelės funkciją. Mobiliojo e. parašo technologija suteikia dar didesnio patogumo pasirašinėjantiems dokumentus skaitmeniniu būdu [28, 49, 51].

Prieš metus Lietuvos Respublikos Vyriausybės, pirmaujančių šalies įmonių ir asociacijos „Langas į ateitį“ pasirašyta Elektroninio parašo proveržio programa [13] ir metus

trukęs bendras darbas davė pirmųjų rezultatų. Pagal Elektroninio parašo proveržio programos grupės technines rekomendacijas sukurti ir rinkai pradėti siūlyti pirmieji Lietuvoje kvalifikuoti saugūs mobilieji e-parašai. Mobilusis e-parašas leidžia atsisakyti papildomų prietaisų, nes nuskaitymo įrenginį pakeičia mobilusis telefonas, kuriame įdedama nauja SIM kortelė su e-parašo galimybe. Vartotojui, norinčiam naudotis mobiliuoju e-parašu, tereikia savo turimą SIM kortelę pasikeisti naująja ir pasirašyti e-tapatybės sutartį (priedai nr.1; 2; 3; 4) [44].

Mobilusis e-parašas yra nesudėtingas ir patogus naudoti. Kadangi Lietuvoje mobiliojo ryšio skverbtis yra viena didžiausių pasaulyje, galima prognozuoti, kad naujasis sprendimas sparčiai populiarės [48].

Kol kas mobiliuoju e-parašu gali naudotis tik „Omnitel“ vartotojai, jungdamiesi prie „Hansabanko“ internetinės bankininkystės sistemos. Bankai tapo mobiliojo e-parašo galimybių naudojimo pionieriais, kadangi jie turi daug aktyvių internetinės bankininkystės sistemų naudotojų ir siekia pasiūlyti jiems saugesnį ir patogesnį įrankį prie šių sistemų prisijungti [29, 30].

Bankai, diegdami įvairius klientų identifikavimo sprendimus, išpopuliarino internetinę bankininkystę ir perkėlė daugelį santykių su klientais į elektroninę erdvę. Mobiliojo e-parašo srityje žengiami dar pirmieji žingsniai, bet, remiantis pasauline praktika, galima tikėtis nemažai naujų sprendimų, palengvinančių kasdienybės rūpesčius, o įmonėms leidžiančių perkelti vis daugiau savo procesų į elektroninę erdvę. Kvalifikuotas mobilusis e-parašas - tai elektroninis pasas, su kurio pagalba klientas, atėjęs į interneto banką, galės gauti visas paslaugas, kurias jis gauna banko padalinyje. Prisijungimas prie internetinio banko "hanza.net" mobiliuoju e-parašu turėtų būti išties patogi priemonė banko klientams pasiekti savo sąskaitas internete. Didžiausi mobiliojo e-parašo privalumai internetinėje bankininkystėje yra patogumas, universalumas, išlaikant ne prastesnį saugumo lygį.

Specialistų vertinimu, lietuvių sukurta mobiliojo e-parašo infrastruktūra yra itin saugi: asmeninį raktą mobiliajame telefone nuo neteisėto panaudojimo saugo netgi du kodai – telefono ir pasirašymo, kuriuos žino tik pats vartotojas. Net jeigu jis telefoną praranda, svetimas žmogus, nežinodamas kodo, e-parašu pasinaudoti negalės. O užblokavus SIM kortelę, nelieka jokių galimybių neteisėtai pasinaudoti mobiliuoju e-parašu.

„Omnitel“ vartotojai, norintys pradėti naudotis mobiliuoju e-parašu, turi pasikeisti savo turimas SIM korteles į naujas. Tai vartotojai galėjo padaryti atvykę į „Omnitel“ stendą parodoje „Infobalt“, kuri vyko 2007 m. spalio 25-27 dienomis. Dviejų savaičių bėgyje SIM korteles vartotojai galėjo keistis ir „Omnitel“ salonuose. Keisdami SIM korteles, vartotojai privalo pateikti asmens tapatybę patvirtinančius dokumentus. Šiuo metu SIM kortelės "Omnitel" vartotojams keičiamos nemokamai [51].

Savo sistemas mobiliojo e-parašo naudojimui jau pradėjo adaptuoti ir SEB Vilniaus bankas, „Parex“ bankas, „DnB Nord“ bankas bei "Sodra".

Iniciatyvinė mobiliojo e-parašo grupė siekia sudaryti palankias sąlygas elektroniniam parašui Lietuvoje plisti, kad per trejus ateinančius metus jo naudojimas mūsų šalyje taptų masinis, o aktyviai besinaudojančių sukurta e-parašo infrastruktūra interneto ir mobiliųjų vartotojų skaičius siektų ne mažiau kaip 300 tūkstančių.

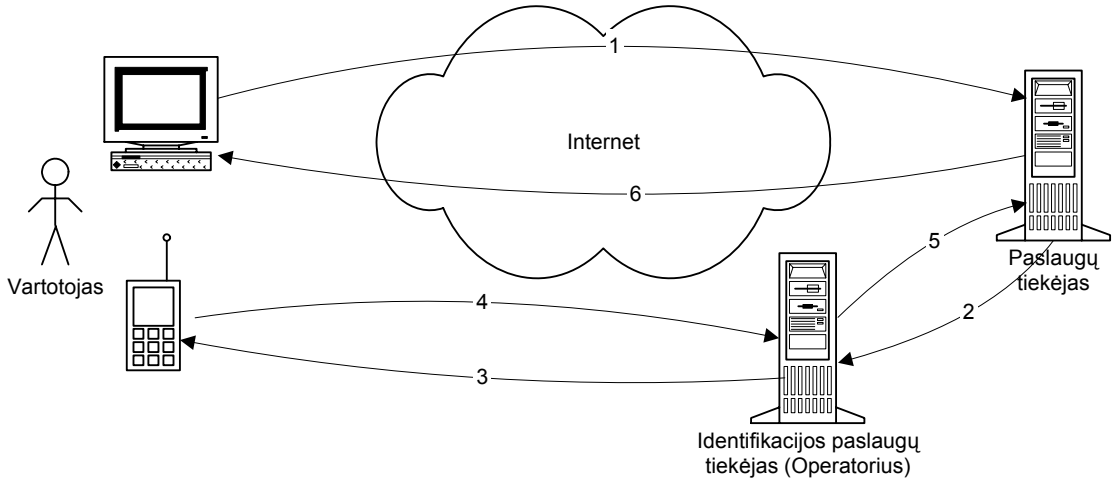
Elektroninio parašo proveržio programoje šiuo metu dalyvauja Lietuvos Respublikos Vyriausybė, "Hansabankas", SEB Vilniaus bankas, "DnB Nord" bankas, "Parex" bankas, "Omnitel", "Bitė Lietuva", asociacija "Langas į ateitį", "Sodra", Informacinės visuomenės plėtros komitetas prie LRV, Vidaus reikalų ministerija ir Valstybinė mokesčių inspekcija.

Mobiliojo GSM ryšio operatoriai savo versle naudoja SIM korteles, kurios iš esmės yra SMART tipo kortelės, saugiai saugojančios korinio mobiliojo ryšio abonento duomenis [50]. Mobilusis GSM telefonas yra SMART kortelių skaitytuvas. Mobilusis telefonas turi saugią duomenų perdavimo jungtį su serverine dalimi (SMS ir/arba GPRS), veikiančia bet kurioje pasaulio šalyje, palaikančioje GSM standarto telefonijos tinklus. Taigi, GSM infrastruktūra turi visus esminius elementus, leidžiančius sukurti mobiliąją EP infrastruktūrą.

Mobilioji GSM ryšio operatorių infrastruktūra yra palanki diegti EP taikymams:

- vartotojas asmeninį GSM telefoną pastoviai nešiojasi su savimi, jo netektis pastebima iš karto,
- GSM technologijos patikimumas ir saugumas yra visuotinai pripažinti,
- nėra reikalavimų instaliuoti ir prižiūrėti specialios programinės įrangos ir išmokti ja naudotis.

Mobilioji EP infrastruktūra yra sukuriama, į SIM korteles įdiegiant privačiuosius vartotojų raktus, bei juos užregistruojant sertifikatų centre. Tik nuo sertifikatų centro atestacijos priklauso, ar tokios infrastruktūros pagalba sukurtas elektroninis parašas bus kvalifikuotas ar ne. Operatoriaus pusėje instaliuojama papildoma įranga, suteikianti paslaugų tiekėjams prieigą prie mobiliosios EP infrastruktūros. Vartotojams pateikiama patogi, lengvai suprantama ir intuityvi dialogo formos sąsaja, kurios nereikia specialiai mokytis. Vartotojas, įregistruodamas asmens duomenis sertifikatų centre, gauna pasirašymo operacijoms skirtą PIN kodą, kurį privalo saugoti ir kuris naudojamas visoms elektroninio pasirašymo operacijoms įvykdyti.



3 pav. Mobiliosios EP infrastruktūros panaudojimo schema

Įprastinė EP infrastruktūros panaudojimo schema: vartotojas inicijuoja užklausą paslaugų tiekėjui elektroniniu kanalu, paslaugų tiekėjas suformuoja dokumentą, kuris adresuojamas vartotojui ir perduodamas į jo asmeninį mobilųjį telefoną per identifikacijos paslaugų tiekėją (žr. pav.). Vartotojas pasirašo užklausą, įvesdamas pasirašymo PIN kodą, o paslaugų tiekėjas, gavęs pasirašytą dokumentą, patikrina jį ir suteikia paslaugą vartotojui.

Didžiausias iššūkis verslui, norinčiam sukurti atsiperkančią EP infrastruktūrą yra – sukurti paslaugą(-as), kurios panaudojimas būtų pakankamai paprastas ir pakankamai fundamentalus, t.y. toks, kad ją būtų galima naudoti kuo įvairesniuose taikymuose. Šiuo atveju pasirinkta sekanti paslauga: “Elektroniniu paštu siunčiamo bet kokio formato kompiuterinės bylos pasirašymas”.

Elektroninis paštas yra plačiai paplitusi paslauga, ja naudojasi didžioji interneto vartotojų dalis, elektroninio pašto mobilioji atmaina (SMS žinutės) yra intensyviai naudojama GSM vartotojų tarpe, todėl tikimasi, kad elektroninio pašto sąsaja tiek vartotojams tiek sąveikaujančioms paslaugų tiekėjų sistemoms bus priimtiniausia. Patrauklu ir tai, kad vartotojams į savo personalinius kompiuterius nereikia instaliuoti papildomos programinės įrangos, bei turėti pastovaus internetinio ryšio.

Tam, kad vartotojams nereikėtų rūpintis papildomais įrankiais, yra pateikiamos dvi paslaugos:

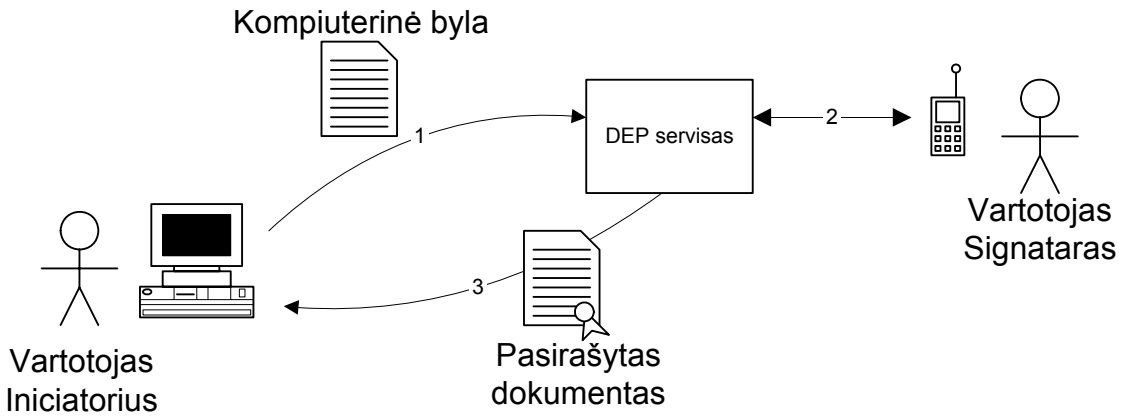
- Dokumento Elektroninio Pasirašymo paslauga (DEP servisas),
- Pasirašyto Dokumento Validavimo/perskaitymo paslauga (PDV servisas).

Dokumentų elektroninio pasirašymo paslauga (DEP servisas) yra skirta sukurti elektroniniu parašu patvirtintam dokumentui. Įėjimo parametras – bet kokia kompiuterinė byla, išėjimo parametras – pasirašytas dokumentas. Bet kuris elektroninio pašto vartotojas gali inicijuoti pasirašyto dokumento sukūrimą, tačiau elektroniniu parašu patvirtinti konkretų dokumentą gali tik asmuo, turintis mobiliojo EP infrastruktūrą (t.y. turintis galiojantį sertifikatą).

4 pav. yra pateiktas pasirašymo mechanizmo veikimas. Vartotojas-iniciatorius siunčia e-pašto žinutę (1) su prisegta bet kokio formato kompiuterine byla specialiu DEP serviso adresu, kuriame nurodamas vartotojas-signataras. DEP servisas patikrina, ar vartotojas-signataras turi galiojantį sertifikatą, tinkamą kvalifikuotam elektroniniam parašui sukurti ir inicijuoja pasirašymo procedūrą (2), kurios metu sukuriami elektroninio parašo duomenys. DEP servisas surenka elektroninio parašo duomenis į vieną dokumentą ir persiunčia jį vartotojui-iniciatoriui.

Sėkmės atveju, dokumento pasirašymo procedūros pabaigoje vartotojas-iniciatorius gauna elektroninio pašto žinutę, kurioje prisegtas elektroniniu vartotojo-signataro parašu patvirtintas dokumentas, atitinkantis standartą.

Jei dokumento pasirašyti nepavyksta, vartotojas-iniciatorius informuojamas apie nesėkmę e-pašto žinute.

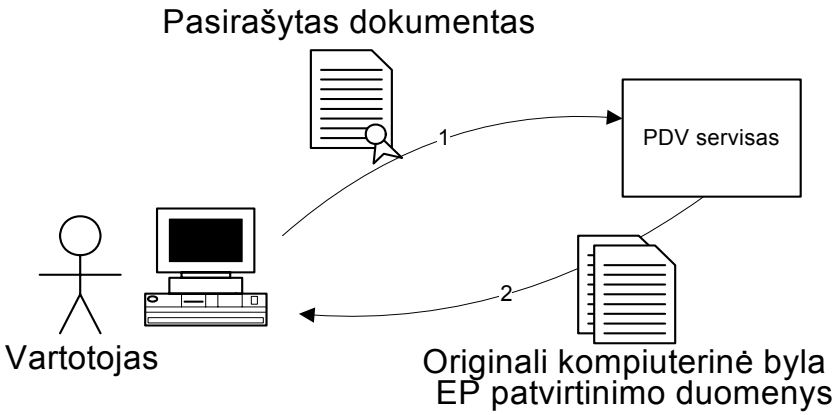


4 pav. Dokumentų Elektroninio Pasirašymo mechanizmo veikimas

Vartotojas, turintis elektroniniu parašu patvirtintą dokumentą negali peržiūrėti jo turinio be specialios programinės įrangos. Esant reikalui (pvz., jei vartotojas labai dažnai validuoja pasirašytus dokumentus), šią įrangą vartotojas gali nemokamai parsisiųsti iš interneto ir instaliuoti savo kompiuteryje. Siekiant vartotojo nesusaistyti tokiais reikalavimais, kaip programinės įrangos instaliavimas, yra sukurta elektroniniu paštu iškviečiama paslauga, atskleidžianti pasirašyto dokumento turinį ir patikrinantį signataro elektroninio parašo galiojimą (PDV servisas).

Pasirašyto dokumento validavimo paslaugos įėjimo parametras – pasirašytas dokumentas, atitinkantis standartą, išėjimo parametras – originali kompiuterinė byla. Bet kuris elektroninio pašto vartotojas gali inicijuoti pasirašyto dokumento validavimo paslaugą.

5 pav. yra pateiktas validavimo mechanizmo veikimas:



5 pav. Pasirašyto Dokumento Validavimo mechanizmo veikimas

Vartotojas siunčia e-pašto žinutę (1) su prisegtu pasirašytu dokumentu specialiu PDV serviso adresu. Pasirašyto Dokumento Validavimo servisas patikrina, ar dokumentas nebuvo neteisėtai modifikuotas ir ar visų signatarų elektroniniai parašai yra galiojantys. Tuo atveju, jei patikrinimo rezultatas yra sėkmingas, PDV servisas persiunčia vartotojui originalią kompiuterinę bylą, bei duomenis apie ją pasirašiusius signatarus (2). Jei dokumento turinys buvo pakeistas, arba signatarų parašai nėra galiojantys, vartotojas gauna e-pašto žinutę apie klaidą.

Schemoje nedalyvauja GSM telefonai ar kita įranga, susijusi su signataru, todėl ja be apribojimų gali naudotis bet kuris elektroninio pašto vartotojas.

Mobilioji elektroninio parašo infrastruktūra paslaugų tiekėjams yra pasiekiama internetu (žr. 5 pav.). Visoje EP infrastruktūroje yra septyni tinklo elementai, kuriuos galima analizuoti saugumo aspektu:

1.mobilusis telefonas, jame esanti SIM kortelė.

2.ryšys tarp mobiliojo telefono ir Identifikacijos Paslaugų Tiekėjo serverinės dalies.

3.identifikacijos Paslaugų Tiekėjo serverinė dalis.

4.ryšys tarp Identifikacijos Paslaugų Tiekėjo serverinės dalies ir Paslaugų Tiekėjo serverinės dalies.

5.paslaugų Tiekėjo serverinė dalis.

6.ryšys tarp Paslaugų Tiekėjo serverinės dalies ir vartotojo kompiuterio.

7.vartotojo kompiuteris.

Pirmieji keturi punktai, priklausantys nuo GSM operatoriaus, yra reglamentuojami standartų ir prižiūrimi specialiųjų tarnybų, todėl yra laikomi saugūs. Silpniausia grandimi yra laikomi 6 ir 7 įrenginiai, priklausantys pačiam vartotojui. Paslaugų tiekėjai privalo pasirūpinti, kad vartotojo ir sistemos dialogo metu būtų išvengta rizikos, jog pasirašomo dokumento turinys bus pakeistas. Tai pasiekiama, protingai parenkant pasirašomų duomenų surinkimo procedūrą arba organizacinėmis priemonėmis – pasirašymo procedūrą organizuojant taip, kad pasirašomo dokumento turinio pakeitimas būtų pastebėtas prieš jį panaudojant. Organizacinės priemonės pavyzdžiu galėtų būti reikalavimas vartotojui, prieš pasirašant tekstą, atidžiai jį perskaityti mobiliojo telefono ekrane.

DEP serviso atveju silpniausia grandis saugumo prasme yra 6, t.y. elektroninio pašto sistema, tarnaujanti transportu tarp vartotojo ir DEP serviso. Kadangi standartinėmis elektroninio pašto priemonėmis saugumo problemos išspręsti neįmanoma, paslaugos vartotojams yra keliamas papildomas reikalavimas – perskaityti pasirašomo teksto turinį, prieš jį pasirašant, arba atlikti pasirašyto dokumento validavimo ir autentiškumo patikrinimo veiksmą iš karto, kai tik šis dokumentas bus sukurtas. Tuo atveju, jei vartotojai šio reikalavimo griežtai laikosi, DEP servisą galima laikyti saugiu.

PDV serviso, kaip ir DEP serviso atveju silpniausia grandis saugumo prasme yra 6. Dėl elektroninio pašto pažeidžiamumo, vartotojai neturėtų šiuo servisu pasitikėti, išskyrus atvejus, kai jie pasitiki savo vietiniu tinklu ir interneto paslaugų tiekėju (tais atvejais, kai naudojama lokali elektroninio pašto klientinė programinė įranga) arba elektroninio pašto paslaugų tiekėju (jei naudojama internetinė elektroninio pašto sistema, turinti www vartotojo sąsają). Atvejais, kai pasirašytų dokumentų validavimas yra atliekamas reguliariai, yra naudotina speciali klientinė programinė įranga, įdiegiama vartotojo kompiuteryje, o PDV serviso naudojimas nerekomenduojamas.

1.3. Asmens identifikavimas per bankų sistemą

Šiuo metu e.paslaugoms teikti reikalinga asmens identifikavimo procedūrą atlieka Lietuvos bankai per savo e.bankininkystės sistemas. Tai nėra pats saugiausias būdas. Jis paremtas pasitikėjimu banku, ir tarp banko ir kliento. Todėl šiuo metu susiklosčiusi situacija verčia valstybę teikiančią e.valdžios paslaugas pasitikėti privačiomis struktūromis – bankais.

Dešimt Lietuvos komercinių bankų 2007 metų spalio pradžioje turėjo 1,62 mln. internetinės bankininkystės paslaugų vartotojų - 40 proc. daugiau nei pernai tuo pačiu metu, kai jų skaičius siekė 1,16 milijono. Palyginti su šių metų pradžia, kai bankai turėjo 1,31 mln. internetinės bankininkystės naudotojų, jų skaičius išaugo 24 proc., rodo bankų BNS pateikti duomenys.

Bankai prognozuoja, kad 2007 metų pabaigoje jie turės 1,72 mln. šių paslaugų vartotojų. Beveik tokią pačią prognozę (1,73 mln.) bankai buvo pateikę ir šių metų pradžioje [23].

"Vartotojai, kurie anksčiau galbūt dvejojo interneto nauda jų gyvenime, dabar jau įpranta tvarkyti savo finansinius reikalus internetiniame banke ir tai tampa neatsiejama gyvenimo dalimi", - BNS sakė "Hansabanko" produktų ir elektroninių kanalų departamento direktorius Ramūnas Strauka. Pasak jo, 40 proc. per metus išaugęs vartotojų skaičius rodo, kad pasitikėjimas internetine bankininkyste šalyje stiprėja.

Internetinės bankininkystės lyderiu išlieka "Hansabankas", spalio pradžioje turėjęs 668,1 tūkst. internetinės bankininkystės klientų - 31,6 proc. daugiau nei pernai spalio 1-ąją (507,5 tūkst.).

SEB Vilniaus bankas spalio pradžioje turėjo 606 tūkst. šių paslaugų vartotojų. Per metus šis skaičius išaugo 35 procentais.

Į internetinės bankininkystės lyderių trejetuką taip pat patenka "DNB Nord" bankas, kuris per metus šių paslaugų vartotojų skaičių padidino 50 proc. iki 160,8 tūkstančio.

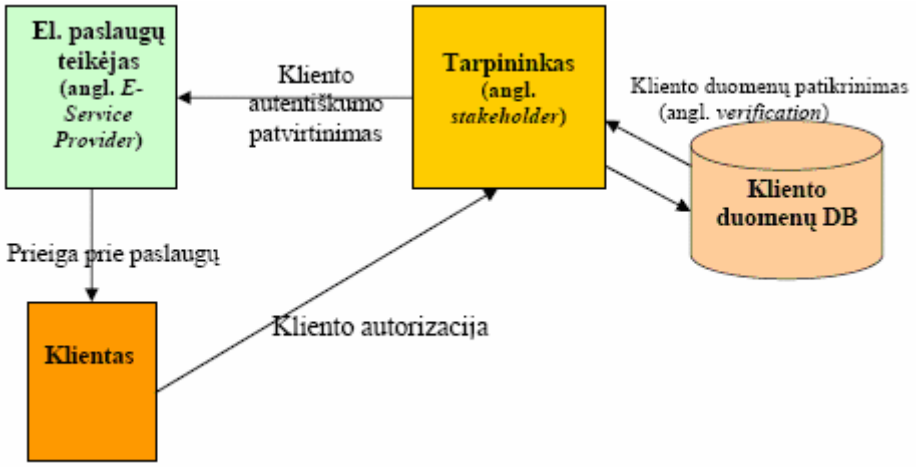
Iš šių trijų bankų prognozių nepakeitė tik "Hansabankas", kuris, kaip ir metų pradžioje, 2007-ųjų sausio 1-ąją tikėjosi turėti apie 706,6 tūkst. internetinės bankininkystės klientų. Tuo tarpu SEB Vilniaus bankas prognozes sumažino nuo 650 tūkst. iki 640 tūkst., o "DNB Nord" - nuo 180 tūkst. iki 170 tūkst. Nuo internetinės bankininkystės lyderių kiek atsilieka "Snoras", kuris spalio pradžioje turėjo 68,8 tūkst. internetinės bankininkystės klientų - 66,5 proc. daugiau nei pernai tuo pat metu (41,3 tūkst.). Internetinės bankininkystės "vidutiniokais" spalio pradžioje buvo bankai "Sampo", "Nordea Bank Lietuva" ir Ūkio bankas, turėję po daugiau nei 25 tūkst. šių paslaugų klientų."Parex" šiemet spalio 1-ąją turėjo 10,7 tūkst. internetinės bankininkystės klientų ir pagal šį rodiklį aplenkė Šiaulių banką (10,5 tūkst.). Dar šių metų viduryje Šiaulių bankas lenkė "Parex" banką.

Tačiau tai nereiškia, kad tiek Lietuvos žmonių naudojosi, nes vartotojais gali būti tiek fiziniai tiek juridiniai asmenys (direktorius gali būti vartotojas ir kaip fizinis ir kaip įgaliotasis juridinio asmens), bei vienas asmuo gali būti kelių e.bankininkystės sistemų vartotoju.

Norint pasinaudoti viešąja elektronine paslauga elektroninių valdžios vartų portale, identifikuojant save per bankų sistemą, pirmiausia reikėtų pasirinkti banką, kuriame turima prisijungimo prie elektroninės bankininkystės sistemos galimybę [43]. Šiuo metu e-valdžios portale gali identifikuotis šių bankų elektroninės bankininkystės sistemų vartotojai: AB „SNORAS“, AB „Hansabankas“, AB „SAMPO“, AB „DnB NORD“, AB „SEB Vilniaus bankas“, AB „PAREX“, AB „Šiaulių bankas“. Reikia būti pasirašiusiam elektroninių paslaugų sutartį (priedas Nr.5). Prisijungus prie banko, asmuo paklausiamas dėl asmens kodo naudojimo ir

turi sutikti, kad bankas suteiktų šiai sistemai vartotojo asmens kodą. Tokiu būdu yra užtikrinama tapatybė. Asmuo, davęs sutikimą suteikti asmens kodą, grąžinamas į šią sistemą ir gauna laikiną elektroninio dokumentų pasirašymo galimybę , todėl gali matyti bei pasirašyti elektroninius dokumentus.

Schema su tarpininku taikomos daugelyje šalių, kaip laikina klientų autentifikavimo priemonė, kol nebus sukurta funkcionuojanti PKI ir išleistos ID kortelės [4]. Tokios schemos yra grynai komercinio pobūdžio (mokamų tarpininkavimo paslaugų teikimas). Tokias paslaugas teikia komercinės organizacijos, turinčios dideles klientų duomenų bazes (bankų e.bankininkystės sistemos, telekomunikacijų kompanijos). Tokių schemų saugumas yra žymiai mažesnis už PKI naudojančias schemas. Visas saugumas remiasi paslaugų teikėjo pasitikėjimu savo klientais (ir pastarųjų baudimu (banko arba telekomunikacijų) paslaugų teikimo nutraukimu arba netgi patraukimu teismo atsakomybėn), o taip pat vartotojo pasitikėjimu paslaugų teikėjo sąžiningumu. Todėl tokios paslaugos reikalauja papildomų, nestandartinių teisinės ir techninės kontrolės sprendimų. Žemiau pateikta paprasta autentifikacijos schema su tarpininku.



6 pav. Paprasta autentifikacijos schema su tarpininku

- Tarpininkas autorizuoja klientą pagal nustatytą schemą (pvz., banko kortele) ir perduoda autentifikavimo duomenis.
- Tarpininkas sutikrina gautus savo kliento duomenis su DB patalpintais duomenimis, ir sėkmės (t.y. duomenų atitikimo) atveju patvirtina kliento autentiškumą elektroninių paslaugų teikėjui (SP).
- El. paslaugų teikėjas suteikia klientui prieigą prie teikiamų paslaugų.

Šiuo metu tokia schema naudojasi e.paslaugų teikėjai autentifikuojantys klientus per e.bankininkystės sistemas.

Kiekviena Interneto bankininkystės autentifikavimo sistema turi būti užregistruota e-valdžios portale su tokiais parametrais:

- Unikalus ID
- Pavadinimas
- Pradinio autentifikavimo puslapio Interneto adresas (URL). Į šitą adresą bus persiunčiama autentifikavimo procedūros inicijavimo komandą su nuoroda į šaltinį – Komiteto Portalą. Tuomet banko sistemoje po sėkmingo autentifikavimo galėtų būti realizuotas automatinis atgalinis peradresavimas ir autentifikavimo paketo grąžinimas į Portalą.
- Banko viešas raktas gaunamų iš banko paketų skaitmeninio parašo kontrolei

Kiekvieno banko sistemoje turi būti užregistruoti ir naudojami tokie parametrai:

- Portalo puslapio Internet adresas (URL), į kurį nukreipiamas vartotojas, sėkmingai praėjęs autentifikavimo procedūrą ir į kurį nusiunčiamas autentifikavimo paketas
- Banko privatus raktas skaitmeninio parašo pagaminimui
- Komiteto viešas raktas gaunamų iš Komiteto Portalo paketų skaitmeninio parašo kontrolei

Banko portalo serverių laikrodžiai turi būti sinchronizuojami su Internet atominiais laikrodžiais, nes vienas iš autentifikavimo paketo parametru yra tikslus autentifikavimo laikas. Toks pat reikalavimas galioja ir Portalo serveriams.

Banko portale turi būti realizuotas autentifikavimo paketų formavimo ir nukreipimo į Portalą priemonės pagal žemiau išdėstytus techninius reikalavimus.

Normaliame darbo režime, banko portalo puslapiuose turi būti nuorodos, meniu arba kiti valdymo elementai, kurių pagalba sėkmingai autentifikuotas banko sistemoje vartotojas galėtų interaktyviai inicijuoti perėjimą į Portalą be pakartotino autentifikavimo.

Autentifikavimo duomenų perdavimas realizuojamas „Server - Client – Server“ principu, kuomet persijungimai tarp portalų ir autentifikavimo paketų persiuntimai fiziškai realizuojami per Internet naršyklę vartotojo lokaliame kompiuteryje, nors inicijuojami ir transportuojami duomenys generuojami Portalo ir banko portalų serveriuose.

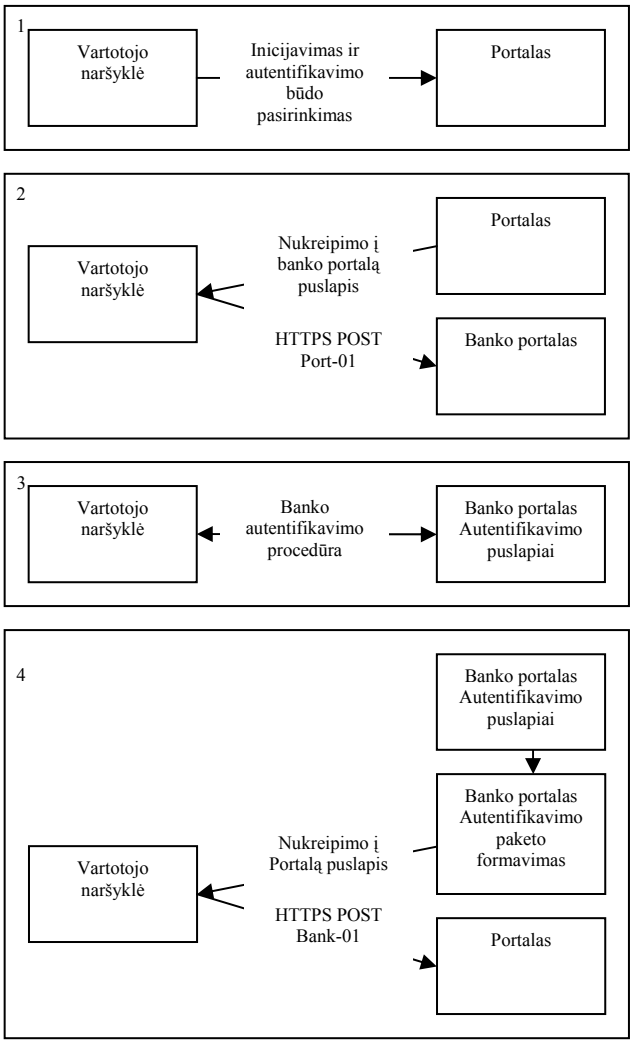
Integruotas autentifikavimas vyksta 2 būdais:

- Vartotojas pradeda darbo seansą Komiteto Portale

iliustruoja šitą scenarijų:

1. vartotojas pradėjo darbą Portale, pasirenka norimą banką pagal iš anksto užregistruotų bankų sąrašą ir paspaudžia autentifikavimo pradžios mygtuką.
2. inicijuojamas peradresavimas į pasirinkto banko portalo pradinį puslapį HTTPS POST metodu, perduodant parametrus, identifikuojančius Portalą (paketas Port-01).
3. banko portale vyksta įprasta vartotojo autentifikavimo procedūra.

4. sėkmingai identifikavus vartotoją, banko portale suformuojamas autentifikavimo paketas. Automatiškai inicijuojamas peradresavimas į Portalą, persiunčiant autentifikavimo paketą HTTPS POST metodu (paketas BANK-01).



7 pav. 1 Seanso inicijavimas Komiteto Portale

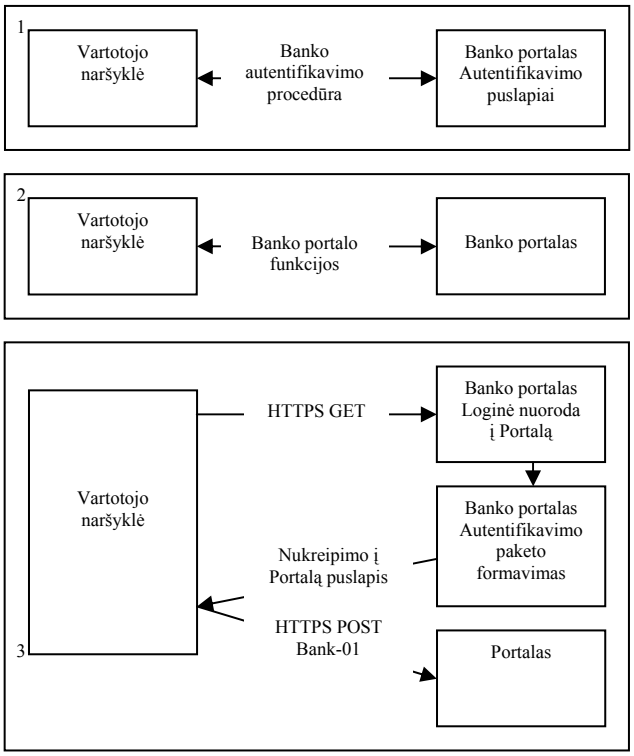
- Vartotojas pradeda darbo seansą banko portale

iliustruoja šitą scenarijų:

1. vartotojas iš karto pradeda darbo seansą banko portale ir praeina įprasta autentifikavimo procedūra.

2. vartotojas vykdo banko portale norimas funkcijas

3. numatytame banko portalo skyriuje vartotojas pasirenka perėjimą prie Portalo ir paspaudžią atitinkamą mygtuką. Tuomet banko portale suformuojamas autentifikavimo paketas ir automatiškai inicijuojamas peradresavimas į Portalą, persiunčiant autentifikavimo paketą HTTPS POST metodu (paketas BANK-01).



8 pav. 2 Seanso inicijavimas banko portale

Banko sistemoje turi būti nustatomi ir perduodami Komiteto Portalui tokie vartotojo autentifikavimo duomenis:

- Asmens kodas
- Vardas
- Pavardė
- Vartotojo autentifikavimo banko sistemoje einamasis laikas sekundės tikslumu.

Tekstiniai paketo duomenys pateikiami standartinėje *Windows Baltic* koduotėje *windows-1257*.

Autentifikavimo duomenis perduodami Komiteto Portalui atskiruose paketo BANK-01 parametruose.

Autentifikavimo metu pateikti fizinio asmens duomenys Portalui bus papildomai sutikrinami su galiojančiais Lietuvos Respublikos Gyventojų registro įrašais. Pateiktų autentifikavimo duomenų nesutapimo su turimais galiojančiais Lietuvos Respublikos Gyventojų registro duomenimis atvejais, pateikti autentifikavimo paketai bus atmetami Portalo pusėje.

Komiteto Portalo pusėje asmens identifikavimui bus naudojamas tik asmens kodas, tuo metu, kai vardas ir pavardė tarnauja tik autentifikavimo žurnalo pildymui ir neautomatizuotam konfliktinių situacijų sprendimui. Tuo atveju, jeigu vardas arba pavardė pagal ilgį netilps į pakete BANK-01 nustatytą simbolių limitą, turi būti atmetama perteklinė simbolių dalis ir tai neturi pakenkti asmens identifikavimui Portale.

Duomenų transportavimo saugumas užtikrinamas HTTPS protokolu, kuriuo vyksta duomenų apsikeitimas, kaip nukreipiant vartotoją tarp Portalo ir banko portalų, taip ir tų portalų viduje.

Autentifikavimo duomenys turi būti skaitmeniniu būdu pasirašomi su banko privačiu raktu, pritaikant algoritmą **RSASSA-PKCS1-v1_5** su **SHA-1** HASH-funkcija. Porinis banko viešas raktas, naudojamas parašo kontrolei, turi būti perduotas Komitetui ir užregistruotas Portale galutinės sutarties sudarymo momentu. Skaitmeninis parašas turi būti išskaičiuojamas tekstinei eilutei, sudarytai iš visų autentifikavimo duomenų parametrų

SRC || *TIME* || *PERSON_CODE* || *PERSON_FNAME* || *PERSON_LNAME*

Čia || - yra tekstinių eilučių apjungimo operacija, o ne skiriamieji simboliai. Parametrų vardai pateikti pagal paketą BANK-01. Išskaičiuotas skaitmeninis parašas turi būti perduodamas Komiteto Portalui atskirame paketo BANK-01 parametre.

Vartotojo nukreipimo į banko portalą parametrai (paketas Port-01) turi būti pasirašyti Portalo pusėje, siekiant užtikrinti kreipinio šaltinio autentiškumą. Pasirašoma su Komiteto privačiu raktu, pritaikant algoritmą **RSASSA-PKCS1-v1_5** su **SHA-1** HASH-funkcija (tokį pat, kaip ir autentifikavimo duomenų pasirašymo atveju).

Skaitmeninis parašas turi būti išskaičiuojamas tekstinei eilutei, sudarytai iš nukreipimo duomenų paketo parametrų

SRC || *TIME*

Čia || - yra tekstinių eilučių apjungimo operacija, o ne skiriamieji simboliai. Parametrų vardai pateikti pagal paketą Port-01. Porinis Komiteto viešas raktas, naudojamas parašo kontrolei, turi būti perduotas bankui galutinės Portalo sutarties sudarymo metu.

Apsaugai nuo pakartotino to pačio autentifikavimo paketo panaudojimo, numatytas autentifikavimo paketo parametras – tikslus paketo formavimo laikas (TIME). Šis parametras įeina į pasirašomą tekstinę duomenų eilutę, todėl negali būti padirbtas perdavimo metu, kaip ir kiti pasirašyti parametrai.

POST Paketai, Port-01 - Šitas parametrų paketas siunčiamas iš Portalo į banko portalo pradinį autentifikavimo puslapį HTTPS POST metodu.

Konkretaus banko puslapio adresas (URL) registruojamas Portale kartu su kitais banko parametrais – identifikatoriumi, pavadinimu ir viešu raktu.

2 lentelė. Paketo parametrų struktūra:

Parametras	Maksimalus ilgis	Paskirtis
SRC	20	Užklausos šaltinio kodas - **Komiteto įstaigos kodas**
TIME	20	Vartotojo nukreipimo iš Portalo į banko portalą data ir laikas sekundžių tikslumu. Data perduodama tekstiniame pavidale formate ***YYYY.MM.DD hh:mm:ss***
SIGNATURE	100	SRC ir TIME parametrų Komiteto skaitmeninis parašas, konvertuotas į BASE64 formatą. Parašas išskaičiuojamas pagal algoritmą, aprašytą *3.4. Portalo nukreipimų į banko portalą pasirašymas.*
TYPE	10	Užklausos tipas. Fiksuota reikšmė: *Port-01*
SRC	20	Užklausos šaltinio kodas – **banko kodas.**
TIME	20	Vartotojo nukreipimo iš Portalo į banko portalą data ir laikas sekundžių tikslumu. Data perduodama tekstiniame pavidale formate ***YYYY.MM.DD hh:mm:ss***
PERSON_CODE	20	Asmens kodas
PERSON_FNAME	100	Asmens vardas
PERSON_LNAME	100	Asmens pavardė
SIGNATURE	300	Autentifikavimo duomenų skaitmeninis banko parašas, konvertuotas į BASE64 formatą. Parašas išskaičiuojamas pagal algoritmą, aprašytą *3.3. Autentifikavimo duomenų pasirašymas*
TYPE	10	Užklausos tipas. Fiksuota reikšmė: *BANK-01*

BANK-01 - Šitas parametrų paketas siunčiama HTTPS POST metodu iš banko portalo į Portalo autentifikavimo puslapį adresu

http://paslaugos.evaldzia.lt/remote.php?ru=bS9tX2JhbmsvYWRtaW4vYV9mcm9tX2JhbmsucGhw

1.4. Asmens tapatybės kortelės

Lietuvoje asmens identifikavimo tikslais šiuo metu išduodama asmens tapatybės kortelė turi tik vizualią informaciją, ir neturi jokio lusto. Kitų šalių patirtis rodo, kad tapatybės kortelės (angl. ID cards, smartcards) su lustu (-ais) gali žymiai praplėsti kortelės funkcionalumą ir galimybes, ypatingai e.paslaugų atžvilgiu. Be to tokios lustinės kortelės gali būti išduodamos ir užsieniečiams besilankantiems Lietuvoje integruojant lustus į leidimus laikinai/nuolat gyventi. 2006 rugsėjo mėn. paruoštas investicinis projektas (galimybių studija) "Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas" [4]. Projektą vykdo Lietuvos Respublikos vidaus reikalų ministerija (atsakingasis partneris) ir Asmens dokumentų išrašymo centras prie VRM [59].

Pagrindinės lustinių kortelių funkcijų grupės ir poreikis joms:

- elektroninė asmens identifikacija. Šiuo metu esanti vizualinė asmens identifikacija netenkina tobulėjančių tapatybės vagystės ir kortelių falsifikavimo priemonių. Kyla poreikis padidinti kortelės apsaugą nuo falsifikavimo, bei atlikti tikslesnę asmens identifikaciją asmens biometrinių duomenų pagalba. Šie uždaviniai buvo įgyvendinti sukuriant naujus biometrinius pasus, kuriuos išduoda ir Lietuva. Šių naujos kartos pasų specifikacijos standartai apibūdinti ICAO doc 9303 standarte ir ES pasų specifikacijose. Nors ir ES neturi teisinio pagrindo reglamentuoti tapatybės kortelių išdavimą, tačiau numatoma išleisti rekomendacinio pobūdžio teisės aktus, kurie nustatytų kortelėms tokius pačius standartus kaip ir pasų atveju. Be to ruošiamas reglamentas leidimų gyventi atžvilgiu, kuriems numatoma taip pat nustatyti e.pasų pavyzdžio standartus. Todėl rekomenduojama į tapatybės korteles ir leidimus gyventi integruoti elektroninės identifikacijos funkciją taip vadinamu ICAO formatu;
- e.parašo funkcionalumas. E.parašas turi dvi skirtingas raktų poras skirtingoms funkcijoms atlikti: viena asmens autentifikacijai nuotoliniu būdu norint naudotis nuotolinėmis e.paslaugomis, ir kita e.dokumentų pasirašymui. ES Taryba 2001 m. nustatė 20 prioritetinių elektroninių viešųjų paslaugų, kurios buvo patvirtintos ir Lietuvos strateginiuose dokumentuose [34]. Šiuo metu visos šitos paslaugos intensyviai perkeliamos į e.terpę. Visoms joms reikalinga asmens identifikacija nuotoliniu būdu. Tam šiuo metu naudojamos komercinės struktūros (e.bankininkystės sistemos), kurios turi kelis esminius trūkumus: saugumas remiasi pasitikėjimu banku ir banko pasitikėjimu savo klientais, neįmanoma tiksli vartotojo autentifikacija, kiekvienam paslaugų teikėjui reikės dubliuoti tokių sistemų integracijos darbus. Komercinių struktūrų siūlomi e.parašo sprendimai kainuoja pakankamai brangiai. Todėl valstybės lygiu kyla poreikis sukurti valstybinę asmens autentifikacijos e.valdžios paslaugoms teikti sistemą, kuri būtų paremta e.parašu. Vis dažniau piliečiams naudojantis e.paslaugomis palaipsniui iškils poreikis ir sandorius sudaryti e.terpėje. Tam irgi būtinas e.parašas.
- e.paslaugų funkcionalumas. Šiuo metu kuriamoms įvairioms e.paslaugoms numatoma išduoti lustines korteles. Jos skirtos tiek asmeniui identifikuoti sistemoje, tiek saugoti paslaugai reikalingus duomenis, kuriuos galima panaudoti neprisijungus prie paslaugos DB (off-line režimu). Be to Lietuvoje daugelis komercinių organizacijų išduoda didelį kiekį skirtingų kortelių skirtų praėjimo kontrolei (bibiliotekos, sporto klubai, ofisų praėjimo kontrolei) bei lojalumo/nuolaidų tikslais (įvairios parduotuvės, video nuomos punktai). Asmuo per kelis metus surenka didelį pluoštą kortelių kuriose dažnai netgi dubliuojama informacija. Natūralu, kad asmuo norėtų turėti tik vieną kortelę. Žemiau pateiktos e.paslaugos, kurios numato ar jau išduoda įvairaus tipo korteles:
  - e.bilietai (viešajame transporte, koncertuose ir pan.),
  - e.sveikatos aplikacijos (e.receptas, e.paciento kortelė ir kt.),

- socialinio draudimo aplikacijos ir pašalpos,
- praėjimo kontrolės autorizavimo aplikacijos,
- e.lojalumo programos.

Pagrindinis projekto rezultatas: išrašoma daugiafunkcinė mikroprocesorinė asmens tapatybės kortelė su dviem įmontuotais (angl. embedded) nepriklausomais lustais (angl. chips) (mikroprocesoriais):

1. pirmasis lustas – kontaktinis, su kelių aplikacijų įdiegimo ir priežiūros galimybėmis (daugiaaplikacinis). Jame įdiegtos:

a. pagrindinė aplikacija. PKI aplikacija arba e.parašo aplikacija, skirta elektroninės valdžios e.paslaugų vartotojų patikimai elektroninei autentifikacijai (eAuthentication su PIN arba biometrinių duomenų teikiama apsauga) užtikrinti;

b. papildomos aplikacijos (diegiamos po kortelės išdavimo (angl. post-issuing applications)): gali būti diegiamos (ir šalinamos iš jo) aplikacijos, turinčios bet kokius identifikacinius arba konfidencialius kortelės turėtojo (angl. card holder) duomenis (pvz., elektroninį receptą).

2. antrasis lustas – nekontaktinis, su kelių aplikacijų įdiegimo ir priežiūros galimybėmis (daugiaaplikacinis). Šis lustas turi atitikti reikalavimus rinkmenų struktūrų priežiūrai, taip pat reikalavimus biometriniams duomenims. Jame įdiegtos:

a. pagrindinė aplikacija. ICAO LDS formato MRTD aplikacija, skirti patikimai fizinei identifikacijai;

b. papildomos aplikacijos (diegiamos po kortelės išdavimo (angl. post-issuing applications)): gali būti diegiamos (ir šalinamos iš jo) aplikacijos, neturinčios jokių identifikacinių arba konfidencialių kortelės turėtojo duomenų, tačiau reikalaujančios užtikrinti minimalią kriptografinę apsaugą (DES šifravimo algoritmo ir/arba elektroninio parašo) (pvz., transporto e.bilietai, prekių ir paslaugų nuolaidų kortelėms, socialinėms lengvatoms, praėjimo kontrolei).

Pagrindinis projekto tikslas: aprūpinti Lietuvos piliečius asmens tapatybės kortele, kuri šalia pagrindinės dokumento paskirties – vizualios verifikacijos - vykdytų elektroninio asmens identifikavimo bei elektroninio parašo funkcijas ir suteiktų galimybes asmenims naudotis e.valdžios bei kitomis e.paslaugomis. Projekto rezultate sukurtą daugiafunkcinių asmens tapatybės kortelių išrašymo sistemą turi būti galima pritaikyti ir daugiafunkcinių leidimų gyventi užsieniečiams išrašymui su tokia pačia struktūra, atsižvelgiant į ES kuriamą teisinę bazę šių dokumentų srityje.

Šio projekto kaip papildomas sukuriamas rezultatas –sukurta PKI infrastruktūra, reikalinga e.parašo raktų valdymui po kortelės išdavimo.

Projektas atitinka BPD 3.3 gairių pareiškėjams specifiniams atrankos kriterijams:

- BPD 3.3 priemonės remiama veiklos sritis „Elektroninių viešųjų paslaugų plėtra“; 5 pogrupis „Viešosios elektroninės paslaugos“;
- daugiafunkcinė mikroprocesorinė kortelė bus naudinga labai didelei Lietuvos gyventojų daliai, nes ją privalo išsiimti visi gyventojai, kuriems sukanka 16 metų;
- projektas atitinka šiuos Vidaus reikalų ministerijos programinius tikslus:
  - sukurti skaidrią, veiksmingą, orientuotą į rezultatus ir tinkamą asmenų aptarnavimą viešojo administravimo sistemą, pagrįstą informacinėmis technologijomis,
  - plėtoti saugių informacinių ir ryšių technologijų infrastruktūrą, skatinti viešųjų paslaugų teikimą naudojant skaitmenines technologijas,
  - įgyvendinti valstybės politiką laisvo asmenų judėjimo, vizų, prieglobsčio ir migracijos srityse, plėtoti asmens dokumentų išdavimo sistemą, modernizuoti esamas ir kurti naujas su LR piliečių ir užsieniečių migracijos procesų valdymu susijusias duomenų bazes ir registrų sistemas, tobulinti valstybės valdžios, valdymo įstaigų ir institucijų, taip pat piliečių ir užsieniečių aptarnavimą,
  - skatinti Lietuvos regionų informacinės visuomenės ir žinių bei informacinės infrastruktūros plėtrą.

Projekto uždaviniai:

- sukurti infrastruktūrą, technines ir programines priemones reikalingas daugiafunkcinei mikroprocesorinei asmens tapatybės kortelei išrašyti,
- sukurti PKI infrastruktūrą sėkmingam e.parašo naudojimui,
- pasiekti kritinį e.parašo vartotojų skaičių,
- sukurti universalią platformą kortelėje, kuri leistų į ją įrašyti įvairias e.paslaugų aplikacijas,
- sukurti e.parašo infrastruktūros valdymo dokumentaciją,
- informuoti Lietuvos visuomenę apie naujas tapatybės kortelės funkcijas,
- informuoti e.paslaugų teikėjus apie galimybę pasinaudoti daugiafunkcine kortele teikiant e.paslaugas.

Projekto nauda gyventojams ir ūkio subjektams:

- kortelės pagalba bus suteikta galimybė saugiau naudotis e.paslaugomis, o tai suteiks:
  - Mobilumą - nepriklausomybę nuo asmens geografinės padėties;

- Geresnes galimybes neįgaliems asmenims pasinaudoti e.paslaugomis;
- Nepriklausomybę nuo paslaugų teikėjų darbo laiko – galimybę atlikti e.paslaugą ne darbo metu;

- kortelės pagalba bus suteikta galimybė įvairius sandorius atlikti elektroniniu būdu (e.parašo pagalba), o tai suteiks tokius pačius privalumus kaip ir aukščiau išdėstytame punkte;
- aukštesnis kortelės ir tapatybės saugumas – kortelę bus sunku padirbti ar pavogti kito asmens tapatybę,
- kortelė suteiks galimybę ją naudoti kaip kelionės dokumentą, nes ji atitiks paso funkcionalumą;
- sumažės gyventojų turimų ir įvairių paslaugų teikėjų išleidžiamų kortelių skaičius, pakeičiant jas aplikacijomis vienoje tapatybės kortelėje – padidės gyventojų patogumas ir bus sutaupomos kortelių išdavimo (gamybos) sąnaudos.

Projekto nauda pareiškėjui ir partneriams:

- bus aukštesnis e.paslaugų teikimo saugumas ir tikslesnė bei saugesnė asmenų autentifikacija;
- pasai ir kortelės turės vienodą ICAO struktūrą asmens elektroninio identifikavimo tikslams, todėl nekils suderinamumo problemų įsigyjant įrangą asmens dokumentus išduodančiose Migracijos tarnybose ir diplomatinėse atstovybėse, pasienio ir kituose dokumentų patikros postuose,
- padidės e.paslaugų integracija dėl naudojamos vienodos vartotojų identifikacinės priemonės, bei dėl e.paslaugų aplikacijų saugojimo vienoje kortelėje.

Prielaidos ir poreikis Gyvenamosios vietos deklaravimo elektroninei paslaugai sukurti:

- bus sukurtas e.valdžios portalas, kuris palaikys asmens identifikavimo ir apmokėjimo už e.paslaugas funkcionalumą;
- e.paslaugų teikėjai sutiks pakeisti korteles į aplikacijas tapatybės kortelėje;
- aktyvėjantis piliečių naudojimasis viešomis paslaugomis internetu;
- aktyvėjantis piliečių laisvas judėjimas po Europos ir kitas šalis;
- viešos e.paslaugos bus vystomos darniai, kartu visos Lietuvos ir ES mastu;
- bus palanki teisinė bazė e. paslaugų realizavimui;
- bus sukurta gera interneto prieigos infrastruktūra;
- vartotojų kompiuterinis raštingumas bus pakankamas e.paslaugos naudojimui;

Paslaugoms, kurios prieinamos daugiafunkcinių mikroprocesorinių kortelių pagalba paklausą turi tiek Lietuvos piliečiai, tiek užsieniečiai gyvenantys Lietuvoje. Lietuvoje išduodami šie asmens tapatybę patvirtinantys dokumentai:

9 pav. Asmens tapatybės kortelė, leidimas nuolat gyventi

Lietuvos piliečiams – asmens tapatybės kortelė, užsieniečiams – leidimai gyventi (nuolat ir laikinai) [57].

Potencialūs paslaugos vartotojai – visi Lietuvos ir užsienio piliečiai. Asmens tapatybės kortelę privaloma turėti tik nuo 16 metų amžiaus.

Šiuo metu išduodamos kortelės atitinka ID1 dydį pagal ICAO Doc. 9303 standartą (ISO 7810). Pagal susitarimą tarp ICAO ir ISO, mašininio nuskaitymo kelionės dokumentų (MRTD – machine readable travel documents) standartus nustato ICAO, o ISO pritaiko greitojo patvirtinimo (angl. "fast-track") procedūrą.

ICAO pagrindinis standartas reguliuojantis kelionės dokumentų parametrus yra Doc.9303. Šiuo metu galiojantis yra 6 leidimas. Šį dokumentą sudaro trys dalys:

- 1 dalis – pasų standartas,
- 2 dalis – vizų standartas,
- 3 dalis – kitų kelionės dokumentų (kortelių) standartas.

Visų šalių narių prašymu ICAO nusprendė standartizuoti biometrinių duomenų įrašymą į MRTD. Standarto kūrimu užsiima TAG/MRTD (Technical Advisory Group - MRTD techninių patarėjų grupė). Šiuo metu yra standartizuotas tik biometrinių duomenų įrašymas į pasus. Todėl 1 dalis turi du tomus: pirmame apibrėžiami įprastieji pasai, o antrame su biometrijos integravimu į pasus susiję aspektai. Tačiau pažymima, kad antrame tome pateikti standartizacijos aspektai gali būti identiškai pritaikyti ir kortelių atveju.

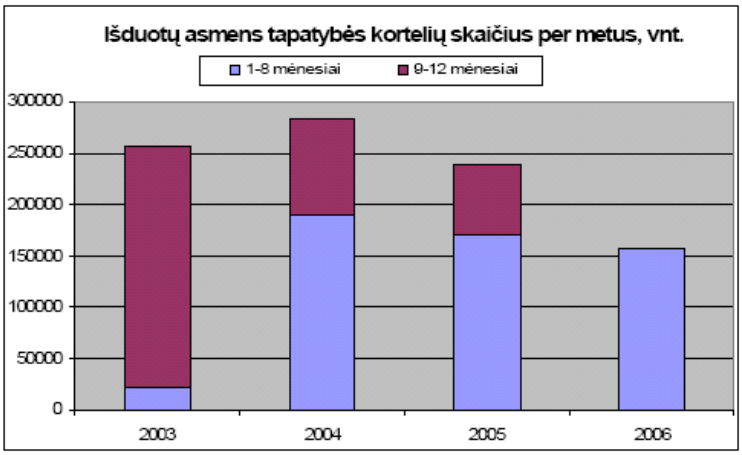
Šiuo metu Lietuvoje išduodamose kortelėse nėra integruota jokių lustų. Todėl jos turi tik vizualinę informaciją ir barkodą.

Daugelio funkcijų asmens tapatybės kortelės būtų naudojamos kaip priemonė gauti

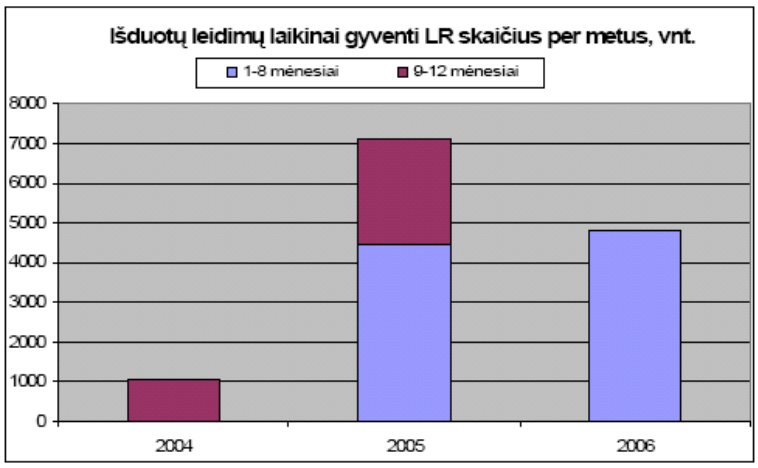
įvairias viešąsias paslaugas elektroniniu būdu. Daugumos viešųjų paslaugų teikimui el. terpėje trečiame ir ketvirtame brandos lygmenyje reikalingas technologiškai patikimas asmens tapatybės identifikavimas. Vienintelis teisiškai pripažintas ir įgyvendintas daugelyje valstybių asmens tapatybės elektroninis nustatymo būdas yra el. parašo infrastruktūra. Dėl to norint teikti bet kokias viešąsias paslaugas el. terpėje 3 arba 4 brandos lygmenyje turi būti įgyvendintas projektas, leidžiantis kiekvienam Lietuvos piliečiui gauti priemonę, kurioje bus saugomas tapatybę patvirtinantis elektroninis parašas.

Lietuvai įstojus į Europos Sąjungą ypač svarbus uždavinys – sukurti priemones, sudarančias sąlygas naudotis elektroniniu parašu e-valdžios funkcijų įgyvendinimui bei e-valdžios viešųjų paslaugų teikimui, tiek nacionaliniame tiek Europos lygmenyje: mokesčių mokėjimas, mokesčių, gyvenamosios vietos ir pan. deklaravimas, registracijos, pažymų gavimas bei pateikimas, valstybės tarnautojo identifikavimas, vykdant el. valdžios funkcijas, dokumentų autentiškumo užtikrinimas, įėjimo kontrolė ir pan. Neįgyvendinus šio projekto, Lietuva ateityje negalės visapusiškai dalyvauti diegiant ir teikiant elektronines viešojo sektoriaus paslaugas Europos Sąjungos mastu. Projekto įgyvendinimas taip pat būtinas siekiant Lietuvos Respublikos Vyriausybės (2000-02-08 nutarimu Nr.229 „Dėl Lietuvos nacionalinės informacinės plėtros koncepcijos“) patvirtintoje koncepcijoje įvardintų strateginių tikslų bei siekiamo rezultato - išduoti mikroprocesorines korteles su elektroniniu parašu e-valdžios funkcijų vykdymui ir darbui su elektroniniais dokumentais.

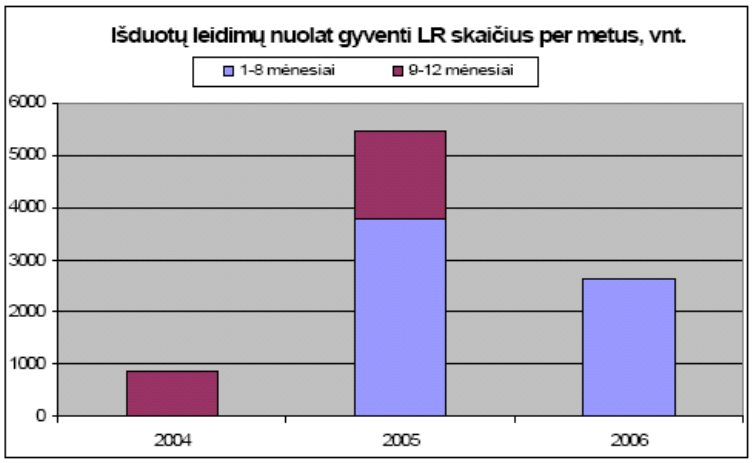
Pateikiami statistiniai duomenys [47]:



10 pav. Išduotų asmens tapatybės kortelių skaičius per metus



11 pav. Išduotų leidimų laikinai gyventi LR skaičius per metus



12 pav.Išduotų leidimų nuolat gyventi LR skaičius per metus

Vidaus reikalų ministerija ir jai pavaldus Asmens dokumentų išrašymo centras yra tiesiogiai atsakingos už asmens tapatybės kortelės išrašymą. Ministerijai ir jai pavaldžioms įstaigoms priklauso išimtinė kompetencija įgyvendinti valstybės politiką vizų ir imigracijos, prieglobsčio ir Lietuvos Respublikos pilietybės procedūrų, asmens tapatybę ir pilietybę patvirtinančių dokumentų, kelionės dokumentų, leidimų gyventi Lietuvos Respublikoje ir kitų dokumentų išdavimo ir apskaitos, gyvenamosios vietos deklaravimo ir laisvo asmenų judėjimo srityse (VRM nuostatai 1.14 punktas).

Vidaus reikalų ministerija kartu su ADIC kasmet vykdo ADIS atnaujinimo darbus, skelbia viešuosius pirkimus ir užtikrina sėkmingą sistemos funkcionavimą. 2006 metais buvo atnaujinta dokumentų išrašymo sistema integruojant į juos biometrinius duomenis pagal ES nustatytas pasų specifikacijas ir ICAO reikalavimus. Todėl ADIC su VRM turi patirtį išrašant dokumentus su bekontakčiu lustu pagal ES specifikacijas ir ICAO reikalavimus. Taip pat yra suformuota PKI infrastruktūra šiems dokumentas išrašyti ir apsaugoti.

ADIC darbuotojai naudojasi IVPK išduotomis tarnautojams skirtomis kortelėmis su

e.parašo funkcija. Todėl turi patirtį naudojant e.parašo funkcionalumą.

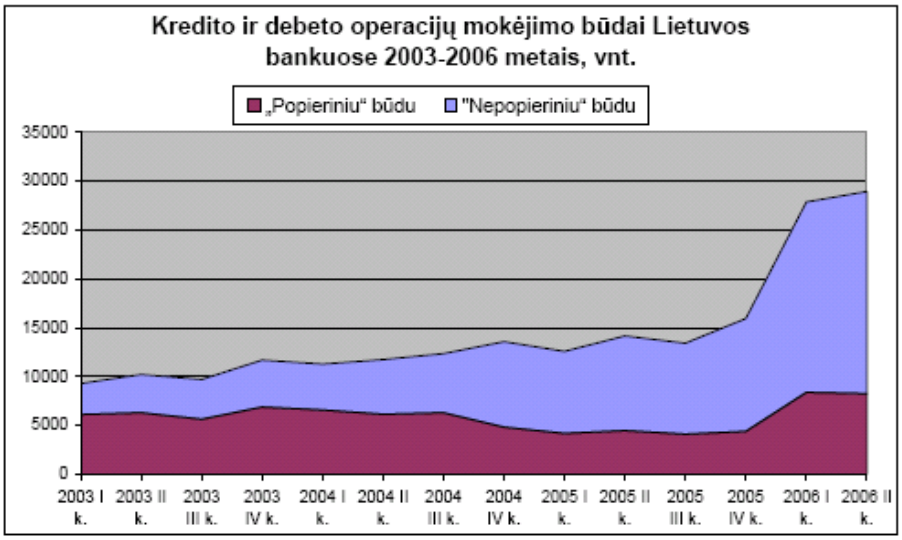
Projekto įtaką aplinkai galima apibrėžti šiais pagrindiniais aspektais:

- daugiafunkcinė mikroprocesorinė asmens tapatybės kortelė užtikrins tikslesnį asmens tapatybės nustatymą naudojant biometrinius duomenis, todėl sumažės tapatybės vagysčių atveju,
- įrašius asmens bendruosius ir biometrinius duomenis pagal ICAO LDS struktūrą, bus praktiškai neįmanoma sufalsifikuoti dokumento jo naudojimo fazėje,
- asmenys keičiantys ar naujai įsigyjantys kortelę kartu gaus ir e.parašą, kas padidins e.parašo vartotojų skaičių,
- bus sukurta patikima, valstybės įsteigta e.parašo infrastruktūra, ir išaugs gyventojų pasitikėjimas e.parašu,
- bus sukurtas papildomas ir saugesnis būdas identifikuoti asmenį teikiant e.paslaugas,
- asmuo turės galimybę pasirašyti dokumentus elektroniniu būdu,
- sumažės e.paslaugoms reikalingų ir lojalumo programų tikslais išduodamų kortelių skaičius, nes ši informacija galės būti saugoma vienoje asmens tapatybės kortelėje. E.parašo paklausą netiesiogiai sąlygoja e.paslaugų (ir ne tik e.valdžios paslaugų) pasiūla ir paklausa. Pastaruoju metu vis dažniau gyventojai naudojasi e.paslaugomis tiek e.valdžios, tiek privataus sektoriaus. Lietuvoje daugiausia vartotojų turi e.bankininkystės paslaugas teikiantys bankai ir Valstybinė mokesčių inspekcija teikianti pajamų mokesčio deklaravimo e.paslaugą.

Pagal Lietuvos banko statistiką, 2006 m. II ketvirtį Lietuvoje atlikta 28 954 kredito ir debeto pervedimų (Lietuvoje ir tarptautiniai pavedimai). Iš jų net 71,5 proc. buvo atlikti nepopieriniu būdu (elektroniniu duomenų perdavimo tinklu, internetu, telefonu, įrašu klientų sąskaitose). Nors šie skaičiai rodo ir fizinių ir juridinių asmenų atliekamas operacijas, tačiau dėsningumai aiškiai matomi žemiau pateiktame grafike.

Pagal VMI duomenis 2006 metais e.būdu deklaravo (už 2005 metus) 46 proc., o 2005 metais (už 2004 metus) – 25 proc. gyventojų.

Didėjanti e.valdžios ir e.paslaugų pasiūla, o tuo pačiu ir paklausa didina e.parašo poreikį.



13 pav. Kredito ir debeto operacijų mokėjimo būdai Lietuvos bankuose 2003-2006metais

2. NAUJAUSIŲ TECHNOLOGIJŲ TAIKYMAS SPRENDŽIANT ASMENS IDENTIFIKAVIMO PROBLEMAS

Kompiuterių sistemose vartojant slaptažodžius, dažniausiai kalbama apie tikimybę juos atspėti arba laiką, reikalingą jiems rasti, bandant visus įmanomus variantus. Taip savotiškai apibūdinamas sistemos saugumas. Nurodžius slaptažodį, sistema beveik negali apsirikti: pateikus galiojantį, leidžiama prisijungti. Ar tą slaptažodį parašė tikrasis vartotojas, ar piktavalis, visai nesvarbu [25].

Biometrijoje absoliutaus "slaptažodžio" nėra. Įtaisai privalo įvertinti šimtus ar net tūkstančius atskirų kūno detalių sąlygiškam "raktui" sukurti, kuris kiekvieno skaitymo metu gali būti vis kitoks. Tačiau vartotojas atpažįstamas tol. Kol "raktas" per daug nenukrypsta nuo iš anksto numatytų normų.

Biometrinių sistemų patikimumas apibrėžiamas trimis vertėmis:

FAR (False Acceptance Rate) – tikimybė, kad biometrinė sistema svetimą žmogų atpažins kaip savą . 0,0001 proc. rodo, kad vieną žmogų iš milijono sistema gali atpažinti, nors jo piršto anspaudo duomenų bazėje nėra. FAR turi būti kuo mažesnė, ypač jei biometriniai skaitytuvai pasikliauja tik vienos rūšies asmenybės patvirtinimu (pvz., piršto anspaudu) ir nereikalauja papildomai įvesti kodo ar pateikti kortelės.

FRR – (False Rejection Rate) – tikimybė, kad registruotas vartotojas bus neatpažintas (reikės dar kartą nuskaityti asmens duomeni). Tai nepavojinga, tačiau kelia nepatogumų vartotojams.

EER – (Equal Error Rate) – FAR ir FRR verčių aukso vidurys. Sujungus FAR ir FRR diagramas, ERR taške tikimybė būti neteisingai atpažintam yra vienoda. Kuo EER vertė mažesnė, tuo geriau.

Mažesnės FAR ir FRR vertės – geresnė sistema. Deja, mažinant FAR vertę (didinant patikimumą), dažniausiai padidėja FRR ir atvirkščiai. Kiekvieną biometrinę sistemą galima sureguliuoti taip, kad beveik nė vienas pašalinis asmuo nebūtų atpažintas kaip savas. Tačiau tokiu atveju ir registruoti vartotojai dažniausiai neatpažįstami. Nei FAR, nei FRR atskirai nepakanka sistemai tinkamai apibūdinti. Geriausia remtis EER duomenimis. Realiomis sąlygomis veikianti sistema turėtų būti vertinama esant FAR = 0 (kai blogiukai apskritai negali prisijungti).

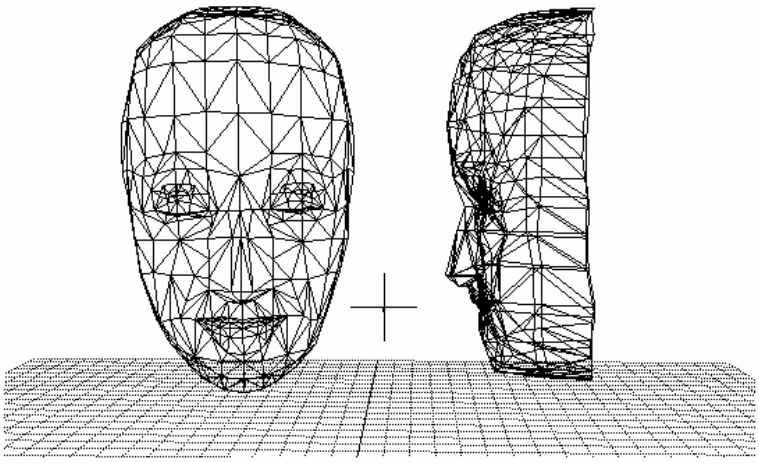
Pirštų antspaudai. Daugumos šiuolaikinių pirštų antspaudų skaitytuvų EER vertė yra pernelyg didelė – 1-5 proc. Geriausiu atveju pasiekiama 0,2-0,3 proc. EER vertės. Vis dėlto artimiausiu metu pirštų antspaudų apdorojimo algoritmai turėtų gerokai patobulėti . Pvz.

“Warwick Warp” bendrovė tiria būdus, kaip “išlyginti” suteptus, iškraipytus antspaudus. Taip būtų naudinga visiems: vartotojai skaitytuvus galėtų liesti beveik bet kaip, nesirūpindami, ar pirštas kryptelės ar nuslys, o teismo ekspertai galėtų pasinaudoti nusikaltimo vietose aptiktus prastos kokybės antspaudus, kurie dabar yra “nurašomi”.

14 pav. Pirštų antspaudai

Biometrinės sitemos apskritai paplis tada, kai neliks apribojimų. Pvz., juk nesvarbu kaip pakeliame telefono ragelį ir pridedame prie ausies – pašnekovą vis tiek girdime. Taip pat nesudėtingai turi veikti ir biometrinės sistemos.

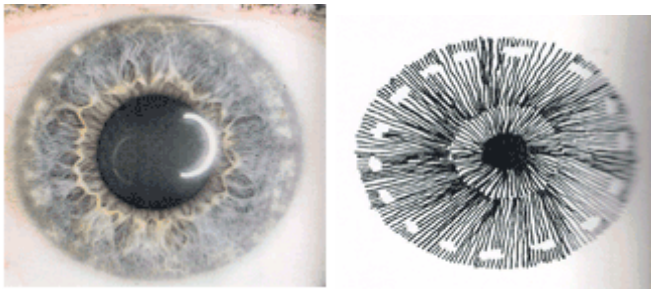
3D veido pažinimas – tai patobulintas žmogaus atpažinimo pagal veidą būdas. Iš pradžių dėl techninių priemonių ribotumo buvo taikomas dviejų matavimų vaizdo (nuotraukos) analizės metodas. Sparčiai plėtojantis technologijoms, šiandien 3D veido kopiją galima tirti pasitelkus paprastą įrangą.



15 pav. 3D veido atpažinimas

3D skaitytuvų neklaidina veido išraiškos, skirtingos apšvietimo sąlygos, makiažas ar galvos padėtis.

Akies rainelė – matomas spalvotas skritulys aplink juodą lęšiuką – yra tokia pat išskirtinė kaip ir pirštų antspaudai. Dėl painaus rašto nelengva sukurti rainelės analizavimo algoritmus. Mes dažniausiai pastebime akių spalvą, tačiau biometrijoje tai visiškai nesvarbu (nebent vadinamojo *soft biometrics* srityje). Viską lemia unikalus rainelės raštas.



16 pav. Akies rainelė

Pastaraisiais metais tyrimai šioje srityje suaktyvėjo, mat 2005 m. nustojo galioti Leonardo Flomo ir Arano Safiro patentas (gautas 1987 m.), kuriame aprašomas identifikavimo pagal akies rainelę metodas. 1994 m. Johnas Daugmanas gavo sudėtingo akies rainelės rašto tyrimo patentą. Šiuo metu patentas priklauso bendrovei Iridian Technologies, parduodančiai licencijas savo partneriams: OKI, Panasanic, Securimetrics, IrusGuard ir daug kitų bendrovių naudojasi Iridian licencija.

Apmaudu tai, kad netobula patentų sistema sustabdė inovacijas identifikavimo pagal akies rainelę srityje. Dažnai bendrovės ar atskiri asmenys gauna patentą, tačiau jo niekur nepanaudoja. Tenka laukti, kol baigsis jo galiojimo laikas. Didžiosios bendrovės dėl visa ko patentuoja viską iš eilės, kad tik konkurentai neužbėgtų už akių. Kartais jos, sukaupusios strategiškai vertingus patentus, užsiima patentiniu reketu: paduoda kitas bendroves į teismą ir gauna milijonines kompensacijas už neteisėtą patentuotų technologijų panaudojimą.

ICE 2006 – pirmasis nepriklausomas akies rainelės algoritmų palyginimo testas. Paaiškėjo, kad kol kas akies rainelės biometrinės sistemos nėra gerokai pranašesnės už veido atpažinimo sistemas, nors dažnai teigiama priešingai. Taip yra todėl, kad veido atpažinimo technologijos plėtojosi laisvai ir gerokai sparčiau, tuo tarpu perspektyvus atpažinimas pagal akies rainelę buvo dirbtinai pristabdytas.

OKI pernai sukūrė savo identifikavimo algoritmą, kurį galima panaudoti bet kuriame įtaise su įrengta 1 Mp ar geresne vaizdo kamera. Anksčiau reikėdavo specialių infraraudonųjų spindulių kameros, tačiau dabar tinka įprastos. Identifikavimas vyksta programiniu lygmeniu, tad

esamos techninės įrangos keisti nereikia. OKI programa, veikianti Windows mobile 2003, Windows XP ir Symbian aplinkose, gerai prisitaiko prie ribotų mobiliųjų telefonų ir delninukų procesorių galimybių. Programa veikia gana tiksliai (suklysta 1 kartą iš 100 000, arba FAR = 0,001 proc.) ir geba atskirti tikrą akį nuo nuotraukos.

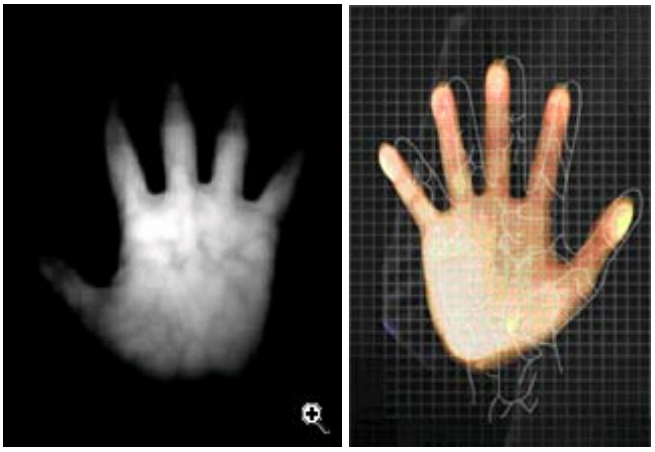
OKI tarpinė programinė įranga (middleware) nuo 2007 liepos mėn. Prieinama Japonijos mobiliojo ryšio operatoriams ir telefonų gamintojams. Programa priderinama prie kiekvieno telefono techninių savybių ir užima tik 200 KB.

Akies tinklainė. Akies obuolio dugne išsiraizgiusios kraujagyslės suformuoja unikalų raštą, kurį galima panaudoti asmenybei nustatyti. Tai daroma akį apšviečiant nežalingais neintensyviais infraraudonaisiais spinduliais. Kraujagyslės sugeria daugiau šių spindulių, tad jas įmanoma nufotografuoti ir gautą vaizdą išanalizuoti. Tačiau tam žmogus turi stovėti nejudėdamas ir mažu atstumu priešais vaizdo kamerą. Tinklainės privalumai: nesikartojantis raštas; skaitoma vidinė dalis, kurios neįmanoma imituoti.

Tačiau tinklainę veikia įvairios ligos (diabetas, glaukoma ar katarakta), tad ilgainiui sistema gali neatpažinti vartotojo. Pritaikius tinkamus algoritmus, skaitytuvai ne tik identifikuotų asmenį, bet aptikę pakitimų įspėtų apie galimą ligą.

Venų raštas. Nustatyti asmens tapatybę pagal venų struktūrą pasiūlyta gana neseniai – tik 1992 metais. Tokia mintis pirmą kartą išdėstyta Hokaido (Japonija) universitete rašytoje disertacijoje.

Fujitsu identifikuoja pagal delnų venų raštą:



17 pav. Venų raštas

Šis būdas veiksmingas tuo, kad venos yra tokios pat unikalios kaip ir pirštų antspaudai (galima atskirti net identiškus dvynus). Dėl vidinės struktūros jas sunkiau pažeisti ar suklastoti.

Išoriniai rankos nešvarumai, randai, įpjovos, tatuiruotės ar odos spalva neturi įtakos skaitytuvo darbui. Venų išsidėstymas nulemiamas dar vaisiui esant gimdoje ir žmogui augant nesikeičia. Be to, Fujitsu įtaisai nustato asmenybę be kontakto: ranka tiesiog kelioms akimirkoms palaikoma virš skaitytuvo.

Kaip tai veikia? Skaitytuvas ranką apšviečia infraraudonojo spektro šviesa. Pro odą tokia šviesa prasiskverbia, tačiau deguonies netekęs veninis kraujas (hemoglobinas) ją sugeria ir tampa matomas. Kapiliarai ir arterijos, kuriais teka deguonies prisotintas hemoglobinas, yra "permatomi". Gautas vaizdas panašus į juodų venų raizginį. Kadangi sistemai būtina gyva ranka, nėra tikslo žaloti žmogaus siekiant pavogti jo "raktą" (nupjauti ranką. Lieka tikėtis, kad plėšikai irgi šitą žino. Be to, žmonės ant daiktų nepalieka venų antspaudų (kitaip nei pirštų antspaudų), tad juos nukopijuoti itin sudėtinga.

Venų raštui taikomi specialūs algoritmai, nustatantys duomenų taškus: venų skaičių, jų susikirtimus. Gauti duomenys suglaudinami, užkoduojami ir išsaugomi duomenų bazėje. Vėliau procedūra kaskart kartojama ir gautas "raktas" lyginamas su išsaugotu šablonu.

Fujitsu sistema nusipelno pagyrimo už ypatingą patikimumą: FRR – 0,01 proc. (tik 1 iš 10 000 registruotų žmonių neatpažįstamas); FAR 0,00008 proc. (tik 1 iš daugiau nei 1 000 000 neregistruotų žmonių pripažįstamas savu).

Bendrovė tikisi skaitytuvą sumažinti tiek, kad jis tiktų net delninukams ar mobiliems telefonams. Tokyo-Mitsubishi bankas naudoja venų rašto skaitytuvus savo bankomatuose, o 2007 m. vasarą Karolinos (JAV) ligoninėse venų rašto skaitytuvai buvo pasirinkti pacientų duomenims registruoti ir apsaugoti. Carolinas HealthCareSystem ligoninės ilgai ieškojo tinkamos nekontaktinės biometrinės sistemos, ir Fujitsu pasirodė tiksliausia ir ergonomiškiausia.

Fujitsu 2007 m. rugpjūtį vieną skaitytuvą išleido kaip atskirą įtaisą, o kitą įrengė kompiuterio pelėje. Bendrovės darbuotojai gerokai patobulino savo technologiją, tad ir dabar nereikia naudoti pagalbinio "gido" (delną prilaikančio rėmelio), o ranka nuskaitomą net ją pakreipus. Atstumas tarp delno ir skaitytuvo taip pat gali būti įvairus. Be to, anksčiau identifikavimui atlikti reikėjo specialios tarnybinės stoties, o nuo šiol viską daro stalinis kompiuteris.

Per trejus metus Fujitsu planuoja parduoti 200 tūkst. Vieno delno skaitytuvų. Tai gana ambicingi užmojai, atsižvelgiant į technologijos novatoriškumą.

Įvesties įtaisai (pelės, klaviatūros) su biometriniais skaitytuvais – diskutuotinas dalykas,mat žmonės priversti naudotis tik tam tikrais gaminiais. Jie negali rinktis kitokių pelių, nors jos galbūt patogesnės ir techniškai pažangesnės. Tad pirmumą reikėtų teikti atskirai jungiamiems skaitytuvams.

Apdovanojimai ir konkursai visame pasaulyje jau nestebina. Jais siekiama skatinti diegti naujoves, tirti ir kurti naujas technologijas, gaminius. Gerai žinomi IDEA, IF dizaino apdovanojimai, X prizas. Mokslininkų ir bendrovių pastangos neretai įvertinamos įspūdingomis sumomis.

Biometrijos srityje taip pat rungtyniaujama. Siekiant nešališkumo, sudaromos nepriklausomos duomenų bazės, nauji biometrinių duomenų apdorojimo algoritmai lyginami vienodomis sąlygomis.

3. GERIAUSIOS PRAKTIKOS PAVYZDŽIAI PASAULYJE, PRIEMONĖS EUROPOS SĄJUNGOJE

Šiame skyriuje yra pateikiamos geriausios praktikos pavyzdžiai pasaulyje: apžvelgiama viešųjų raktų infrastruktūros (PKI – *Public Key Infrastructure*) diegimo tendencijos Europos Sąjungos šalyse bei Kanadoje [38]. Aprašytos veikiančios ir diegiamos, bei planuojamos diegti sistemos [11].

Europoje elektroninės identifikavimo kortelės (EIK) yra arba artimu laiku bus labai plačiai vartojamos. EIK projektų sudarymas ir įgyvendinimas yra labai lėtas procesas, daugelyje šalių vykdomas jau keletą metų [52]. Šiuo metu galima išskirti keletą pagrindinių EIK panaudojimo būdų:

- autorizuotų asmenų autentifikavimas;
- įmonių autentifikavimas ir autorizavimas bendraujant su kitais viešojo administravimo vienetas;
- įteisintų elektroninių parašų palaikymas;
- piliečių elektroninės identifikavimo kortelės;
- piliečio socialinio draudimo identifikavimas;
- vietinio paslaugų naudojimo.

Pagrindinės problemos su kuriom susidurdavo valstybės diegiant e-vyriausybės projektus yra dėl vyriausybės servisų trūkumo ir politikos inicijuoti bendroves, piliečius atlikti sudarytas programas. Taip pat naujų technologijų kaina yra pakankamai didelė. Tačiau visuose projektuose po adaptacinio periodo buvo gerai priimtas EIK panaudojimas.

Šiuo metu galima skirstyti visas Europos valstybes pagal e-vyriausybės plėtojimą į tris grupes:

Įžvalgūs pasiekėjai – į šią grupę įeina valstybės, kurios teikia daug įvairių paslaugų internete ir sudarė ne perdaug sudėtingą sistemą. Į šią grupę įeina Austrija, Olandija, Suomija ir Didžioji Britanija.

Nuoseklūs pasiekėjai – į šią grupę įeina tos vyriausybės, kurios siūlo nemažai internetinių paslaugų, taip pat vykdomi įvairūs nauji projektai. Į šią grupę įeina Prancūzija, Ispanija, Islandija, Portugalija, Vokietija ir Belgija.

Žemo lygio e-vyriausybės - valstybės kurios yra patenkintos egzistuojančiu koordinuotu agentūrų tinklu. Vienintelė tokia Europos valstybė yra Italija.

Europos Komisija nuo 2001 m. nuolat atlieka Europos pagrindinių elektroninių viešųjų paslaugų tyrimus pagal rodiklius, kurie buvo apibrėžti, siekiant stebėti e. valdžios planus

Europos Sąjungos valstybėse narėse ir Norvegijoje, Islandijoje bei Šveicarijoje. Minėti tyrimai yra atliekami pagal Europos Sąjungos šalyse naudojamą metodiką, kuri remiasi Europos Komisijos (COM081299) 1999 m. kaip gaire pasiūlytu ir 2000 m. Vidaus rinkos tarybos patvirtintu E. Europos 20 pagrindinių viešųjų paslaugų sąrašu (12 iš jų yra skirtos gyventojams, 8 – verslo įmonėms). Šis viešųjų paslaugų sąrašas nurodytas ir Elektroninės valdžios koncepcijoje, patvirtintoje Lietuvos Respublikos Vyriausybės nutarimu. Tyrimo metu vertinama, koks yra kiekvienos iš šių 20 pagrindinių paslaugų perkėlimo į internetą lygis (pradedant 1 lygiu, kuriam būdingas tik informacijos apie paslaugą pateikimas internete, baigiant 4 lygiu, kuris apima pilną paslaugos gavimo ciklą nuo užsakymo iki įvykdymo, pvz., užsakyto dokumento pristatymo).

2006 m. liepos mėnesį CapGemini atliktas tyrimas parodė [1], kad Europos Sąjungos viešųjų paslaugų, perkeltų į elektroninę terpę procentas išaugo iki 75 proc. (palyginimui 2004 m. – 65 proc.). Geriausi šioje srityje yra Austrija, Malta, Estija, Norvegija. Elektroninių viešųjų paslaugų perkėlimo į internetą lygis 2006 m. balandžio mėn. Lietuvoje siekė 68 proc. (nuo 2004 m. spalio mėn. iki 2006 m. balandžio mėn. padidėjo 9 proc.) [2].

3.1. Estija

Pirmosios asmens tapatybės kortelės Estijoje išduotos 2001 gruodžio 18 d. Kortelės gali būti naudojamos tokiems tikslams, kaip banko paslaugos internetu, elektroninės mokesčių deklaracijos, skaitmeninis parašas, įėjimo kontrolė, elektroniniam balsavimui ir t.t Per kelis metus išduota daugiau kaip 850 000 vnt. Vyriausybė atlieka pagrindinį vaidmenį teisiškai reglamentuojant skaitmeninius parašus ir paslaugų teikėjų registraciją (Skaitmeninio parašo įstatymas Estijoje priimtas 2000 m.). Asmens tapatybės kortelės skatina greitą e-paslaugų plėtotę privačiame ir valstybiniame sektoriuose.

Estija tapo pirmąją pasaulyje valstybe, kurioje balsavimas parlamento rinkimuose vyko internetu. Tai iškėlė Estiją į pirmaujančių, technologiškai pažangiausių, pasaulio valstybių tarpą. Balsuojant internetu rinkėjas turi turėti Estijos asmens tapatybės kortelę, PIN kodą ir prieįimą prie kompiuterio su kortelės nuskaitymo įrenginiu, instaliuotu tapatybės kortelės draiveriu ir Windows arba Linux operacinę sistemą. Balsuoti labai paprasta: rinkėjui tereikia įdėti asmens tapatybės kortelę į kortelės nuskaitymo įrenginį ir toliau sekti instrukcijas ekrane – patenkama į vyriausios rinkimų komisijos interneto puslapį, kuriame (remiantis rinkėjo identifikaciniu numeriu) pateikiamas balsuotojo rinkimų apylinkės kandidatų sąrašas. Rinkėjas pasirenka kandidatą, patvirtina savo sprendimą, kuris yra užkoduojamas, ir balsavimo pabaigoje pasirašo

elektroniniu parašu. Sistema patvirtina, kad balsavimas buvo užregistruotas – rinkėjas atliko savo pareigą.

18 pav. Estijos piliečio lustinė asmens tapatybės kortelė

3.2. Austrija

Šiuo metu Austrijoje nėra vieningos asmens identifikavimo numerių sistemos, panašios į kitų Europos sąjungos valstybių asmens identifikavimo numerių sistemas. Tačiau kiekvienas dirbantis asmuo turi savo socialinio draudimo numerį. Privataus sektoriaus asmenys yra įtraukti į bendrovių registrą, kur jiem priskirti atitinkami registruotų bendrovių numeris. Fiziniams asmenims suteikti numeriai susideda iš keleto skaitmenų, neturinčių jokių kitų reikšmių ir paskirtų eilės tvarka. Kiekvienas numeris yra neatsiejamai susijęs su tam tikru asmeniu. Numerius paskiria vidaus reikalų ministerija, valdanti centrinį registrą. Kiekvienas numeris susiejamas su pavarde, pirmais vardais , lytimi ir gimimo data. Jie nefiksuojami niekur kitur, kaip tik centriniame registre, todėl apie jų išorinį panaudojama dar nieko nenuspręsta.

Dabar yra vykdomas projektas sukurti piliečių elektronines identifikavimo korteles (EIK) kaip socialinio draudimo kortelių praplėtimą. Šios kortelės turėtų elektroninę mikroschemą ir ją būtų galima panaudoti kaip elektroninio parašo arba privatų raktą. Svarbios informacijos saugojimas jose nėra numatytas. Planuojama padalinti EIK į keletą atskyrų skyrių ir bandoma apibrėžti, kas galėtų panaudoti tokį kortelės funkcionalumą. Iš pradžių kortelės būtų naudojamos sveikatos apsaugai, tačiau ten nebūtų surašomi asmens medicininiai duomenys. Jos būtų skirtos tik administracinių procedūrų palengvinimui. Taip pat neplanuojama panaudoti EIK kaip elektroninės mokėjimo kortelės.

Austrijos įstatymai buvo pritaikyti pagal Europos direktyvą dėl elektroninių parašų 1999/93/EC dar 1999 metais. Autentifikavimuisi keičiantis elektroniniais duomenimis viešajame sektoriuje elektroninis parašas taps identifikavimo pagrindu.

Austrijos pagrindiniai projektai ir paslaugos apžvelgiami priede Nr.6

3.3. Suomija

Suomijoje yra sudaryta vieninga tiek fizinių tiek juridinių ir netgi didesnių techninių vienetų identifikavimo numerių sistema. Į asmens identifikavimo numerį įeina skaičių grupės užkoduojančios tam tikrą asmeninę informaciją. Pirmi 6 skaičiai nurodo gimimo datą, po kurio eina amžiaus kodas (19 amžiaus kodas -, 20 +, o 21 A). Kiti skaičiai dar nurodo lytį. Identifikavimo numeris niekada nesikeičia, nebent asmeniui atliekama lyties pakeitimo operacija. Identifikavimo numerius paskiria gyventojų registravimo centras. Juos gauna ką tik gimę kūdikiai ir nuolat Suomijoje gyvenantys užsieniečiai. Gyventojų registravimo centras yra atsakingas už asmens duomenų saugojimą ir tvarkymą. Identifikavimo numeris yra visiškai susijęs su pavarde, pirmais vardais, lytimi, gimimo data, gimimo vieta, pilietybe, buvusią pilietybe, šeimynine padėtim ir buvusiom santuokom, tėvų vardais, vaikų vardais, tėvų identifikacijos numeriais, religija, profesija, kita informacija (teistumas ir pan.). Suomijoje naudojami identifikavimo numeriai yra tikrai vieningai naudojami viešajame administravime. Šių numerių naudojimą saugo įstatymas, stengiamasi jį naudoti taip dažnai kaip tik įmanoma. Taip pat jis naudojamas kontaktuojant piliečiams, bei privatiems asmenims. Jis naudojamas šiuose oficialiuose dokumentuose: identifikavimo kortelėse, pasuose, vairuotojo pažymėjimuose, socialinio arba sveikatos draudimo pažymėjimuose, mokesčių dokumentuose ir dokumentuose, kurie susiję su vaikų išsilavinimu. Juridiniai asmenys naudoja identifikavimo numerius sudarytus iš atsitiktinių skaičių. Visi kompanijų duomenys saugojami centrinėje duomenų bazėje, kurią naudoja verslo registras ir mokesčių departamentas. Šios sistemos reorganizavimas visiškai nebūtinas, kadangi jau yra pradėtas elektroninių identifikacijos kortelių įvedimas. Pavyzdžiui gyventojų registravimo centras jau tiekia EIK ir suteikia keletą PKI paslaugų.

Suomijoje EIK jau yra gana plačiai naudojamos. Jos jau atlieka identifikavimo, elektroninio parašo ir saugaus priėjimo prie administracijos duomenų bazių funkcijas. Jos turi savyje sertifikatus ir privačius raktus, bet neturi asmens identifikavimo numerio, kurį pakeitė kortelės serijinis numeris. Užtenka paminėti, kad kai kurie bankai, net priima šias korteles kaip internetinio bankninkavimo autentifikavimosi alternatyva.

Elektroninių transakcijų aktas, sudarytas 2000 metų sausio mėnesį, valdo piliečių elektroninius parašus viešajame administravime. Valstybinis pasiūlymas dėl akto buvo įtvirtintas 2001 rugsėjo mėnesį. Vyriausybė sudarė elektroninio autentifikavimosi principus dar 1998 vasario mėnesį. Elektroninio identifikavimo kortelės naudojamos nuo 2000 metų pradžios, taip pat tuo metų buvo pradėti naudoti PKI servisai. Šiuo metu elektroninis parašas keičiantis elektroniniais duomenimis naudojimą tik tarp nutolusių vartotojų, tačiau vidaus reikalų ministerija ruošiasi panaudoti EIK taip pat ir įvairiuose vidinėse IT procedūrose. Tačiau šis procesas dar yra lėtas ir sudėtingas.

Suomijos pagrindiniai projektai ir paslaugos apžvelgiami priede Nr.7.

3.4. Olandija

Olandijoje fiziniai asmenys naudoja du identifikavimo numerius – administracinį numerį (A – numerį) ir socialinį- finansinį numerį (sofi numerį). Taip pat du numerius turi ir juridiniai asmenys – prekybos registravimo numerį (KVK numerį) ir finansinį numerį (fi numerį). Tačiau kūkininkai ir kitų gausių profesijų atstovai neįeina į prekybos registrą. A – numeris sudarytas iš atsitiktinių skaičių sekų sudarytų pagal tam tikrą algoritmą, Sofi – numeriai sudaryti didėjimo tvarka. Nei vienas, nei kitas niekada nesikeičia. A – numeris skiriamas visiems Olandijoje gimusiems asmenims, jei jų tėvai registruoti GBA (Komunalinėje gyventojų registravimo bazėje) sistemoje ir taip pat asmenims kurie per paskutinius 6 mėnesius Olandijoje gyveno bent 4. Numeriai skiriami komunalinėse įstaigose, jiems visada yra paskirimas numerių rezervas. Sofi numeris skiriamas visiems asmenims, kurie moka mokesčius. Nėra jokios centralizuotos A – numerių duomenų bazės, vietinės atstovybės atsakingos už duomenų registravimą ir keitimą. Ir tik viena vyriausybinė agentūra yra atsakinga už šio tinklo palaikymą. Sofi numeriai – laikomi centralizuotoj duomenų bazėje , kuri yra pasiekiama viešo administravimo įstaigoms, bei keletai pusiau viešom organizacijom. Duomenų bazėje su identifikavimo numeriais yra susijama tokia informacija: pavardė, pirmieji vardai, lytis, gimimo data, gimimo vieta, gyvenimo vieta, tautybė ir kita. Abu šie numeriai yra vartojami, kartais net abu kartu. Kol kas neplanuojama artimiausiu laiku perorganizuoti esamą tvarką. Tuo tarpu galimybė panaudoti elektroninį identifikavimą tam, kad pasiekti savo informacija centrinėje duomenų bazėje, reikės pakeisti keletą esamos sistemos aspektų.

Olandijoje nėra oficialios elektroninės identifikavimo kortelės, tam reikalui naudojamas pasas. Tačiau šiuo metu yra kuriama elektroninė identifikavimo kortelė. Į ją planuojamą sudėti biometrijos, viešo rakto ir elektroninę identifikavimo kortelės technologijas. Tokia identifikavimo kortelė būtų naudojama kaip identifikavimo kortelė kelionėse po Europą, identifikavimo kortelė ir elektroniniam parašui. Tai būtų lyg raktas į elektroninius į elektroninės vyriausybės paslaugas. Paslaugų tiekėjai patys būtų atsakingi už tam tikros paslaugos pasiekiamumą.

Buvo sudaryti reikalingi įstatymų pakeitimai dėl elektroninio parašo sistemų. PKI infrastruktūros praplėtimas tarp piliečių, viešojo administravimo įstaigų ir privačių įmonių buvo suplanuotas iki 2006 metų. Olandų PKI yra sudaryta tokios hierarchinės struktūros, kad būtų galima pasiekti maksimalų sistemos lankstumą. Bus sudarytas centrinis valstybės PA (*policy authority*) ir trys probleminių sričių PA (valstybės – valstybės įstaigų bendravimui, valstybės įmonių – piliečių bendravimui ir valstybės – verslo įmonių bendravimui). CA (*certification*

authority) funkcija ir RA funkcija (*registry authority*) bus skirtingos sertifikatų paslaugų tiekėjo funkcijos. Pagal šią schemą vyriausybė sudarys PKI diegimo šabloną ir nustatys taisykles kuriomis turės vadovautis privačios bendrovės.

Olandijos pagrindiniai projektai ir paslaugos apžvelgiami priede Nr.8

3.5. Didžioji Britanija

Didžiojoje Britanijoje fiziniai ar juridiniai asmenys neturi vieno identifikavimo numerio. Viešajame administravime būna įvairių dokumentų, tarp kurių gali būti naudojami kokie nors numeriai. Svarbiausias iš jų yra nacionalinio draudimo numeris, kuris lieka su tam tikru asmeniu visą gyvenimą ir kartais naudojamas įvairiuose mokesčių procedūrose. Tačiau nei nacionalinio saugumo kortelė, nei nacionalinės sveikatos apsaugos kortelė nėra identifikacinė kortelė.

Didžiojoje Britanijoje nėra numatytas elektroninių identifikavimo kortelių naudojimas ir toks klausimas yra politiškai jautri vieta. Kitas numatytas sprendimas yra užtikrinti ginamą identifikavimą asmenų, kurie susiję su viešojo administravimo sistemom tam, kad atlikti elektroninius pervedimus, pavyzdžiui mokesčiams mokėti. Pervedimamas, kuriems reikia griežto autentifikavimosi, bus sudaryti skaitmeniniai sertifikatai. Vyriausybės politika yra tokia, kad vyriausybės vartai (*Goverment Gateway*) naudoja *Tscheme* patvirtintą patikimo paslaugų tiekėjo tam, kad panaudoti sertifikatą per vartus. *Tscheme* nepriklausomai užtikrina, kad patikimas paslaugų tiekėjas atitiks griežtus reikalavimus. Akredituotas patikimas paslaugų tiekėjas sudaro sertifikatą, kurį gali naudoti verslo įmonės ir piliečiai, kad pasiektų e-vyriausybės paslaugas.

Šiuo metu yra visiškai užbaigta konsultacija bendruomenės šablono įgyvendinimui. Tam dabar vadovauja prekybos ir pramonės departamentas. E-pasiuntinybės ofisas pradėjo dviejų politikų vystymą griežtų autentifikavimo paslaugų panaudojimui. Vieną prižiūrinčią vyriausybės - verslo pervedimus ir kitą prižiūrinčią vyriausybės – piliečių pervedimus. Jos jau yra taip pat pirmoje įgyvendinimo stadijoje. Taip pat jau yra įkurtas pagrindinis HMG autoritetingas šaltinis, kuris yra Didžiosios Britanijos pasitikėjimo pagrindas. Departamentinis PKI bus sertifikuojamas per HMG autoritetingą šaltinį, taip vyriausybėje sudarant hierarchinį PKI. Nors kol kas dar nei vienas departamentas nėra sertifikuotas, tačiau planuojama tai padaryti netolimoje ateityje.

Didžiosios Britanijos pagrindiniai projektai ir paslaugos apžvelgiami priede Nr.9

3.6. Švedija

Mokesčių inspekcija vykdo pilotinį projektą su grupe kompanijų kasmėnesiniam mokesčių paskelbimui. Šiam pilotiniam projektui yra naudojamas Švedijos *Post* sertifikatas.

Dalis Švedijos agentūrų tikisi panaudoti elektroninį parašą elektroninių paslaugų pateikimui viešai. Į šias paslaugas:

- įeina paskolų suteikimas,
- naujų kompanijų kūrimas,
- sveikatos draudimas.

Vyriausybė pradėjo kurti portalą "Vyriausybė 24 valandas", kuris pristato formas ir informaciją tinkamo darbo paieškai.

Artimiausioje ateityje numatoma vykdyti dar visą eilę programų, kurioms reikės elektroninio parašo.

Švedijos vyriausybė vykdo SHS (SHS: Spridnings och HämtningSystem in Swedish) projektą. SHS - Švedijos nacionalinė infrastruktūra duomenų apsikeitimui - yra ir koncepcija, ir standartas duomenų apsikeitimui Švedijos viešojo administravimo įstaigoms. Koncepcija ir standartas buvo sukurti bendromis Švedijos Administravimo vystymo agentūros, Mokesčių inspekcijos ir Nacionalinės draudimo tarybos jėgomis. Projektą koordinuoja Administravimo vystymo agentūra. Įgyvendinimui buvo įsigyti programiniai produktai iš dviejų tiekėjų: Frontec ir Hewlett-Packard.

Švedijos Koncepcija, SHS naudojimo scenarijaus pavyzdys, architektūra, technologiniai sprendimai ir saugumas apžvelgiami priede Nr.10

3.7. Kanada

Keletas su PKI susijusių pilotinių projektų yra perimti federalinių agentūrų ir yra atrinkti, kaip specialūs projektai GOC PKI *Pathfinder* programai. Šią programą atstovauja federalinės valdžios perimti novatoriškiausi projektai, orientuoti į praktinį įgyvendinimą, taikymus ir PKI technologijų panaudojimą.

Yra apie 17 *Pathfinder* projektų ir daugiau kaip 100 PKI pilotinių projektų naudojančių internetą ir PKI on-line paslaugų teikimui.

PKI projektai ir taikomosios programos plačiau apžvelgiami priede Nr.11

4. GYVENTOJŲ NAUDOJAMŲ BŪDŲ IDENTIFIKUOTIS ELEKTRONINĖJE ERDVĖJE TYRIMAS

Tai nedidelės apimties žvalgybinis tyrimas, kurio tikslas yra ištirti, kokias būdais respondentai dažniausiai naudojasi identifikuojant save elektroninėje erdvėje, kokiomis viešosiomis paslaugomis naudojasi.

Tyrimo objektas - gyventojų nuomonės apie viešasias elektronines paslaugas bei asmens identifikavimo būdus įvertinimas.

Buvo apklausta 50 respondentų. Jiems buvo pateikta 15 klausimų anketa (priedas Nr.13). Pirmoje anketos dalyje pateikiami klausimai apie šiuo metu naudojamus būdus asmens identifikavimui viešųjų elektroninių paslaugų portale - naudojantis bankų sistema bei elektroniniu parašu. Antrąja anketos dalimi siekiama išsiaiškinti viešųjų elektroninių paslaugų naudojimosi galimybes. Trečioji dalis skirta išsiaiškinti respondentų demografiją. Šių duomenų reikia tam, kad būtų galima nustatyti elektroninės bankininkystės bei elektroninio parašo naudojimą, požiūrį į tai tarp skirtingų žmonių grupių.

Tyrimo metu buvo aiškinamasi, ar respondentai naudojantis viešosiomis elektroninėmis paslaugomis teikia pirmenybę identifikuoti asmenybę per bankų sistemą, jei ne – kokios priežastys tai sąlygoja; su kokiu banku yra sudarę elektroninių paslaugų sutartis, ar pasitiki identifikavimo sistema, kaip vertina elektroninės bankininkystės patogumą; ar naudojasi viešosiomis paslaugomis, prieinamomis per bankų sistemas; ar pageidautų, kad jų skaičius didėtų; kokios jau egzistuojančios paslaugos yra reikalingos. Taip pat buvo aiškinamasi, ar respondentai žino, kas yra elektroninis parašas, ar juo naudojasi.

4.1 Aprašomoji analizė

Aprašomoji statistika (angliškai descriptive statistics) — tai statistinių duomenų skaitiniai ir grafiniai pateikimo metodai: dažnių lentelės, statistinių charakteristikų skaičiavimas, didelė grafikų įvairovė.

Atliekant tyrimą buvo apklausti atsitiktinai parinkti 50 asmenų. Jų pasiskirstymą pagal lytį matome lentelėje Nr.3. Buvo apklausta 29 moterys ir 21 vyras.

Respondentų pasiskirstymą pagal lytį matome 3 lentelėje.

3 lentelė. Tiriamųjų pasiskirstymas pagal lytį

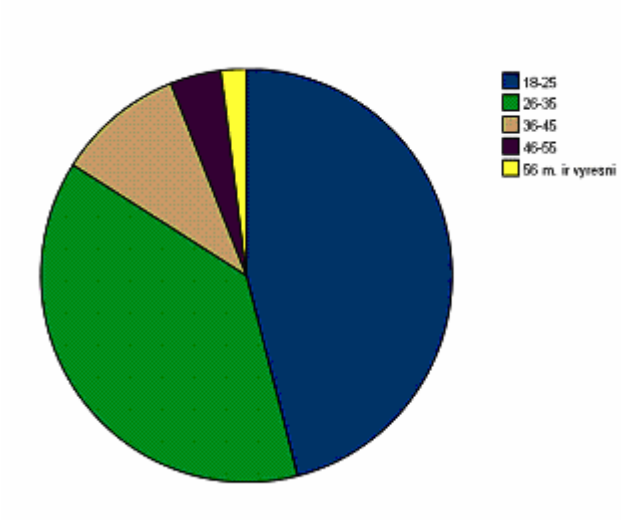
	Frequency Dažnis	Percent Dažnis %	Valid Percent Teisingų dažnis%	Cumulative Percent Sukauptasis dažnis%
Moteris	29	58,0	58,0	58,0
Vyras	21	42,0	42,0	100,0
Iš viso:	50	100,0	100,0	

Respondentų pasiskirstymas pagal amžiaus grupes yra lentelėje Nr.4. Daugiausiai atsakiusiųjų į anketą yra 18-25 metų grupėje. Mažiausiai, t.y. 1 asmuo, yra grupėje vyresnių nei 56 metai.

4 lentelė. Tiriamųjų pasiskirstymas pagal amžių

	Frequency Dažnis	Percent Dažnis %	Valid Percent Teisingų dažnis%	Cumulative Percent Sukauptasis dažnis%
18-25	23	46,0	46,0	46,0
26-35	19	38,0	38,0	84,0
36-45	5	10,0	10,0	94,0
46-55	2	4,0	4,0	98,0
56m. ir vyresni	1	2,0	2,0	100,0
Iš viso:	50	100,0	100,0	

Grafinį respondentų pasiskirstymą pagal amžiaus grupes matome 19 pav.



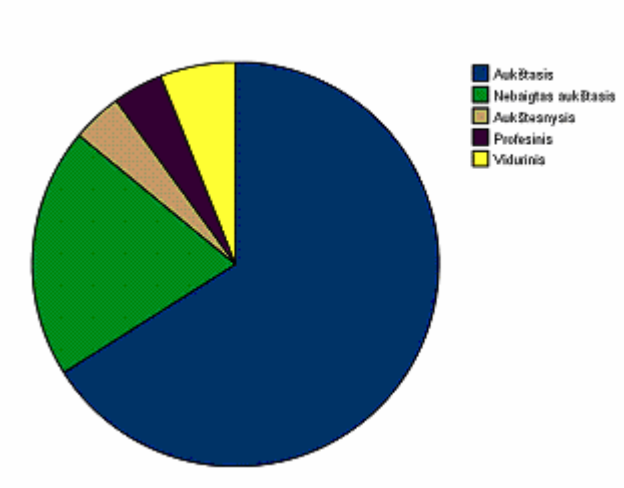
19 pav. Tiriamųjų pasiskirstymas pagal amžių

Respondentų pasiskirstymas pagal išsilavinimą yra lentelėje Nr.5. Daugiausiai respondentų įgiję aukštąjį išsilavinimą. Mažiausiai, t.y. po 2 asmenis, yra grupėse, įgijusių aukštesnįjį bei profesinį išsilavinimus.

5 lentelė. Tiriamųjų pasiskirstymas pagal išsilavinimą

	Frequency Dažnis	Percent Dažnis %	Valid Percent Teisingų dažnis%	Cumulative Percent Sukauptasis dažnis%
Aukštasis	33	66,0	66,0	66,0
Nebaigtas aukštasis	10	20,0	20,0	86,0
Aukštesnysis	2	4,0	4,0	90,0
Profesinis	2	4,0	4,0	94,0
Vidurinis	3	6,0	6,0	100,0
Iš viso:	50	100,0	100,0	

Grafinį respondentų pasiskirstymą pagal amžiaus grupes matome 20 pav..



20 pav. Tiriamųjų pasiskirstymas pagal išsilavinimą

Dauguma respondentų – 60 proc. naudojantis viešosiomis elektroninėmis paslaugomis identifikavimui naudoja bankų sistemas. Bankai, diegdami įvairius klientų identifikavimo sprendimus, išpopuliarino internetinę bankininkystę ir perkėlė daugelį santykių su klientais į elektroninę erdvę. Kadangi 2007 metų pabaigoje bankai prognozavo turėti 1,72 mln. elektroninių paslaugų vartotojų, ši paslauga nieko nekainuoja, taip pat pagal tyrimo rezultatus galime matyti, jog šis būdas labiausiai paplitęs.

Mažuma respondentų - tik 4 proc. - naudojantis viešosiomis elektroninėmis paslaugomis identifikavimui naudojasi asmeniniais sertifikatais. Asmeninis skaitmeninis sertifikatas yra pakankamai brangus, pasirašymo veiksmas yra palyginti retas įvykis daugumai piliečių, vartotojams neapsimoka mokytis naujų procedūrų, jei jomis bus naudojamasi itin retai. todėl tarp eilinių vartotojų šis identifikavimo būdas nėra paplitęs.

Likusieji respondentai visiškai nesinaudoja elektrininėmis viešosiomis paslaugomis. Priežastys – respondentams to nereikia, nesinaudoja kompiuteriu arba nepakanka informacijos apie teikiamas viešąsias elektronines paslaugas.

4.2 Koreliacijos koeficientas

Koreliacija yra ryšys tarp atsitiktinių dydžių, kurių nesieja griežta funkcinė priklausomybė. Koreliacijos koeficientas yra tiesinės priklausomybės tarp kintamųjų kiekybinio įvertinimo kriterijus arba ryšio stiprumo matas. Matuojamų pagal rangų skalę kintamųjų (tik skaitmeninių reikšmių) yra skaičiuojamas Spirmeno (Spearmen) koreliacijos koeficientas.

Paskaičiuosime koreliacijos koeficientą tarp respondentų išsilavinimo ir jų naudojimosi e-bankininkyste (6 lentelė).

6 lentelė. Respondentų išsilavinimo ir naudojimosi e.bankininkyste koreliacijos koeficientas

	Value Reikšmė	Asymp. Std. Error(a)	Approx. T(b)	Approx. Sig. p-reikšmė
Spirmeno koreliacijos koeficientas	0,574	0,102	4,859	0,000(c)

Kadangi kintamieji nepriklauso intervalų skalei, Pirsono koreliacijos koeficiento reikšmės nenagrinėjame. Spirmeno koreliacijos koeficiento reikšmė vidutinė (0,574). Tokia koeficiento reikšmė reiškia, kad koreliacija vidutinė, todėl yra vidutinis ryšys tarp respondentų išsilavinimo ir jų naudojimosi elektronine bankininkyste.

Kriterijaus p-reikšmė yra mažesnė už reikšmingumo lygmenį α=0,05 (koreliuoja).

Paskaičiuokime dar vieną koreliacijos koeficientą: tarp respondentų lyties ir pasitikėjimo elektroninės bankininkystės identifikavimo sistema (7 lentelė).

7 lentelė. Lyties ir pasitikėjimo e.bankininkystės identifikavimo sistema.koreliacijos koeficientas

	Value Reikšmė	Asymp. Std. Error(a)	Approx. T(b)	Approx. Sig. p-reikšmė
Spirmeno koreliacijos koeficientas	-0,141	0,140	-0,986	0,329(c)

Šiuo atveju Spirmeno koreliacijos koeficientas yra mažesnis (-0,141). Galima sakyti, kad visiškai nėra jokio ryšio tarp respondentų lyties ir pasitikėjimo elektroninės bankininkystės identifikavimo sistema.

Gautas rezultatas nėra statistikai reikšmingas, nes kriterijaus p-reikšmė yra žymiai didesnė už reikšmingumo lygmenį α=0,05. Taigi, nulinė hipotezė (koreliacijos tarp dviejų kintamųjų nėra), negali būti atmesta.

4.3 Klasterinė analizė

Klasterinė analizė — tai metodas identifikuoti homogenines objektų arba stebėjimų grupes (klasterius) — objektai suskirstomi taip, kad skirtumai klasterių viduje būtų kuo mažesni, o tarp klasterių — kuo didesni.

Skiriamos dvi pagrindinės klasterinės analizės metodų klasės — hierarchiniai ir nehierarchiniai metodai.

Hierarchiniais metodais nustatoma bendra visų klasterių tarpusavio priklausomybių struktūra ir tik tada sprendžiama, koks klasterių skaičius optimalus. Savo ruožtu hierarchiniai metodai skirstomi į jungimo ir skaidymo metodus. Taikant jungimo metodus, iš pradžių visi stebėjimai traktuojami kaip atskiri klasteriai. Pirmuoju žingsniu du stebėjimai yra sujungiami į klasterį, kiekvienu kitu žingsniu naujas stebėjimas yra jungiamas prie esamo klasterio arba du

klasteriai sujungiami. Suformuotas klasteris vėliau jau negali būti skaldomas — jis gali būti tik jungiamas su kitais klasteriais.

Darant šią analizę pasirinkau atlikimą pagal demografinius klausimus, kokio banko elektroninėmis paslaugomis naudojasi respondentai, kaip vertina e.bankininkystės patogumą, ar žino, kas yra e.parašas, ar juo naudojasi.

8 lentelėje matome klasterizavimo eigos schemą. Stulpelyje Cluster Combined pateikiamas duomenų jungimo į klasterius eiliškumas.

8 lentelė. Duomenų jungimo į klasterius eiliškumas (Agglomeration Schedule)

	Cluster Combined			Stage Cluster First Appears		
Stage	Cluster 1	Cluster 2	Coefficients	Cluster 1	Cluster 2	Next Stage
1	40	45	,000	0	0	3
2	31	44	,000	0	0	13
3	16	40	,000	0	1	7
4	37	39	,000	0	0	5
5	33	37	,000	0	4	17
6	32	34	,000	0	0	7
7	16	32	,000	3	6	16
8	23	30	,000	0	0	10
9	26	29	,000	0	0	19
10	19	23	,000	0	8	17
11	13	20	,000	0	0	12
12	13	43	,808	11	0	19
13	22	31	,808	0	2	21
14	27	41	1,169	0	0	24
15	14	42	1,505	0	0	26
16	16	35	1,505	7	0	23
17	19	33	1,505	10	5	25
18	4	6	1,505	0	0	38
19	13	26	1,708	12	9	24
20	2	24	1,977	0	0	35
21	22	36	2,043	13	0	25
22	5	7	2,237	0	0	35
23	16	28	2,257	16	0	36
24	13	27	2,412	19	14	29
25	19	22	2,585	17	21	30
26	9	14	3,350	0	15	39
27	8	11	3,406	0	0	34
28	10	12	3,482	0	0	31
29	13	25	3,581	24	0	33
30	19	38	5,090	25	0	33
31	10	21	5,507	28	0	37
32	15	17	6,522	0	0	43
33	13	19	6,571	29	30	36
34	8	18	8,056	27	0	37
35	2	5	10,127	20	22	40
36	13	16	10,334	33	23	38
37	8	10	11,190	34	31	41

38	4	13	11,948	18	36	39
39	4	9	12,539	38	26	40
40	2	4	14,774	35	39	42
41	3	8	15,853	0	37	42
42	2	3	17,611	40	41	44
43	1	15	23,232	0	32	44
44	1	2	28,026	43	42	0

9 lentelėje surašyta klasterių narystė. Parodoma kuriam klasteriui priskiriamas kiekvienas atvejis. Klasterių kiekis buvo pasirinktas nuo 2 iki 3. Todėl lentelėje su klasterių naryste yra pateikiami 2 stebėjimų priskyrimo atskiriems klasteriams variantai. Iš lentelės duomenų matome, kad pirmam klasteriui priklauso 1 atvejis, antram – 44.

9 lentelė. Klasterių narystė (Cluster Membership)

Case	3 Clusters	2 Clusters
1:Case 1	1	1
2:Case 3	2	2
3:Case 4	2	2
4:Case 6	2	2
5:Case 7	2	2
6:Case 8	2	2
7:Case 9	2	2
8:Case 10	2	2
9:Case 11	2	2
10:Case 13	2	2
11:Case 14	2	2
12:Case 15	2	2
13:Case 16	2	2
14:Case 17	2	2
15:Case 18	3	1
16:Case 19	2	2
17:Case 20	3	1
18:Case 21	2	2
19:Case 22	2	2
20:Case 23	2	2
21:Case 24	2	2
22:Case 25	2	2
23:Case 26	2	2
24:Case 27	2	2
25:Case 28	2	2
26:Case 29	2	2
27:Case 30	2	2
28:Case 31	2	2
29:Case 32	2	2
30:Case 33	2	2
31:Case 34	2	2
32:Case 35	2	2
33:Case 36	2	2
34:Case 37	2	2

35:Case 38	2	2
36:Case 39	2	2
37:Case 40	2	2
38:Case 41	2	2
39:Case 42	2	2
40:Case 43	2	2
41:Case 44	2	2
42:Case 45	2	2
43:Case 46	2	2
44:Case 47	2	2
45:Case 48	2	2

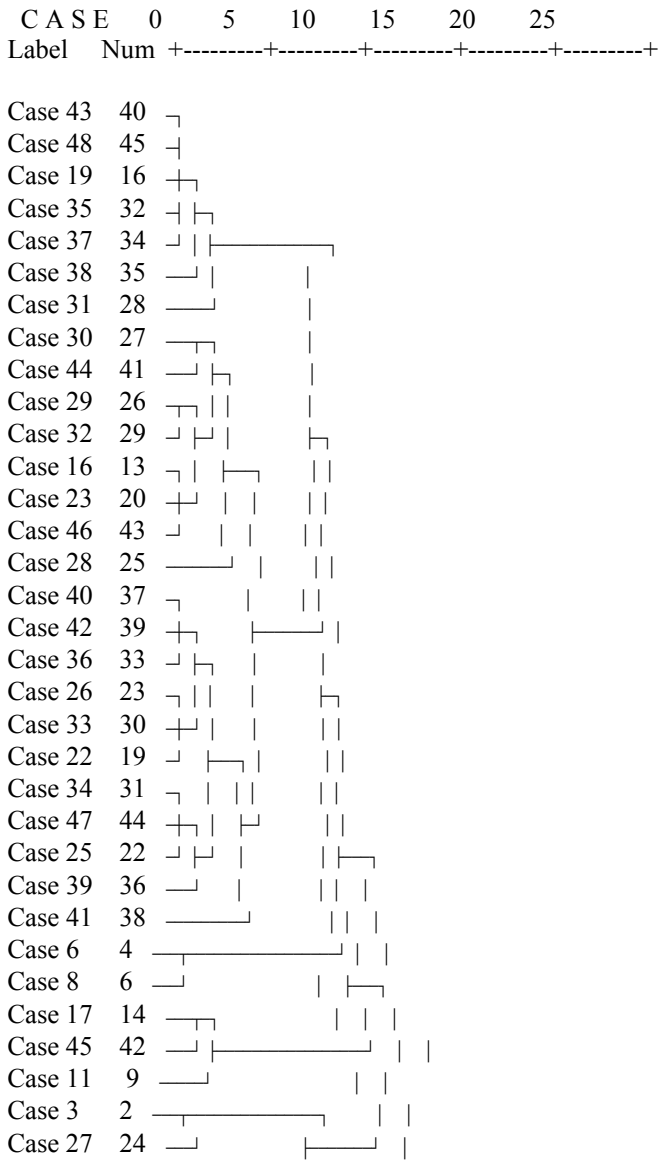
Grafinį pasiskirstymą į klasterius galime matyti 1 dendogramoje.

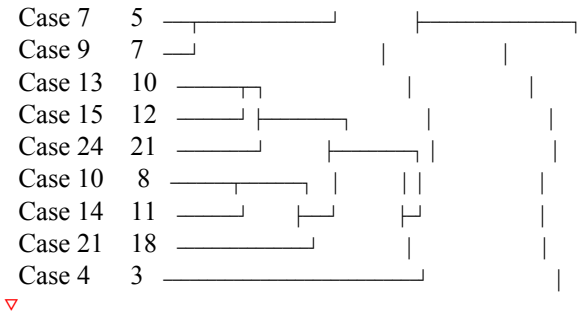
1 dendograma Pasiskirstymas į klasterius

* * * * * * H I E R A R C H I C A L C L U S T E R A N A L Y S I S * * * * * *

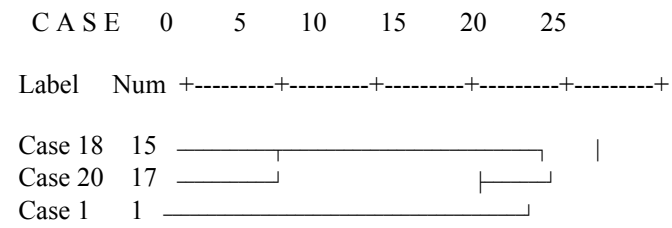
Dendrogram using Average Linkage (Between Groups)

Rescaled Distance Cluster Combine





* * * * * * H I E R A R C H I C A L C L U S T E R A N A L Y S I S * * * * * *



Atlikus tyrimą galime matyti, kad išsilavinę respondentai labiau linkę į naujoves – jie labiau linkę naudotis viešosiomis elektroninėmis paslaugomis. Tačiau vartotojų motyvacija yra vienas didžiausių barjerų, bandanti įdiegti viešąsias elektroninio parašo infrastruktūras.

IŠVADOS

1. Tikslai, kurie buvo iškelti ir e.valdžios koncepcijoje, ir i-komunikate – kad jau nuo 2005 m. viešosios paslaugos Lietuvos Respublikos gyventojams ir verslo subjektams būtų teikiamos panaudojant skaitmenines technologijas, įgyvendinti nepilnai. Iki 2005 metų visos viešosios paslaugos, kurias administruoja institucijos, iki trečiojo lygio turėjo būti perkeltos į internetą ar teikiamos kitais nuotoliniais būdais. Šiuo metu į trečiąjį lygį perkelta 31, į ketvirtąjį – tik 12 viešųjų paslaugų. Pirmojo ir antrojo lygio viešųjų e.paslaugų yra 377.

2. Elektroninio parašo paplitimui ypatingai svarbi problema yra tai, kad verslui neapsimoka diegti e.parašo infrastruktūros tol, kol nėra pakankamai didelio elektroninių paslaugų rato. Tuo tarpu elektroninės paslaugos nėra sparčiai kuriamos ir plėtojamos, apeliuojant į elektroninio parašo infrastruktūros nebuvimą. Tai sudaro uždarą ratą ir stabdo e.paslaugų ir e.parašo plėtrą.

3. Asmeninis skaitmeninis sertifikatas yra pakankamai brangus (kaina metams 90 Lt - 149 Lt), todėl tarp eilinių vartotojų jis nėra paplitęs. Kadangi tai yra vienas iš būdų atlikti asmens tapatybės nustatymo procedūrą (identifikuotis) “Elektroninių valdžios vartų” portale, vartotojai renkasi kitą nieko nekainuojantį būdą – identifikavimąsi per bankų sistemas.

4. Svarbi asmens identifikavimo pasinaudojant bankų internetinės bankininkystės sistemomis problema yra saugumas. Jis remiasi pasitikėjimu banku ir banko pasitikėjimu savo klientais. Kita svarbi problema, stabdanti bankų sistemų naudojimą identifikuojantis gaunant viešąsias paslaugas, yra ta, kad bankai nėra suinteresuoti tokios paslaugos teikimu. Tai yra šalutinė funkcija, apkraunanti bankų internetines sistemas, reikalaujanti galingesnės techninės įrangos, galinti sutrikdyti sistemos darbą, esant dideliam vartotojų srautui.

5. Mobiliųjų technologijų patrauklumas įtakoja pakankamai aukštą jų paplitimo lygį tarp gyventojų. Ši situacija yra išnaudojama kuriant naują perspektyvų ir patrauklų asmens identifikavimo būdą elektroninėje erdvėje – mobilųjį parašą. Mobilusis parašas gali plačiai paplisti, kadangi Lietuvoje mobiliojo ryšio skverbtis yra viena didžiausių pasaulyje. Be to vartotojas asmeninį GSM telefoną pastoviai nešiojasi su savimi, GSM technologijos patikimumas ir saugumas yra visuotinai pripažinti, nėra reikalavimų instaliuoti ir prižiūrėti specialios programinės įrangos ir išmokti ja naudotis.

6. Asmens tapatybės kortelės su lustu gali žymiai praplėsti šių kortelių funkcionalumą ir galimybes, ypatingai e.paslaugų atžvilgiu. Jos gali būti naudojamos e.rinkimuose, viešajame transporte kaip e.bilietai, kaip e.paciento kortelė, praėjimo kontrolės sistemose ir t.t. Tai įrodo kitų šalių patirtis, pvz. Estijos, Austrijos.

7. Pagrindinis 2006 m. rugsėjo mėn. investicinio projekto “Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas” tikslas: aprūpinti Lietuvos piliečius asmens tapatybės kortelėmis, kurios šalia pagrindinės dokumento paskirties – vizualios verifikacijos - vykdytų elektroninio asmens identifikavimo bei elektroninio parašo funkcijas ir suteiktų galimybes asmenims naudotis e.valdžios bei kitomis e.paslaugomis.

8. Asmens identifikavimui elektroninėje erdvėje gali būti naudojamos naujos biometrinės sistemos, pvz., pirštų antspaudai, 3D veido atpažinimas, akies rainelė ir kt. Tai nauji ir perspektyvūs būdai, tačiau jų vystymąsi stabdo teisinės problemos, netobula patentų sistema.

9. Atlikus žvalgybinį tyrimą galime matyti, kad vartotojų motyvacija yra vienas didžiausių barjerų, bandant įdiegti viešąsias elektroninio parašo infrastruktūras. Pasirašymo veiksmas yra palyginti retas įvykis daugumai piliečių. Vartotojams neapsimoka mokytis naujų procedūrų, jei jomis bus naudojamasi itin retai. Daugumoje atvejų, kai pasirašomi dokumentai, vartotojui tas nieko ar beveik nieko nekainuoja. Tik retesniais atvejais vartotojui reikia nuvykti į konkrečią vietą, laukti eilėje ir tik tada pasirašinėti (gaištamas laikas, pinigai kelionei). Fizinis kontaktas dokumentų pasirašymo metu suteikia papildomą vertę vartotojui: paslaugos tiekėjo atstovas suteikia papildomos informacijos, paaiškina, konsultuoja, pataiso dokumento užpildymo klaidas ir pan.

LITERATŪROS SĄRAŠAS

1. Capgemini (2006 m.). Viešosios paslaugos internetu: kokia yra Europos pažanga? // http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/evaldzia/CAPGEMINI_2006.pdf, prisijungimo laikas 2007-12-09;
2. Capgemini (2007 m.). „Paslaugos naudotojo iššūkis. Viešųjų elektroninių paslaugų teikimo tyrimas“ // http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/egov_benchmark_2007.pdf, prisijungimo laikas 2007-12-09;
3. Civilka M., Elektroninio parašo reglamentavimo problemos // http://www.itc.tf.vu.lt/mokslas/, prisijungimo laikas 2007-10-10;
4. Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas, investicinis projektas (galimybių studija) // 2006;
5. Domarkas V., Lukoševičienė V., Elektroninė valdžia informacijos teikimo visuomenei aspektu // Viešoji politika ir administravimas. 2006, Nr.16;
6. E parašas sunkiai skinasi kelią // Veidas. 2006 10 19;
7. E.parašas – kas tai? Animacinis filmukas apie e. parašo naudojimą // http://epp.ivpk.lt/lt/apie/naudotojams, prisijungimo laikas 2007-12-08;
8. Elektroninės paslaugos Lietuvoje. Kas naudingo? // http://www.smn.lt/files/e-paslaugos.pdf, prisijungimo laikas 2007-09-15;
9. Elektroninės valdžios plėtra Lietuvoje // http://www.infobalt.lt/main.php?&s=62&r=348&i=7518, prisijungimo laikas 2007-12-09;
10. Elektroninės viešosios paslaugos Lietuvoje // http://www.ivpk.lt/main-aktual.php?cat=61&gr=1&n=11, prisijungimo laikas 2007-10-01;
11. Elektroninio parašo įdiegimo viešajame administravime parengiamieji darbai, IVPK prie LR Vyriausybės ir Vilniaus universiteto darbo ataskaita II etapas (atnaujinta versija) // http://www.ivpk.lt/dokumentai/ataskaitos/epdiegimodarbai(II%20etapas).doc, prisijungimo laikas 2007-12-10;
12. Elektroninio parašo priežiūros institucijos Lietuvos Respublikos Elektroninio parašo įstatymo įgyvendinimo metinė ataskaita // www3.lrs.lt/docs2/LVXJZCFZ.DOC, prisijungimo laikas 2007-12-09;
13. Elektroninio parašo proveržio programa // http://www.omnitel.lt/includes/bin/219_377794_ep.pdf, prisijungimo laikas 2007-12-10;

14. Elektroninis parašas kol kas nepakeičia rašalinio pirmtako // http://www.doclogix.lt/index.php?mid=26&lang=lt&nid=164, prisijungimo laikas 2007-12-09;
15. Elektroninių viešųjų paslaugų modelio įgyvendinimo aprašymas // http://www.epractice.eu/files/media/media_253.pdf, prisijungimo laikas 2007-12-08;
16. Elektroninių viešųjų paslaugų siekiamo modelio aprašymas // http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_siekiamasV1.pdf, prisijungimo laikas 2007-12-08;
17. E-valdžia – įrankis, tarnaujantis žmogui // http://www.vrm.lt/index.php?id=633, prisijungimo laikas 2007-08-15;
18. Europos Bendrijos Komisijos komunikatas i2010 e. vyriausybės veiksmų planas: e. vyriausybės plėtros spartinimas Europoje visų labui, 2006 04 25;
19. Europos Bendrijos Komisijos komunikatas, i2010 – Europos informacinė visuomenė augimui ir užimtumui skatinti. 2005.06.01;
20. Europos bendrijų komisijos komunikatas, Visą Europą apimančių e. vyriausybės paslaugų sąveika. 2006.02.13;
21. Funkat D., Elektroninio parašo reguliavimas // http://www.ic.lt/e-teise/Default.asp?DL=L&TopicID=11, prisijungimo laikas 2007-08-15;
22. i2010 elektroninės valdžios veiksmų planas // http://www.vrm.lt/index.php?id=465, prisijungimo laikas 2007-12-09;
23. Internetinės bankininkystės vartotojų skaičius per metus išaugo 40 proc. // http://www.it-partner1.com/lt/news/31/46/Internetines_bankininkystes_vartotoju_skaicius_per_metus_isaugo_40_proc..html, prisijungimo laikas 2007-02-12;
24. Jastiuginas S., Elektroninės valdžios koncepcijos įgyvendinimo eiga ir rezultatai // www3.lrs.lt/docs2/MNLXZOIK.PPT, prisijungimo laikas 2007-10-01;
25. Jonaitis A. Akys nemeluoja, pirštai garantuoja // Kopiuterija. 2007-10;
26. Juškaitė J., A. Zabulis: Elektroninė valdžia – neįvertinta nauda valstybei // http://www.verslosavaite.lt/content/view/1457/119/, prisijungimo laikas 2007-12-10;
27. Kalinauskas R., Elektroninis parašas ir elektroninis dokumentas // www.ivpk.lt/renginiai/pranesimai/r.kalinauskas.ppt, prisijungimo laikas 2007-09-01;
28. Kuriami Baltijos šalių elektroninės tapatybės nustatymo standartai // http://www.elektronika.lt/articles/computers/7512/, prisijungimo laikas 2007-12-10;
29. Kurcevičius A., E-parašo naudojimas banko teikiamose paslaugose. Hansabankas; 2007
30. Kurcevičius A., Mobilus E-parašas Hansabanke. Hansabankas;

31. Lamanauskas T., Elektroninio parašo įstatymas Lietuvoje: privalumai ir trūkumai // http://www.ic.lt/e-teise/Default.asp?DL=L&TopicID=11, prisijungimo laikas 2007-08-15;
32. Lietuvos Respublikos elektroninio parašo įstatymas // Valstybės žinios. 2002, Nr. VIII-1822;
33. Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr. 2115 " Dėl elektroninės valdžios patvirtinimo" // Valstybės žinios. 2003, Nr. 2-47;
34. Lietuvos Respublikos Vyriausybės 2003 m. lapkričio 25 d. nutarimas Nr. 1468 " Dėl elektroninės valdžios koncepcijos įgyvendinimo priemonių plano patvirtinimo" // Valstybės žinios. 2003, Nr. 112-5022;
35. Limba T., Elektroninės valdžios diegimas ir perspektyvos Lietuvoje: visuomenės ir valdžios institucijų sąveika // Informacijos mokslai. 2007 42-43;
36. Malinauskienė E., Elektroninės valdžios plėtros gairės: ateities scenarijai ir tyrimų kryptys // http://www.egovrtd2020.org/EGOVRTD2020/navigation/events/conferences/ISTAfrica_Presentation; prisijungimo laikas 2007-11-01;
37. Pagrindinių viešųjų paslaugų perkėlimo į elektroninę terpę laiko juosta iki 2012 metų // http://www.vrm.lt/fileadmin/Padaliniu_failai/Informacines_politikos_dep/evaldzia/1.gif, prisijungimo laikas 2007-12-09;
38. Portalas www.epractice.eu, prisijungimo laikas 2007-12-09;
39. Portalas www.ssc.lt/, prisijungimo laikas 2007-10-01;
40. Portalas www.eparasas.lt; prisijungimo laikas 2007-11-29;
41. Portalas www.epaslaugos.lt; prisijungimo laikas 2007-09-01;
42. Portalas www.esaugumas.lt; prisijungimo laikas 2007-11-15;
43. Portalas www.evaldzia.lt; prisijungimo laikas 2007-06-01;
44. Portalas www.parasas.lt, prisijungimo laikas 2007-11-29;
45. Pukėnas K., Sportinių tyrimų duomenų analizė SPSS programa // Kaunas, 2005;
46. Siūlomas informacinės visuomenės paslaugų reglamentavimo modelis // http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_reglamentavimasV1.pdf, prisijungimo laikas 2007-12-08;
47. Statistikos departamento prie Lietuvos Respublikos Vyriausybės duomenys;
48. Šablinskas R., E-parašo plėtra Lietuvoje: iššūkiai; Konferencija: Informacinė visuomenė: inovatyvios technologijos verslui ir mokslui.2007-10-22;
49. Šablinskas R., Mobile PKI: one step toward electronic society. Konferencija: Informacinė visuomenė: inovatyvios technologijos verslui ir mokslui.2007-10-22;

50. Šablinskas R., Mobilioji vartotojų identifikacija ir elektroninio parašo infrastruktūra mobiliuosiuose įrenginiuose;
51. Šablinskas R., Kurcevičius A., Elektroninis parašas // Infobalt, „Langas į ateitį“ seminaras, 2007-11-05;
52. Šalių teisės aktai, reglamentuojantys e.parašą // https://dsls.rechten.uvt.nl/, prisijungimo laikas 2007-12-08;
53. Šiandien Lietuvoje pradeda veikti mobilusis e-parašas // http://www.omnitel.lt/?m3_lt212535_213203z_393130, prisijungimo laikas 2007-10-19;
54. Trakimavičius A., Viešųjų elektroninių paslaugų, teikiamų per internetą, plėtra, problemos ir perspektyvos // www.ivpk.lt/dokumentai/prezentacijos/seminaras/vep.ppt, prisijungimo laikas 2007-10-15;
55. Undzėnas V., Elektroninė komercija (elektroninio parašo klausimai) // Vilnius, 2006;
56. Valdžios elektroninių vartų funkcionavimo teikiant viešąsias elektronines paslaugas taisyklės, patvirtintos Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2005 m. gruodžio 30 d. įsakymu Nr. T-127 // Valstybės žinios. 2006, Nr.3-90;
57. Viešosios paslaugos „Asmens dokumentai“ perkėlimas į elektroninę terpę investicinis projektas (galimybių studija) // 2006;
58. Viešųjų paslaugų tiekimo esamos būklės analizė ir modelio aprašymas // http://epp.ivpk.lt/epp/Dokumentai/IVPK_elmodelis_esamasV1.pdf, prisijungimo laikas 2007-12-08;
59. VRM vykdomų projektų e. valdžios srityje pristatymas // http://www.vrm.lt/index.php?id=465, prisijungimo laikas 2007-12-09;
60. Zabulis A., Informacinė visuomenė ir e. valdymo plėtra, bendradarbiaujant viešajam ir privačiam sektoriui // www.egovernance2007.lt/c/document_library/get_file?folderId=11&name=DLFE-113.ppt, prisijungimo laikas 2007-12-09;
61. Židonis E., Elektroninio parašo diegimas viešajame administravime: galimybės ir problemos // www.ivpk.lt/dokumentai/prezentacijos/seminaras/el_parasas.ppt, prisijungimo laikas 2007-10-01;

SANTRAUKA

Informacinių technologijų pasiekimų pritaikymas valstybės valdymui atveria naujas didžiules galimybes gyventojų bendradarbiavimui su valdžios institucijomis, skaidresniam valdymui, aiškesniam sprendimų priėmimui. Jis sudaro gyventojui visiškai naujas galimybes bendrauti ir dirbti su viešojo administravimo institucijomis sau patogiu laiku, bet kurioje vietoje ir įvairiais būdais. Kai paslaugos pradėtos perkelti į elektroninę erdvę, iškilo svarbus klausimas: kaip atpažinti asmenį prieš suteikiant jam informaciją? Prieš pateikiant duomenis informacijos tiekėjas turi įsitikinti, kad perduoda duomenis būtent tam asmeniui, kuris padarė užklausą. Atitinkamai užklausą padaręs asmuo turi autentifikuoti save, arba kitaip sakant įrodyti savo tapatybę. E-valdžios koncepcijoje taip pat buvo planuota sukurti asmens identifikavimo sistemą, atitinkančią Europos Sąjungos reikalavimus. Ji turėtų neklystamai identifikuoti asmenį ir informacinių technologijų pagalba bendrauti su viešojo administravimo institucijomis.

Darbo tikslas – įvertinti galimus ir perspektyvius asmens identifikavimo būdus; išanalizuoti jų patikimumo, saugumo ir sąveikumo aspektus; pateikti numatomų priemonių rekomendacijas.

Uždaviniai:

1. išnagrinėti esamus bei alternatyvius asmens identifikavimo elektroninėje erdvėje būdus;
2. apžvelgti naujausių technologijų siūlomus asmens identifikavimo būdus;
3. išanalizuoti geriausius asmens identifikavimo pavyzdžius Europos Sąjungoje bei kitose užsienio šalyse;
4. atlikus tyrimą įvertinti asmens identifikavimo problemas Lietuvoje, pasiūlyti sprendimo būdus.

Teorinę darbo dalį sudaro pirmieji trys skyriai. Pirmajame skyriuje nagrinėjami esami bei alternatyvūs asmens identifikavimo elektroninėje erdvėje būdai: elektroninis parašas, mobilus elektroninis parašas, asmens identifikavimas per bankų sistemas, apžvelgiamas investicinis projektas (galimybių studija) "Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas". Antrajame skyriuje apžvelgiamas naujausių technologijų taikymas sprendžiant asmens identifikavimo problemas. Trečiajame skyriuje analizuojami geriausios praktikos pavyzdžiai pasaulyje, priemonės Europos Sąjungoje.

Praktinė dalis – ketvirtasis skyrius, atliktas gyventojų naudojamų būdų identifikuotis elektroninėje erdvėje tyrimas. Tyrimo tikslas – ištirti, kokias būdais respondentai dažniausiai naudojasi identifikuojant save elektroninėje erdvėje, kokiomis viešosiomis paslaugomis naudojasi.

SUMMARY

Adaptation of information technologies to the country's administration opens up new opportunities for residents' cooperation with the governmental institutions, for more transparent administration and clearer decision-making process. It also presents new possibilities for a citizen to communicate and work with public administration institutions on convenient time, place and ways. When some services were moved to electronic space, an important question was raised: how to recognise people before any information was presented to them? Information supplier has to make sure he was transferring requested information to the person who had placed the request. Also, the person, who placed the request, has to identify himself or to prove his identity. The identification system meeting the requirements of the European Union was also planned to be created while drafting the concept of e-government. This system should infallibly identify a person and communicate with public administration institution with the help of information technologies.

The aim of the paper – is to evaluate possible and promising person identification ways; to analyse the aspects of their reliability, safety and interaction; and to supply recommendations of anticipatory measures.

Objectives:

1. to discuss current and alternative ways to identify a person in electronic space;
2. to review identification solutions presented by the newest information technologies;
3. to analyse the best examples of person identification systems in the European Union and other foreign countries;
4. having conducted a research, to evaluate person identification problems in Lithuania and offer possible solutions.

The theoretical part consists of the first three chapters. The first chapter discusses the current and alternative ways to identify a person in electronic space: e-signature, mobile e-signature, person identification via banking systems and the investment project (a study of possibilities) "Daugiafunkcinių mikroprocesorinių asmens dokumentų išrašymas ir panaudojimas". The second chapter presents the adaptation of the newest technologies to solve problems of identifying a person, and the third chapter analyses the most effective examples of identification systems in the world as well as measures applied in the European Union.

The practice part is the fourth chapter, which presents the research into people's ways to identify themselves in electronic space. The aim of the research was to learn which ways were used by respondents most frequently to identify themselves in electronic space and which public services they used most.

Priedas Nr. 1

ELEKTRONINIO PARAŠO PASLAUGŲ TEIKIMO SUTARTIES BENDROSIOS SĄLYGOS

Elektroninio parašo paslaugas teikia AB Sertifitseerimiskeskus, Piarnu 12, Talinas, Estija, kuris veikia kaip sertifikavimo tarnyba (**toliau vadinama CA**) ir UAB Omnitel, Ševčenkos 25, Vilnius, Lietuva, kuri veikia kaip registravimo tarnyba (**toliau vadinama RA**) ir atstovauja CA.
Sertifikavimo Tarnybų kiekis gali keistis be išankstinio kliento įspėjimo. Tuo atveju, jei sertifikavimo paslaugas atlieka kita CA, yra laikoma, jog visos Elektroninio parašo paslaugų teikimo sutarties bendrosios sąlygos (toliau - „Bendrosios sąlygos“) galioja.

1. Apimtis.
Bendrosios sąlygos reglamentuoja sertifikavimo paslaugų teikimą klientui iš CA pusės ir sertifikavimo paslaugų naudojimą iš kliento pusės.

2. Objektas.
Klientui teikiamos sertifikavimo paslaugos atitinka apibendrintą sertifikavimo paslaugų teikimo politiką, aprašomą dokumentu „Apibendrintos sertifikavimo veiklos nuostatos“ (**toliau tekste vadinama G-CPS**) ir sertifikato politika, aprašomą dokumentu „Sertifikato taisyklės“ (**toliau tekste vadinama CP**). Šie du dokumentai yra pridedami prie Bendrųjų sąlygų kaip priedai Nr. 1 ir Nr. 2.

3. Apibrėžimai.
Bendrosiose sąlygose taikomi terminai, sutrumpinimai ir apibrėžimai yra įvardinti G-CPS dokumento punkte Nr. 5 „Žodynas ir sutrumpinimai“.

4. CA atsakomybė.
Teikiant sertifikavimo paslaugas CA vykdo savo įsipareigojimus, įvardintus sertifikavimo paslaugų teikimo nuostatose (CPS). Klientui patvirtinus sertifikato galiojimą, CA garantuoja savo įsipareigojimų įvykdymą.

5. Duomenų registravimo funkcijų perdavimas.
RA perima iš CA dalį sertifikavimo paslaugų: tarpininkauja tarp kliento ir CA, atlikdama sekančias paslaugas:
5.1 Užklausų dėl sertifikato išdavimo ir atšaukimo priėmimas ir apdorojimas;
5.2 Užklausų pateikėjų tapatybės nustatymas;
5.3 Asmeninių duomenų saugojimas, išpildant vietos įstatymų reikalavimus;
5.4 Kriptografinių raktų generavimas ir šių raktų nešėjų pateikimas klientams.

6. Kliento sutikimas.
Pasirašydamas šias Bendrąsias sąlygas klientas pripažįsta ir sutinka, kad:
6.1 Galiojančio sertifikato panaudojimas atitinka ranka pasirašomą parašą ir turi tokias pat juridines pasekmes;
6.2 Jis/ji perskaitė dokumentus G-CPS ir CP;
6.3 Jis/ji gavo instrukciją apie sertifikato aktyvavimą, panaudojimą bei įspėjimus dėl jo saugumo;
6.4 Jis/ji supranta CA paslaugų pobūdį ir pobūdį paslaugų, kurias teikia trečiosios šalys - paslaugų teikėjai, savo veikloje taikantys sertifikatus;
6.5 Jis/ji supranta CA įsipareigojimus ir atsakomybę bei šios atsakomybės ribas, aprašomas dokumentuose G-CPS ir CP;
6.6 CA ir/arba RA gali atsisakyti klientui suteikti sertifikavimo paslaugas, nepaaiškinant savo tokio atsisakymo priežasčių;
6.7 RA gali pareikalauti atšaukti kliento sertifikatą, jei klientas to pageidauja arba jei RA gauna informaciją, jog:
6.7.1. Klientui suteiktas privatusis raktas, atitinkantis viešąjį raktą, įvardintą sertifikate, buvo galimai arba realiai pamestas, atskleistas, pavogtas ar kitaip pažeistas;
6.7.2. Buvo prarasta/pažeista privataus rakto kontrolė dėl "signataro PIN" (**toliau vadinamas sPIN**) kodo vagystės ar dėl kitų priežasčių;
6.7.3. Sertifikate įrašyti duomenys yra netikslūs arba pasikeitę;
6.7.4. Sertifikatas buvo sukurtas/suteiktas klaidingai dėl sekančių priežasčių:
- Pažeista asmens duomenų registracijos ir/arba patikrinimo procedūra arba yra nustatyta, jog registracijos metu pateikti duomenys yra nepilni ir/arba yra negaliojantys, ir/arba neįmanoma nustatyti šių duomenų autentiškumo ar galiojimo;
- Turima faktų arba pagrįstų spėjimų, jog sertifikato išdavimas buvo neteisėtas;
- Žinomos aplinkybės, kurios pagrįstai įtakoja sertifikato arba su juo susijusių kriptografinių raktų patikimumą, saugumą ar integralumą.
6.8 Sertifikate pateikiami asmens duomenys (vardas, pavardė, asmens tapatybės kodas) yra traktuojami kaip vieša informacija, pasiekiama trečiosioms šalims;
6.9 CA sprendžia visus ginčus, susijusius su nesutarimais, liečiančiais sertifikavimo paslaugas, CA suteiktus sertifikatus ir skaitmeninius parašus, patvirtintus šiais sertifikatais. Bet kokios užklausos, skundai, ieškiniai ar įspėjimai į CA patenka per RA, kuris gautą informaciją nukreipia į CA.

7. Kliento įsipareigojimai ir atsakomybė.
7.1 Pateikdamas užklausą sertifikatui gauti klientas sutinka:
7.1.1. Pateikti tikslią ir detalią asmeninę informaciją;
7.1.2. Patikrinti asmens duomenis ir patvirtinti jų korektiškumą aktyvuojant sertifikatą. O taip pat įspėti RA apie bet kokius duomenų neatitikimus.
7.2 Priimdamas sukurtą sertifikatą klientas įsipareigoja/atsako už tai, jog:
7.2.1. Duomenys sertifikate yra tikslūs;
7.2.2. Pasirašymo sPIN kodas yra žinomas tik jam/jai ir niekam kitam;
7.2.3. Jis/ji naudosis kriptografiniais raktais ir sertifikatais taip, kaip tą apibrėžia dokumentas CP;
7.2.4. Jis/ji panaudos visas protingas priemones, siekiant užkirsti kelią tretiesiems asmenims pasinaudoti kriptografiniais raktais, susietais su sertifikatu;
7.2.5. Jis/ji nedelsiant praneš RA, jog atšaukia sertifikatą tais atvejais, kai jis/ji turi pagrįstų įtarimų, jog kriptografiniai raktai, SIM kortelė ir/arba sPIN kodas buvo pažeisti, pamesti ar jų saugumas paveiktas kokiais nors kitais būdais;
7.2.6. Jis/ji padengs mokesčius, susijusius su sertifikavimo paslaugomis.

8. Sertifikato priėmimas.
Sertifikatas laikomas kliento priimtu/patvirtintu po sertifikato aktyvavimo procedūros įvykdymo.

9. Sertifikato galiojimo terminai ir apmokėjimo sąlygos.
Klientui išduotas sertifikatas galioja 1 metus.. Sertifikatas gali būti atšauktas blokavus kriptografinių raktų nešėją. Klientas apmoka už sertifikavimo paslaugas pagal RA pateikiamas sąskaitas.

10. Atsakomybės apribojimai.
CA atsakomybės teiginiai, išdėstyti dokumentuose G-CPS ir CP, yra taikomi visiems ieškiniams, kylantiems dėl sertifikatų ir sertifikavimo paslaugų, atliekamų iš CA ir RA pusės, teikimo. Atsakomybės apribojimai yra taikomi visiems ieškiniams prieš CA ir/ar RA. Apribojimai taikomi konkrečiam sertifikatui, nežiūrint į tai, kiek operacijų atlikta, kiek dokumentų pasirašyta, kiek įvyko priežastinių pasekmių ar kiek suteikta paslaugų dėl sertifikato panaudojimo. Šie apribojimai yra taikomi bet kokiai atsakomybei, kylančiai dėl kontraktų, civilinės teisės pažeidimų (įskaitant aplaidumą) ar atsakomybei pagal bet kurią kitą atsakomybės teoriją, apimant tiesioginę, netiesioginę, specialią, nuobaudos, įprastinę, šalutinę, priklausomą ar netyčinę žalą.

11. Duomenų apsauga ir privatumas.
Klientas suteikia teisę viešai publikuoti duomenis, pažymėtus kaip "sertifikato informacija" ir „sertifikato statusas“. Šis publikavimas bus atliekamas internete ar kitomis CA pasirinktomis priemonėmis tam, kad teikti sertifikavimo paslaugas. Klientas suteikia teisę CA ar RA atskleisti bet kokią su sertifikatais susijusią informaciją, kaip būdą išsiaiškinti sertifikatų patikimumą arba išsiaiškinti sertifikatų bei jais paremtų elektroninių parašų juridinės galios statusą, nežiūrint į tai, jog konkretus sertifikatas yra galiojantis, atšauktas arba jo galiojimo laikas pasibaigęs.

12. Nuostolių padengimas.
Klientas įsipareigoja padengti nuostolius ir atleisti nuo atsakomybės CA, RA, jų vadovus bei darbuotojus, agentus ar susijusius asmenis, jei klientas naudoja sertifikatus kitiems tikslams ar pažeidžia sertifikatų naudojimo taisykles, kaip tai numatyta Bendrosiose sąlygose ir su jomis susijusiuose dokumentuose.

13. Elektroninės sutartys.
Pasirašydamas Bendrąsias sąlygas bei sutartį dėl elektroninio parašo paslaugų teikimo, klientas sutinka, jog kontraktų, sutarčių sudarymas, pranešimų siuntimas ir komunikacija, gali būti atliekami elektroniniais būdais.

14. Nutraukimas.
Sutartį dėl elektroninio parašo paslaugų teikimo gali nutraukti bet kuri iš pasirašiusiųjų šalių bet kuriuo metu. Tuo atveju, jei klientas nutraukia šią sutartį be priežasties, kliento sumokėti mokesčiai nėra grąžinami. Tuo atveju, kai sutartį be priežasties nutraukia CA, ji grąžina kliento mokesčius pagal bendrąją tokiems atvejams taikomą mokesčių grąžinimo politiką. Jei CA nutraukia sutartį dėl tam tikrų priežasčių (pvz.: kai klientas pažeidžia sutarties sąlygas), kliento sumokėti mokesčiai nėra grąžinami. Visais atvejais sutartis yra nutraukiama jei pasikeitė kliento informacija, pateikta šios sutarties užsakymo lape, duomenų laukeliuose 1, 3 arba 8.

15. Vientisumas.
Jei bet kuris Bendrųjų sąlygų punktas, sakinys ar frazė yra pripažįstami kaip negaliojantys ar prieštaraujantys įstatymams, tuomet tai neįtakoja kitų Bendrųjų sąlygų punktų, sakinių ar frazių galiojimo.

16. Taikoma teisė.
Bendrosios sąlygos bei sutartis dėl elektroninio parašo paslaugų teikimo yra interpretuojamos pagal Lietuvos Respublikos įstatymus ir šalys sutinka vadovautis išskirtinai Lietuvos teismų jurisdikcija.

Priedas Nr. 2

PRIEDAS NR. 1
APIBENDRINTI SERTIFIKAVIMO VEIKLOS NUOSTATAI (G-CPS)

1. **Įvadas**

Šis dokumentas yra sertifikavimo tarnybų sertifikavimo veiklos nuostatų apibendrinimas, nusakantis aplinką, kurioje yra kuriami kvalifikuoti sertifikatai, teikiami UAB OMNITEL abonentams.

Šis dokumentas nėra taikomas konkrečiai sertifikavimo tarnybai, tačiau visų sertifikavimo tarnybų, teikiančių kvalifikuotus sertifikatus UAB OMNITEL abonentams, nuostatai yra suderinami su teiginiais, išsakytais šiame dokumente. Šiame dokumente pateikti pagrindiniai ir esminiai teiginiai, su kuriais klientui būtina susipažinti prieš pradedant naudoti savo kvalifikuotą sertifikatą. Šalims, kurios pasitiki sertifikatais, šis dokumentas nėra pakankamas – šios šalys privalo analizuoti sertifikavimo veiklos nuostatus kiekvienos tarnybos, teikiančios kvalifikuotus sertifikatus UAB OMNITEL abonentams.

2. **Taikymo sritis**

2.1 Sertifikavimo Tarnyba (toliau vadinama CA)

CA sukuria kvalifikuotus sertifikatus, atitinkančius sertifikato taisykles (**toliau tekste vadinama CP**. Žiūr. priedą Nr.2 „Sertifikato taisyklės"), prisilaikydama savo veiklos nuostatų. Sertifikavimo tarnyba rūpinasi kvalifikuoto sertifikato gyvenimo ciklo užtikrinimu.

2.2 Registravimo Tarnyba (toliau vadinama RA)

RA veikia kaip CA atstovas santykiuose tarp *vartotojo* ir CA.

2.3 Vartotojas

2.3.1. Klientas

Klientas yra kvalifikuoto sertifikato turėtojas (UAB OMNITEL abonentas).

2.3.2. Pasitikinčioji šalis

Pasitikinčioji šalis yra šalis, kuri nusprendžia pasitikėti konkrečios CA išduotu kvalifikuotu sertifikatu.

Pasitikinčioji šalis:

- įvertina sertifikavimo veiklos nuostatus (G-CPS), sertifikato taisykles (CP), registracijos taisykles (RP), kitus susijusius dokumentus;
- patikrina kvalifikuoto sertifikato galiojimą;
- patikrina kvalifikuoto sertifikato atitikimą jo pritaikymo sričiai;
- patikrina parašą ir susijusius duomenis, bei identifikuoja pasirašiusįjį asmenį

3. **Bendrosios sąlygos**

3.1. Pareigos

3.1.1. Sertifikavimo tarnybų pareigos

Sertifikavimo tarnybos užtikrina, kad:

- Sertifikavimo paslaugos teikiamos prisilaikant vietos įstatymų;
- Sertifikavimo paslaugos teikiamos prisilaikant savo sertifikavimo veiklos nuostatų, kurie yra suderinami su šiuo dokumentu.

Sertifikavimo tarnybos:

- viešai skelbia savo sertifikavimo veiklos nuostatus ir sertifikato taisykles (CP), ir šie dokumentai yra pasiekiami internetu;
- užtikrina neskelbiamų asmens duomenų konfidencialumą;
- palaiko savo išduotus sertifikatus (valdo jų gyvenimo ciklą);
- priima kvalifikuotų sertifikatų atšaukimo užklausas 24 valandas per parą;
- užtikrina pastovią galimybę internetu patikrinti savo išduotų sertifikatų galiojimą;
- išsaugoja visus su sertifikatais susijusius dokumentus iki savo veiklos nutraukimo;
- atlieka kasmetinį savo sistemų auditą ir viešai publikuoja audito išvadas;
- internete skelbia savo privalomojo veiklos draudimo polisus.

Sertifikavimo tarnybos užtikrina, jog jų darbuotojai neturi teistumo dėl tyčinių nusikaltimų

3.1.2. Registravimo tarnybos pareigos

RA priima paraiškas kvalifikuotiems sertifikatams gauti ir jiems panaikinti, šias paraiškas patikrina, prisilaikydama procedūrų, aprašytų registracijos taisyklėse (RP). RA pateikia klientams pasirašymo įrangą ir perduoda surinktus asmens duomenis į CA sertifikatų gamybai.

3.1.3. Kliento pareigos

Klientas privalo pateikti apie save teisingą ir išsamią informaciją. Pasikeitus asmens duomenims, klientas privalo apie tai informuoti RA. Klientas privalo nedelsiant pranešti, jei jam suteikta pasirašymo įranga galimai pasinaudojo tretieji asmenys. Klientas yra išimtinai atsakingas už jam suteiktos pasirašymo įrangos priežiūrą. Klientas privalo žinoti, jog pasirašinėti atšauktais arba pasibaigusio galiojimo sertifikatais yra neleistina.

3.1.4. Pasitikinčiosios šalies pareigos

Pasitikinčioji šalis išanalizuoja atsakomybes ir rizikas, susijusias su pasitikėjimu panaudojant sertifikatą. Atvejais, kai nėra pakankamai įrodymų dėl sertifikato galiojimo jo panaudojimo momentu, pasitikinčioji šalis privalo analizuoti atšauktų sertifikatų sąrašą, galiojusį tuo metu, kai buvo panaudotas sertifikatas. Pasitikinčioji šalis privalo sekti sertifikato taisyklėse numatytus apribojimus ir naudoti sertifikatą tik pagal paskirtį.

3.1.5. Publikavimo tarnybos pareigos

Publikavimo tarnyba privalo pateikti visoms suinteresuotoms šalims informaciją apie sertifikatus ir jų galiojimą:

- Tarnyba saugo visus galiojančius sertifikatus ir jų statusą;
- Tarnyba veikia 24 valandas per parą;
- Tarnyba turi apsaugos priemones nuo simuliacijos ir užtikrina pateikiamų duomenų integralumą.

3.2. Atsakomybė

CA atsakinga už savo pareigų, įvardintų punktuose 3.1.1 ir 3.1.5 vykdymą taip, kaip numatyta vietos įstatymuose. CA nėra atsakinga už klientų privačių raktų apsaugą, neteisingą sertifikatų panaudojimą, neadekvačius pasitikinčiųjų šalių tikrinimus.
Nenugalimos jėgos (Force majeure) įvykių atvejais, sertifikavimo veiklos nuostatų (CPS) nevykdymas nėra laikomas pareigų nesilaikymu.
RA atsakinga už savo pareigų, įvardintų 3.1.2. prisilaikymą.

3.3. Ginčų sprendimas

Visi ginčai tarp šalių sprendžiami derybų būdu. Šalims nepavykus susitarti, ginčas sprendžiamas teisme, Vilniuje.
Susijusios šalys informuojamos apie problemą/ieškinį ne daugiau, kaip 30 dienų įvykus problemai, išskyrus įstatymuose numatytus atvejus.

4. Fizinės ir organizacinės saugumo priemonės

Saugumo valdymo prasme CA vadovaujasi visuotinai pripažintais standartais, pvz. ISO 13335, ISO 13569. Kiekviena CA laikosi vietos įstatymų/reglamentų, reguliuojančių kvalifikuotų sertifikatų išdavimą. Atvejais, kai vietos įstatymai nenusako kitaip, laikoma, kad CA užtikrina saugomų objektų saugumą su EAL-4 patikimumo lygiu, nustatomu standarte ISO/IEC 15408-1.
Privatiesiems raktams techninės saugumo priemonės aprašomos CP dokumente. Kiti techniniai saugumo klausimai (pvz., CA sistemų saugumas prieigos kontrolei, programinės įrangos saugumas, tinklų saugumas ir pan.), slaptos informacijos apsauga ir t.t. aprašomi kiekvienos CA sertifikavimo veiklos nuostatose.

5. Žodynas ir sutrumpinimai

Kursyvu paryškinti žodžiai šiame dokumente turi sekančią prasmę:

Raktinis žodis	Apibrėžimas
Autentifikacija	Asmens tapatybės nustatymas
Kvalifikuotas sertifikatas	Įstatymų reikalavimus atitinkantis paliudijimas, jog konkrečios pasirašymo įrangos turėtojas yra konkretus fizinis asmuo
Sertifikavimo tarnyba (CA)	Tarnyba, savo *skaitmeninių parašu* pasirašanti elektroninius asmens tapatybės paliudijimus ir vėliau tuos paliudijimus prižiūrinti
Sertifikato taisyklės (CP)	Dokumentas, nusakantis sertifikato savybes, turinį bei sertifikato panaudojimo sritis
Sertifikavimo veiklos nuostatos (CPS)	Rinkinys taisyklių, nusakančių kaip sertifikavimo tarnyba vykdo savo veiklą
Sertifikavimo paslaugos	Sekančios paslaugos: sertifikatų sukūrimas, sertifikatų patikrinimo priemonių palaikymas, sertifikatų atšaukimas
Pasirašymo įranga	Techninė priemonė sauganti slaptus raktus panaudojamus *skaitmeniniams parašams* sukurti
Klientas	Fizinis asmuo, sertifikato turėtojas , UAB OMNITEL abonentas
Negaliojančių sertifikatų registras (CRL)	Sąrašas sertifikatų, paskelbtų negaliojančiais
Skaitmeninis parašas	Speciali informacija (pridedama prie pasirašomo dokumento), leidžianti dokumento gavėjui nustatyti kas dokumentą pasirašė ir ar nebuvo dokumentas pakeistas po pasirašymo
Publikavimo tarnyba	Sertifikatų galiojimo informacijos publikavimo tarnyba
Pasitikinčioji šalis	Šalis, kuri priima sprendimą remdamasi skaitmeniniu parašu
Privatusis raktas	Slaptas raktas, saugomas *pasirašymo įrangoje*. Šiuo raktu *užkoduojamas* pasirašomas turinys
Registracijos taisyklės	Taisyklės, nusakančios kaip RA suteikia *klientui pasirašymo įrangą* ir kaip inicijuojamas *kvalifikuoto sertifikato* sukūrimas
Registravimo tarnyba (RA)	Tarnyba, veikianti kaip CA atstovas, priimantis vartotojų paraiškas *kvalifikuotiems sertifikatams* gauti, šias paraiškas patikrinanti ir perduodanti surinktus asmens duomenis į CA.
sPIN	Signataro (pasirašančiojo asmens) PIN kodas, aktyvuojantis *privatųjį raktą* prieš kiekvieną pasirašymą (*skaitmeninio parašo* sukūrimą)
Užkodavimas	Informacijos transformacija tokiu būdu, jog ją galima perskaityti tik turint atitinkamą raktą
Viešasis raktas	Raktas, leidžiantis patikrinti *skaitmeninio parašo* teisingumą (atkoduoti *privačiuoju raktu užkoduotą* informaciją)

Priedas Nr. 3

PRIEDAS NR. 2

SERTIFIKATO TAISYKLĖS (CP)

Šis dokumentas pateikia sertifikato (elektroninio asmens tapatybės paliudijimo) ir šio sertifikato panaudojimo sritie/sąlygų aprašymą. Šis dokumentas yra viešai prieinamas ir yra skirtas visiems sertifikato vartotojams. Visos sertifikavimo tarnybos, išduodančios UAB OMNITEL klientams elektroninius asmens tapatybės paliudijimus - sertifikatus, privalo užtikrinti, kad jų sukuriami sertifikatai atitinka šias Sertifikato Taisykles.

Reikalavimai sertifikatams, leidžiantiems identifikuoti asmenis ir kurti asmeninius elektroninius parašus

1. **Įvadas**

Ši dokumentas (Sertifikato Taisyklės arba CP) yra kvalifikuoto sertifikato kaip produkto aprašymas. CP aprašo šio produkto savybes ir panaudojimo principus.

Trumpas produkto aprašymas:

Klientui pateikiamas vienas kvalifikuotas sertifikatas, kuris gali būti naudojamas kurti **skaitmeniniams parašams** (turintiems tokias savybes ir tokią juridinę galią, kaip ir ranka pasirašytas asmens parašas) bei kliento **autentifikavimui**. Sertifikatas yra susiejamas su privačiuoju raktu, kuris saugiai patalpintas pasirašymo įrangoje (specialioje SIM kortelėje) ir gali būti aktyvuotas tik sertifikato turėtojo, žinančio slaptą pasirašymo PIN kodą - sPIN. Skaitmeninis parašas gali būti sukuriamas bet kokiems duomenims, jis yra unikalus būtent tiems pasirašomiems duomenims, nėra techninių priemonių, leidžiančių tokį pat parašą sukurti kitam asmeniui. Klientas vienu metu gali turėti tik vieną kvalifikuotą sertifikatą, susietą su pasirašymo įranga.

Šis dokumentas aprašo pagrindinius aspektus, nusakančius UAB OMNITEL (veikiančios kaip registravimo tarnyba (RA)) klientams suteikiamus kvalifikuotus sertifikatus.

2. **Taikymo sritis**

2.1. **Sertifikavimo tarnyba (CA)**

Kvalifikuotus sertifikatus pagamina Sertifikavimo Tarnyba (CA). Yra keletas sertifikavimo tarnybų, bendradarbiaujančių su RA, pateikiant klientams kvalifikuotus sertifikatus ir juos vėliau prižiūrint. Kiekviena CA veikia skirtingoje saugioje aplinkoje, kuri aprašoma šių tarnybų patvirtintose sertifikavimo veiklos nuostatose (CPS), kurios yra vieši dokumentai, publikuojami internete. Klientui susipažinimui yra pateikiami "apibendrinti sertifikavimo veiklos nuostatai", kurie yra suderinami su atskirų CA CPS ir yra sutrumpinta jų versija. Visų susijusių CA sąrašas yra pateikiamas internete adresu www.omnitel.lt. Atvejais, kai šiame CP dokumente pateikiami nuostatai prieštarauja CPS, yra laikoma, kad galioja CP nuostatai.

2.2. **Registravimo tarnyba (RA)**

RA veikia kaip CA atstovas santykiuose tarp kliento ir CA visais kvalifikuotų sertifikatų (siejamų su mobiliaja pasirašymo įranga SIM kortelėse) klausimais.

RA veikia pagal registracijos taisykles (**toliau tekste vadinama RP**. Žiūr. priedą Nr.3 „Registravimo taisyklės") - viešai skelbiamą dokumentą. RA ir CA santykiai yra reguliuojami atskirų susitarimu ir atitinka CP bei RP. 24 valandas per parą veikianti klientų aptarnavimo/pagalbos telefono linija įgalina klientus atšaukti kvalifikuotus sertifikatus (žiūr. www.omnitel.lt).

2.3. **Klientas**

Klientas yra fizinis asmuo, atstovaujantis save ir esantis aktyvus UAB OMNITEL mobiliojo ryšio abonentas. Klientui pateikiamas kvalifikuotas sertifikatas, atitinkantis šias CP ir RP. Sertifikatas (elektroninis asmens tapatybės paliudijimas) susieja viešąjį raktą (atitinkantį privatųjį raktą saugomą mobiliajame pasirašymo įrenginyje - SIM kortelėje) su kliento asmenine informacija.

2.4. **Sertifikato taikymo sritys**

Sertifikatas, išduodamas pagal šį CP yra laikomas **kvalifikuotu sertifikatu** ir gali būti naudojamas:

- **-skaitmeniniam pasirašymui**, kaip tai apibrėžta LR Elektroninio Parašo Įstatyme,
- **-elektroninei identifikacijai** nustatant sertifikato turėtojo tapatybę,
- **-duomenų užkodavimui**.

Šios CP neriboja sertifikato panaudojimo kitiems uždaviniams.

3. **Bendrosios sąlygos**

3.1. **Sertifikavimo tarnybų pareigos**

CA teikia sertifikavimo paslaugas, derančias su šiomis CP ir su priedo Nr.1 G-CPS punktu 3.1.1. CA pagaminti sertifikatai yra nedelsiant paskelbiami internete (detalus publikavimo vietų sąrašas pateikiamas www.omnitel.lt). Atšaukti sertifikatai yra nedelsiant pašalinami iš publikuojamų sertifikatų sąrašų ir paskelbiami negaliojančių sertifikatų sąrašuose, kurie atnaujinami kas 12 valandų.

3.2. **Registravimo tarnybų pareigos**

Registravimo tarnyba priima iš klientų paraiškas dėl sertifikatų suteikimo ir jų atšaukimo. Paraiškose pateikiami duomenys patikrinami pagal procedūras, nustatytas RP. RA perduota visus surinktus duomenis į CA. CA papildomai:

- Užtikrina, kad saugumo priemonės yra suderintos su šiomis CP ir su priedu Nr. 1 (G-CPS);
- Pateikia klientui pasirašymo įrangą (specialią SIM kortelę su privačiuoju raktu), prisilaikydama RP aprašytų procedūrų;

- Pateikia klientui priemones aktyvuoti kvalifikuotą sertifikatą.

3.3. Kitos pareigos

Klientas privalo pateikti apie save teisingą ir išsamią informaciją. Pasikeitus asmens duomenims, klientas privalo apie tai informuoti RA. Klientas privalo nedelsiant pranešti, jei jam suteikta pasirašymo įranga galimai pasinaudojo tretieji asmenys.
Klientas yra išimtinai atsakingas už jam suteiktos pasirašymo įrangos priežiūrą. Klientas privalo žinoti, jog pasirašinėti atšauktais arba pasibaigusio galiojimo sertifikatais yra neleistina.

4. Sertifikato gyvavimo ciklas

4.1. Paraiška sertifikatui gauti

Paraiška suteikti kvalifikuotą sertifikatą gali būti pateikiama tik akivaizdiniu būdu. Pareiškėjo asmens tapatybė nustatoma pagal galiojantį asmens dokumentą. Klientui pateikiama speciali SIM kortelė ir privataus rakto aktyvavimo PIN kodas (sPIN). Detaliai procedūra aprašoma RP.

4.2. Kvalifikuoto sertifikato sukūrimas

Kvalifikuoto sertifikato sukūrimas vyksta tik kai:

- Mobiliojo ryšio funkcija išduotoje SIM kortelėje yra aktyvuota,
- Klientas patvirtina savo asmens duomenų, susietų su konkrečia SIM kortele teisingumą,
- Klientas pasikeičia pradinį suteiktą sPIN į naują, tik jam žinomą kodą.

Sertifikato sukūrimo užklausa ir susiję asmens duomenys perduodami į CA, kvalifikuoto sertifikato sukūrimui. Sprendimą dėl sertifikato suteikimo asmeniui priima RA, CA gamybos veiksmą atlieka automatiškai. Sertifikato aktyvavimo informacija pateikiama vartotojui SMS žinute. Sukurti ir galiojantys kvalifikuoti sertifikatai talpinami viešoje sertifikatų saugykloje, pasiekiamoje internetu 24 valandas per parą.

4.3. Sertifikato atnaujinimas

Pasibaigus sertifikato galiojimo laikui arba panaikinus sertifikatą, RA įspėja apie tai klientą SMS žinute. Klientas gali aktyvuoti naują sertifikatą (žiūr priedą Nr. 3 „Registravimo taisyklės"). Negaliojantys sertifikatai išimami iš viešos aktyvių sertifikatų saugyklos.

4.4. Sertifikato sustabdymas

Sertifikato sustabdymas nepalaikomas. Esant reikalui, SIM kortelė gali būti blokuojama - tokiu būdu tik uždaroma prieiga prie pasirašymo įrenginio.

4.5. Sertifikato atšaukimas

Sertifikatas privalo būti atšauktas:

- Kliento prašymu;
- Automatiškai, kai kliento mobiliojo ryšio paslauga atšaukiama, panaikinama;
- Kai klientas praneša apie galimai pamestą SIM arba neteisėtą SIM kortelės panaudojimą iš trečiųjų asmenų pusės;
- Kai sPIN tampa žinomas tretiesiems asmenims, arba įtarus, kad tretieji asmenys sužinojo sPIN;
- Kai tampa žinoma, jog klientas pažeidė savo įsipareigojimus;
- Kai pasikeičia kliento asmens duomenys (vardas, pavardė, asmens kodas);
- kai to pareikalauja teismas ar ikiteisminio tyrimo institucijos, turinčios tam tinkamus įgaliojimus ir raštišką pagrindą;
- Kai RA įtaria, jog sertifikatą naudoja kiti asmenys ar RA įtarus, jog sPIN tapo žinomas tretiesiems asmenims.

RA perduoda sertifikato panaikinimo užklausą į CA. CA nedelsiant išima sertifikatą iš viešosios aktyvių sertifikatų saugyklos ir atnaujina negaliojančių sertifikatų registrą (CRL).

4.6. Nenumatytų situacijų valdymas

Tuo atveju, jei konkretaus CA veikla netikėtai nutrūksta ir jos nepavyksta atstatyti per 24 valandas, RA suteikia galimybę klientams atšaukti savo sertifikatą ir aktyvuoti naują sertifikatą, sukuriamą kito veikiančio CA.

4.7. CA veiklos nutraukimas

Tuo atveju, kai konkretus CA nutraukia savo veiklą, visi jo sukurti sertifikatai yra atšaukiami. Klientas gali aktyvuoti naują sertifikatą, kuris bus sukurtas kitame CA.

5. Techninės saugumo priemonės

5.1. Kliento raktai

Kriptografiniai raktai yra generuojami arba saugiai patalpinami į SIM kortelę gamybos metu. Raktų kopijų nekuriama ir neegzistuoja žinomų būdų, kaip atstatyti privatųjį raktą SIM kortelę jau pagaminus. Privatusis raktas gali būti aktyvuojamas tik įvedant sPIN (nuo 4 iki 8 skaičių) kodą. Privataus rakto aktyvavimas negrįžtamai panaikinamas ***penkis*** kartus neteisingai suvedus sPIN.
Pradinis sPIN yra atspausdintas ant SIM kortelės plastiko, paslėptas po nutrinamų dažų sluoksniu, sPIN kopijos niekur nesaugomos. RA garantuoja dėl pradinio sPIN apsaugos iki SIM kortelės perdavimo klientui momento, SIM kortelė klientui visada įteikiama tik asmeniškai, kliento prašoma įsitikinti sPIN kodo apsauga prieš priimant naują SIM kortelę.

Klientas yra įpareigojamas saugoti pasirašymo įrenginį, neleisti juo naudotis kitiems asmenims ir laikyti paslaptyje sPIN. Įtarus, kad sPIN tapo žinomas kitiems asmenims, vartotojas privalo arba pasikeisti sPIN, arba pakeisti SIM kortelę į naują.

5.2. Sistemų ir duomenų apsauga

Techninės saugumo priemonės, susijusios su CA veikla, aprašomos priede Nr. 1 (G-CPS).
Techninės priemonės, susijusios su RA veikla, aprašomos priede Nr. 3 (RP).

Neskelbiami asmens duomenys yra saugomi RA, CA ir pasitikinčiųjų šalių pagal galiojančius vietos įstatymus ir atitinka ES galiojančius reglamentus.

6. Techninis sertifikatų aprašymas

Sertifikatai apima sekančius duomenis:

- Sertifikato leidėjo duomenys (pavadinimas, registracijos numeris);
- Sertifikato turėtojo (subjekto) duomenys (žiūr. DN lauko aprašymą žemiau);
- Sertifikato galiojimo datas (nuo kada sertifikatas įsigalioja ir kada jo galiojimas baigiasi);
- Techninius duomenis, o t.y.:
  1. Sertifikato formato versija;
  2. Sertifikato serijos numeris;
  3. Algoritmas, naudotas pasirašant sertifikatą;
  4. Sertifikate naudojamas viešasis raktas ir jo atvaizdavimo metodas;
  5. CA viešojo rakto identifikatorius;
  6. Asmens viešojo rakto identifikatorius;
  7. Rakto panaudojimo laukas;
  8. Sertifikato taisyklių, kurios atitinka šias taisykles, numeris;
  9. Nuoroda į negaliojančių sertifikatų skelbimo servisą (CDP);
  10. CA papildoma informacija;
  11. Išplėstinis raktų panaudojimo laukas (tik autentifikacijos sertifikate);
  12. CA papildomų paslaugų identifikatorius ir nuoroda.

6.1. Vardai sertifikatuose

Sertifikatas saugo 2 skiriamuosius vardus: sertifikato leidėjo ir sertifikato turėtojo. Šiems vardams taikomi kodavimo reikalavimai, aprašyti RFC3280.

Sertifikato turėtojo skiriamasis vardas (DN) apima sekančius atributus:

Atributas	Aprašymas	Pavyzdys
CountryName	2-jų raidžių šalies kodas	LT
O (Organisation)	Sertifikato tipas	OMNITEL
SN (Surname)	Asmens pavardė	Šablinskas
GN (GivenName)	Asmens vardas	Ramūnas
Serialnumber	Asmens kodas, unikalus CountryName kontekste	37102230096
CN (CommonName)	Pavardė, vardas ir asmens kodas atskirti kableliais. Nenaudojami diakritiniai ženklai (lietuviškos raidės pakeičiamos į lotyniškas).	Sablinskas, Ramunas, 37102230096

Pastaba: Subjekto (SUBJECT) lauke, GN ir SN atributuose gali būti panaudoti lietuviški diakritiniai ženklai:

Žymėjimas	Virš. registras (Unicode žym.)	Apatin. reg.(Unicode žym.)
Latin A with ogonek	Ą (U+0104)	ą (U+0105)
Latin C with caron	Č (U+010C)	č (U+010D)
Latin E with ogonek	Ę (U+0118)	ę (U+0119)
Latin E with dot above	Ė (U+0116)	ė (U+0117)
Latin I with ogonek	Į (U+012E)	į (U+012F)
Latin S with caron	Š (U+0160)	š (U+0161)
Latin U with ogonek	Ų (U+0172)	ų (U+0173)
Latin U with macron	Ū (U+016A)	ū (U+016B)
Latin Z with caron	Ž (U+017D)	ž (U+017E)

CA užtikrina, kad skiriamieji vardai galiojančiuose sertifikatuose būtų skirtingi.

6.2. Techniniai sertifikato duomenys

Sertifikato formato versija ("version")
Šiame lauke nurodoma sertifikato formato versija (reikšmė 2 šiuo atveju naudojama nusakyti X.509 v3 versijos sertifikatams).
Sertifikato serijinis numeris (serialNumber)
Šiame lauke saugomas unikalus sertifikato eilės numeris (unikalumas konkretaus CA kontekste).
Sertifikato parašo algoritmas (signatureAlgorithm)
Šis laukas apima nuorodą į algoritmą, kuriuo apsaugota pasirašytoji sertifikato informacija. Šiuo atveju naudojamas SHA-1 santraukos algoritmas, pasirašomas RSA metodu: sha1WithRSAEncryption { 1, 2, 840, 113549, 1, 1, 5 }.
Sertifikato galiojimo laikas (validity)
Sertifikato galiojimo pradžios ir pabaigos data ir laikas. Šis laikas paprastai nustatomas 1 (vieneriems) metams. Datos ir laikai saugomi formatu, apibrėžtu RFC3280.
Viešasis raktas ir jo atvaizdavimo metodas (subjectPublicKeyInfo)

Šis laukas saugo sertifikato turėtojo viešąjį raktą. Sekantis kodavimo algoritmas yra panaudojamas: rsaEncryption { 1, 2, 840, 113549, 1, 1, 1 }.

Papildoma sertifikato informacija

Naudojami sekantys nustatymai ("Kritinis" reiškia, jog programos naudojančios sertifikatą privalo patikrinti lauko turinį):

Nustatymo pavadinimas	Sertifikate	
	Nustatytas?	Kritinis?
AuthorityKeyIdentifier	TAIP	NE
SubjectKeyIdentifier	TAIP	NE
KeyUsage	TAIP	TAIP
CertificatePolicies	TAIP	NE
SubjectAltName	TAIP	NE
IssuerAltName	TAIP	NE
CRLDistributionPoints	TAIP	NE
ExtKeyUsage	TAIP	TAIP (autentifikacijai)
Authority Information Access	TAIP	NE
Basic Constraints	TAIP	NE

CA viešojo rakto identifikatorius (authorityKeyIdentifier)

Šis laukas saugo CA viešojo rakto, kuriuo pasirašytas sertifikatas, identifikatorių. Naudojamas tik "keyIdentifier" laukas.

Asmens viešojo rakto identifikatorius (subjectKeyIdentifier)

Šis laukas saugo viešojo rakto reikšmę sertifikate. To reikia greitam viešojo rakto identifikavimui (jei sertifikato turėtojas turi keletą sertifikatų iš to paties CA). Pagal RFC3280 panaudojamas metodas 1.

Rakto panaudojimas (keyUsage)

Tai yra kritinis laukas, kuriam priskiriamos sekančios reikšmės:

· digitalSignature
· nonRepudiation (naudojamas tik su autentifikacijos sertifikatu)
· keyEncipherment
· dataEncipherment

Sertifikato taisyklės (certificatePolicies)

Šis laukas saugo nuorodą į sertifikato taisykles, kurios iš esmės atitinka šį dokumentą. Šių taisyklių buvo prisilaikoma sukuriant ir palaikant konkretų sertifikatą. Lauke saugoma URL nuoroda ir OID identifikatorius.

CRL sklaidos nuoroda (cRLDistributionPoints)

Šis laukas saugo adresą, kuriuo galima gauti paskutinį galiojantį konkretaus CA atšauktų sertifikatų sąrašą. Lauke saugoma URL nuoroda.

Papildoma CA informacija (IssuerAltName)

Čia saugoma CA pasirašymo sertifikato lauko SubjAltName reikšmė ir joje paprastai patalpinama papildoma informacija apie CA.

papildomas raktų panaudojimas (ExtendedKeyUsage)

Tai kritinis laukas, kuriame saugoma reikšmė: ClientAuthentication.

Papildomos CA paslaugos (AuthorityInformationAccess)

Šis laukas saugo informaciją apie papildomas CA paslaugas. Pvz., OCSP (Online Certificate Status Protocol) paslaugos URL nuoroda.

Baziniai apribojimai

Šis plėtinys nusako, jog sertifikato subjektas yra galutinis vartotojas.

CRL profilis

CRL formatas yra x.509v2 (apibrėžtas RFC3280).

CRL plėtinys

Visi CRL, išduoti CA turi sekančius laukus: Authority Key Identifier, CRL number. Laukas authorityKeyIdentifier saugo CA viešojo rakto identifikatorių, šį raktą atitinkantis privatusis raktas panaudojamas pasirašyti CRL. CRLnumber laukas auga nuosekliai ir žymi CA publikuojamo CRL failo eilės numerį.

CA naudoja CRL Entry extensions pagal rekomendacijas pateiktas RFC3280.

7. Sertifikato pavyzdys

Sertifikato laukas	Lauko reikšmės pavyzdys	Komentaras
VERSION	**V3**	konstanta
SERIAL NUMBER	**41db f209**	unikalus skaičius CA ribose
SIGNATURE ALGORITHM	**sha1RSA**	konstanta
ISSUER	CN = **EID-SK** SN = **1** O = **AS Sertifitseerimiskeskus** C = **EE**	konstanta
VALID FROM	*10 may 2005. a. 17:48:14*	Data, laikas (GMT/CET)
VALID TO	*11 may 2010. a. 17:48:14*	nusako RA, žr. RP
SUBJECT	*Serial Number*=**37102230096** *GN* = *Ramūnas*	pavyzdys

	SN = Šablinskas *CN = Ramunas,Sablinskas,***37102230096** *OU = mobile signature* **O = OMNITEL** **C = LT**	
PUBLIC KEY	**3081 8902 8181 00C2 AFE1 0488 4987 6C2D 4382 78FF D4E6 9F2C AEE7 2676 F3E7 33C1 8A38 706C 0F95 DF89 596A 95B8 B808 5A09 9FC7 4390 B642 AE78 AB46 00AF 647A 283B 7A44 7E25 1827 C0F5 06A0 30C1 75C1 8159 FAC5 455F 6BDB 844A 8665 1A36 2126 1370 A480 E9D5 719C 6F7D E8F5 04BF 87BF 25C3 3F20 9635 A273 05EE EB64 20BE A39E 42C6 B1D2 58A6 5425 B302 0301 0001**	*RSA(1024 bitų raktas) pvz.*
EXTENDED KEY USAGE	Client Authentication(**1.3.6.1.5.5.7.3.2**)	
CERTIFICATE POLICIES	Policy Identifier=1.3.6.1.4.1.10015.10.1.1.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.sk.ee/repository/eid-sk-1.0.pdf	
QUALIFIED CERTIFICATE STATEMENT	(1.3.6.1.5.5.7.1.3)	konstanta pagal RFC3739
AUTHORITY KEY IDENTIFIER	*KeyID=b4 bc 27 70 9e 07 cb c5 64 c3 32 19 6c dc 1f 7a 29 2e 37 a5*	pavyzdys
SUBJECT KEY IDENTIFIER	*17 b2 52 f8 40 b6 82 94 6e d6 a9 41 71 85 74 e4 79 82 4f b8*	pavyzdys
KEY USAGE	**Digital Signature , Key Encipherment , Data Encipherment(B0), Non-Repudiation (40)**	konstanta
CRL DISTRIBUTION POINTS	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.sk.ee/crls/eid-sk/eid.crl	konstanta (pvz)
BASIC CONSTRAINTS	Subject Type=End Entity Path Length Constraint=None	konstanta
THUMBPRINT ALGORITHM	**sha1**	konstanta
THUMBPRINT	**973B 877E 12BB 5302 2EB6 88CC 9D04 6D9C D374 35E1**	pavyzdys

Priedas Nr. 4

PRIEDAS NR. 3
REGISTRAVIMO TAISYKLĖS (RP-M)

Registravimo tarnybos procedūros, suteikiant kvalifikuotus sertifikatus mobiliose registracijos vietose.

1. **Įvadas**

Šis dokumentas (**toliau tekste Registracijos Taisyklės Mobilioms RA darbo vietoms arba RP-M**) papildo įprastai taikomą RP dokumentą ir aprašo procedūras, kurių Registravimo Tarnyba (RA) prisilaiko aptamaudama klientus nestandartiniais atvejais, pvz., seminaruose, parodose, konferencijose. Šios taisyklės galioja visiems UAB OMNITEL aptamaujamiems klientų kvalifikuotiems sertifikatams, kai registracijos procedūra atliekama ne RA patalpose. Įprastines registracijos procedūras, kai registracija vyksta RA patalpose, aprašo dokumentas RP.

RA funkcijų sąrašas:

Funkcija 1.Paraiškos gauti *kvalifikuotam sertifikatui* ir SIM kortelės aktyvavimo procedūros:

- Kliento paraiškos sertifikatui gauti registracija (Kliento asmens duomenų surinkimas);
- SIM kortelės pakeitimas/suteikimas (suteikimas specialios SIM, jos PIN, pasirašymo kodo sPIN, šios SIM kortelės aktyvavimas mobiliojo ryšio tinkle).

Funkcija 2. *Kvalifikuoto sertifikato* aktyvavimas.

2. **Bendrosios sąlygos**

RA pareigos:

- Išduoti pasirašymo įrenginį (specialią SIM kortelę) klientui;
- Teikti klientui informaciją ir pagalbą, susijusius su pasirašymo įrenginiu, sertifikatais ir jų panaudojimu;
- Užtikrinti, kad RA darbuotojai būti tinkamai apmokyti ir sugebėtų teikti klientui aukštos kokybės paslaugas;
- Užtikrinti, kad darbuotojai susiję su sertifikatų palaikymu neturėtų kriminalinių įrašų už tyčinius nusikaltimus;
- Užtikrinti, kad teikiamos paslaugos atitiktų vietos įstatymus.

3. **Kliento identifikacija**

RA pateikia vieną elektroninės identifikacijos produktą - **asmeninį kvalifikuotą sertifikatą**. Sertifikatas yra susietas su specialia SIM kortele ir konkrečiu fiziniu asmeniu, tos kortelės realiu turėtoju. Asmuo gali turėti vieną kvalifikuotą sertifikatą. Tik **fiziniai asmenys**, atstovaujantys patys save gali teikti paraiškas kvalifikuotam sertifikatui gauti. Bet kuris pilnametis Lietuvos pilietis - UAB OMNITEL reguliaraus mokėjimo abonentas, teisėtai turintis SIM kortelę (kortelė nebūtinai turi priklausyti abonentui kaip fiziniam asmeniui) gali teikti paraišką sertifikatui gauti. Paraiškos teikiamos akivaizdiniu būdu. Galiojantis asmens tapatybės dokumentas privalo būti pateiktas kaip asmens tapatybės įrodymas. RA gali atmesti paraišką, jei nepavyksta patikimai nustatyti asmens tapatybės arba jei abejojama, jog abonentas yra teisėtas SIM kortelės turėtojas.

4. **Registravimo paslaugų teikimo sąlygos**

4.1. **Funkcija 1: Paraiškos gauti kvalifikuotam sertifikatui ir SIM kortelės aktyvavimo procedūros**

Kliento paraiška aptamaujama per keletą žingsnių.

Žingsnis I : kliento asmens duomenų surinkimas

Šis žingsnis inicijuojamas, klientui gyvai bendraujant su RA darbuotoju ir pareiškus norą gauti paslaugą. RA darbuotojas:

- Prašo kliento pateikti galiojantį asmens tapatybės dokumentą (asmens tapatybės kortelę arba pasą), senąją SIM kortelę ir lustinę banko mokėjimo kortelę;
- Paprašo klientą autorizuoti lustine kortele (klientui įvedant PIN kodą) nedidelės sumos mokėjimą (arba abonento sąskaitos apmokėjimą/papildymą), išsaugant POS terminalo kvitą su užrašu "PIN įvestas teisingai" ir kliento vardą bei pavardę (ir/arba banko kortelės skenuotą vaizdą su iš dalies uždengtu banko kortelės numeriu);
- Įvertina tapatybės dokumento autentiškumą;
- Įvertina asmens biometrinių duomenų atitikimą dokumentui;
- Skenuoja asmens tapatybės dokumentą ir įveda asmens duomenis į provizijos sistemą:
  - Asmens kodą;
  - Asmens vardą ir pavardę;
  - Asmens kontaktinius duomenis: gyvenamąjį adresą, mobiliojo telefono numerį, e-pašto adresą;
  - Dokumento numerį, galiojimo datą.
- Pateikia klientui susipažinimui užpildytą paraiškos formą, priedus G-CPS, CP, RP-M bei gauna kliento parašą;
- Paaiškina vartotojui sertifikato aktyvavimo procedūrą.

Kliento dokumentas yra patikrinamas policijos negaliojančių dokumentų duomenų bazėje. Paraiškos formą RA darbuotojas patvirtina savo elektroniniu parašu, ši pasirašyta forma išsaugoma sistemoje.

Žingsnis II : SIM kortelės pakeitimas

Šiame žingsnyje klientui perduodamas pasirašymo įrenginys ir jo priedai:

- Speciali SIM kortelė su saugiai patalpintais privačiaisiais raktais;

- SIM kortelės PIN kodas po nutrinamų dažų sluoksniu;
- pradinis signataro sPIN kodas, skirtas pasirašymo įrenginio aktyvavimui (privačiųjų raktų aktyvavimui) po nutrinamų dažų sluoksniu.

Klientas privalo patikrinti, ar nėra pažeistas PIN kodų slaptumas. Papildomai šiame žingsnyje gali būti atliekamas senosios SIM kortelės įrašų perkėlimas į naująja SIM kortelę.

Žingsnis III : SIM kortelės aktyvavimas

SIM kortelė yra aktyvuojama po tam tikro laiko, pvz. sekančios dienos rytą. Prieš naujosios SIM kortelės aktyvavimą klientas įspėjamas SMS žinute į senąją SIM kortelę.

4.2. Funkcija 2: Kvalifikuoto sertifikato aktyvavimas

Klientui sertifikatas aktyvuojamas automatiniu būdu po SIM kortelės aktyvavimo vienu iš dviejų galimų būdų:

Būdas 1: kai automatinės sistemos informuoja sertifikavimo tarnybą aktyvuoti sertifikatą: lustinės mokėjimo kortelės inicijuotas mokėjimas/sąskaitos papildymas duoda signalą CA aktyvuoti kvalifikuotą sertifikatą. Po sėkmingos operacijos vartotojas įspėjamas apie pagamintą sertifikatą SMS žinute, bei primenama, jog būtina pasikeisti sPIN slaptažodį.

Būdas2: kai nėra automatinės sistemos, sugebančios perduoti signalą į CA, šią funkciją atlieka RA agentas, nedalyvavęs registracijos procedūroje: agentas papildomai analizuoja kliento pateiktus tapatybės įrodymus (įskaitant apmokėjimą banko kortele), bei priima sprendimą dėl tapatybės suteikimo ir inicijuoja sertifikato aktyvavimo procedūrą. Apie operacijos baigtį klientas įspėjamas SMS žinute, kurioje pateikiami sertifikato duomenys, bei priminimas, jog būtina pasikeisti sPIN slaptažodį.

5. Dokumentų ir įvykių apskaita

Visos su kvalifikuotu sertifikatu susijusios operacijos yra išsaugomos saugioje įrašų saugojimo sistemoje ne trumpesniam, nei 36 mėnesių laikotarpiui. Popierinės sutartys saugomos sutinkamai su LR įstatymais ir susijusiais teisės aktais. RA užtikrina saugomų įrašų ir dokumentų nepažeidžiamumą bei konfidencialumą.

6. Saugumo priemonės

RA sistemos palaiko saugumo politikas ir praktiką, garantuojančius saugias operacijas (susijusias su kvalifikuotų sertifikatų gyvavimo ciklo valdymu) su patikimumu ne mažesniu, nei EAL-4 pagal ISO/IEC 15408-1 standartą.

Priedas Nr. 5

ELEKTRONINIŲ PASLAUGŲ TEIKIMO SUTARTIS
AGREEMENT OF ELECTRONIC SERVICES

DATA / DATE _____

KLIENTO DUOMENYS / CUSTOMER INFORMATION

VARDAS, PAVARDĖ / JURIDINIO ASMENS PAVADINIMAS FORENAME, SURNAME / FULL NAME OF LEGAL PERSON		ASMENS KODAS / REGISTRACIJOS KODAS PERSONAL CODE / REGISTRATION CODE
ADRESAS ADDRESS		
KONTAKTINIS TELEFONAS CONTACT PHONE	FAKSAS FAX	EL. PAŠTAS E-MAIL

NAUDOTOJO DUOMENYS / USER INFORMATION

NAUDOTOJO ID USER ID	VARDAS, PAVARDĖ FORENAME, SURNAME	ASMENS KODAS PERSONAL CODE	KALBA LANGUAGE

SUTARTIES DUOMENYS / AGREEMENT PARTICULARS

ELEKTRONINIŲ PASLAUGŲ TEIKIMO SUTARTIES SĄLYGAS, BANKO KLIENTŲ APTARNAVIMO IR PASLAUGŲ TEIKIMO BENDRĄSIAS SĄLYGAS IR GALIOJANČIUS BANKO PASLAUGŲ IR OPERACIJŲ ĮKAINIUS GAVAU (ESU GAVĘS) IR SU JAIS SUSIPAŽINAU (ESU SUSIPAŽINĘS):
I HAVE RECEIVED AND FAMILIARISED MYSELF WITH SPECIFIC TERMS OF THE AGREEMENT OF ELECTRONIC SERVICES, GENERAL TERMS OF BANK CUSTOMER SERVICING AND THE EFFECTIVE BANK CHARGES FOR SERVICES AND OPERATIONS APPLIED BY THE BANK.

KLIENTO VARDAS, PAVARDĖ, PARAŠAS / JURIDINIO ASMENS ATSTOVO PAREIGOS, VARDAS, PAVARDĖ, PARAŠAS, ANTSPAUDAS CUSTOMER'S FORENAME, SURNAME, SIGNATURE / LEGAL PERSON REPRESENTATIVE'S DUTIES, FORENAME, SURNAME, SIGNATURE, STAMP	BANKO ATSTOVO VARDAS, PAVARDĖ, PARAŠAS BANK REPRESENTATIVE'S FORENAME, SURNAME, SIGNATURE

ELEKTRONINIŲ PASLAUGŲ TEIKIMO SUTARTIES SĄLYGOS

1. Pagrindinės Sutartyje vartojamos sąvokos

1.1. Sutartis – Ši Elektroninių paslaugų teikimo sutartis.

1.2. Klientas – Sutartyje nurodytas Sąskaitos savininkas, Šia Sutartimi suteikiantis teisę Naudotojui atlikti Operacijas Elektroniniais kanalais.

1.3. Naudotojas – Sutartyje nurodytas fizinis asmuo, kuriam Klientas suteikia teisę atlikti Operacijas Elektroniniais kanalais. Naudotojas ir Klientas gali būti tas pats fizinis asmuo.

1.4. Bankas – AB bankas „Hansabankas", juridinio asmens kodas 112029651.

1.5. Interneto bankas – Banko paslauga, kuria naudodamasis Naudotojas gali atlikti Operacijas internetu, prisijungęs prie Banko tarnybinės stoties Banko nurodytu interneto adresu.

1.6. Bankas telefonu – Banko paslauga, kuria naudodamasis Naudotojas gali atlikti Operacijas telefonu, paskambinęs Banko nurodytu telefono numeriu (-iais) Banko specialistui.

1.7. Automatinė paslauga – Banko paslauga, kuria naudodamasis Naudotojas gali atlikti Operacijas telefonu, paskambinęs Banko nurodytu telefono numeriu (-iais) į autoatsakiklį.

1.8. Mobilus bankas – Banko paslauga, kuria naudodamasis Naudotojas gali atlikti Operacijas mobiliuoju ryšiu, Banko nurodytu telefono numeriu siųsdamas ir gaudamas trumpąsias žinutes ir/arba Banko nurodytu adresu prisijungęs prie Banko tarnybinės stoties.

1.9. Elektroniniai kanalai – Interneto bankas, Bankas telefonu, Automatinė paslauga ir Mobilus bankas.

1.10. Sąskaita – Sutartyje nurodyta Kliento banko, vertybinių popierių sąskaita, indėlio ir/arba kitokia sąskaita ar sąskaitos, atidarytą(-os) Banke. Jeigu Sutartyje neišvardijamos atskiros Kliento sąskaitos ir nurodoma, kad Sutartis taikoma visoms Kliento sąskaitoms, arba išvardijamos atskiros Sąskaitos ir nurodoma, kad Sutartis taikoma visoms kitoms Kliento sąskaitoms, pasirašius Sutartį Naudotojas turi teisę Elektroniniais kanalais atlikti Operacijas visose Kliento sąskaitose, kuriose Bankas leidžia atlikti Operacijas Elektroniniais kanalais, įskaitant ir sąskaitas, kurias Bankas Klientui atidarys ateityje po Sutarties pasirašymo.

1.11. Operacijos – lėšų pervedimas iš Sąskaitos, informacijos apie Sąskaitoje atliktas operacijas ir lėšų likutį pateikimas, Kliento prašymų bei pranešimų pateikimas Bankui Elektroniniais kanalais ir kitos operacijos, susijusios su Banko teikiamomis paslaugomis, kurias galima atlikti arba kuriomis galima naudotis visais ar vienu iš Elektroninių kanalų, įskaitant indėlių ir kitų Banko siūlomų sutarčių sudarymą Interneto banku, taip pat su trečiųjų asmenų (įskaitant Banko grupės įmones) teikiamomis paslaugomis susijusios operacijos, kurias Bankas leidžia atlikti Elektroniniais kanalais.

1.12. Tapatybės patvirtinimo priemonės – Banko Naudotojui pagal šią Sutartį (jeigu Sutartyje nurodomas Klientas ir Naudotojas yra tas pats asmuo) arba kitą tarp Banko ir Naudotojo sudarytą sutartį suteiktas Naudotojo identifikavimo numeris (toliau – naudotojo ID), identifikavimo kodai, nuolatinis slaptažodis, mobiliojo telefono numeris, taip pat kitos Naudotojo tapatybės patvirtinimo priemonės, jeigu Naudotojas ir Bankas atskirai yra susitarę dėl kitų tapatybės priemonių naudojimo.

1.13. Vietinis mokėjimo pavedimas – Naudotojo pateiktas nurodymas Bankui pervesti iš Sąskaitos lėšas gavėjui, kai lėšų gavėjo sąskaita yra Banke ar kitame banke Lietuvos Respublikoje.

1.14. Tarptautinis mokėjimo pavedimas – Naudotojo pateiktas nurodymas Bankui pervesti iš Sąskaitos lėšas gavėjui, kai lėšų gavėjo sąskaita yra kitame banke ar jo skyriuje užsienio valstybėje.

2. Sutarties objektas

2.1. Sutartis reglamentuoja Kliento ir Banko santykius, atsirandančius Naudotojui atliekant Operacijas Elektroniniais kanalais.

2.2. Tuo atveju, jeigu Sutartyje nurodytas Klientas ir Naudotojas yra tas pats asmuo, Sutartis taip pat reglamentuoja Banko ir Naudotojo santykius, susijusius su Tapatybės patvirtinimo priemonių suteikimu bei naudojimu.

2.3. Šios Sutarties reglamentuojamus santykius taip pat reglamentuoja Lietuvos Respublikos civilinis kodeksas, kiti įstatymai ir teisės aktai, Banko klientų aptarnavimo ir paslaugų teikimo bendrosios sąlygos bei Operacijų atlikimą reglamentuojantys Banko vidaus aktai, su kuriais Klientas gali susipažinti Sutartyje numatytu būdu arba kitu Banko nurodytu būdu.

2.4. Jeigu paslaugas Elektroniniais kanalais teikia Banko nustatyti tretieji asmenys, įskaitant Banko grupės įmones, Bankas neatsako už tuos trečiuosius asmenis ir už tų trečiųjų asmenų teikiamų paslaugų kokybę.

3. Techniniai reikalavimai

3.1. Naudotojas gali naudotis Elektroniniais kanalais, jeigu Naudotojo turimos techninės priemonės, ryšio ir programinė įranga atitinka Banko nustatytus reikalavimus. Bankas turi teisę keisti techninių priemonių, ryšio ir programinės įrangos reikalavimus, apie tai Elektroniniais kanalais arba kitu būdu informavęs Naudotoją ir/arba Klientą.

3.2. Naudotojas įsipareigoja naudotis Elektroniniais kanalais tik tuo atveju, jeigu jo turimos kompiuterinės sistemos saugumo priemonės leidžia Operacijas Sąskaitoje atlikti saugiai, neatskleidžiant jokių duomenų tretiesiems asmenims. Tuo tikslu Naudotojas įsipareigoja savo kompiuterinėje sistemoje laikytis visų įmanomų saugumo priemonių ir yra atsakingas už visas pasekmes, susijusias su nepakankama savo kompiuterinės sistemos apsauga.

3.3. Naudotojas techninėmis priemonėmis ir programine įranga naudojasi savo ir/arba Kliento sąskaita ir rizika. Ryšio išlaidas, susijusias su naudojimusi Elektroniniais kanalais, padengia Klientas ir/arba Naudotojas.

4. Operacijų atlikimas

4.1. Jeigu Sutartyje neišvardytos Operacijos, kurias turi teisę atlikti Naudotojas, o nurodyta, kad galimos visos Operacijos, pasirašius Sutartį Naudotojas turi teisę atlikti visas Operacijas, kurias Bankas leidžia atlikti naudojantis atitinkamu Elektroniniu kanalu, įskaitant ir tas Operacijas, kurias Bankas leis atlikti naudojantis atitinkamu Elektroniniu kanalu ateityje po Sutarties pasirašymo.

4.2. Naudotojas gali naudotis Elektroniniais kanalais Banko nustatytu paros laiku, nurodytu naudojimosi atitinkamais Elektroniniais kanalais instrukcijose (atmintinėse). Bankas gali keisti naudojimosi Elektroniniais kanalais laiką, apie tai atitinkamu Elektroniniu kanalu arba kitu būdu informavęs Klientą. Bankas taip pat turi teisę dėl svarbių priežasčių (techninės profilaktikos, programinės įrangos keitimo arba pietros ir pan.) sustabdyti naudojimąsi Elektroniniais kanalais.

4.3. Klientas sutinka, kad Naudotojui atliekant Operacijas Elektroniniais kanalais Bankas įrašinėtų visus pokalbius ir registruotų Naudotojų pateikiamus nurodymus atlikti Operaciją. Šie įrašai prireikus gali būti panaudoti Elektroniniais kanalais pateiktiems Kliento nurodymams ir atliktoms Operacijoms įrodyti.

4.4. Galiojant Sutarčiai Bankas ryšius su Klientu ir Naudotoju palaiko lietuvių kalba arba, jeigu Klientas ar Naudotojas nemoka lietuvių kalbos, Banko nurodyta užsienio kalba. Bankas turi teisę nevykdyti Operacijų, jeigu Naudotojas nurodymą atlikti Operaciją Banku telefonu pateikia ne lietuvių ir ne Banko nurodyta užsienio kalba.

4.5. Bankas Elektroniniais kanalais pateiktus nurodymus atlikti Operaciją vykdo tarp Banko ir Kliento sudarytoje banko sąskaitos ar kitoje atitinkamoje sutartyje numatytomis sąlygomis bei terminais, o jeigu tokie terminai nenumatyti – įstatymo numatytais terminais. Elektroniniais kanalais pateiktas nurodymas atlikti Operaciją yra neatšauktinas, išskyrus tuos atvejus, kai Klientas ir Bankas yra susitarę kitaip ir Bankas dar nėra įvykdęs pateikto nurodymo.

4.6. Bankas nevykdo Kliento pateiktų nurodymų atlikti Operacijas Sąskaitoje, jeigu Kliento Elektroniniais kanalais pateikiami nurodymai atlikti Operacijas Sąskaitoje neatitinka Sutarties sąlygų ir/arba Banko reikalavimų, taip pat kitais įstatymo ar tarp Banko ir Kliento sudarytoje banko sąskaitos sutartyje numatytais atvejais, kai Bankas turi teisę arba privalo nevykdyti nurodymų nurašyti lėšas iš Kliento sąskaitos.

5. Operacijų limitai

5.1. Sudarant Sutartį Kliento ir Banko susitarimu yra nustatomi Vietinių mokėjimo pavedimų ir/ar Tarptautinių mokėjimo pavedimų limitai dienai ir mėnesiui, kurių Naudotojas negali viršyti. Jeigu Naudotojas viršija šiuos limitus, Bankas nevykdo Naudotojo Elektroniniais kanalais arba atitinkamu Elektroniniu kanalu pateikiamų nurodymų. Šiame punkte paminėti limitai netaikomi, jeigu: (i) vykdant Vietinius mokėjimo pavedimus lėšos pervedamos tarp Kliento sąskaitų, esančių Banke, (ii) Klientas perka ar parduoda valiutą, (iii) Bankas vykdo lėšų gavėjo inicijuotus debeto mokėjimo pavedimus nurašyti lėšas iš Sąskaitos, (iv) Sutarties 5.7. punkte nurodytu atveju du Kliento nurodyti asmenys (naudotojai) privalo patvirtinti Vietinį mokėjimo pavedimą ir/arba Tarptautinį mokėjimo pavedimą (tokiu atveju limitai netaikomi pirmajam atitinkamą dieną pavedimą tvirtinančiam asmeniui).

5.2. Klientas, norėdamas pakeisti Operacijų limitus, privalo atvykti į Banką ir pasirašyti naują Elektroninių paslaugų teikimo sutartį arba kitą atitinkamą sutartį.

5.3. Šalys susitaria, kad Bankas turi teisę vienašališkai nustatyti bendrus limitus kiekvienu Elektroniniu kanalu atliekamoms Operacijoms arba jų skaičiui, ir jeigu Naudotojas viršys tuos limitus, Bankas nevykdys Naudotojo Elektroniniais kanalais arba atitinkamu Elektroniniu kanalu pateikiamų nurodymų.

5.4. Kliento pageidavimu Sutartyje gali būti nustatytas papildomo operacijos patvirtinimo limitas Interneto banku ir Mobiliu banku pateikiamiems Vietiniams ir Tarptautiniams mokėjimo pavedimams. Jeigu nustatytas toks limitas, Bankas Kliento pateiktą mokėjimo nurodymą, kurio suma lygi arba didesnė už papildomo operacijos patvirtinimo limito sumą, vykdys tik tuo atveju, jeigu Bankas, paskambinęs Kliento nurodytu kontaktiniu telefonu, gaus papildomą tokio mokėjimo nurodymo pateikimo patvirtinimą žodžiu. Bankas Klientui skambina Sutartyje Kliento nurodyto kontaktinio telefono numeriu arba kitu telefono numeriu, jeigu Klientas atskirai nurodo kitą numerį Bankui kaip kontaktinio telefono numerį. Klientas privalo užtikrinti, kad Sutartyje nurodytu jo kontaktiniu telefonu atsilieps tik Kliento įgaliotas asmuo, kuris žinos apie Kliento pateikiamus mokėjimo nurodymus ir galės patvirtinti arba paneigti atitinkamo nurodymo pateikimo faktą. Bankas netikrina telefonu atsiliepusio asmens įgaliinimų ir neprivalo identifikuoti tokio asmens. Jeigu asmuo, atsiliepęs kontaktiniu telefonu nepatvirtina nurodymo arba Bankui iki Banko darbo dienos, einančios po nurodymo pateikimo, pabaigos nepavyksta susisiekti Kliento nurodytu kontaktiniu telefonu, Bankas Kliento pateikto mokėjimo nurodymo nevykdo.

5.5. Papildomo operacijos patvirtinimo limitas yra atskira Banko paslauga, teikiama Kliento pageidavimu ir Kliento rizika, o papildomas mokėjimo nurodymo pateikimo patvirtinimas telefonu nelaikomas savarankišku

Priedas Nr. 6 Austrijos pagrindiniai projektai ir paslaugos

Verslo – administracijos projektai:

- saugaus elektroninio parašo ir informacijos dėžių

Piliečių – administracijos projektai:

- socialinio draudimo kortelių
- saugaus eletroninio parašo
- informacijos dežių

2000 metų lapkričio mėnesį vyriausybė panaudojo elektroninį parašą tam, kad pakeisti socialinio draudimo korteles į asmens korteles. Asmens kortelės atlieka tris skirtingas funkcijas – socialinio draudimo kortelės, saugaus elektroninio parašo ir informacijos dežės. Visos sistemos kainą sudaro apie 95 milijonai eurų – už maždaug 8 milijonus elektroninių kortelių ir 13000 terminalų.

Priedas Nr.7 Suomijos pagrindiniai projektai ir paslaugos

Verslo – piliečių projektai:

- Satakunta: tai pilotinis projektas – pagrįstas suomių ID kortelėmis sveikatos apsaugos ir socialinio draudimo sektoriuose.
- Šiaurės Karelijos Ligonių apygarda siekia įkurti vientisą sveikatos apsaugos tinklą, leisiantį paprastą bendravimą tarp gydytojų ir pacientų.

Adminstracijos – piliečių projektai:

- darbo adminstravimo
- FINEID – (*FINnish Electronic Identity Card*) Sumių elektroninė identifikavimo kortelė

Priedas Nr. 8 Olandijos pagrindiniai projektai ir paslaugos

Olandijos vyriausybės suformuota darbo grupė grupė išskyrė tris pagrindines veiklos sritis:

- sąveika vyriausybė – piliečiai;
- sąveika vyriausybė – verslas;
- sąveika tarp vyriausybinių organizacijų.

Vyriausybė – piliečiai

Šioje srityje numatytos tokios programos, kurioms reikia PKI:

- Elektroninis balsavimas;
- Elektroninis vyriausybės pasiekiamumas;
- Įvairių mokesčių programos;
- Studentų paskolų programa;
- Centrinis rinkliavos biuras teisingumo departamentui (bilietai, mokesčiai ir t.t.)
- Žemės registravimas;
- Būsto prašymų registravimas;
- Prašymai subsidijoms ir licenzijoms.
- nacionaliniai registravimai internetu; Olandijos teisingumo departamentas pradėjo naudoti video, audio ir internetines nuorodas, kad laikyti teismo įrašus.
- vyriausybės – piliečių bendravimo;
- skaitmeninis mokečių inspekcijos ofisas leis susimokėti mokesčius internetu;
- socialinio saugumo ir darbo biržos;.
- darbo paieškos bankas; sudaro galimybę nesunkiai peržiūrėti siūlomus darbus ir taip pat internetu pasiūlyti savo kandidatūrą
- sveikatos apsaugos; laikant tam tikrus sveikatos įrašus EIK, būtų galima geriau ir greičiau gauti duomenis apie pacienta tuo pačiu suteikiant kokybiškesnę pagalbą.

Yra diegiami tokie pilotiniai projektai:

- "Lengvi mokesčiai": Mokesčių inspekcijos projektas, susijęs su įvairių elektroniniu formų pateikimu mokesčių grąžinimui.
- Pilotinis socialinių paslaugų projektas, į kurį įeina:
  - ✓ Nuotolinis dirbančiųjų asmenų formų užpildymas;
  - ✓ Elektroninis pajamų apskaičiavimas;
  - ✓ Bedarbių/darbuotojų registracija;
  - ✓ Kandidatų darbui registracija.
- Elektroninė identifikavimo (ID) kortelė: Olandų miestų organizacija kuria skaitmeninės ID kortelės sistemą, kuri leistų piliečiams bendrauti su vietinės valdžios institucijomis per internetą.

Vyriausybė – verslas

Šioje srityje numatomos tokios programos:

- Mokesčių programos;
- Prašymų patalpoms registravimas;
- Prašymas subsidijų ir licencijoms gauti registravimas.
- Hagos municipalinė mokesčių inspekcija; piliečiai ir privatūs asmenys galės pasiekti internetu visą nuosavybės apmokestinimo informaciją. Ši programa žinoma kaip GeoMedia® technologija leidžianti nuosavybės savininkams nustatyti ar turto įvertinimas teisingas ir nuspęsti ar verta apskųsti mokesčius.
- EIK susijusios su bendru PKI; EIK panaudojimas bus galimas nuo 2002 metų pabaigos
- duomenų pasikeitimo; administracinių procedūrų tarp piliečių, verslo įmonių ir vyriausybės agentūrų supaprastinimas, pavyzdžiui pateikiant beveik užpildytas formas; taip pat administracinių išlaidų mažinimas surašant visus duomenys į vieną centralizuotą duomenų bazę.

Šioje srityje vykdomi pilotiniai projektai:

- mokesčių inspekcijos projektas;
- prekybos rūmų projektas.

Tikslas įgalinti registruoti/atnaujinti verslo įmonių duomenis per internetą.

Vyriausybinių organizacijų viduje

Yra identifikuotos tokios galimos šios srities programos:

- Vyriausybės vidinis tinklas;
- Saugaus elektroninio pašto tarp administracinių vienetų programa;
- Sąlygų tarnautojams, dirbantiems namuose, užtikrinimas.

Šiuo metu jau yra diegiami tokie pilotiniai projektai:

- Saugaus mobilaus bendravimo užtikrinimas tarp muitinių ir policijos;
- Saugus elektroninis paštas Teisingumo departamentui.

Priedas Nr. 9 Didžiosios Britanijos pagrindiniai projektai ir paslaugos

Šiuo metu vykdomi tokie projektai:

- įdarbinimo klausimų sprendimas; Siūlomas būdas keistis elektronine informacija smulkiam verslui įdarbinimo klausimais: tikrinant įmanoma įsidarbinimą vaikų proiežiūros srityje, padeda ir pataria susirasti darbą, taip pat informuoja apie įdarbinimo įstatymus Didžiojoje Britanijoje.

- butų fondų planavimas; Pateikiama Nacionalinė žemės panaudojimo duomenų bazės informacija apie butų fondų politiką, apylinkės atnaujinimą ir butų fondus ir pan.
- prekyba; Prekybos rūmai teikia įvairią elektroninę verslo įmonių informaciją pasiekiamą per internetą. Paskolų teikimo paslaugos puslapis tiekia naudotojams įvairias formas. Naudotojai taip pat gali čia ieškoti paskolų teikimo teisininkų. Taip pat čia yra elektroninės nuorodos iš teismo apie paskolų bylas. Teikiama informacija apie *copyrights*, projektus, patentus ir prekinius ženklus. Didžiosios Britanijos bendrovės taip pat gali gauti prekybos ir investicijų informaciją.
- iždas ir mokesčiai; Iš vidaus pajamų interneto puslapio galima gauti informaciją apie akcinių bendrovių mokesčius.
- informacija apie pašalpas; Čia galima rasti informaciją apie vaikų pašalpas ir taaip pat galima atsisiųsti pašalpos prašymo formą. Taip pat galima gauti informaciją apie numatomą pensiją.
- vartotojai; Čia galima ieškoti informacijos apie vartotojų klasuimus. Taip pat rasti keletą nuorodų į panašius puslapius. Galima nusipirkti televizijos licenziją.
- įdarbinimas; Siūlomi įvairūs darbai.
- aplinka; Aplinkos apsaugos agentūros puslapis pateikia informaciją apie aplinką ir su ja susijusius klausimus. Taip pat čia galima rasti informaciją apie kokybę.
- vyriausybė; piliečiai gali užpildyti ir išsiųsti formas dėl mokesčių grąžinimo.
- palikimas; Galima aplankyti viešųjų įrašo ofiso interneto puslapio 1000 metų žemės nuosavybės dokumentus. Taip pat galima aplankyti muziejų interneto puslapius.
- parlamentas; Per įvairius interneto puslapius galima aplankyti ir sužinoti kas dedasi parlamente, lordų rūmuose ir liaudies rūmuose. Taip pat galima susisiekti su vyriausybe internetu.
- nuosavybė; nekilnojamo turto kainos.
- socialinis aukojimas; Pateikia patogų būdą aukojimams darbu, laiku, pinigais.
- kelionės; Pateikiama informacija apie lankytinas vietas, apie siūlomas keliones. Taip pat galima užsakyti vizas, atnaujinti pasą ir pan.
- sveikata; Teikia informacija apie sveikatą, siūlomi sveikatos patarimai.
- išsilavinimas; Siūlomi suaugusių internetiniai mokymosi kursai. Taip pat galima ieškoti laisvų vietų universitetuose, mokytojų patarimų, mokyklų ir koledžų mokymosi rezultatų lentelių.
- nusikalstamumas; Teikiama informacija apie nusikalstamumo padrytos žalos atlyginimą ir pateikiamos prašymo formos.

- teismų paslaugos; Siūlo daug internetinės informacijos apie įstatymus, siūlo internetinius patarimus. Taip pat galima informuoti policiją apie padarytus nedidelius nusikaltimus.
- transportas; Pateikia vairavimo teorijos egzamino testą.

Priedas Nr. 10 Švedija. Koncepcija

SHS infrastruktūra pirmiausia skirta informacijos apsikeitimui tarp viešojo administravimo įstaigų, bet ji numatoma naudoti ir viešojo administravimo įstaigų bendravimui su Švedijos piliečiais bei verslo įmonėmis. Pagrindinis SHS projekto tikslas yra sukurti bendrą infrastruktūrą, pasižyminčią aukštu saugumo lygiu ir suderinamumu, informacijos apsikeitimui viešajame sektoriuje.

SHS projekte yra išskirtos trys apsikeitimo elektronine informacija sritys:

- Pateikimas specifinės informacijos asmenims ir verslo įmonėms, kai būtina užtikrinti informacijos saugumą ir integralumą.
- Gavimas specifinės informacijos iš asmenų ir verslo įmonių, kai būtina užtikrinti informacijos saugumą ir integralumą.
- Viešojo administravimo įstaigų veiklos procesų racionalizavimas ir jų efektyvumo didinimas, formuojant virtualią Vyriausybę, t.y. e-Vyriausybę.

Pirmosios dvi sritys naudoja SHS kaip įrankį viešojo administravimo įstaigoms, leidžiantį užtikrinti, kad asmenys ir verslo įmonės turi abipusio elektroninio bendravimo galimybę, įgalinančią siųsti ir gauti informaciją. Svarbu pažymėti, kad asmenims ir verslo įmonėms nebūtina žinoti, į kurią konkrečiai agentūrą jiems reikia kreiptis, o pakanka žinoti, kokių paslaugų jiems reikia. Taip pat turi būti užtikrinama galimybė grupei viešojo administravimo įstaigų ir/arba trečiųjų šalių pateikti priėjimą prie viešojo administravimo elektroninių paslaugų (e-paslaugų) per vieną ar daugiau portalų. Tokiu būdu, naudojant SHS infrastruktūrą, galima asmenims ir verslo įmonėms sudaryti galimybę gauti viešojo administravimo įstaigų teikiamas paslaugas “per vieną langelį”.

Trečioji sritis užtikrina efektyvų informacijos apsikeitimą tarp viešojo administravimo įstaigų. Reikia pastebėti, kad tai yra būtina sąlyga “vieno langelio” principo užtikrinimui asmenims ir verslo įmonėms. Informacija apie visas teikiamas viešojo administravimo e-paslaugas yra saugoma globaliame SHS paslaugų kataloge (*service directory*). SHS projekte yra numatomi 2 informacijos apsikeitimo tarp viešojo administravimo įstaigų būdai:

- failų persiuntimas;
- užklausos/atsakymai.

Failų persiuntimas naudojamas, kai reikia perduoti didesnius informacijos kiekius, užklausos/atsakymai dažniausiai naudojami apsikeitimui tarp viešojo administravimo įstaigų nedideliais informacijos kiekiais.

Esminis vaidmuo SHS projekte skiriamas elektroniniam parašui, įgalinančiam užtikrinti perduodamų duomenų saugumą ir integralumą.

SHS naudojimo scenarijaus pavyzdys

Viena pirmųjų e-paslaugų, pagrįstų SHS platforma, Švedijoje buvo Kontaktas-N, skirta personalinių įmonių registravimo procedūros supaprastinimui. Tipinis įmonės registravimo procesas reikalauja bendravimo su daugeliu įstaigų ir todėl yra daug laiko reikalaujantis ir sudėtingas asmenims, norintiems įkurti naują įmonę. Tą pačią informaciją dažnai reikia pateikti daugeliui įstaigų, tarp kurių nėra koordinuoto apsikeitimo informacija. Naudodamasis internetu ir SHS, pareiškėjas turi vienintelį valstybinį kontaktą (*one government contact to one customer - 1G21C*), valstybinės institucijos naudoja SHS bendravimui tarpusavyje (*government to government exchange -G2G*) ir pareiškėjui nereikia žinoti, kokios viešojo administravimo įstaigos dalyvauja procese.

Patobulintas procesas yra toks:

- Pareiškėjas užpildo, pasirašo ir išsiunčia naujos įmonės registravimo formą, naudodamas internet naršykle. Saugų duomenų perdavimą užtikrina SHS.
- Gavėjas yra Patentų ir registravimo tarnyba. Atėjus paraiškai, SHS apibrėžta funkcija persiunčia informaciją Mokesčių inspekcijai.
- Mokesčių inspekcija išsiunčia patvirtinimą ir leidimą registruoti naują įmonę pareiškėjui.
- Patentų ir registravimo tarnyba išsiunčia patvirtinimą ir naujos įmonės resgitravimo dokumentus pareiškėjui.

Architektūra, technologiniai sprendimai ir saugumas

SHS yra suprojektuota taip, kad ji būtų visai nepriklausoma nuo vidinių viešojo administravimo įstaigų taikomųjų sistemų. Tam, kad viena taikomoji sistema galėtų keistis informacija su kita taikomąja sistema kitoje (arba net toje pačioje) organizacijoje, tereikia papildyti dalykinę informaciją minimaliais duomenimis, būtinais jos perdavimui. Pagrindinis SHS projekto principas – bendraujančios taikomosios sistemos turi būti minimaliai priklausomos.

Informacija apie SHS adresus, produktus, paslaugas ir veikėjus yra saugoma globaliame SHS paslaugų kataloge (*service directory*). Be to, informacijos apsikeitimas tarp viešojo administravimo įstaigų yra pagrįstas dvišalėmis sutartimis, kas užtikrina griežtai struktūrizuotus duomenų srautus viešojo administravimo sektoriuje ir aukštą integralumo lygį.

SHS projekte informacijos perdavimas ir saugumas yra atskirti nuo pačios perduodamos dalykinės informacijos. Tai daro SHS nepriklausomą nuo apsikeičiamos informacijos formatų. SHS dokumentas sudaromas iš specialios SHS antraštės ir vieno ar daugiau dalykinių duomenų elementų, kurie gali būti pateikti praktiškai bet kokiu formatu: nuo garso įrašų, paveiksliukų, dokumentų iki struktūrizuotų duomenų, aprašytų XML ar EDIFACT. Kiekvienas duomenų elementas gali būti pasirašytas elektroniniu parašu.

SHS remiasi patvirtintais standartais ir technologijomis: TCP/IP, HTTP, SSL, S/MIME, XML, PKI, X.500 ir LDAP. SHS suprojektuotas veikti bet kokiame TCP/IP tinkle: nuo privačių tinklų, VPN iki globalaus interneto.

Saugumo užtikrinimas yra realizuotas keliais lygiais. Perduodama informacija apsaugoma griežtu autentifikavimu ir šifravimu: visa informacija siunčiama į/iš ir SHS viduje yra šifruojama, naudojant SSL ir X.509 sertifikatus. Sertifikatai ir jų raktai gali būti saugomi kompiuterio diske arba kortelėje. Šiuo metu informacijos perdavimo tarp viešojo administravimo įstaigų saugumo užtikrinimui SHS naudojami sertifikatai, išduoti dviejų Sertifikavimo centrų (*certificate authorities - CA*). Be to, saugumo lygis padidinamas, naudojant šifravimą ir elektroninius parašus sistemose, kurios keičiasi informacija. Papildomai SHS kuria įrašus duomenų perdavimo auditui ir saugo kiekvieno SHS dokumento istoriją.

Pačios SHS diegimas neapima sertifikatų, kuriuos laisvos rinkos principais teikia Sertifikavimo centrai, t.y. kiekviena viešojo administravimo įstaiga arba jų grupės gali apsispręsti, kuriuo Sertifikavimo centru pasitikėti. Abi bendraujančios pusės turi pasitikrinti, kad kitos pusės sertifikatas yra galiojantis, išduotas patikimo Sertifikavimo centro ir nėra įtrauktas į atšauktų sertifikatų sąrašą.

Kaip jau buvo minėta, esminė SHS konfigūracijos informacija yra saugoma globaliame SHS paslaugų kataloge (*service directory*), tačiau našumo padidinimui SHS turi automatinio periodinio konfigūracinių duomenų replikavimo į lokalius katalogus funkcijas.

Joks bendravimas SHS nėra galimas be sutarčių informacijos apsikeitimui. Sutartys gali būti dvišalės arba viešos (*open-ended, public agreements*). Viešos sutartys naudojamos įstaigos bendravimui su daugeliu kitų, pavyzdžiui, Mokesčių inspekcija ir visi asmenys, pateikiantys deklaracijas. SHS naudojamos sutartys nėra teisinės sutartys, tačiau daugeliu atveju yra SHS sutartis atitinkantys teisiniai dokumentai. SHS sutartys yra svarbus mechanizmas informacijos perdavimo tinkle apibrėžimui ir kontrolei, jomis remiasi adresavimas SHS tinkle.

Priedas Nr. 11 Kanada. PKI projektai ir taikomosios programos

Keletas su PKI susijusių pilotinių projektų yra perimti federalinių agentūrų ir yra atrinkti, kaip specialūs projektai GOC PKI *Pathfinder* programai. Šią programą atstovauja federalinės valdžios perimti novatoriškiausi projektai, orientuoti į praktinį įgyvendinimą, taikymus ir PKI technologijų panaudojimą.

Yra apie 17 *Pathfinder* projektų ir daugiau kaip 100 PKI pilotinių projektų naudojančių internetą ir PKI on-line paslaugų teikimui.

1) Saugios taikomosios sistemos ir raktų valdymo paslaugos (*Secure Application and Key management services SAKMS*) – ši programa buvo pradėta 1995 metų gruodžio mėnesį kaip Vyriausybės komunikacijos ir informacijos paslaugų (*the Government Telecommunications and Informatics Services GTIS*) PKI. Kadangi ji sudaryta iš įvairiapusiškų paslaugų, SAKMS sudaro galimybę kitiems departamentams išbandyti saugius GTIS sprendimus arba panaudoti GTIS sertifikavimo centrus (*Certification Authority*), kaip vidines kūriamų elektroninio verslo sistemų komponentes.

2) Investicijų analizė – elektroninio duomenų surinkimo pilotinis projektas (*Investment Review – Electronic Filing Pilot*). Investicijų analizės padalinys (*Investment Review Division IRD*), į kurio funkcijas įeina daugiau kaip 1000 programų stebėjimas, kiekvienais metais iš daugiau kaip 200 firmų visoje Kanadoje surenka duomenis apie vykdomas programas. Tradiciškai duomenys pildomi popieriuje ir persiunčiami paprastu paštu arba faksu. Tam, kad pagerinti patį duomenų surinkimo procesą ir sumažinti reikiamas išlaidas, IRD inicijuoja pilotinį projektą saugiam elektroniniam informacijos pildymui naudojant PKI technologiją.

3) Radijo dažnių licencijavimo pilotinis projektas (*Spectrum Radio Licensing Pilot*). Kanados radijo dažnių informacinių technologijų ir telekomunikacijų tarnyba (*Spectrum Information Technologies and Telecommunications SITT*) yra atsakinga institucija išduoti licenzijos radijo dažniui Kanados vyriausybės vardu. Kiekvienais metais gaunama daugiau kaip 850.000 prašymų iš mažų, didelių firmų ir kitų organizacijų. Vartotojai moka licencijų mokestį kiekvienais metais ir iš to valstybė gauna daugiau kaip 150 milijonų dolerių per metus. Radijo dažnių elektroninio verslo pilotinio projekto tikslu yra galimybė klientams saugiai užpildyti reikiamas formas ir išsiųsti elektroniniu paštu, naudojant PKI technologiją su elektroniniu parašui konfidencialumui užtikrinti.

4) Administravimo elektroninių dokumentų tvarkymo pilotinis projektas (*Electronic Regulatory Filing Project*). Nacionalinė energijos taryba (NEB) yra nepriklausoma federalinė reguliavimo agentūra įkurta 1959 metais. Ši taryba reguliuoja tam tikrus energetikos pramonės aspektus, susijusius su šalies ir tarptautinių elektros linijų, elektrinių statyba ir valdymu; gamtinių dujų eksportu ir importu; naftos ir elektros eksportu; ir kitomis su nafta ir gamtinėmis

dujomis susijusiomis veiklomis. NEB per metus gauna apie 750 prašymų, kurių kiekvienas yra nuo 20 iki 3000 puslapių apimties. Kartais atsiunčiamos 20 – 35 prašymų ir kitų su jais susijusių dokumentų kopijos. NEB 1992 metų pabaigoje priėmė sprendimą dėl perėjimo nuo popierinių prie elektroninės formos dokumentų. Administravimo elektroninių dokumentų tvarkymo pilotinis projektas buvo sugalvotas kaip būdas palengvinti elektroninių dokumentų tvarkymą. Jis paliečia tris pagrindinius aspektus: keitimąsi elektroniniais dokumentais, sudarymą dokumentų saugyklų, skirtų viešam priėjimui, ir taip pat tarybos informacinės sistemos ir procesų pakeitimus.

5) Tinklo saugumo strategija (*Network Security Strategy*). INAC (*Indian and Northern Affairs Canada*) tinklas valdo saugotinus resursus, todėl būtina užtikrinti šio tinklo saugumą. Tačiau realūs faktoriai šį saugumą objektyviai mažina: tokie kaip poreikis dalį informacijos pateikti viešai, poreikis dalintis informacija su kitomis vyriausybinėmis įstaigomis. Tinklo saugumo strategijos uždavinys yra saugoti kolektyvinio naudojimo saugotiną informaciją. Kai kurios šios sistemos dalys realizuotos, panaudojant specifinius, sistemose įdiegtus servisus. Kiti komponentai realizuoti, naudojant PKI šifravimams ir skaitmeniniams parašams.

6) Darbo biržos vystymo projektas *(Labour Market Development Agreement (LMDA) Connectivity Project)*. Žmogiškųjų resursų ir plėtros ministerija (*The Ministry of Human Resources and Development Canada HRDC*) bendrauja su atskiromis veiklos sferomis ir teritorijomis, kuriose galėtų įsidarbinti nauji žmonės, juos apmokius pagal darbo vietų poreikius. Šiems ryšiams palaikyti reikalinga duomenų bazė. Taip pat yra būtinas saugumas ir griežtai autentifikuotas priėjimas prie duomenų. Projektą apsunkina tai, kad atskiros sistemos dalys yra labai smarkiai išskaidytos. HRDC tinklas yra gerai apsaugotas nuo išorinio priėjimo *Eagle Raptor* ugniasienėm ir *KyberPass* autentifikavimo serveriais. Duomenų kodavimas tarp HRDC tinklo ir partnerių stočių yra atliekamas remiantis PKI technologija. Griežtas partnerių autentifikavimas yra pasiekiamas, realizuojant *KyberWin* klientą su viešojo rakto kriptografijos programine įranga nutolusiose darbo stotyse. Viešųjų raktų infrastruktūra yra HRDC pagrindas griežto autentifikavimo ir šifravimo paslaugoms. 1997 metų vasarą HRDC buvo įkurtas sertifikavimo departamentas ir sudaryta galimybė naudoti raktų poras ir viešųjų raktų sertifikatus, palengvinančius PKI panaudojimą. Iki šios dienos jau yra išduota 2-3 tūkstančiai sertifikatų.

7) Kanados švietimo subsidijų sistema (*Canada Educational Savings Grant (CESG) System*). 1998 metų vasario mėnesį federalinė vyriausybė paskelbė naują švietimo aprūpinimo tvarką - Kanados švietimo subsidijų projektą. Pagal šią programą tėvai gali potencialiai pridėti iki 7200 dolerių (plius visi gauti procentai) į vaiko ateities fondą. CESG sistema yra labai svarbi šiai naujai programai. Tai saugus sprendimas, suprojektuotas teikti saugius, abipusius svarbių

duomenų apsikeitimus ir finansinius pervedimus per internetą tarp HRDC sistemų ir finansinių fondų. Orientuojamasi į 30 milijonų saugių elektroninių transakcijų CESG programos pirmais veikimo metais bei apie 100 finansinių institucijų partnerių.

8) Kelionių organizavimo sistema (*Travel management System)*. Paprastai kelionių organizavimas neautomatizuotas ir neefektyvus procesas, naudojantis daug popierinių formų. Šios formos turi būti užpildytos ir pasirašytos klientų, o tada siunčiamos pasirašyti atitinkamų atsakingų kelionių organizatoriams. Siekiant sumažinti su tuo susijusias išlaidas, procesas gali būti automatizuojamas. Kuriamas pilotinis projektas, įgalinantis naudoti elektronines formas bei organizuojantis dokumentų srautus, naudojant PKI technologiją, kuri įgalina elektroninius parašus parašus ir reikiamą saugumo lygį.

9) Verslo registravimo internetu pilotinis projektas (*Business Registration On-line Internet Pilot*). Verslo pajamų ir mokesčių direktoratas BRPP yra atsakingas už verslo įmonių registravimą ir apskaitą. Norint pagerinti teikiamas paslaugas ir sumažinti popierinių dokumentų poreikį, BRPP inicijuoja verslo įmonių registravimo internetu pilotinį projektą, kuris registravimo procesą perveda į internetą. Naudotojai gali pateikti reikiamą informaciją dialoginiu režimu (*on-line*).

10) Saugių žinučių pilotinis projektas (*Secure Messaging Pilot*). Šio pilotinio projekto pirminė iniciatyva yra GOC PKI realizavimas. Tikslas – sistemingai, praktiškai patikrinti viešųjų raktų infrastruktūros veiksmingumą. Patirtis ir rezultatai duos reikiamą tikrosios viešųjų raktų naudos įvertinimą.

11) Saugių elektroninių paslaugų suteikimas (*Secure Electronic Service Delivery SESD*). SESD - tai trijų metų bendras projektas, dalyvaujant saugumo departamentui bei Kanados sveikatingumo centrui, ir yra skirtas teikti svarbiausias informacijos saugaus apsikeitimo paslaugas tarp departamentų. Pagrindiniai tikslai yra sudaryti standartą, koordinuoti ir integruoti internet paslaugų sprendimą, tenkinantį saugumo departamento reikalavimus.

12) Internetinis radijo dažnių aukcionas (*Spectrum Internet Auction*). Kanados radijo dažnių informacinių technologijų ir telekomunikacijų tarnyba yra atsakinga už radijo dažnių paskirstymą. Ji turi užtikrinti radijo dažnių naudojimo suderinamumą. Radijo dažnių resursas yra deficitinis ir dažnai paklausa viršija pasiūlą. Radijo dažnių aukcionas yra rinka pagrįstas įrankis, kurį departamentas naudoja radijo dažniams paskirstyti. Kanados internetinio radijo dažnių aukciono saugumas buvo užtikrintas, įdiegiant naujausią PKI šifravimo ir elektroninio parašo technologijas. Tai ura vienas didžiausiu pirmųjų verslo ir vyriausybės elektroninės prekybos projektų, kuris atliekamas internetu. Taikomoji aukciono programinė įranga buvo panaudota standartinė, o šifravimo ir elektroninio parašo paslaugos suteiktos privačiame sektoriuje.

13) Nauja Kanados atlyginimų skaičiavimo sistema – saugus tinklo pilotas(*New Canada Payroll Savings - Secure Web Site Pilot*). Kanados bankas (BoC) inicijavo saugios internetinės aplikacijos sukūrimą, kurios paskirtis padėti mažoms kompanijoms su maža IT patirtimi, pasinaudojant BoC internetine atlyginimų skaičiavimo sistema. Aplikacijos saugumas turi užtikrinti, kad tik teisėti vartotojai gali prisijungti ir peržiūrėti savo darbuotojų duomenų sąrašą. Sprendimas buvo panaudoti PKI šifravimą ir autentifikavimą. Pilotinis projektas baigtas 1999 gruodžio mėnesį ir iš pradžių įsitraukė virš 50 kompanijų, kur kiekvienoje vidutiniškai dirbo daugiau kaip 120 darbuotojų. Orientacinis vartotojų padidėjimas metų laikotaryje – iki 5000 darbdavių.

14) Didelių sumų perdavimo sistema (*Large Value Transfer System LVTS*). LVTS yra visai nauja elektroninio kreditavimo sistema, sudaryta tam, kad būtų galima atlikti didelių sumų arba laikui jautrių sumų (dėl valiutų kurso svyravimo) mokėjimus Kanadoje. Ji įgalina verslą ir vyriausybę atlikti mokėjimus labai greitu, saugiu ir efektyviu būdu. Sistema tvarkosi su dabartinio laiko rizikomis ir užtikrina transakcijų saugumą, stabilumą, korektiškumą ir greitą atlikimą. LVTS naudoja SWIFT (*Society of Worldwide Interbank Financial Telecommunications*) tinklą mokėjimų siuntimui, bet pagrindinis darbas yra atliekamas naudojant privatų LVTS tiesioginį tinklą. Šis LVTS tiesioginis tinklas naudoja PKI, sudarant šifrą, skaitmeninį parašą ir žymę, bei slaptažodį, kad apsaugotų siuntimus.

15) Darbuotojų registravimo pilotinis (*Record of Employment on Web Pilot*). Kiekvienas darbo nutraukimas, reiškia, kad darbuotojas turi užpildyti tam tikrą formą. Kiekvienas iš daugiau nei 1 milijono darbdavių sudaro ir užpildo 8 milijonus kelių dalių formų. Iš viso tai būtų apie 36000 formų per dieną. HRDC inicijavo saugaus formų perdavimo per internetą pilotinį projektą. HRDC sudaro dviejų rūšių elektroninės formas: žemo lygio – kur naudotojai patys peržiūri, užpildo ir išsiunčia formas – ir aukšto lygio – keletas formų iškart siunčiamos per FTP patikrinimui ir priėmimui. Kadangi abu procesai turi savyje svarbios informacijos perdavimą, todėl būtina sudaryti saugumo mechanizmą, garantuojantį slaptumą.

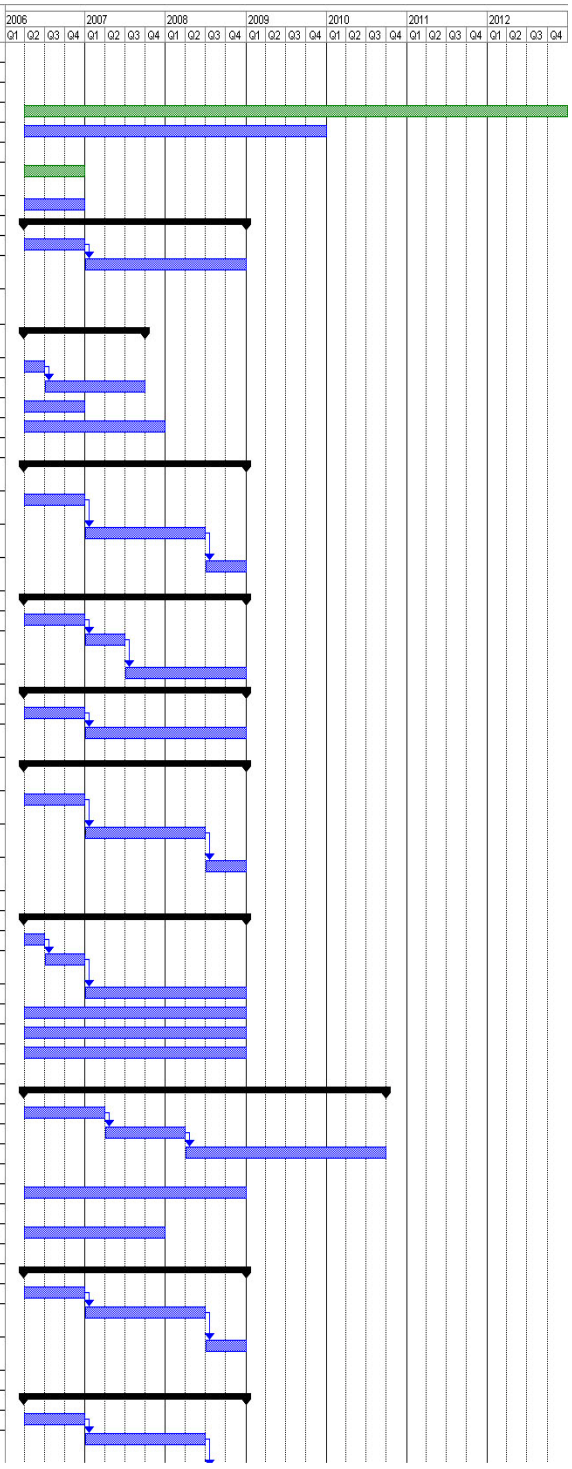
16) Muitinių interneto tinklo projektas (*Customs Internet Gateway Project*). Muitinių automatinio apsikeitimo duomenimis sistema (*Customs Automated Data Exchange CADEX*) buvo realizuota 1988 metais, kaip sistema, kuri leidžia persiųsti duomenis iš importuotojų/tarpininkų į Kanadą. Muitinių interneto tinklo projektas turėjo sudaryti galimybes išsiųsti ir parsisiųsti *CADEX, CUSDEC, ACROSS ir RNS* duomenis per internetą. Saugumą turi užtikrinti PKI. CCRA turi turėti sertifikavimo centrus, kad galėtų išleisti PKI sertifikatus savo verslo partneriams. Dalyviai turi būti užregistruoti ir jiems turi būti išduoti CCRA PKI sertifikatai, programinė įranga, reikalinga sertifikato naudojimui, bei vartotojo instrukcija.

Programinės įrangos licencija bei sertifikatas priklauso CCRA ir gali būti naudojami tik CCRA reikmėms.

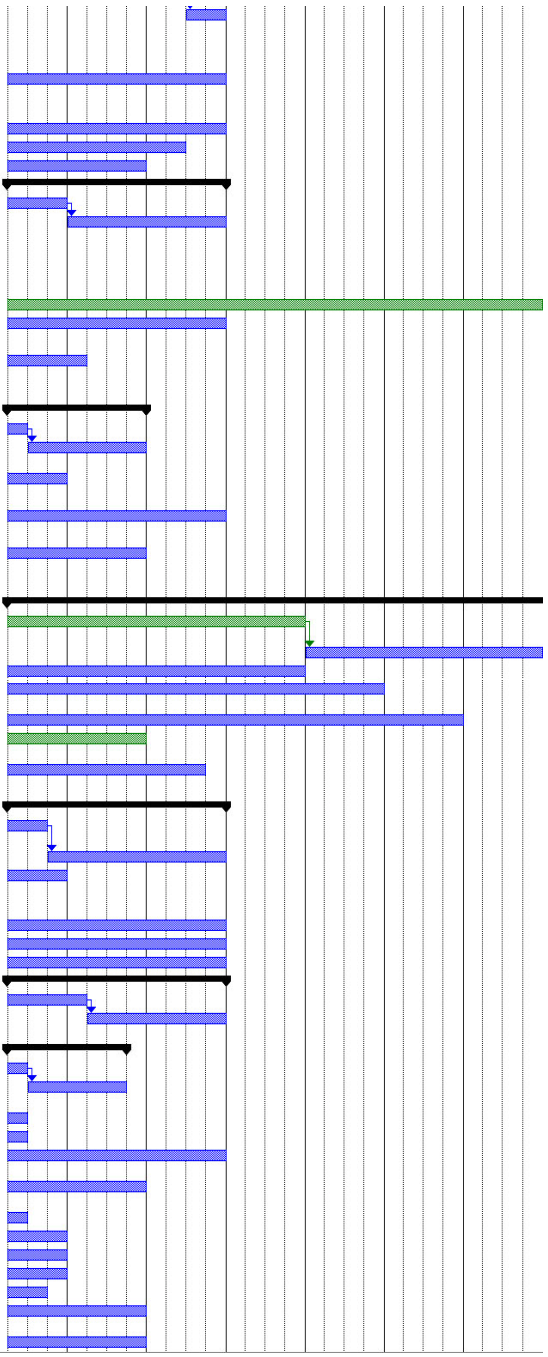
17) GENet saugus nutolęs priėjimas (*GENet Secure Remote Access SRA*). Saugus nutolęs priėjimas yra virtualaus privataus tinklo (VPN) paslauga, tiekiama komunikacijų bei informacinių paslaugų vyriausybės įmonėms. VPN suteikia departamentams nutolusį prisijungimą prie LAN/WAN labai aukšto saugumo interneto paslaugų lygyje (iki B saugumo lygio). Tai leidžia vyriausybės tarnautojams (nesvarbu, ar darbuotojas būtų namie, ar kelyje, ar mobiliame ofise) saugiai pasiekti savo departamentus per intranetą, pasitikrinti elektroninį paštą, pasinaudoti taikomosiomis programomis, pasiekti bylas, duomenų bazes ir dar daugiau. Sistema pagrįsta šifravimų ir autentifikavimu remiantis Kanados vyriausybės viešųjų raktų infrastruktūra.

Priedas Nr. 12

Priemonės pavadinimas	Esamas lygis	Siekiamas lygis	Atsakingi vykdytojai
1. Teikti viešąsias paslaugas, numatytas ES programiniuose dokumentuose, gyventojams naudojant IRT			
1.1. Pajamų, turto deklaravimas			
1.1. Pajamų, turto deklaravimas	4		
1.1.1. Priimti mokesčių deklaracijas ir grąžinti sumokėtą gyventojų pajamų mokestį		Tobulinti	VMI prie FM
1.1.2. Konsultuoti mokesčių mokėtojus		4	VMI prie FM
1.2. Laisvų darbo vietų paieška	4		
1.2.1. Patobulinti laisvų darbo vietų paieškos sistemą, gyventojams sudarant sąlygas patogesniu būdu ieškoti darbo ir užsakyti darbo pasiūlymus		4	SADM; LDB prie SADM
1.2.2. Išduoti užsieniečiams leidimus dirbti Lietuvoje		3	SADM; LDB prie SADM
1.2.3. Organizuoti konkursus valstybės tarnautojo pareigoms			
1.2.3. Parengtas investicijų projektą; pakeisti teisės aktus		4	VRM, VTD prie VRM
1.2.3. Sudarytos sąlygos pretendentams el. būdu pateikti prašymą dalyvauti konkurse ir gauti pranešimą apie konkursą; patikrinti kompiuteriu pretendentų žinias, tvarkyti pretendentų sąrašą		4	VRM, VTD prie VRM
1.3. Socialinio draudimo išmokų ir kompensacijų (nedarbo socialinio draudimo išmokos, stipendijos, socialinė parama šeimai ir vaikams ir kt.) skyrimas	1-2		
1.3.1. Skirti socialinio draudimo išmokas, kai tam reikalinga papildoma informacija turima arba ją galima gauti elektroniniu būdu			
1.3.1. Parengti investicijų projektą - galimybių studiją		4	SADM, Sodra
1.3.1. Sukurti informacinę sistemą, leidžiančią prašymus pateikti naudojantis IRT; pakeisti teisės aktus.		4	SADM, Sodra
1.3.2. Teikti bedarbiams informaciją apie nedarbo socialinio draudimo išmokas		4	SADM, LDB prie SADM
1.3.3. Registruoti klientus neįgalumui ir darbingumui nustatyti		2	SADM, NDNT prie SADM
1.4. Asmens dokumentų išdavimas	1-3		
1.4.1. Išduoti užsieniečiams leidimus laikinai (nuolat) gyventi Lietuvos Respublikoje, Europos Bendrijų valstybės narės piliečio leidimus gyventi			
1.4.1. Parengti galimybių studiją - investicijų projektą		2	VRM, MD prie VRM, GRT prie VRM, ADIC prie VRM, Klp. sav.
1.4.1. Remiantis investicijų projektu, pakeisti teisės aktus; vadovaujantis teisės aktais ir remiantis investicijų projektu, sukurti techninę specifikaciją		2	VRM, MD prie VRM, GRT prie VRM, ADIC prie VRM
1.4.1. Gyventojams, siekiantiems pradėti leidimų laikinai (nuolat) gyventi Lietuvos Respublikoje, Europos Bendrijų valstybės narės piliečio leidimų gyventi gavimo procedūrą, sudaryti sąlygas pateikti reikiamus duomenis naudojant IRT		2	VRM, MD prie VRM, GRT prie VRM, ADIC prie VRM
1.4.2. Pakeisti (išduoti) vairuotojo pažymėjimus			
1.4.2. Parengti galimybių studiją - investicijų projektą		3	VRM, Regitra, ADIC prie VRM
1.4.2. Remiantis investicijų projektu, pakeisti teisės aktus; vadovaujantis teisės aktais ir remiantis investicijų projektu, sukurti techninę specifikaciją		3	VRM, Regitra, ADIC prie VRM
1.4.2. Gyventojams, norintiems pakeisti (gauti) vairuotojo pažymėjimą, sudaryti sąlygas pateikti reikiamus duomenis naudojant		3	VRM, Regitra, ADIC prie VRM
1.4.3. Išduoti tarnybinius pasus, valstybės tarnautojo pažymėjimus			
1.4.3. Parengti Valstybės tarnybos valdymo informacinės sistemos plėtros investicijų projektą		3	VRM, VTD prie VRM, ADIC prie VRM
1.4.3. Sukurti ir įdiegti Valstybės tarnybos valdymo informacinės sistemos tarnybinio paso išdavimo (keitimo) ir apskaitos, valstybės tarnautojo pažymėjimo išdavimo (keitimo) ir apskaitos posistemius		3	VRM, VTD prie VRM, ADIC prie VRM
1.4.4. Išduoti asmens dokumentus (pasą, asmens tapatybės kortelę, asmens be pilietybės kelionės dokumentą, užsieniečio pasą)			
1.4.4. Parengti galimybių studiją - investicijų projektą		2	VRM, MD prie VRM, GRT prie VRM, ADIC prie VRM, Klp. sav.
1.4.4. Remiantis investicijų projektu, pakeisti teisės aktus; vadovaujantis teisės aktais ir remiantis investicijų projektu, bus sukurta techninė specifikacija		2	VRM, MD prie VRM, GRT prie VRM, ADIC prie VRM
1.4.4. Gyventojams, siekiantiems pradėti asmens dokumento gavimo procedūrą, sudaryti sąlygas pateikti reikiamus duomenis naudojant IRT; bus naudojama asmens dokumentų išdavimo sistema.		2	VRM, MD prie VRM, GRT prie VRM, ADIC prie VRM
1.5. Transporto priemonių registravimas	1		
1.5.1. Teikti transporto priemonių registravimo paslaugas			
1.5.1. Parengti galimybių studiją - investicijų projektą		3	VRM, Regitra
1.5.1. Remiantis investicijų projektu, pakeisti teisės aktus, reglamentuojantys transporto priemonių registravimą; vadovaujantis teisės aktais ir remiantis investicijų projektu, sukurti techninę specifikaciją		3	VRM, Regitra
1.5.1. Gyventojams ir verslo subjektams sudaryti sąlygas naudojant IRT gauti kelių transporto priemonių registravimo paslaug		3	VRM, Regitra
1.5.2. Teikti pažymas apie laivo įregistravimą Lietuvos Respublikos jūrų laivų registre		3	SM, LSLA
1.5.3. Teikti laivo istorijos tęstinio įrašo dokumentus		3	SM, LSLA
1.5.4. Teikti duomenis apie laivą ir laivo savininką		4	SM, LSLA
1.6. Statybos leidimų išdavimas	1-2		
1.6.1. Išduoti statybos leidimus			
1.6.1. Sukurti IS – I etapą: parengtos IS komponentų duomenų bazės ir taikomosios programos		3	AM, VTPSI prie AM
1.6.1. Sukurti IS – II etapas: parengtos IS komponentų duomenų bazės ir taikomosios programos; įdiegti IS 3-ią lygį		3	AM, VTPSI prie AM
1.6.1. Sudaryti sąlygas pateikti ir gauti dokumentus naudojant IRT; veiks bendra informacijos apie statybų būklę šalyje sistema		4	AM, VTPSI prie AM
1.7. Pranešimų policijai teikimas	1-2		
1.7.1. Priimti pranešimus policijai		3	VRM, PD prie VRM
1.8. Leidinių, publikacijų paieška viešosiose bibliotekose	3-4		
1.8.1. Plėsti leidinių, publikacijų paieškos ir užsakymo viešosiose bibliotekose galimybes		3	KM, apskričių viršininkai, savivaldybės
1.9. Gimimo, mirties, santuokos ir ištuokos liudijimų išdavimas	1		
1.9.1. Sudaryti sąlygas užsakyti ir išduoti liudijimus (gimimo, mirties, santuokos ir ištuokos)			
1.9.1. Parengti galimybių studiją - investicijų projektą		3	VRM, GRT prie VRM, Jurb. sav.
1.9.1. Remiantis investicijų projektu, pakeisti teisės aktus, reglamentuojančius liudijimų išdavimą; vadovaujantis teisės aktais ir remiantis investicijų projektu, sukurti techninę specifikaciją		3	VRM
1.9.1. Gyventojams, siekiantiems pradėti liudijimų gavimo procedūrą, sudaryti sąlygos pateikti reikalaujamus duomenis naudojant IRT; bus naudojama gimimo, mirties, santuokos ir ištuokos liudijimų išdavimo sistema		3	Savivaldybės
1.10. Gyvenamosios vietos deklaracijų priėmimas	1-2		
1.10.1. Priimti gyvenamosios vietos deklaracijas			
1.10.1. Parengti galimybių studiją - investicijų projektą		3	VRM, GRT prie VRM, Jurb. sav.
1.10.1. Remiantis investicijų projektu, pakeisti teisės aktus, reglamentuojančius gyvenamosios vietos deklaravimą; vadovaujantis teisės aktais ir remiantis investicijų projektu, sukurti techninę specifikaciją		3	VRM



1.10.1. Gyventojams, siekiantiems pradėti gyvenamosios vietos deklaracijų pateikimo procedūrą, sudaryti sąlygas pateikti reikiamus duomenis naudojant IRT; bus naudojama gyvenamosios vietos deklaracijų išdavimo sistema		3	Savivaldybės
1.11. Konsultacijų dėl sveikatos priežiūros įstaigų teikiamų paslaugų teikimas ir registracija į priėmimą pas sveikatos priežiūros specialistą	1-2		
1.11.1. Konsultuoti pacientus dėl sveikatos priežiūros įstaigų teikiamų paslaugų ir registruoti į priėmimą pas sveikatos priežiūros specialistą		4	SAM, SADM, savivaldybės, apskričių viršininkai, sveikatos priežiūros įstaigos
1.12. Paraiškų mokytis universitete, kelti kvalifikaciją teikimas	3		
1.12.1. Vykdyti priėmimą į aukštąsias mokyklas		4	LAMA BPO
1.12.2. Konsultuoti gyventojus dėl išsilavinimo įgijimo galimybių		3	ŠMM
1.12.3. Išduoti užsienyje įgytų kvalifikacijų vertinimo pažymas darbo ar studijų tikslais		3	SKVC
1.12.4. Sudaryti sąlygas valstybės tarnautojams registruotis siekiant kelti kvalifikaciją			
1.12.4. Parengti Valstybės tarnybos valdymo informacinės sistemos plėtros investicijų projektą		4	VRM, VTD prie VRM
1.12.4. Valstybės tarnautojams sudaryti sąlygas naudojant IRT gauti informaciją apie mokymus kvalifikacijai tobulinti, elektroniniu būdu registruotis į šiuos mokymus;		4	VRM, VTD prie VRM
2. Teikti viešąsias paslaugas, numatytas Europos Sąjungos programiniuose dokumentuose, verslo subjektams naudojant IRT			
2.1. Verslo subjektų mokesčių deklaravimas	4		
2.1.1. Priimti mokesčių deklaracijas		Tobulinti	VMI prie FM
2.1.2. Gražinti (įskaityti) mutus		4	MD prie FM, MISC
2.2. Naujų įmonių registravimas	2		
2.2.1. Sudaryti sąlygas juridiniams asmenims pateikti visus Juridinių asmenų registrui teikti-nus duomenis ir doku-mentus, gauti išrašus iš Juridinių asmenų registro naudojant IRT		3	TM, Registrų centras
2.3. Duomenų teikimas Statistikos departamentui prie Lietuvos Respublikos Vyriausybės	3		
2.3.1. Priimti verslo statistikos tyrimų duomenis			
2.3.1. Parengti Integruotos statistikos informacinės sistemos techninį projekta (specifikaciją)		3	STD
2.3.1. Įvykdytas investicijų projektą „Integruotos statistikos informacinės sistemos sukūrimas" – sukurti integruotą statistikos informacinę sistemą		3	STD
2.3.2. Sudaryti sąlygas gauti statistikos leidinius elektronine forma		4	STD
2.4. Viešieji pirkimai naudojant IRT	4		
2.4.1. Palaipsniui perkelti viešuosius pirkimus į elektroninę terpę		4	VPT prie LRV, IVPK prie LRV
2.5. Valstybinio socialinio draudimo įmokų mokėjimas	3		
2.5.1. Priimti draudėjų Valstybinio socialinio draudimo fondo valdybai prie Socialinės apsaugos ir darbo ministerijos teikiamas deklaracijas		4	SADM, Sodra
2.6. Muitinės deklaracijų pateikimas	4		
2.6.1. Tobulinti elektroninių muitinės deklaracijų priėmimo paslaugas			
2.6.1. Atnaujinti prekių eksporto / importo sistemą susietą su kuriama naują Europos Sąjungos automatizuota eksporto / importo sistema		4	MD prie FM, MISC
2.6.1. Elektronines muitinės deklaracijas priimti viename prieigos taške, veikiančiame vieno langelio principu		4	MD prie FM, MISC
2.6.2. Registruoti Europos Sąjungos valstybėse narėse įgaliotus ekonominių operacijų vykdytojus		4	MD prie FM, MISC
2.6.3. Teikti nacionalinių muitinės administracijų ir Europos Komisijos sukauptą informaciją apie importo ir eksporto operacijas			MD prie FM, MISC
2.6.4. Teikti informaciją apie prekybos tarifinio reguliavimo priemones		4	MD prie FM, MISC
2.6.5. Tobulinti elektroninių Intrastato (duomenų apie Lietuvos prekybą su Europos Sąjungos valstybėmis surinkimo sistemos) ataskaitų pateikimo paslaugas		4	MD prie FM, MISC
2.6.6. Priimti krovinių ir prekių, gabenamų per Klaipėdos valstybinį jūrų uostą, deklaracijas		4	SM, KVJUD
2.7. Leidimų, kuriuos reikia derinti su aplinkos apsaugos tarnybomis, išdavimas	1		
2.7.1. Išduoti leidimus, susijusius su aplinkos apsauga			
2.7.1. Įgyvendinti projektą „Projekto „E. pas-laugos „Aplinkosaugos leidimų išdavimas" sukūrimas" įgyvendinimui reikalingos dokumentacijos parengimas", parengti aplinkosaugos leidimų išdavimo informacinės sistemos sukūrimo galimybių studiją		4	AM, AAA, AM RAAD, VAAI
2.7.1. Verslo subjektams sudaryti sąlygas naudojant IRT užsakyti ir gauti leidimus		4	AM
2.7.2. Tobulinti Teritorijų planavimo dokumentų registrą ir skeltsi jo duomenis naudojant IRT, sujungti šį registrą su kitais susijusiais registrais			AM, AAA
3. Teikti kitas viešąsias paslaugas gyventojams ir verslo subjektams, naudojant IRT			
3.1. Įdiegti vartotojų švietimo ir konsultavimo informacinę sistemą		3	TM, NVTAT prie TM
3.2. Sukurti ir įdiegti vartotojų skundų ir pražymų nagrinėjimo internetinę sistemą		3	TM, NVTAT prie TM
3.3. Išduoti dokumentus, susijusius su ginklais, pirotechnikos priemonėmis, asmens ir turto sauga		3	VRM, PD prie VRM
3.4. Pateikti informaciją apie eismo sąlygas valstybinės reikšmės keliuose			
3.4. Parengtas valstybinės reikšmės kelių eismo informacinės sistemos investicijų projektą (galimybių studiją)		3	SM, LADK prie SM
3.4. Naudojant IRT, teikti informaciją apie eismo sąlygas valstybinės reikšmės keliuose (oro sąlygas, kelio dangos būklę, eismo intensyvumą, eismo apribojimus ir kita)		3	SM, LADK prie SM
3.5. Teikti asmeninę informaciją valstybinio socialinio draudimo išmokų gavėjams ir apdraustiesiems			
3.5. Parengti investicijų projektą - galimybių studiją		4	SADM, Sodra
3.5. Sukurti ir įdiegti informacinę sistemą - valstybinio socialinio draudimo išmokų gavėjai ir apdraustieji informaciją iš informacinės sistemos gaus naudodami IRT		4	SADM, Sodra
3.6. Teikti Lietuvos Respublikos vidaus vandenų laivų registro duomenis internetu pagal registro duomenų teikimo sutartį		4	SM, VVVLI
3.7. Atestuoti įmones, kurių veikla susijusi su saugia laivyba, teikti atestacijos pažymėjimus		3	SM, LSLA
3.8. Teikti informaciją apie išduodamų dokumentų (jūrinio laipsnio diplomų, kvalifikacijos liudijimų, jūrininkų knygelių ir panašiai) autentiškumą		4	SM, LSLA
3.9. Dalyvauti įdiegiant Lietuvos Respublikos ir ES/EEE valstybių narių sveikatos draudimo kompetentingų įstaigų keitimosi duomenimis sistemą naudojant IRT		4	SAM, VLK prie SAM
3.10. Teikti Lietuvos Respublikos geležinkelių riedmenų ir konteinerių registro duomenis internetu pagal registro duomenų teikimo su		4	SM, VGI prie SM
3.11. Sudaryti sąlygas ieškoti informacijos apie dizainą		1	VPB
3.12. Sudaryti sąlygas Sutarčių registro duomenų teikėjams pateikti duomenis registrui elektroniniu būdu		3	TM, CHĮ
3.13. Sudaryti sąlygas Sutarčių registro duome-nų teikėjams pranešimus apie įregistravimą gauti elektroniniu būdu		3	TM, CHĮ
3.14. Sudaryti sąlygas Turto arešto aktų registro duomenų teikėjams turto arešto aktų duomenis registrui pateikti elektroniniu būdu		3	TM, CHĮ
3.15. Sudaryti sąlygas kreditoriams elektroniniu būdu gauti pažymėjimų apie hipotekos, įkeitimo, priverstinės hipotekos, priverstinio įkeitimo įregistravimą (išregistravimą) duomenis		3	TM, CHĮ
3.16. Sudaryti sąlygas stebėti studijų programos arba mokslinių tyrimų ir eksperimentinės plėtros (toliau vadinama – MTEP) produkt		4	SKVC



Priedas Nr. 13

MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR FINANSŲ VALDYMO FAKULTETAS
INFORMATIKOS IR STATISTIKOS KATEDRA

Laba diena, gerbiamas (-oji) respondente. Aš, Mykolo Romerio universiteto magistrantūros studentė, atlieku tyrimą tema "Asmens identifikavimas elektroninėje erdvėje". Jūsų nuomonė šiuo klausimu yra labai svarbi. Jūsų pateikti duomenys bus naudojami tik apibendrinti, todėl anonimiškumas garantuojamas. Atidžiai susipažinkite su kiekvienu klausimu ir pažymėkite (X) ar įrašykite Jūsų nuomonę atitinkantį atsakymą.

Ačiū už dalyvavimą apklausoje.

1. Ar naudojatės elektronine bankininkyste?

Taip	
Ne	

Jei atsakėte „TAIP", pereikite prie 2-ojo klausimo.
Jei atsakėte „Ne", atsakykite į 1a klausimą.

1a. Pažymėkite priežastį kodėl nesinaudojate elektronine bankininkyste:

Nesinaudoju kompiuteriu	
Man to nereikia	
Nežinau kas tai yra	
Kita priežastis	

2. Kokio banko elektroninėmis paslaugomis naudojatės?

Hansabankas	
SEB Vilniaus bankas	
Sampo bankas	
DnB Nord bankas	
Parex bankas	
Ūkio bankas	
Medicinos bankas	

3. Ar pasitikite elektroninės bankininkystės identifikavimo sistema?

1	2	3	4	5
Nepasitikiu				Pasitikiu

4. Įvertintumėte elektroninės bankininkystės sistemos patogumą.

1	2	3	4	5
Nepatogu				Patogu

5. Ar naudojatės viešosiomis elektroninėmis paslaugomis, kurios pasiekiamos elektroninės bankininkystės pagalba?

Taip	
Ne	

6. Ar norėtumėte, kad viešųjų elektroninių paslaugų, pasiekiamų per bankų sistemas, skaičius didėtų?

Taip	
Ne	

7. Ar pakanka informacijos apie teikiamas viešąsias elektronines paslaugas?

Taip	
Ne	

8. Ar reikalingos egzistuojančios viešosios elektroninės paslaugos (VEP)?

Centrinė hipotekos įstaigos teikiamomis VEP	
Gyventojų registro tarnybos teikiamomis VEP	
Informatikos ir ryšių departamento teikiamomis VEP	
Sodros teikiamomis VEP	
Valstybinė ligonių kasos teikiamomis VEP	
Vilniaus miesto savivaldybės administracijos el. paslaugos	

9. Ar žinote, kas yra elektroninis parašas?

Taip	
Ne	

10. Ar naudojatės elektroniniu parašu?

Taip	
Ne	

Jei atsakėte „TAIP",atsakykite į 10a klausimą.
Jei atsakėte „Ne", atsakykite į 10b klausimą.

10a. Kokios įmonės jis išduotas?

UAB Skaitmeninio sertifikavimo centro	
Kitu	

10b. Kodėl nesinaudojate?

Man jo nereikia	
Nesaugu	
Nepraktiska	
Nežinau kas tai yra	

11. Jūsų lytis:

Moteris	
Vyras	

12. Jūsų amžius:

18-25	
26-35	
36-45	
46-55	
56 m. ir vyresni	

13. Jūsų išsilavinimas

Aukštasis	
Nebaigtas aukštasis (studentas)	
Aukštesnysis	
Profesinis	
Vidurinis	

14. Jūsų pareigos:

Aukščiausios grandies vadovas	
Vadovas	
Specialistas	
Tarnautojas	
Darbininkas	

15. Jūsų mėnesinės pajamos:

Iki 1000 Lt	
1001 – 2000 Lt	
2001 – 3000 Lt	
Virš 3001Lt	

Ačiū už Jūsų atsakymus.
Geros dienos