KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Vygintas Šėža

Ribotos sumos elektroninių pinigų cirkuliacijos sistema

Magistro darbas

Darbo vadovas
prof. dr. E. Sakalauskas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Vygintas Šėža

Ribotos sumos elektroninių pinigų cirkuliacijos sistema

Magistro darbas

Recenzentas

doc. dr. J. Čeponis

2010-05-28

Vadovas

prof. dr. E. Sakalauskas

2010-05-28

Atliko

IFN-8/3 gr. stud.
Vygintas Šėža

2010-05-25

Kaunas, 2010

LIMITED AMOUNT ELECTRONIC MONEY CIRCULATION SYSTEM

SUMMARY

Fast developing and growing of e-commerce determined the coming of modern payment systems. Intention of users to pay safely on the internet impacted the decrease of use of traditional payment system such as credit cards. It's started to look for and design alternative ways of payment, such as smart cards systems or systems using software for saving monetary value.

Traditional payment systems currently used by most e-commerce sites are not suitable for high volume, tiny valued transactions. There is a need of payment system that is cost effective, secure and easy to use. The purpose of this work is to propose a model of semi-online electronic money circulation system for small and average payments, which is based on a concept of R. Rivest and A. Shamir created micropayment system called Payword. The proposed model's architecture and protocol are explained in detail. To increase performance of the system there was done a research to find out which hash algorithm and electronic signature algorithm is most suitable for the proposed model.

TURINYS

ĮVADAS

Sparti elektroninės komercijos plėtra ir augimas natūraliai sąlygojo modernių, *online* aplinkai pritaikytų atsiskaitymo, mokėjimo sistemų atsiradimą. Itin svarbu tai, kad technologijų tobulėjimo pasėkoje ne tik eksponentiškai išaugo perduodamos informacijos kiekis, tačiau pakito pačios informacijos prigimtis – ji pati savaime, *per se*, tapo ekonominę vertę turinčiu objektu [7].

Vartotojų noras saugiai atsiskaityti internete įtakojo, kad „online“ aplinkoje mažėja naudojimas tokių tradicinių atsiskaitymo priemonių kaip mokėjimo kortelės. Interneto vartotojai vis rečiau pasitiki šiuo mokėjimo įrankiu, kadangi vartotojai, pateikdami pardavėjui savo mokėjimo kortelės duomenis, susiduria su neteisėta šių duomenų panaudojimo rizika.

Dėl šių tradicinių mokėjimo priemonių trūkumų imta ieškoti ir kurti alternatyvūs atsiskaitymo būdai. Tokias alternatyvas sudaro išmaniųjų kortelių (angl. smart card) sistemos, kurios paremtos piniginės vertės išsaugojimu daugiafunkciniame kortelės luste ir sistemos, naudojančios kompiuteryje įdiegtą programinę įrangą, kurioje saugoma piniginė vertė.

Pagal mokėjimo patvirtinimo būdą atsiskaitymo sistemas galima suskirstyti į tris grupes. Vienose jų mokėjimo patvirtinimas vykdomas prijungties režime (angl. *online*), kitose atjungties režime (angl. *offline*), o trečiose dalinai prijungties režime (angl. *semi-online*). Prijungties režime vykdomo patvirtinimo atveju reikalinga vartotojo (pirkėjo) ir pardavėjo komunikacija su trečiąja šalimi. Šiam tipui priskiriamos Ecash, CyberCash, NetBill sistemos. Atjungties režime vykdomam patvirtinimui komunikavimas vyksta tik tarp vartotojo ir pardavėjo. Tokio tipo techninės įrangos panaudojimu pagrįsta atsiskaitymų sistema yra „Mondex“. Kuomet mokėjimo patvirtinimas atliekamas dalinai prijungties režime, reikalinga tam tikra komunkacija su trečia šalimi, tačiau ne kiekvienam mokėjimui. Viena tokių sistemų yra Milicent. Analizės dalyje pateikiami detalūs minėtų sistemų bruožai.

Šiuo metu naudojamos tradicinės atsiskaitymo sistemos nėra tinkamos dideliam kiekiui mažos vertės transakcijų atlikti. Todėl kai teikiama nedidelės vertės informacija, tokia kaip muzika ar internetiniai straipsniai, tradiciniai elektroniniai atsiskaitymai nėra efektyvūs. Kuomet transakcija vykdoma perduodant nedidelę vertę, toks mokėjimas vadinamas mikromokėjimu. 1996 metais R. Rivest ir A. Shamir pasiūlė mikromokėjimų sistemą Payword, kuri vartotojui internete leidžia pirkti nedidelės vertės prekes.

Šiame darbe pateikiamas siūlomas dalinai prijungties režime veikiančios elektroninių pinigų cirkuliacijos sistemos, skirtos mažiems ir vidutiniams mokėjimams, modelis, besiremiantis sukurta Payword mikromokėjimų sistemos koncepcija.

1. ELEKTRONINIŲ PINIGŲ CIRKULIACIJOS SCHEMŲ ANALIZĖ

1.1. Analizės tikslas

Analizės tikslas yra susipažinti su elektroniniais pinigais, jų savybėmis, išnagrinėti elektroninių pinigų cirkuliacijos schemas (atsiskaitymų sistemas), ištirti jų veikimą, saugioms transakcijos atlikti realizuotus saugumo sprendimus, išanalizuoti elektroninių pinigų paėmimo ir išleidimo protokolus.

1.2. Tyrimo sritis, objektas ir problema

Tyrimo sritis. Tyrimo sritį sudaro elektroninių pinigų cirkuliacijos schemos (atsiskaitymų sistemos), šių schemų teikiamos galimybės ir saugumo sprendimai.

Tyrimo objektas. Tyrimo objektas – elektroninių pinigų cirkuliacijos schema.

Tyrimo problema. Elektroninių pinigų cirkuliacijos schemos atlieka elektroninės vertės transakcijas. Turi būti užtikrintas išduodamų e. pinigų vientisumas, įvertinti galimi saugumo mechanizmai, apsaugantys nuo dvigubo e. pinigų išleidimo, klastojimo, atlikta vartotojų autentifikacija, panaudojant elektroninius parašus. Parenkant saugumo mechanizmus kartu turi būti atsižvelgta ir į algoritmo našumą, t.y. įvertintas saugumo ir našumo santykis.

1.3. Darbo tikslas

Darbo tikslas yra išanalizuoti elektroninių pinigų cirkuliacijos schemas bei jose realizuotus elektroninių pinigų paėmimo, išleidimo protokolus ir pasiūlyti saugų elektroninių pinigų cirkuliacijos sistemos modelį bei protokolą. Siūlomame modelyje efektyvumo užtikrinimui panaudoti didelių skaičiavimų nereikalaujančius sprendimus.

Darbo tyrime atlikti .NET karkase esančių maišos algoritmų ir elektroninio parašo algoritmų našumo bandymus bei pagal gautus rezultatus parinkti tinkamus saugumo ir našumo atžvilgiu.

1.4. Elektroniniai pinigai

E. pinigu vadinsime vartotojui banko išduotą e. dokumentą, kuriame nurodytas e. pinigo numeris, nominalas ir kuris pasirašytas banko parašu [3]. Pinigų institucijų Europos direktyva elektroninius pinigus apibrėžia kaip piniginę vertę, pareikštą emitento, kuri yra [6]:

- saugoma elektroniniame įrenginyje
- išleista gavus lėšas, kurios savo verte yra ne mažesnės nei išleista piniginė vertė

– pripažinta kaip mokėjimo priemonė

Elektroniniai pinigai skirstomi į du skirtingus tipus: identifikuoti e. pinigai ir anoniminiai e. pinigai. Identifikuoti e. pinigai turi informaciją atskleidžiančią asmens, kuris išėmė pinigus iš banko, tapatybę. Taip pat identifikuoti e. pinigai leidžia bankui atsekti pinigų judėjimą ekonomikoje. Anoniminiai e. pinigai veikia taip pat kaip tikri popieriniai pinigai. Vos tik e. pinigai išimami iš sąskaitos, jie gali būti išleisti ar perduoti nepaliekant transakcijos pėdsako. Anoniminiai e. pinigai sukuriami naudojant aklus e. parašus (angl. *blind signatures*).

Taip pat apibrėžiamos dvi rūšys kiekvienam iš e. pinigų tipų: prijungties režimo (angl. *online*) e. pinigai ir atjungties režimo (angl. *offline*) e. pinigai. Prijungties režimas reiškia, kad reikia bendrauti su banku (per modemą ar tinklą) tvarkant transakcijas su banku arba trečiąja šalimi. Atjungties režime transakcijas galima tvarkyti be tiesioginio banko įsikišimo. Anoniminiai atjungties režime veikiantys e. pinigai yra sudėtingiausia e. pinigų forma, nes atsiranda dvigubo pinigų išleidimo problema [5].

Pinigų modeliai apibūdina vertės apsikeitimo priemones mokėjimo transakcijos metu. Galimi tokie pinigų modeliai [10]:

– Monetos modelis. Apsikeitimo priemonė pažymi suteiktą vertę kaip tradiciniuose piniguose. Monetos pačios turi vertę arba jų vertė paremta pasitikint jas išleidusiais subjektais. Monetos nepalaiko skolos. Skaitmeninių monetų sistemos, turinčios fiksuotos reikšmės monetas susiduria su problema kaip atiduoti grąža, jei vartotojas neturi tiksliai kainai sumokėti reikalingų monetų.
– Notacinis (ženklų) modelis. Vertė yra saugoma ir keičiama pagal įgaliojimus kaip banko sąskaitoje. Bankas prižiūri sąskaitoje esančią sumą. Notacinės sistemos palaiko skolą, kai yra leidžiami neigiami balansai. Apsikeitimai paremti pinigų nurašymu nuo mokėtojo sąskaitos ir įrašymu į gavėjo sąskaitą.

Elektroniniams pinigams keliami reikalavimai [1]:

– Nesuklastojami. Turi būti sudėtinga sukurti daugiau pinigų nei teisėtai gauta pradžioje
– Efektyviai patikrinami juos naudojant atjungties (angl. *offline*) režime. E. pinigai turi būti patikrinami kiekvienam, kuris naudoja verifikavimo įrankį, geriau be banko komunikacijos.
– Anoniminiai. Panaudojus pinigus pirkimui ar sugrąžinus į banką, turi būti sunku nusakyti, kas juos iš pradžių paėmė.
– Perduodami. Turi būti leidžiama perduoti iš vieno dalyvio kitam.

1 lentelėje pateikti elektroninių pinigų privalumai ir trūkumai [4].

1 lentelė. Elektroninių pinigų privalumai ir trūkumai

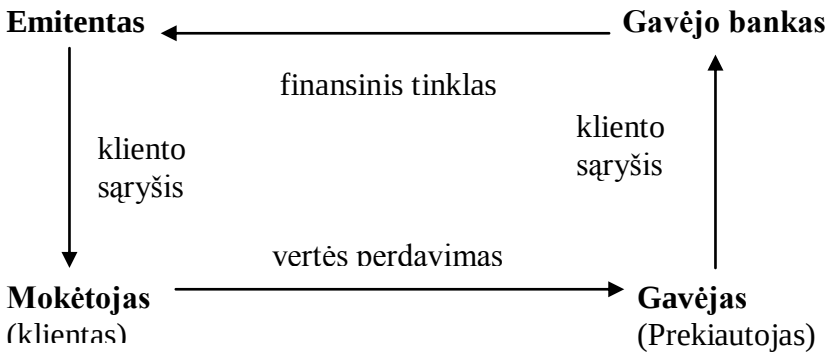
Privalumai	**Trūkumai**
PIN apsauga	E. pinigų naudojimas reikalauja tam tikros programinės įrangos
Pigesnė priežiūra	E. pinigų vartotojai negali aptikti sukčiavimo
Elektroniniai pinigai yra švarūs (angl. *clean*)	Sukčiavimas gali sukelti sisteminę riziką
Elektroniniai pinigai gali būti perduoti per tinklus (pvz.: internetas)	Brangus saugumas ir anonimiškumo konfliktai
Galimas bekontaktis mokėjimas	E. pinigai netinkami kaupimui
Galimas papildymas per telefoną, internetą	
Programiškumas	

Kaip matome, e. pinigai turi nemažai privalumų lyginant su trūkumais, iš kurių saugumu susijusius atvejus galima būtų eliminuoti naudojant patikimus ir pripažintus saugos mechanizmus, tokius kaip šifravimas, autentifikavimas, e. parašai.

1.5. Elektroninių pinigų cirkuliacijos schemų savybės

Elektronine atsiskaitymo sistema (e. pinigų cirkuliacijos schema) vadiname sistemą, kuri tenkina sekančius apribojimus: sistema iššaukia monetarinės vertės perdavimą tinklais iš pirkėjo prekiautojui, leidžia pirkėjams sumokėti prekiautojams be jokių verslo santykių tarp jų, susilpnina abipusį pasitikėjimo lygį, reikalingą tarp skirtingų šalių, reguliuodama, apsaugodama ir inkapsuliuodama atsiskaitymo procesą bei duomenis, taip pat pateikdama pakankamus įrodymus, kad įvykdyta atsiskaitymo transakcija. Prekiautojams sistema pilnai automatizuotai apdoroja atsiskaitymo transakcijas, o pirkėjams leidžia pasiruošti ir atlikti atsiskaitymus esant prijungties režime efektyviai ir saugiai [10].

Elektroninių atsiskaitymų sistemos tikslas perduoti monetarinę vertę iš mokėtojo gavėjui. Pagrindinė elektroninių atsiskaitymų įvykių seka ir pagrindiniai jos dalyviai parodyti 1 pav.:



1 pav. Pagrindinė elektroninių atsiskaitymų įvykių seka

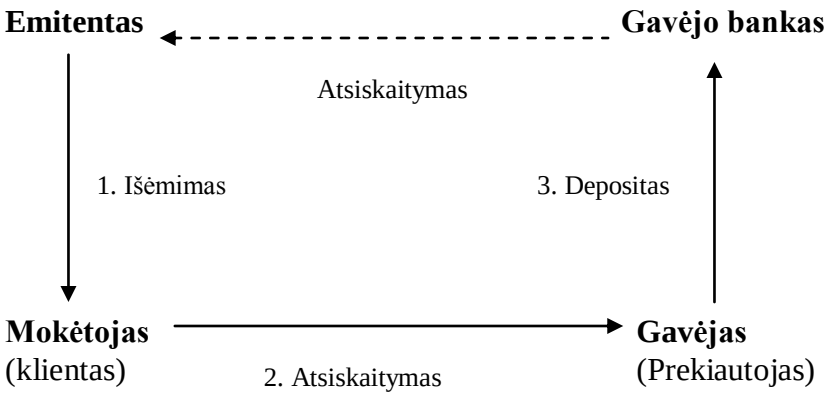
Sistemos dalyviai:

- Mokėtojas, kuris atlieka mokėjimą. Tai dažniausiai būna yra klientas arba pirkėjas.
- Gavėjas, kuris gauna mokėjimą. Tai dažniausiai būna prekiautojas arba pardavėjas.
- Emitentas - trečioji šalis (angl. *third party*) , kuri bendrauja su mokėtoju ir banku.
- Gavėjo bankas - trečioji šalis, kuri bendrauja su gavėju (prekiautoju).

1.5.1. Elektroninių pinigų cirkuliacijos schemų modeliai

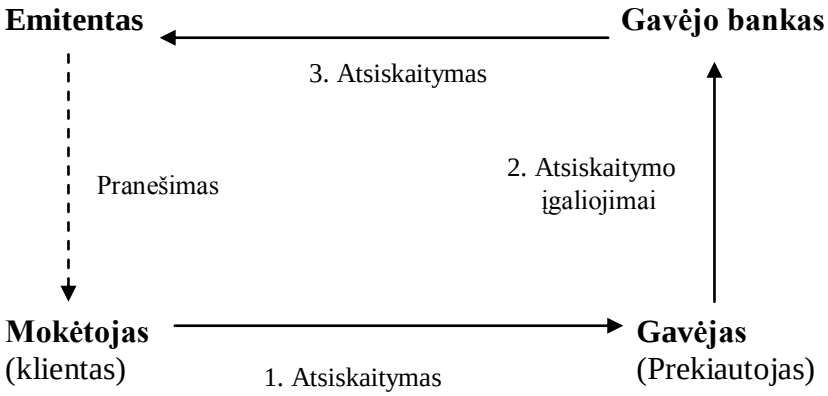
Atsiskaitymų (cirkuliacijos schemų) modeliai klasifikuoja elektroninių atsiskaitymų sistemas pagal informacijos srautus tarp elektroninės transakcijos dalyvių. Pagrindinis skirtumas yra tiesioginio bendravimo tarp mokėtojo ir gavėjo būvimas arba nebūvimas. Netiesioginio bendravimo atveju atsiskaitymas siejasi tik atsiskaitymo iniciatoriumi, kuris gali būti mokėtojas arba gavėjas, ir emitentu ir gavėjo banku. Netiesioginio atsiskaitymo sistemomis elektroninių atsiskaitymų naudojant internetą kontekste dažniausiai yra laikoma namų bankininkystės dalis. Kitas atvejis yra kuomet, kai monetarinė vertė yra paimama iš mokėtojo (pvz. išankstinio mokėjimo sistemos). Išankstinio mokėjimo sistemos dažniausiai žinomos kaip grynųjų tipo (angl. *cash-like*), o vėlesnio apmokėjimo (angl. *post-paid*) dažniausiai įvardijamos kaip sąskaita paremtos (angl. *account-based*).

Apžvelgsime keletą esamų elektroninių atsiskaitymų modelių. Vienas iš jų yra tiesioginiais pinigais paremto atsiskaitymų modelio (angl. *direct cash like*) sistemose mokėtojas paima pinigus iš emitento nusiunčia gavėjui, kuris padeda mokėjimą į banką. Toks būdas pavaizduotas 2 pav. Šio tipo sistemos naudoja monetos tipo pinigų modelį. Tokios atsiskaitymo sistemos dažniausiai apima klastojimui atsparią techninę įrangą kaip intelektualiosios kortelės (angl. *smart card*) arba emitento prijungties režimu atliekamą patvirtinimą (pvz. Ecash sistema) tam, kad būtų apsisaugota nuo pakartotinio elektroninių pinigų išleidimo (angl. *double spending*), nes e. pinigus lengva kopijuoti kaip įprastas bylas.



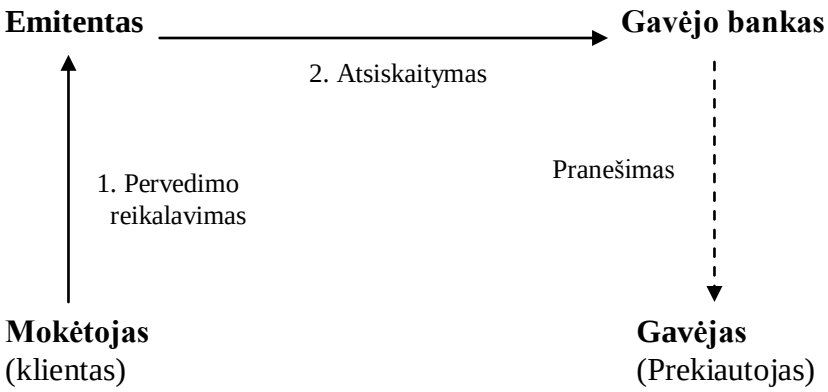
2 pav. Tiesioginiais pinigais paremtas atsiskaitymų modelis

Tiesiogine sąskaita (angl. *account based*) paremto atsiskaitymų modelio sistemos panašios į tradicines čekių sistemas. Jos mokėtojui leidžia perduoti atsiskaitymo įgaliojimus gavėjui, kuris pateikia šiuos įgaliojimus savo bankui ir šis įvykdo apmokėjimą iš emitento. Tuomet emitentas duoda ženklą apie įvykdytą atsiskaitymą. Tokio tipo modelis pateiktas 3 pav.:



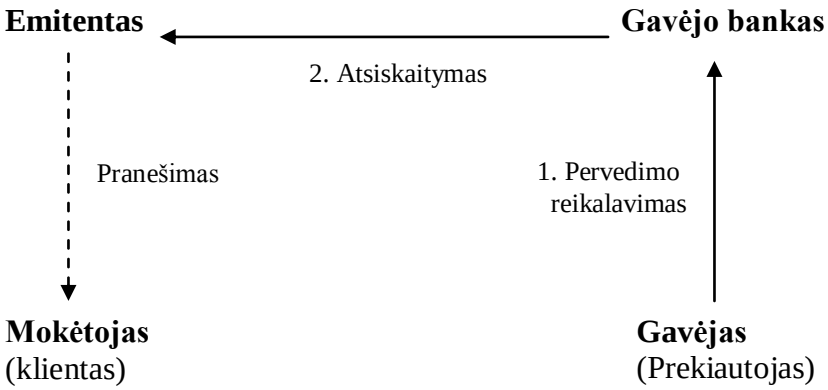
3 pav. Tiesiogine sąskaita paremtas atsiskaitymų modelis

Netiesioginiu spaudimu (angl. *indirect push*) paremtas atsiskaitymų modelis, kuris pavaizduotas 4 pav., grindžiamas tuo, kad mokėtojas duoda nurodymas emitentui perversti lėšas gavėjui į gavėjo banko sąskaitą. Šis modelis yra panašus į tradicinius bankų pervedimus. Gavėjas yra informuojamas apie gaunamą atsiskaitymą.



4 pav. Netiesioginiu spaudimu paremtas atsiskaitymų modelis

Netiesioginiu pareikalavimu (angl. *indirect pull*) paremtame atsiskaitymų modelyje (5 pav.) gavėjas duoda nurodymus savo bankui atlikti pervedimą iš mokėtojo banko. Mokėtojas informuojamas apie vykdomą atsiskaitymą.



5 pav. Netiesioginiu pareikalavimu paremtas atsiskaitymų modelis

Aptarti elektroninių atsiskaitymų modeliai demonstruoja galimas e. pinigų cirkuliacijas tarp transakcijose dalyvaujančių pusių. Kaip matome, galimi ne tik tradiciniai paplitę atsiskaitymo variantai.

1.5.2. Saugumo mechanizmai

Individualių atsiskaitymo sistemų (e. pinigų cirkuliacijos schemų) saugumo mechanizmai priklauso nuo ypatybių, kurias reikia suteikti, ir sudaromų pasitikėjimo prielaidų. Pagrindiniai atsiskaitymo sistemų saugumo reikalavimai yra vientisumas, autorizacija, konfidencialumas, tinkamumas ir patikimumas. Bet kurios atsiskaitymo sistemos protokolas turėtų būti žinomas

viešai auditorijai ir atsiskaitymo sistemos saugumas turėtų nepriklausyti nuo jos naudojamo protokolo slaptumo. Atsiskaitymo sistemos integralumas apibrėžia, kad tik autorizuoti mokėjimai gali būti vykdomi. Joks vartotojas negali prarasti pinigų be to vartotojo autorizacijos. Žinutės autentifikacija suteikia gavėjui jos kilmės identifikaciją. Atsiskaitymo autorizavimas gali būti pasiektas skirtingais būdais.

Šiuo metu yra nemažai kriptografinių metodų, skirtų saugiam informacijos perdavimui ir sistemos dalyvių tapatumams patikrinti. Toliau aptarsime patikimus ir dažnai naudojamus metodus.

Autorizacija per išorinį ryšį (angl. *out-band*) reiškia, kad verifikuojanti pusė, dažniausiai bankas, siunčia pranešimą gavėjui ir reikalauja , kad šis patvirtintų arba paneigtų atsiskaitymą naudojant saugų išorinio ryšio kanalą, pavyzdžiui elektroninį paštą ar telefoną. Tokį būdą naudoja tokios sistemos kaip First Virtual ar PayPal [10].

Padalinto (angl. *shared*) rakto kriptografijoje verifikuojanti šalis reikalauja, kad kiekvienoje mokėjimo žinutėje būtų pasidalinta paslaptimi, kuri būtų žinoma tik autorizuojančiai ir verifikuojančiai pusėms (pvz. PIN kodas). Gauta žinutė autentifikuojama patikrinant kriptografinę reikšmę taip vadinamą žinutes autentifikavimo kodą (MAC). Taip pašalinama nepripažinimo problema, kadangi paslaptį žino tik verifikuojanti ir autorizuojanti pusės.

Šalies patikrinimui galima naudoti ir skaitmeninį parašą, kurio iš autorizuojančios šalies reikalauja verifikuojanti pusė. Tam naudojama žinutės santrauka ir viešojo rakto kriptografija. Viešojo rakto kriptografijoje kiekviena pusė turi savo raktų poras. Elektroninio parašo raktas yra laikomas paslaptyje. Viešas raktas yra visiems žinomas ir susietas su sertifikatu, kuris surištas su savininko tapatybe. Sertifikatai yra pasirašyti patikimos šalies (sertifikatų centro).

Kai kuriais atvejais galima naudoti dvigubą parašą tam, kad sujungti du pranešimus, skirtus dviem skirtingiem gavėjams. Toks atvejis yra realizuotas SET saugos specifikacijoje. Pavyzdžiui, jei norima nusiųsti informaciją apie ketinamą įsigyti prekę pardavėjui ir mokėjimo informaciją bankui, pardavėjui nereikia žinoti pirkėjo kreditinės kortelės numerio, o bankui nereikia žinoti pirkėjo perkamų prekių sąrašo. Todėl pirkėjas, laikydamas šiuos du dalykus atskirai, tarytum turi papildomą privatumo apsaugą. Tačiau šie du dalykai turi būti sujungti tokiu ryšiu, kad kilusį ginčą būtų galima išspręsti remiantis turima informacija. Ryšys turi būti toks, kad pirkėjas galėtų įrodyti, jog konkretus mokėjimas yra skirtas konkrečiai pardavėjo sąskaitai, o ne kokioms nors kitoms prekėms ar paslaugoms [12].

Aklo parašo (angl. *blind signature*) technika gali būti naudojama pasiekti visišką neatsekamumą. Ši technika leidžia emitentui autorizuoti elektroninio atsiskaitymo monetas, sukurtas mokėtojo, be galimybės perskaityti monetos serijinį numerį, kuris buvo sugeneruotas mokėtojo.

Aklojo e. parašo esmė:

- Vartotojas parengia reikalavimą e. pinigui gauti ir taip jį užmaskuoja, kad niekas kitas negalėtų sužinoti reikalaujamo e. pinigo nominalo.
- Bankas pasirašo užmaskuotą e. pinigo reikalavimą, o tuo pačiu ir e. pinigą.
- Vartotojas demaskuoja banko pasirašytą e. pinigą, tačiau išsaugo autentišką banko parašą ant e. pinigo nominalo [3].

Patvirtinimas (angl. *validation*). Tai metodas, kuris užtikrina ryšį tarp tikros vertės perdavimo ir elektroninio mokėjimo [10]. Patvirtinimo metodas priklauso nuo mokėjimo protokolo. E. monetų sistemose (pvz. Ecash) patvirtinimas susideda iš pakartotinio e. pinigo išleidimo patikrinimo, o saugaus kreditinės kortelės duomenų pateikimo atveju tikrinamas turimas kreditas (pvz. CyberCash). Patvirtinimas gali būti vykdomas prijungties režime (angl. *online*), atjungties režime (angl. *offline*) ir dalinai prijungties režime (angl. *semi-online*).

Prijungties režime vykdomo patvirtinimo atveju reikalinga vartotojo (pirkėjo) ir pardavėjo komunikacija su trečiąja šalimi. Šio tipo mokėjimuose vartotojas ir pardavėjas yra tiesiogiai sujungti su trečia šalimi (emitentu ir/arba gavėju), kuri patvirtina mokėjimą, todėl gavėjas yra garantuotas, kad gaus atitinkamą apmokėjimą.

Atjungties režime vykdomam patvirtinimui komunikavimas vyksta tik tarp vartotojo ir pardavėjo. Daugelyje elektroninių mokėjimo sistemų patvirtinimą užtikrina klastojimui atspari techninė įranga kaip intelektualiosios kortelės (angl. *smartcard*) ar elektroninės piniginės (angl. *e-wallet*).

Kuomet mokėjimo patvirtinimas atliekamas dalinai prijungties režime, reikalinga tam tikra komunkacija su trečia šalimi, tačiau ne kiekvienam mokėjimui. Kai kurioms dalinai prijungties režime veikiančioms mokėjimo schemoms (pvz. MiliCent) reikalinga, kad tik pradinis mokėjimas būtų vykdomas prijungties režime, o sekančios transakcijos vyksta tik tarp vartotojo ir pardavėjo.

1.6. Elektroninių pinigų cirkuliacijos schemoms keliami reikalavimai

Šioje dalyje aptarsime elektroninių atsiskaitymų sistemoms (e. pinigų cirkuliacijos schemoms) keliamus reikalavimus. Individualių charakteristikų svarbą nulemia vartotojų

poreikiai. Pavyzdžiui, vienas vartotojas atliekant transakciją gali norėti likti anonimiškas, kitas galbūt tai visai nekelia anonimiškumo reikalavimų.

1.6.1 Transakcijos reikalavimai

Elektroniniai atsiskaitymai (e. pinigų cirkuliacijos schemos) turi tenkinti tam tikras žemiau apibrėžtas sąlygas. Viena iš transakcijos reikalavimų yra nedalumas (angl. *atomicity*). Tai reiškia, kad transakcija turi įvykti pilnai arba visai neįvykti.

Nuoseklumo reikalavimas nusako, kad visos šalys turi būti suinteresuotos transakcijos įvykdymu. Šalys turi sutikti dėl pervedamos sumos, pervedimo priežasties ir dėl paties pervedimo įvykdymo.

Transakcijų atskyrimo reikalavimas teigia, kad operacijos turi būti nepriklausomos viena nuo kitos.

Tenkinant patvarumo reikalavimą turi būti visada įmanoma atstatyti paskutinę stabilią būseną. Net ir po sistemos griūties ši būsena turėtų būti grąžinama, taip pat operacijos galiojusios prieš tai (pvz. turima pinigų suma) [10].

1.6.2. Saugumo reikalavimai

Elektroninių atsiskaitymų sistemos (e. pinigų cirkuliacijos schemos) turėtų atkreipti dėmesį į saugumo klausimus, tokius kaip apsauga nuo sukčiavimo, konfidencialumas, kurie užtikrintų pasitikėjimą sistema. Taip pat vartotojai, leisdami e. pinigus, dažnai reikalauja anonimiškumo [10].

Atsižvelgiant apsaugos nuo sukčiavimo klausimą, elektroninių atsiskaitymų sistemos turėtų būti atsparios sukčiavimui ir atakoms. Reikia numatyti prevencijas neteisėtam e. pinigo panaudojimui arba realizuoti tokio atvejo aptikimo priemones. Apsaugos nuo sukčiavimo trūkumas gali įtakoti pasitikėjimo elektroninio atsiskaitymo sistema praradimą. Pagrindinės atakos, nuo kurių derėtų saugotis pavyzdžiui yra atsiskaitymo pranešimų nepripažinimas, kartojimas, modifikavimas, taip pat paslaugos atmetimas (angl. *denial of service*).

Gana svarbus klausimas į kurį reiktų atkreipti dėmesį yra pakartotinio išleidimo (angl. *double spending*) prevencija. E. pinigas yra elektroninių skaitmenų eilutė [13], todėl ji gali būti nesunkiai nukopijuota ir e. pinigas pakartotinai išleistas. Ši problema liečia ne tik vartotojus, kurie gali panaudoti tą patį e. pinigą keliems pirkimams, bet ir prekiautojus, kurie gali bandyti pateikti e. pinigą išpirkimui keletą kartų.

Dar vienas saugumą liečiantis klausimas yra e. pinigų klastojimo prevencija. Turi būti nesunku atskirti legalius e. pinigus nuo neautorizuotų nelegalių e. pinigų.

E. pinigų išeikvojimas (angl. *overspending*) yra dar vienas sukčiavimo variantas, kuriam būtina prevencija. Toks variantas pasitaiko sąskaita paremtose sistemose.

Nepaneigiamumo reikalavimas pasižymi tuo, kad dalyvaujančioms šalims turi būti leista patikrinti, ar atsiskaitymo operacija buvo įvykdyta ir kokie buvo operacijos duomenys ir suma.

Privatumo kontrolė leidžia klientams pinigų išleidimo įpročius išlaikyti paslaptyje. Dažnai pirkėjai vertina, kad prekiautojai ir kartais netgi bankai negalėtų sekti ir stebėti jų išlaidų [10]. Operacijos elementus sudaro suma, data, laikas, vieta, prekė, pirkėjo ir prekiautojo tapatybės. Informacija gali būti lengvai sekama, arba stebima esant tam tikroms sąlygoms, arba visiškai paslėpta.

Informacijos konfidencialumas yra labai svarbus vartotojams, kurie, naudodami elektroninio atsiskaitymo sistemą, pageidauja vykdyti komercinę veiklą konfidencialiai. Šifruojant duomenis tarp pirkėjo ir prekiautojo atsiskaitymo sistemos užtikrina duomenų neatsekamumą trečioms šalims.

Anonimiškumas užtikrina e. pinigo vartotojo tapatybės apsaugą. Kuomet vartotojo tapatybė yra paslėpta, operaciją galima vadinti anonimiška [10]. Pavyzdžiui, CyberCash sistemoje anonimiškumą galima užtikrinti vietoje tikros tapatybės naudojant pseudonimus, kurie paslepia pirkėjo tapatybę nuo prekiautojo.

Kai du skirtingi to paties pirkėjo atsiskaitymai negali būti susieti, sakoma, kad operacija yra ne tik anonimiška, bet ir neatsekama [10]. Pavyzdžiui, Ecash sistemoje yra naudojami akli parašai (angl. *blind signatures*), kurie užtikrina anonimiškumą ir neatsekamumą.

Apibendrinant aptartus saugumo reikalavimus galima teigti, kad jie yra labai svarbūs atliekant operacijas su e. pinigais ir elektroninės atsiskaitymo sistemos turėtų numatyti minėtus aktualius saugumo įgyvendinimo klausimus ir jų laikytis.

1.7. Mokėjimo schemų palyginamoji analizė

Pasaulinėje rinkoje egzistuoja daug įvairaus tipo elektroninių atsiskaitymo sistemų. Vienos jų liko tik pasiūlymų ar prototipų lygmenyje (pvz. ACC, Brands Cash, iKP), kitos įgijo didelį vartotojų ratą ir yra sėkmingai veikiančios (pvz. PayPal).

1.7.1. CyberCash

CyberCash yra transakcijų sistema, paremta saugiais kreditinės kortelės mokėjimais. Ji naudojasi egzistuojančiais elektroninių atsiskaitymo sistemų privalumais, integruoja prekiautojo pusės programinę įrangą, tarsi tai būtų fizinis POS terminalas, su CyberCash serveriais, kurie veikia kaip tinklo sąsaja tarp prekiautojo internete ir bankų saugių finansinių tinklų. Transakcija gali būti aprašyta tokiais žingsniais[2]:

1. Pirkėjas, atlikęs užsakymą pas pardavėją, gauna sąskaitą (angl. *invoice*).
2. Pirkėjas panaudoja CyberCash piniginę atsiskaitymui, kuri sugeneruoja užšifruotą atsiskaitymą ir nusiunčia pardavėjui.
3. Pardavėjas pasiima užsakymą iš paketo, pasirašo mokėjimo informaciją skaitmeniniu parašu ir siunčia ją į CyberCash serverį
4. CyberCash serveris atjungties režime naudodamas tam tikrą techninę įrangą dešifruoja transakciją, performuoja žinutę ir persiunčia ją pardavėjo bankui.
5. Pardavėjo bankas persiunčia transakciją pirkėjo bankui, kuris siunčia patvirtinimą arba atmetimą atgal pardavėjo bankui.
6. Šis atsakymas siunčiamas atgal CyberCash serveriui.
7. Tuomet CyberCash siunčia patvirtinimą arba atmetimą pardavėjui.

1, 2, 3 ir 7 žingsniai vyksta internete ir naudojama viešo rakto ir simetrinio rakto kriptografija, pasitelkiant naudoja 1024 bitų RSA ir 56 bitų DES šifravimą. 4, 6 žingsniai vykdomi per tam skirtas linijas, o 5 žingsnis egzistuojančiuose finansiniuose tinkluose.

2 lentelė. CyberCash sistemai būdingi požymiai

Atsiskaitymo modelis	Saugus kortelės duomenų pateikimas
Patvirtinimas (angl. validation)	Prijungties režime (angl. online)
Privatumo kontrolė	Pirkėjai naudoja pseudonimus, CyberCash gali perskaityti kreditinės kortelės informaciją, pardavėjas negali. Bankas gali atsekti visas operacijas
Saugumo mechanizmai	RSA ir DES šifravimas, parašai, MAC
Apsauga nuo pakartotinio išleidimo	Nėra duomenų
Apsauga nuo klastojimo	Ne
Apsauga nuo išeikvojimo	Taip, autorizacija prijungties režime
Apsauga nuo nepaneigiamumo	Ne, bet pardavėjo autentifikacija
Anonimiškumas	Dalinis
Atsekamumas	Taip

CyberCash buvo ankstyvasis rinkos lyderis, tačiau kaip ir daugelis pirmųjų elektroninių grynųjų pinigų produktų neatsilaikė prieš laiko išbandymus [8].

1.7.2. Ecash

Ecash yra anoniminė, neatsekama, teikianti e. monetas prijungties režimu elektroninių atsiskaitymų sistema, kurią sukūrė DigiCash kompanija. Ecash sistemos veikimas yra paremtas programine įranga. Vartotojui reikalinga grafinės vartotojo sąsajos principu veikianti e. piniginė. Pardavėjams skirta atitinkama komandinės eilutės veikimu paremta e. piniginė. Ecash sistema leidžia abipusius atsiskaitymus. Tiek pirkėjas, tiek pardavėjas gali teikti ir gauti atsiskaitymus. Pirkėjai gali konvertuoti pinigus iš savo sąskaitos į e. monetas, laikomas personaliniame kompiuteryje e. piniginėje [10].

Ecash sistema veikia tokiu toliau aprašytu principu. Vartotojas prisijungia prie emitento leidžiančio e. pinigus ir nusiperka iš jo kažkokios vertės e. pinigų. Šie e. pinigai yra parsiunčiami į vartotojo kompiuterį. Jie gali būti padaromi anonimiškais panaudojant aklojo parašo kriptografinę techniką. Vartotojas gali išleisti nusipirktus e. pinigus tiesiog tinklu persiųsdamas juos pardavėjui. Pardavėjas turi pateikti gautus e. pinigus emitentui patvirtinti. Šiame etape galima aptikti pakartotinį e. pinigo išleidimą: Digicash serveris turi visų išleistų e. pinigų sąrašą duomenų bazėje. Kiekviena operacija yra tikrinama naudojant šį sąrašą ir jeigu e. pinigas jau buvo išleistas, tai bus aptikta [2].

3 lentelė. Ecash sistemai būdingi požymiai

Atsiskaitymo modelis	Tiesioginiais pinigais paremtas modelis
Patvirtinimas (angl. validation)	Prijungties režime
Privatumo kontrolė	Konfidencialumas, anonimiškumas, neatsekamumas
Saugumo mechanizmai	RSA ir DES šifravimas, aklas parašas, pakartotinio pinigų išleidimo sauga prijungties režime
Apsauga nuo pakartotinio išleidimo	Taip
Apsauga nuo klastojimo	Nėra duomenų
Apsauga nuo išeikvojimo	Nėra duomenų
Apsauga nuo nepaneigiamumo	Nėra duomenų
Anonimiškumas	Taip
Atsekamumas	Ne

Ecash sistema kaip ir CyberCash neįgijo pakankamai vartotojų ir netapo populiari, todėl 1998 metais bankrutavo [10].

1.7.3. First Virtual

First Virtual yra internetinio mokėjimo sistema, kuri naudojasi egzistuojančių elektroninio pašto protokolų teikiamais privalumais apsikeičiant pranešimais tarp pardavėjo ir First Virtual bei First Virtual ir pirkėjo. Tai sumažina specialios programinės įrangos ir protokolų poreikį bei leidžia įgyvendinti sistemą kartu su esančia interneto infrastruktūra [8].

Sistema operacijų metu pirkėjui siūlo anonimiškumą ir jokia asmeninė bankinė informacija nėra siunčiama internetu. Vietoje to naudojama taip vadinama VirtualPIN sistema, kuomet tiek pirkėjas, tiek pardavėjas užsiregistruoja First Virtual sistemoje ir kiekvienam jų yra priskiriama unikalus PIN, kuris naudojamas tapatybei nustatyti vykdomų operacijų metu. Pagrindinė VirtualPIN savybė yra ta, kad negali būti jokių ryšių tarp PIN ir „realaus pasaulio“ finansinių įrankių.

Kiekviena First Virtual sąskaita turi sekančias charakteristikas:

- Susijusį elektroninio pašto adresą.
- Būseną (aktyvi, tik pardavėjas, sustabdyta, negaliojanti).
- Susijusią realią sąskaitą (galimas lėšų pervedimas tarp realios ir First Virtual sąskaitų).
- Iš anksto nustatytą valiutą.

Tipinė First Virtual transakcija yra pasirašyta slapyvardžiu, atsekama, veikianti prijungties režime ir vykdoma tokiais žingsniais [10]:

1. Pirkėjas inicijuoja pirkimą įvesdamas VirtualPIN detales į pardavėjo užsakymo formą.
2. Pardavėjas e. paštu nusiunčia pirkėjo VirtualPIN, savo VirtualPIN ir atitinkama pirkimo aprašymą į First Virtual.
3. First Virtual automatiškai e. paštu siunčia pirkėjui klausdamas patvirtinimo.
4. Pirkėjas atsako „Taip“ kaip patvirtinimą First Virtual.
5. First Virtual naudoja esamus saugius finansinius tinklus operacijai įvykdyti.
6. Esant pavykusiai operacijai pardavėjui yra siunčiamas autorizacijos numeris.

4 lentelė. First Virtual sistemai būdingi požymiai

Atsiskaitymo modelis	Kreditinės kortelės atsiskaitymo tarpininkavimas
Patvirtinimas (angl. validation)	Prijungties režime
Privatumo kontrolė	Pseudonimai
Saugumo mechanizmai	Sauga per išorinį ryšį. Pirkėjo teiravimasis e. paštu dėl kiekvieno pirkimo patvirtinimo. VirtualPIN vietoje

	kreditinės kortelės numerio
Apsauga nuo pakartotinio išleidimo	Nėra duomenų
Apsauga nuo klastojimo	Dalinė
Apsauga nuo išeikvojimo	Nėra duomenų
Apsauga nuo nepaneigiamumo	Nėra duomenų
Anonimiškumas	Dalinis
Atsekamumas	Taip

1.7.4. Mondex

Elektroninių atsiskaitymų sistema Mondex paremta techninės įrangos panaudojimu. Čia lėšos yra laikomos intelektualioje kortelėje (angl. *smart card*) ir sandoriai yra sudaromi ir įvykdomi tiesiogiai tarp šalių, apie sandorį nepranešant centriniam kompiuteriui. Saugumo ir praktiškumo sumetimais, ant kiekvienos tokios intelektualios kortelės yra tam tikros juostelės/pėdsakai, kurie gali būti atsekti kilus ginčams, ištaisyti nepavykusį sandorį, arba jeigu to reikalauja įstatymai. Normaliuose sandoriuose, visgi, individo privatumas yra ginamas, nes mažmenininkas neturi priėjimo prie banko informacijos, kuri asmens vardą susieja su *Mondex* kortelės numeriu [7].

Mondex sistema yra neanoniminė ir veikianti atjungties režime. Ja naudotis pirkėjui reikia turėti Mondex intelektualiąją kortelę. Mondex vartotojas gali atsiskaityti su pardavėju, kuris turi Mondex terminalą. Terminalas naudojamas pinigų persiuntimui iš pirkėjo Mondex kortelės į pardavėjo Mondex kortelę.

Mondex sistemoje nėra reikalinga autentifikacija, tačiau kortelę galima užrakinti naudojant MAC. Mondex kortelė registruoja visas operacijas. Ji saugo unikalią 16 skaitmenų pirkėjo identifikaciją, užregistruotą banke, kuriame saugoma asmeninė pirkėjo informacija.

5 lentelė. Mondex sistemai būdingi požymiai

Atsiskaitymo modelis	Tiesioginiais pinigais paremtas modelis, intelektuali kortelė
Patvirtinimas (angl. validation)	Atjungties režime
Privatumo kontrolė	Nėra duomenų
Saugumo mechanizmai	Intelektualios kortelės, parašai, MAC
Apsauga nuo pakartotinio išleidimo	Taip, užtikrina intelektuali kortelė
Apsauga nuo klastojimo	Taip
Apsauga nuo išeikvojimo	Nėra duomenų
Apsauga nuo nepaneigiamumo	Taip
Anonimiškumas	Ne, informacija saugoma banke
Atsekamumas	Taip

1.7.5. PayPal

PayPal yra iki šiol sėkmingai veikianti elektroninių atsiskaitymų sistema, kuri savo veikimo principu yra panaši į First Virtual. PayPal sistema, kaip finansinių atsiskaitymų brokeris, leidžia siųsti pinigus vienas kito elektroninio pašto adresais. Jokia kita šalis nemato kredito kortelės ar banko informacijos.

PayPal veikia kaip pinigų tarpininkas. Pinigai į PayPal sąskaitą gali būti pervesti iš banko sąskaitos arba iš kreditinės kortelės. Norint pervesti pinigus PayPal gavėjas gali prašyti tai padaryti PayPal, prieš tai sukūrus PayPal sistemoje sąskaitą arba atlikti pervedimą į banko sąskaitą.

Atsiskaitant už pirkimą galima leisti Paypal sistemai paimti pinigus iš kreditinės kortelės ar banko sąskaitos net ir neturint pinigų PayPal sąskaitoje. PayPal sistema nusius apmokėjimą pardavėjui ir tuomet paims pinigus iš pirkėjo sąskaitos. Kitas variantas yra pervesti pinigus į PayPal sąskaita ir juos ten palikti. Tuomet atsiskaitant pinigus galima pervesti tiesiogiai iš PayPal sąskaitos.

Naudotis PayPal sistema yra paprasta. Pagrindiniai keliami reikalavimai yra galiojantis elektroninio pašto adresas ir galiojanti kreditinė kortelė arba banko sąskaita.

6 lentelė. PayPal sistemai būdingi požymiai

Atsiskaitymo modelis	Kreditinės kortelės atsiskaitymo tarpininkavimas
Patvirtinimas (angl. validation)	Prijungties režime
Privatumo kontrolė	Nėra duomenų
Saugumo mechanizmai	SSL 3.0, sauga per išorinį ryšį
Apsauga nuo pakartotinio išleidimo	Taip
Apsauga nuo klastojimo	Taip
Apsauga nuo išeikvojimo	Nėra duomenų
Apsauga nuo nepaneigiamumo	Taip
Anonimiškumas	Ne
Atsekamumas	Taip

1.7.6. Milicent

Digital Equipment kompanijos sukurta Millicent sistema yra specialiai pritaikyta tokiems atsiskaitymams, kurių suma gali nesiekti netgi vieno cento. Ši sistema pagrįsta specialiųjų atsiskaitymo vienetų (angl. *scrips*) išleidimu, kurie galioja ir yra pripažįstami tik vienoje konkrečioje e-parduotuvėje. Toks atsiskaitymo vienetas yra išduodamas brokerio, kuris veikia kaip tarpininkas, tačiau sistema nereikalauja vieneto autentifikacijos. Kadangi konkretus *scrip* galioja ir yra pripažįstamas tik konkrečioje parduotuvėje, pats pardavėjas gali atlikti visą reikalingą ir būtiną atsiskaitomojo vieneto galiojimo patikrinimą. Tai žymiai sumažina atsiskaitymo trukmę ir su tuo susijusias papildomas išlaidas. Toks atsiskaitymo metodas užtikrina šalių anonimiškumą, kadangi konkrečiame *scrip* nėra jokios identifikuojančios informacijos, ją žino tik tretysis asmuo – atsiskaitomąjį vienetą išdavęs brokeris [7].

Bendravimo seka vyksta tokia tvarka:

- Iš pradžių vartotojas įsigyja tam tikrą kiekį brokerio *scrip*.
- Tuomet vartotojas užprašo pardavėjo *scrip*, už kuriuos sumoka brokerio *scrip*.
- Brokeris įsigyja reikiamą pardavėjo *scrip* iš pardavėjo.
- Brokeris parduoda pardavėjo *scrip* vartotojui.
- Vartotojas perka paslaugas naudodamas pardavėjo *scrip*.
- Pardavėjas duoda grąža pardavėjo *scrip*.

Pirmas ir ketvirtas žingsniai yra neatliekamai per kiekvieną operaciją, nes vartotojas tam tikram laiko tarpui gali nusipirkti pakankamai *scrip* iš brokerio. Taip pat ir brokeris gali laikyti pakankamai pardavėjo *scrip* tam, kad aptarnautų daugelį vartotojų.

7 lentelė. Milicent sistemai būdingi požymiai

Atsiskaitymo modelis	Tiesioginiais pinigais paremtas modelis, vartotojų sąskaitos, esančios pas brokerį
Patvirtinimas (angl. validation)	Dalinai prijungties režime. Transakcijos vykdomos tik tarp vartotojo ir pardavėjo. Brokeris reikalingas tik pasiruošimui.
Privatumo kontrolė	Plečiama nuo nekonfidencialios iki konfidencialios, neanoniminė, atsekama
Saugumo mechanizmai	Slaptažodžiai, maišos funkcijos, paprasta apsauga
Apsauga nuo pakartotinio išleidimo	Taip
Apsauga nuo klastojimo	Taip
Apsauga nuo išeikvojimo	Nėra duomenų
Apsauga nuo nepaneigiamumo	Taip
Anonimiškumas	Ne, tačiau nėra autentifikacijos
Atsekamumas	Taip

1.7.7. NetBill

NetBill yra viena iš mikromokėjimams skirtų sistemų. Ji buvo sukurta Carnegie Mellon universitete vystant ankstesnius mokėjimo paslaugų prototipus ir pritaikyta šio universiteto elektroninėje bibliotekoje [11].

Sistema yra naudojama kaip atsiskaitymo metodas už internete perkamas informacines prekes ir paslaugas. NetBill sistema apmokestina vykdomus pervedimus, taip pat pačioje sistemoje (NetBill serveryje) būtina turėti sąskaitą, iš kurios yra nuskaičiuojamos lėšos. NetBill serveris aptarnauja tiek vartotojo sąskaitą, tiek pardavėjo.

NetBill naudoja tiesiogine sąskaita paremtą atsiskaitymo modelį. Sistema pasižymi tokiomis savybėmis, kaip saugių transakcijų vykdymas šifruojant (simetrinio ir viešo rakto kriptografija), elektroniniais parašais, autentifikacija (Kerberos), likutinės sąskaitos tikrinimu, prieigų valdymu, transakcijų registravimu [11].

NetBill sistemos protokolas vykdomas tokia seka [10]:

1. Pardavėjas siunčia prekes užšifruota forma į vartotojo kompiuterį.
2. Vartotojo kompiuteryje esanti programinė įranga patikrina, ar gautos prekės yra tinkamos ir siunčia patvirtinimą pardavėjo programinei įrangai.
3. Pardavėjas siunčia vartotojo patvirtinimo pranešimą, vartotojo sąskaitos informaciją ir dešifravimo raktą NetBill serveriui.
4. NetBill serveris patikrina, ar vartotojo sąskaitoje esančių pinigų pakanka sumokėti už prekes. Jei taip, serveris persiunčia lėšas, išsaugo dešifravimo raktą ir siunčia pranešimą pardavėjo programinei įrangai.
5. Pardavėjas siunčia vartotojui dešifravimo raktą, kurį vartotojo programinė įranga panaudoja prekių dešifravimui. Jei pardavėjo serveris šiame žingsnyje neveikia, raktą galima gauti iš NetBill serverio.

8 lentelė. NetBill sistemai būdingi požymiai

Atsiskaitymo modelis	Tiesiogine sąskaita paremtas modelis
Patvirtinimas (angl. validation)	Prijungties režime
Privatumo kontrolė	Neanonimiškas, atsekamas
Saugumo mechanizmai	Viešo ir simetrinio raktų kriptografija, Kerberos
Apsauga nuo pakartotinio išleidimo	Nėra duomenų

Apsauga nuo klastojimo	Taip
Apsauga nuo išeikvojimo	Taip
Apsauga nuo nepaneigiamumo	Taip
Anonimiškumas	Ne
Atsekamumas	Taip

NetBill protokolas užtikrina nedalumą, privatumą, saugumą ir mažą skaičiavimo savikainą, tačiau atliekama daug centralizuotų skaičiavimų NetBill tarnybinėje stotyje. Taip pat reikalaujama, kad klientas turėtų sąskaitą NetBill tarnybinėje stotyje. Anonimiškumas neužtikrinamas, nes NetBill tarnybinė stotis žino visas vartotojo atliktas operacijas [14].

9 lentelė. Mokėjimo schemų palyginimas

Mokėjimo schema / Būdingi bruožai	CyberCash	Ecash	First Virtual	Mondex	PayPal	Milicent	NetBill
Atsiskaitymo modelis	Saugus kortelės duomenų pateikimas	Tiesioginiais pinigais paremtas modelis	Kreditinės kortelės atsiskaitymo tarpininkavimas	Tiesioginiais pinigais paremtas modelis, intelektuali kortelė	Kreditinės kortelės atsiskaitymo tarpininkavimas	Tiesioginiais pinigais paremtas modelis	Tiesiogine sąskaita paremtas modelis
Patvirtinimas (angl. validation)	Prijungties režime	Prijungties režime	Prijungties režime	Atjungties režime	Prijungties režime	Dalinai prijungties režime	Prijungties režime
Privatumo kontrolė	Pirkėjai naudoja pseudonimus, bankas gali atsekti visas operacijas	Konfidencialumas, anonimiškumas, neatsekamumas	Pseudonimai	Nėra duomenų	Nėra duomenų	Neanonimiškas, atsekamas	Neanonimiškas, atsekamas
Saugumo mechanizmai	RSA ir DES šifravimas, parašai, MAC	RSA ir DES šifravimas, aklas parašas	Pirkėjo teiravimasis e. paštu dėl kiekvieno pirkimo patvirtinimo	Intelektualios kortelės, parašai, MAC	SSL 3.0, sauga per išorinį ryšį	Slaptažodžiai, maišos funkcijos	Viešo ir simetrinio raktų kriptografija, Kerberos
Apsauga nuo pakartotinio išleidimo	Nėra duomenų	Taip	Nėra duomenų	Taip, užtikrina intelektuali kortelė	Taip	Taip	Nėra duomenų
Apsauga nuo klastojimo	Ne	Nėra duomenų	Dalinė	Taip	Taip	Taip	Taip
Apsauga nuo išeikvojimo	Taip, autorizacija prijungties režime	Nėra duomenų	Nėra duomenų	Nėra duomenų	Nėra duomenų	Nėra duomenų	Taip
Apsauga nuo nepaneigiamumo	Ne, bet pardavėjo autentifikacija	Nėra duomenų	Nėra duomenų	Taip	Taip	Taip	Taip

Anonimiškumas	Dalinis	Taip	Dalinis	Ne, informacija saugoma banke	Ne	Ne, tačiau nėra autentifikacijos	Ne
Atsekamumas	Taip	Ne	Taip	Taip	Taip	Taip	Taip

Aukščiau pateiktoje lentelėje (9 lentelė) galime pastebėti, kad vidutiniams ir dideliems mokėjimams skirtose sistemose (CyberCash, Ecash, NetBill) naudojami sudėtingesni saugumo mechanizmai, kurie tuo pačiu apkrauna tinklą ir padidina mokėjimo patvirtinimo kainą. Mažiems mokėjimams (mikromokėjimams) skirtose sistemose naudojami paprastesni saugumo užtikrinimo metodai, tokie kaip maišos funkcijos, slaptažodžiai, kadangi maišos funkcijos skaičiuojamos greičiau, taip pat kiekvienai transakcijai atlikti nereikalinga trečioji šalis.

Apibendrinant aptartas elektroninių atsiskaitymų sistemas, galime pastebėti, kad vienos jų nepasiteisino ir pasitraukė iš rinkos (CyberCash, Ecash), o kitos sėkmingai veikia iki šiol (PayPal). Digicash sukurta Ecash sistema iš tiesų niekada nepasiekė lemiamo pirkėjų, bankų ir pardavėjų daugumos, kurie priimtų ir naudotų jos sukurtą elektroninę valiutą, todėl patyrė bankrotą. CyberCash ir First Virtual šiuo metu taip pat yra pasitraukę iš komercinės veiklos [9].

Pagrindinė nepasiteisinusių elektroninių atsiskaitymo sistemų problema yra ta, kad jos nepakankamai sutelkė dėmesį į klientų elgseną ir požiūrį, todėl nesulaukė susidomėjimo [9].

1.8. Analizės išvados

Analizės dalyje atlikta:

- Išnagrinėti elektroniniai pinigai, nustatyti jų tipai, galimos rūšys ir turimos savybės, nurodyti esami privalumai ir trūkumai.
- Aptartos elektroninių pinigų cirkuliacijos schemų savybės, išsiaiškinti tokių schemų dalyviai, pateikti egzistuojantys e. pinigų cirkuliacijos schemų modeliai.
- Nurodyti e. pinigų cirkuliacijos schemoms keliami saugumo reikalavimai ir išdėstyti patikimi saugumo mechanizmai, tokie kaip šifravimas, viešo rakto kriptografija, skaitmeniniais parašais užtikrinama autentifikacija, dvigubi parašai, pranešimo autentifikavimo kodas (MAC), kurie leidžia užtikrinti keliamus saugumo reikalavimus.
- Per visą laikotarpį nuo e. pinigų evoliucijos pradžios buvo sukurta ar bent jau pasiūlyta prototipų lygyje gana didelis spektras e. atsiskaitymo sistemų. Šiame

darbe nagrinėtos dažniausiai ištirtoje literatūroje aprašomos ar minimos e. pinigų cirkuliacijos schemos (e. atsiskaitymų sistemos). Nemaža jų dalis (CyberCash, First Virtual) nors ir turėjo pakankamai potencialo tapti rinkos lyderiais, tačiau plačiau nepaplito tarp vartotojų, pardavėjų ir bankų. Galima paminėti PayPal sistemą kaip vieną iš sėkmingiausiai veikiančių e. atsiskaitymo sistemų dėl jos integracijos su populiariu E-Bay internetiniu aukcionu ir paprastumo, atsiskaitymams naudojant e. pašto protokolų teikiamas galimybes.

2. RIBOTOS SUMOS ELEKTRONINIŲ PINIGŲ CIRKULIACIJOS SISTEMOS MODELIS

Šiame skyriuje iškeliami funkciniai ir nefunkciniai reikalavimai modeliui, detaliai aptariamas pats siūlomas ribotos sumos elektroninių cirkuliacijos sistemos modelis, jo architektūra ir naudojamas protokolas. Analizuojamas pasiūlyto modelio efektyvumas ir saugumas.

2.1. Reikalavimų specifikavimas

Funkciniai reikalavimai

Reikalavimai sistemai. Sistema turi tenkinti sekančius funkcinius reikalavimus:

- Galimybė sistemos vartotojams registruotis sistemoje.
- Vartotojų autentifikavimas. Autentifikavimas – tai procesas, kurio metu nustatoma sistemos vartotojų tapatybė. Sistemos vartotojams autentifikuoti turi būti realizuotas prisijungimo langas, kuriame galima būtų atlikti tokius veiksmus:
    - Esamo vartotojo identifikavimas ir autentifikavimas leidžiant naudotis sistemos galimybėmis.
    - Naujo vartotojo registracija.
    - Slaptažodžių priminimas elektroniniu paštu.
- Vartotojų autorizavimas. Autorizavimas – tai procesas, kurio metu nustatoma, ar vartotojas turi teisę atlikti tam tikrus veiksmus sistemoje. Prieš atliekant bet kurį veiksmą sistemoje, turi būti tikrinamos vartotojo teisės ir uždraudžiama atlikti veiksmą, jeigu vartotojui nesuteiktos atitinkamos teisės sistemoje.

- Vartotojų registravimosi informacijos keitimo galimybė.
- E. pinigo sertifikato išdavimas. Prisijungusiam vartotojui turi būti leidžiama išsiimti e. pinigo sertifikato failą, jei tai leidžia jo turimas sąskaitos balansas. Sertifikatas turi būti pasirašytas brokerio.
- E. pinigo vertės sukūrimas. Autentifikuotas vartotojas, turintis galiojantį brokerio išduotą e. pinigo sertifikatą, gali sukurti mokėjimams skirtą failą su jame esančia reikiama e. pinigo verte. Turi būti patikrintas sertifikato e. parašas, o sukurtas failas pasirašytas vartotojo.
- Inkasacijos pranešimo sukūrimas. Pardavėjas iš kiekvieno vartotojo gautų pirkimo vykdymo ir mokėjimų pranešimų gali sudaryti inkasacijos pranešimą, kuris įkeliamas į serverį (brokeris). Pranešimas turi būti pasirašytas pardavėjo.
- Vientisumo užtikrinimui naudoti e. parašus.
- Didesnio saugumo užtikrinimui naudoti maišos funkcijas.
- Komunikavimo saugumui užtikrinti tarp visų sistemos šalių naudoti perduodamos informacijos šifravimą panaudojant HTTPS (SSL).

Nefunkciniai reikalavimai

Reikalavimai vartotojo sąsajai. Sistemos vartotojų sąsaja (angl. *GUI – graphic user interface*) realizuojama lietuvių kalba, paprasta, suprantama, lengvai valdoma meniu pagalba, neperkrauta nereikalingais elementais, esami elementai aiškiai ir patogiai išdėstyti, rezultatų atvaizdavimas aiškus, paprastas.

Reikalavimai duomenų apsaugai

Priėjimo prie duomenų apribojimas. Duomenų bazės administratoriaus slaptažodis turi būti žinomas tik tiems sistemos vartotojams, kurie pagal užimamas pareigas turi teisę atlikti duomenų bazės administravimo veiksmus. Informacinės sistemos administratorius turi tikrinti sistemos funkcionavimą ir pastebėti visus sutrikimus.

Apsauga nuo duomenų praradimo. Norint apsaugoti duomenų bazėje esančius duomenis rekomenduojama daryti atsargines duomenų bazės kopijas. Tuo atveju, jei dėl gedimo būna pažeidžiami duomenų failai, bazės darbingumo atstatymas turėtų būti vykdomas veikiančiame serveryje panaudojant paskutinę duomenų bazės kopiją.

Duomenų apsauga tinkle. Duomenys tarp klientinės programinės įrangos ir serverio (sistemos aplikacijų serverio) turėtų būti perduodami užšifruoti panaudojant HTTPS (SSL) protokolą.

Reikalavimai sistemos veikimo aplinkai

Sistemos žiniatinklio programai funkcionuoti lokalioje mašinoje turi būti įdiegta Microsoft .NET Framework paketo antra (2.0) arba aukštesnės (3.0, 3.5) versijos. Taip pat vartotojo užklausoms apdoroti operacinėje sistemoje turi veikti IIS žiniatinklio serveris.

Vartotojai, naudojantys sistemos taikomąją programą, į savo kompiuterius turi būti įdiegę „Microsoft .NET Framework" paketą.

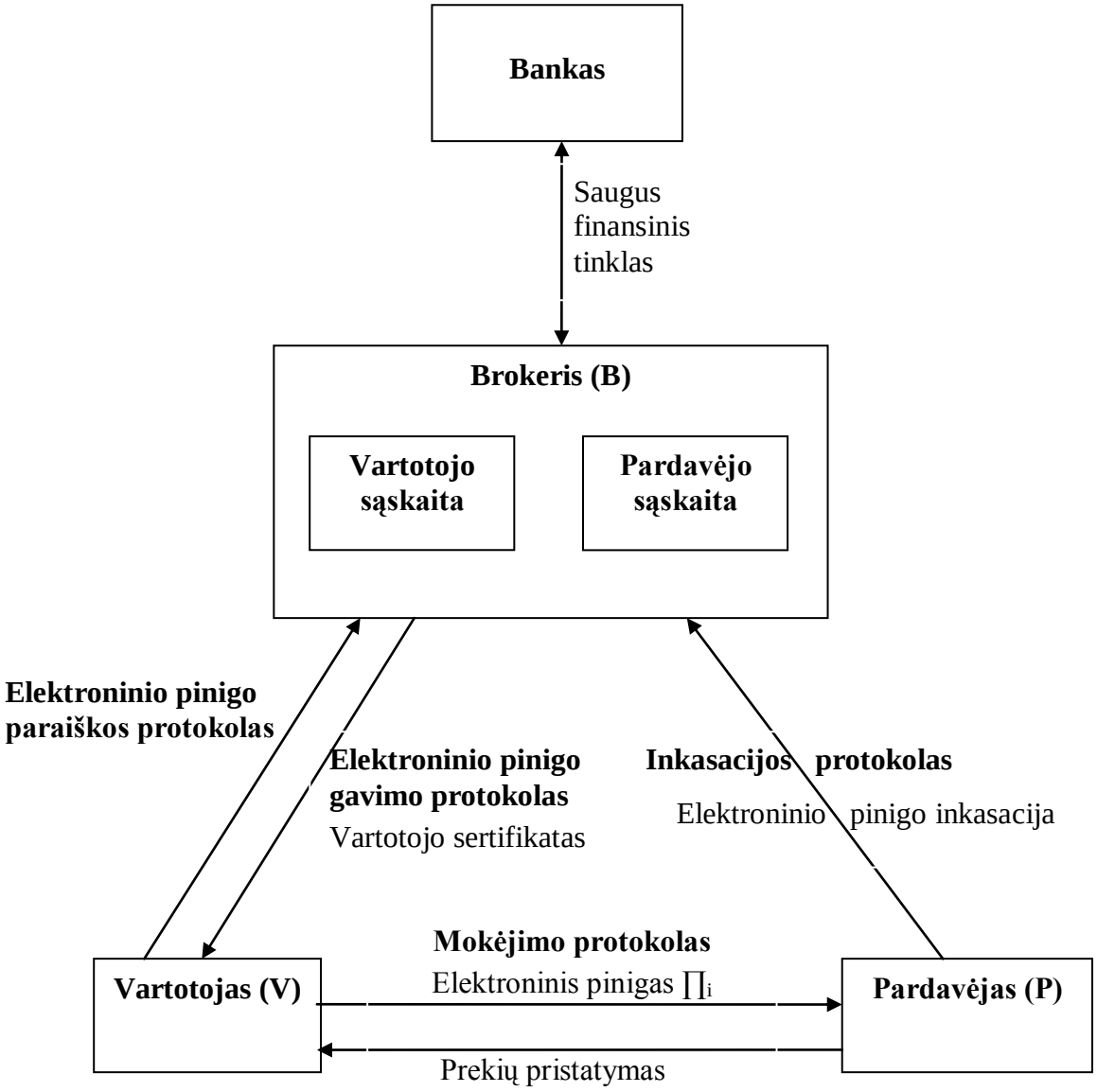
2.2. Ribotos sumos elektroninių pinigų cirkuliacijos sistemos modelio architektūra

Siūlomas modelis paremtas R. Rivesto ir A. Shamiro sukurta Payword mikromokėjimų sistemos koncepcija. Modelio architektūrą sudaro trys pagrindiniai dalyviai: vartotojas, pardavėjas ir brokeris. Brokerio vaidmenį atlieka tinklo serveris, kuris yra sujungtas su banku per saugų finansinį X.25 tinklą. Mokėjimas vykdomas atjungties režimu panaudojant maišos funkcijų šifravimą. Kiekvienoje mokėjimo operacijoje dalyvauja tik vartotojas ir pardavėjas. Brokeris yra atsakingas už vartotojų ir pardavėjų registravimą, dvigubo pinigų išleidimo aptikimą, pardavėjo per didelio apmokestinimo aptikimą ir vartotojų bei pardavėjų sąskaitų palaikymą.

Šiame modelyje vartotojas turi užsiregistruoti pas brokerį ir kreiptis dėl sąskaitos sukūrimo. Prieš prašydamas iš pardavėjo bet kokios paslaugos, vartotojas turi sukurti e. pinigą, sudarytą iš sugeneruotos maišos funkcijos reikšmės, kuria yra atsiskaitoma pardavėjui kaip valiuta. Pardavėjas turi įsitikinti, ar vartotojas tikrai yra tas, kuriuo dedasi ir ar pinigas yra legaliai sugeneruotas. Kuomet e. pinigai sukaupiami iš vartotojo, pardavėjas juos grąžina brokeriui, kuris atlieka pervedimus iš vartotojo sąskaitos į pardavėjo sąskaitą. Šeštame paveiksle pateikta siūlomo modelio architektūra ir ryšiai tarp dalyvių.

Pateiktame modelyje daroma prielaida, kad:

- Brokeris yra sąžiningas ir juo pasitiki tiek vartotojas, tiek pardavėjas.
- Naudojama patikima viešojo rakto infrastruktūra (PKI).
- Atsiskaitoma elektroninėmis prekėmis.



6 pav. Modelio architektūra

Toliau yra nagrinėjamas siūlomo modelio protokolas.

2.3. Ribotos sumos elektroninių pinigų cirkuliacijos sistemos protokolas

Šiame skyriuje detaliai aprašomas ribotos sumos elektroninių pinigų cirkuliacijos sistemos protokolas ir jo etapai.

Tolimesniam nagrinėjimui apsibrėžiame modelio protokole naudojamus simbolinius žymėjimus:

- V – vartotojas, P – pardavėjas, B – brokeris;
- VR_V – vartotojo viešasis raktas, VR_P – pardavėjo viešasis raktas, VR_B – brokerio viešasis raktas;
- σ_V – vartotojo e. parašo funkcija, σ_P – pardavėjo e. parašo funkcija, σ_B – brokerio e. parašo funkcija;
- i-tasis e. pinigas, kuriame yra sugeneruota piniginė reikšmė panaudojant maišos funkciją, žymimas kaip $\prod_i$, kur i =1, 2, 3, …, n.
- Pranešimas P pasirašytas elektroniniu parašu žymimas σ [P].

Tam, kad vartotojo sudaryta e. pinigo reikšme būtų galima atsiskaityti pas visus pardavėjus, vienos monetos vertė turi būti pakankamai maža ir vienoda, pavyzdžiui vienas centas.

Skaičiavimams sumažinti (tiek vartotojo pusėje, tiek pardavėjo pusėje) e. pinigo generavime naudojami du monetų modeliai, o e. pinigo sekimui naudojamas indeksavimas. E. pinigas yra generuojamas naudojant maišos funkcijas *H1* ir *H2*. *H1* funkcijos sugeneruota iš vienetų sudaryta reikšmė žymima h_i^1, H2 funkcijos sugeneruota iš dešimčių sudaryta reikšmė žymima kaip h_j^{10}. Panaudotos maišos funkcijų sugeneruotos e. pinigo reikšmės h_i^1 ir h_j^{10} tolesniam apdorojimui įrašomos vartotojo pusėje ir pardavėjo pusėje.

Sistemos protokolą sudaro tokie etapai:

- Registracija
- Pirkimo inicijavimas
- Transakcija
- Inkasacija

Šie etapai aptariami tolesniuose skyriuose.

2.3.1. Registracija

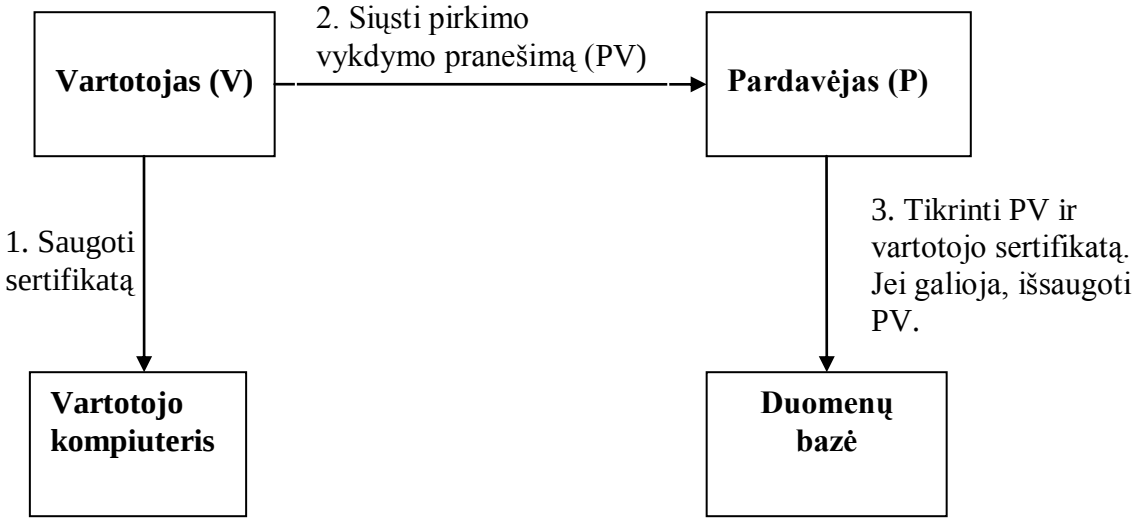
Šiame protokolo etape sukuriami ryšiai tarp vartotojo, pardavėjo ir brokerio. Brokeris yra atsakingas už vartotojo ir pardavėjo registraciją bei sąskaitų sukūrimą. Visų pirma vartotojas ir

pardavėjas turi užsiregistruoti pas brokerį ir gauti sąskaitą. Esant vartotojo ir pardavėjo sąskaitoms, pardavėjas suteikia brokeriui įgaliojimus, kad šis pasirašytų monetas, už kurias registruotas vartotojas galės atlikti pirkimą. Prieš atlikdamas pirkimą vartotojas privalo savo sąskaitą depozituoti tam tikra suma pinigų. Apmokėjimo detalės perduodamos brokeriui per saugų kanalą kaip SSL.

2.3.2. Pirkimo inicijavimas

Šiame etape vartotojas inicijuoja pirkimą. Brokeris apriboja vartotojo išlaidas nustatydamas limitą ir sugeneruoja du pradinius monetų modelius C_0^1 ir C_0^{10}, kuriuos vartotojas naudos generuoti e. pinigui. Šie modeliai yra naudojami ir pardavėjui autentifikuojant e. pinigą. Tuomet brokeris išduoda vartotojui sertifikatą ir pasirašo jį. Sertifikate saugomi monetų modeliai, išlaidų limitas ir vartotojo viešasis raktas. Sertifikatas galioja tam tikrą laiko tarpą (pvz. vieną dieną). Brokeris gali atsisakyti išduoti naują sertifikatą, jeigu vartotojo sąskaitoje nėra pinigų arba vartotojas buvo pagautas sukčiaujant.

Vartotojas, atlikdamas pirkimą, pasirašo pirkimo vykdymo pranešimą ir siunčia jį pardavėjui. Pranešime yra saugomas brokerio pasirašytas sertifikatas, kurį patikrina pardavėjas. Septintame paveiksle pavaizduoti pirkimo inicijavimo pranešimų srautai, kuriuos sudaro žemiau aprašyti žingsniai.



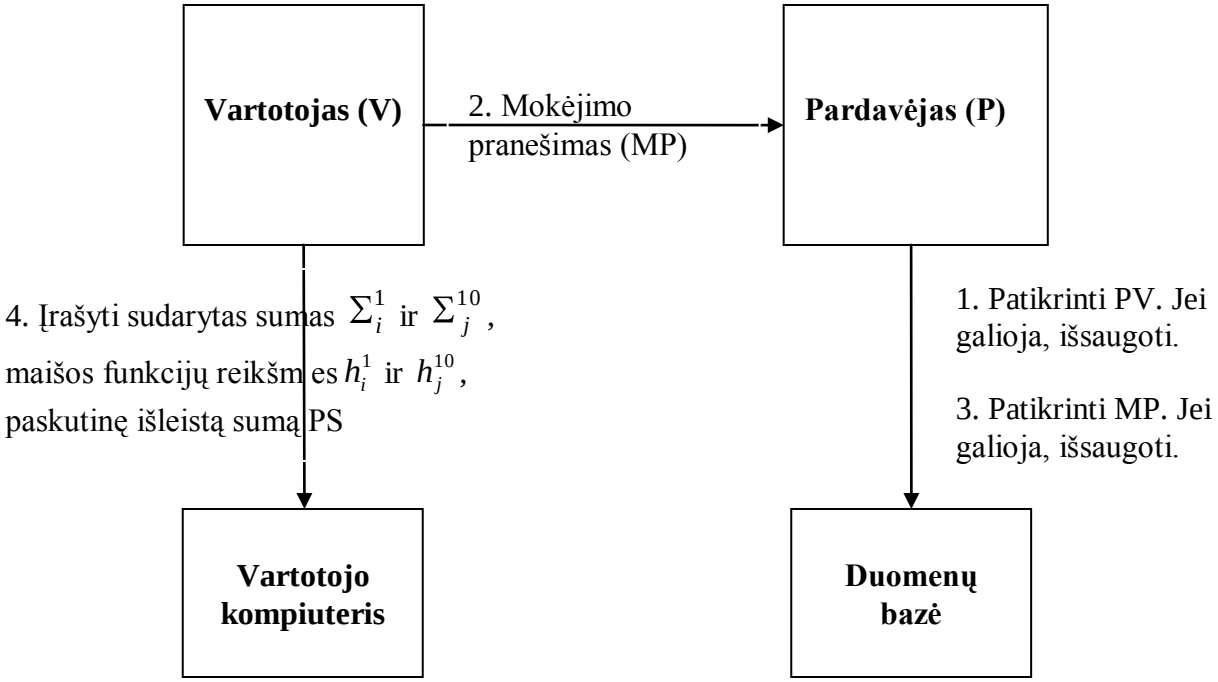
7 pav.. Pranešimų srautai iniciavimo etape

Iniciacijos etapo žingsniai:

- Sertifikato prašymas (e. pinigo paraiškos protokolas). Sėkmingai užsiregistravus ir prisijungus prie serverio (brokeris) vartotojas prašo išduoti sertifikatą (e. pinigo paraiškos protokolas). Sertifikatas leidžia vartotojui sugeneruoti e. pinigus, kurie bus grąžinti iš pardavėjo brokeriui.
- Išlaidų limito nustatymas. Brokeris patikrina vartotojo sąskaitos likutį ir pagal jį nustato išlaidų limitą *Max*, kuris turi būti nedidesnis už sąskaitos likutį. Jei vartotojo sąskaitos balansas lygus nuliui, brokeris praneša papildyti sąskaitą.
- Monetų modelių sukūrimas. Brokeris sukuria šaknines monetų reikšmes C_0^1 ir C_0^{10}, atsitiktinai parinkdamas du didelius skaičius x, y ir suskaičiuodamas maišos funkcijos reikšmes: vieno cento monetos reikšmė $C_0^1 = H(x)$ ir dešimties centų monetos reikšmė $C_0^{10} = H(y)$.
- Sertifikato išdavimas (e. pinigo gavimo protokolas). Brokeris išleidžia sertifikatą, vieną kopiją pasilieka sau, o originalą nusiunčia vartotojui. Sertifikate saugoma informacija: brokerio identifikacija B_{ID}, vartotojo identifikacija V_{ID}, vartotojo viešasis raktas VR_V, sertifikato galiojimo laikas D_G, brokerio sugeneruoti šakniniai monetų modeliai C_0^1 ir C_0^{10}, išlaidų limitas *Max* ir išlaidų limito maišos funkcijos reikšmė H(Max). Vartotojui išduoto sertifikato struktūra apibrėžiama taip $S_B = \sigma_B[\mathrm{B_{ID}}, V_{ID}, VR_V, D_G, C_0^1, C_0^{10}, Max, H(Max)] = \prod$. Čia S_B yra brokerio e. parašo funkcijos reikšmė, iš kurios bus išgaunami monetų modeliai e. pinigo sudarymui.
- Brokerio išduoto sertifikato patikrinimas. Tam, kad patikrinti, ar sertifikatas yra pasirašytas brokerio, vartotojas panaudoja brokerio viešąjį raktą ir patikrina išduotą sertifikatą. Tuomet sertifikatas yra išsaugomas.
- Pirkimo vykdymo pranešimo siuntimas. Prieš siųsdamas pardavėjui e. pinigą, vartotojas jam siunčia pirkimo vykdymo pranešimą *PV*. Pranešimą sudaro vartotojo identifikacija V_{ID}, pardavėjo identifikacija P_{ID}, pirkimo data *D*, vartotojo sertifikatas S_B, . Pranešimas pasirašomas vartotojo privačiuoju raktu. Pirkimo vykdymo pranešimo struktūra $PV = \sigma_V[\mathrm{P_{ID}}, V_{ID}, \mathrm{S_B}, D]$

2.3.3. Transakcija

Vykdant šį etapą vartotojas iš sertifikate esančių šakninių monetų C_0^1 ir C_0^{10} sugeneruoja tam tikros vertės e. pinigą $\prod_i$ priklausomai nuo prekės vertės ir siunčia pardavėjui. Pardavėjas patikrina atsiųsta e. pinigą perskaičiuodamas maišos funkcijų reikšmes. Žemiau esančiame paveiksle (8 pav.) pavaizduoti pranešimų srautai tarp vartotojo ir pardavėjo.



8 pav. Pranešimų srautai transakcijos etape

Transakcijos etapas vykdomas sekančia tvarka:

- Pirkimo vykdymo patvirtinimas. Pardavėjas patikrina vartotojo atsiųstą pirkimo vykdymo pranešimą, kuris pasirašytas vartotojo privačiuoju raktu. Taip pat yra patikrinamas pranešime esantis vartotojo sertifikatas panaudojant brokerio viešąjį raktą. Jei ir pranešimas ir sertifikatas galioja, pardavėjas patikrina, ar pirkimo data D neviršija sertifikato galiojimo datos D_G . Jei viskas tvarkoje, pardavėjas išsaugo pirkimo vykdymo pranešimą.
- E. pinigo vertės generavimas. Vartotojas pagal šaknines reikšmes C_0^1 ir C_0^{10}, paimtas iš sertifikato, sudaro reikiamą sumą. Jeigu vykdomas pirkimas, kurio prekių vertė Σ centų, tuomet reikia sudaryti sumą Σ_i^1 iš vieno cento monetų ir

sumą Σ_j^{10} iš dešimties centų monetų, kur i = mod (Σ,10), j = (Σ / 10). Sudarytos sumos išreiškiamos taip: $\Sigma_i^1 = n * C_0^1$ ir $\Sigma_j^{10} = m * C_0^{10}$. Kur $\Sigma_i^1 + \Sigma_j^{10} \leq Max$ yra e. pinigo $\prod_i$ sudedamoji dalis.

Panaudojant sudarytas sumas apskaičiuojamos maišos funkcijų reikšmės:

$h_i^1 = H(\Sigma_i^1)$ ir $h_j^{10} = H(\Sigma_j^{10})$

- Mokėjimo pranešimo siuntimas. Sugeneravus e. pinigą sudarančią vertę, siunčiamas mokėjimo pranešimas MP, kuris yra pasirašytas vartotojo e. parašu. Pranešimą sudaro iš vieno cento monetų sudaryta suma Σ_i^1, iš dešimties centų monetų sudaryta suma Σ_j^{10}, abiejų sumų maišos funkcijų reikšmės $h_i^1 = H(\Sigma_i^1)$ ir $h_j^{10} = H(\Sigma_j^{10})$, šakninių reikšmių daugikliai n ir m, laiko žymė T, kuri apsaugo nuo pakartotinio siuntimo, suma visų prieš tai atliktų mokėjimų PAMS, jeigu prieš tai buvo atlikti pirkimai, prieš tai atliktų mokėjimų maišos funkcijos reikšmė *H(PAMS)*. Mokėjimo pranešimo sandara:

  $MP = \sigma_v[\Sigma_i^1, \Sigma_j^{10}, h_i^1, h_j^{10}, n, m, T, PAMS, H(PAMS)] = \Pi_i$.

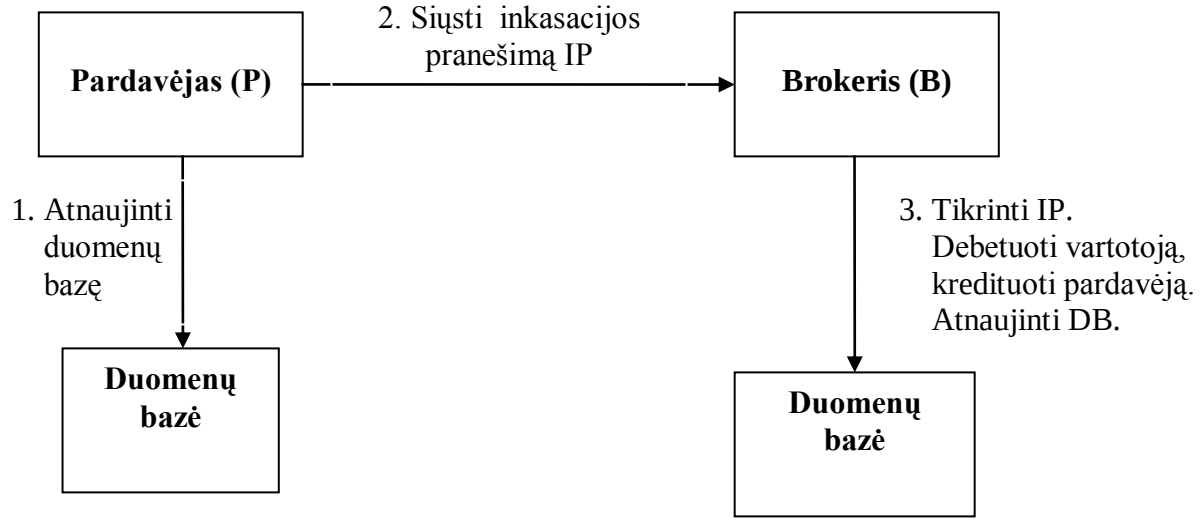
- Mokėjimo pranešimo tikrinimas. Iš pradžių pardavėjas patikrina ir autentifikuoja mokėjimo pranešimą panaudodamas vartotojo viešąjį raktą VR_V. Tuomet iš pranešimo išgaunama prieš tai atliktų mokėjimų suma *PAMS*, apskaičiuojama paskutinė vartotojo išleista suma $PS = \Sigma_{i-n}^1 ... + ... \Sigma_{i-1}^1 + \Sigma_{j-m}^{10} ... + ... \Sigma_{j-1}^{10}$ ir dabartinė suma $DS = \Sigma_i^1 + \Sigma_j^{10}$. Jei *PAMS* + *PS* + *DS* ≤ *Max*, tuomet mokėjimo pranešime esančios sumos Σ_i^1 ir Σ_j^{10} yra galiojančios. Jei *PAMS* + *PS* + *DS* > *Max*, nustatoma, kad vartotojas viršija išlaidų limitą. Pardavėjas patikrina, ar iš vartotojo gautas e. pinigas $\prod_i$ tikras, iš naujo paskaičiuodamas maišos funkcijų reikšmes h_i^1 ir h_j^{10}. Tam pardavėjas pasiima šaknines monetų reikšmes C_0^1 ir C_0^{10} iš sertifikato S_B, sudaro sumas $\Sigma_i^{1'}$ ir $\Sigma_j^{10'}$ suskaičiuodamas $\Sigma_i^{1'} = n * C_0^1$ ir $\Sigma_j^{10'} = m * C_0^{10}$. Tuomet randamos maišos funkcijų reikšmės $h_i^{1'} = H(\Sigma_i^{1'})$ ir $h_j^{10'} = H(\Sigma_j^{10'})$. Pardavėjas palygina gautas maišos funkcijos reikšmes $h_i^{1'}$ ir

h_j^{10}' su mokėjimo pranešime esančiomis reikšmėmis h_i^1 ir h_j^{10}. Jeigu reikšmės sutampa, e. pinigas pripažįstamas galiojančiu, jeigu ne – e. pinigas yra suklastotas.

- E. pinigo reikšmių išsaugojimas. Po e. pinigo patikrinimo pardavėjas išsaugo mokėjimo pranešime atsiųstas sumas Σ_i^1 ir Σ_j^{10}, maišos funkcijų reikšmes h_i^1 ir h_j^{10} duomenų bazėje surišdamas jas su vartotojo identifikacija V_{ID} vėlesniam e. pinigo grąžinimui.

2.3.4. Inkasacija

Vartotojui atlikus piniginės vertės transakcijos operaciją, vykdomas inkasacijos protokolas, kurio metu grąžinami pardavėjo surinkti e. pinigai bei atnaujinamos vartotojo ir pardavėjo sąskaitos. Šio etapo metu pardavėjas surenka visus mokėjimo pranešimus *MP*, sugrupuoja juos pagal vartotojo identifikaciją V_{ID} ir siunčia brokeriui. Brokeris patikrina inkasacijos pranešimą *IP*, perskaičiuoja jame esančias kiekvieno vartotojo išleistas sumas, taip pat patikrina maišos funkcijų reikšmes. Jei viskas tvarkoje, brokeris papildo pardavėjo sąskaitą gauta suma ir nurašo tą pačią sumą nuo vartotojo sąskaitos. Inkasacijos etapą iliustruoja devintame paveiksle pateikta schema, kuri parodo pranešimų (duomenų) cirkuliaciją tarp pardavėjo ir brokerio.



9 pav. Pranešimų srautai inkasacijos etape

Detalesnė inkasacijos etape vykdomo inkasacijos protokolo tvarka atliekama sekančiai:

- Apskaičiuojama vartotojo išleista suma. Vartotojui baigus internetinį apsipirkimą, jis brokeriui siunčia visas sugeneruotas maišos funkcijų reikšmes $h^1_{i-n}...h^1_{i-1}...h^1_i$ ir $h^{10}_{j-m}...h^{10}_{j-1}...h^{10}_j$, išleistas sumas $\Sigma^1_{i-n}...\Sigma^1_{i-1}...\Sigma^1_i, \Sigma^{10}_{j-m}...\Sigma^{10}_{j-1}...\Sigma^{10}_j$. Brokeris apskaičiuoja visą vartotojo išleistą sumą $VIS_1 = \Sigma(\Sigma^1_{i-n}... + ...\Sigma^1_{i-1} + \Sigma^{10}_{j-m}... + ...\Sigma^{10}_{j-1})$.
- Inkasacijos pranešimo tikrinimas. Pardavėjas atsiunčia brokeriui inkasacijos pranešimą *IP* pasirašytą e. parašu σ_P. Inkasacijos pranešimas sudarytas iš pardavėjo identifikacijos P_{ID}, visų vartotojų mokėjimo informacijos: kiekvieno vartotojo pirkimo vykdymo pranešimų *PV*, visų jo mokėjimo pranešimų *MP*, pilnos jo išlaidų sumos *Σ (suma)* ir išlaidų sumos maišos funkcijos reikšmės *H(Σ (suma))*. Apibrėžiama tokia inkasacijos pranešimo struktūra: $IP = \sigma_P[P_{ID,}\Sigma(V_{ID}, PV, \Sigma(MP), \Sigma(suma), H(\Sigma(suma)))]$.

  Brokeris, panaudodamas pardavėjo viešąjį raktą, patvirtina jo e. parašą ant pranešimo, kiekviename pirkimo vykdymo pranešime patikrina sertifikato galiojimo datą, patikrina e. pinigą, perskaičiuodamas maišos funkcijų reikšmes. Jei viskas tvarkoje, brokeris suskaičiuoja kiekvieno vartotojo išleistą sumą $\Sigma(\Sigma^1_i, \Sigma^{10}_j)$ ir palygina ją su pardavėjo atsiųsta suma Σ (Suma). Jei sumos vienodos, brokeris papildo pardavėjo sąskaitą suma Σ (Suma).
- Dvigubo išleidimo tikrinimas. Tikrinant dvigubą e. pinigo išleidimą, brokeris iš visų inkasacijos pranešimų pagal vartotojo identifikaciją V_{ID} išrenka mokėjimo pranešimus, suskaičiuoja kiekvieno vartotojo visą išleistą $VIS_2 = \Sigma(\Sigma^1_{i-n}... + ...\Sigma^1_{i-1} + \Sigma^{10}_{j-m}... + ...\Sigma^{10}_{j-1})$. Jei $VIS_1 < VIS_2$, aptinkamas dvigubas e. pinigo išleidimas.
- Vartotojo ir pardavėjo sąskaitų atnaujinimas. Brokeriui patikrinus inkasacijos pranešimus ir neaptikus pažeidimų atnaujinamos pardavėjo ir vartotojo sąskaitos.

Aptartas siūlomas ribotos sumos elektroninių pinigų cirkuliacijos sistemos modelis, protokolas ir jo etapai. Pateikta modelio architektūra, naudojami sutartiniai žymėjimai, duomenų srautai tarp modelio dalyvių.

2.4. Modelio analizė

Sudarytame modelyje vartotojas generuoja e. pinigus iš brokerio atsiųstų šakninių reikšmių ir juos panaudoja įsigyti prekėms iš pardavėjo. Kiekvieną e. pinigą pardavėjas patikrina ir grąžina brokeriui. Modelyje naudojami saugos mechanizmai remiasi maišos funkcijų generavimu ir elektroniniais parašais.

Pagrindinis šio modelio akcentas yra kuriamai e. pinigo vertei naudojamos dvi šakninės monetų reikšmės, dėl kurių sumažėja maišos funkcijų skaičiavimai lyginant su e. pinigo vertės generavimu, kai naudojama maišos funkcijų grandinėlė. Tai labiau turėtų būti pastebima kuriant didesnę e. pinigo vertę.

Išlaidų sumažinimui kiekvieno mokėjimo metu ir efektyvumo padidinimui siekiama sumažinti didelių skaičiavimų kiekį ir didesnius skaičiavimus atlikti atjungties režime.

Parašo schemos generavimui reikalingos didesnės laiko sąnaudos negu to reikalauja maišos funkcijos [15]. Todėl norint sumažinti viešo rakto operacijų skaičių dažnai naudojamos maišos funkcijos.

Vartotojui pirmą kartą nusiuntus pirkimo vykdymo pranešimą pardavėjas patikrina kartu gautą sertifikatą, užregistruoja jame esančias šaknines monetų reikšmes ir vartotojo identifikaciją. Todėl vykdant transakcijos etapą pardavėjas tikrina tik vartotojo e. parašą ant kiekvieno mokėjimo pranešimo ir iš naujo neverifikuoja brokerio e. parašo ant išduoto sertifikato. Tokiu būdu pasiekiama, kad per transakciją būtų vykdomas tik vienas e. parašo tikrinimas, išskyrus pirmą mokėjimą.

Mokėjimo operacijos vykdomos brokeriui nedalyvaujant, todėl sumažėja tiesioginio komunikavimo su serveriu (brokeriu) apkrovimas. Vartotojas susisiekia su brokeriu tik tada, kai baigia galioti senasis sertifikatas ir prašo išduoti naują. Žvelgiant iš pardavėjo pusės, jis taip pat nebendrauja su brokeriu realiuoju laiku vykdant transakcijas, o susisiekia tik įkeliant inkasacijos pranešimus.

Klastojimo prevencijai naudojamos maišos funkcijos yra vienkryptės ir atsparios kolizijoms, todėl neįmanoma sugeneruoti tokio paties e. pinigo. Maišos funkcijos užtikrina, kad niekas kitas išskyrus vartotoją negali sugeneruoti galiojantį e. pinigą. Be to, norint suklastoti e. pinigą reikia suklastoti ir brokerio e. parašą.

Apsaugai nuo išeikvojimo įvedamas išlaidų limitas, kuris nurodomas brokerio išduotame sertifikate. Išlaidų limito dydis nustatomas priklausomai nuo vartotojo sąskaitos balanso. Šis

apribojamas suteikia mažiau galimybių sukčiauti, kadangi negali būti vykdomi jokie pirkimai, jei vartotojo sąskaitoje nėra lėšų.

Kadangi brokeris tikrindamas išleistus e. pinigus apskaičiuoja visą vartotojo išleistą sumą, nesutapus pardavėjo atsiųstai reikšmei su brokerio apskaičiuota, fiksuojamas pažeidimas. Taip vykdoma dvigubo e. pinigo išleidimo prevencija leidžia apsisaugoti nuo vertės kopijavimo.

2.5. Išvados

Pasiūlytas ribotos sumos elektroninių pinigų cirkuliacijos sistemos modelis:

- Apibrėžti reikalavimai, keliami siūlomam modeliui.
- Modelis remiasi Payword mikromokėjimų sistemos koncepcija.
- Pateikta modelio architektūra, kurią sudaro sąveikaujantys dalyviai ir ryšiai tarp jų.
- Išdėstytas siūlomo modelio protokolas, jo vykdymo etapai.
- Saugumui realizuoti naudojamos maišos funkcijos ir e. parašai, kurie užtikrina perduodamos informacijos vientisumą, vartotojų autentiškumą.
- Sudarytame modelyje vykdoma e. pinigų dvigubo išleidimo ir klastojimo prevencija.
- Vartotojo anonimiškumo užtikrinimui tiek pardavėjo, tiek piktavalio atžvilgiu su kiekviena mokėjimo transakcija būtų galima keisti vartotojo identifikaciją (ID).

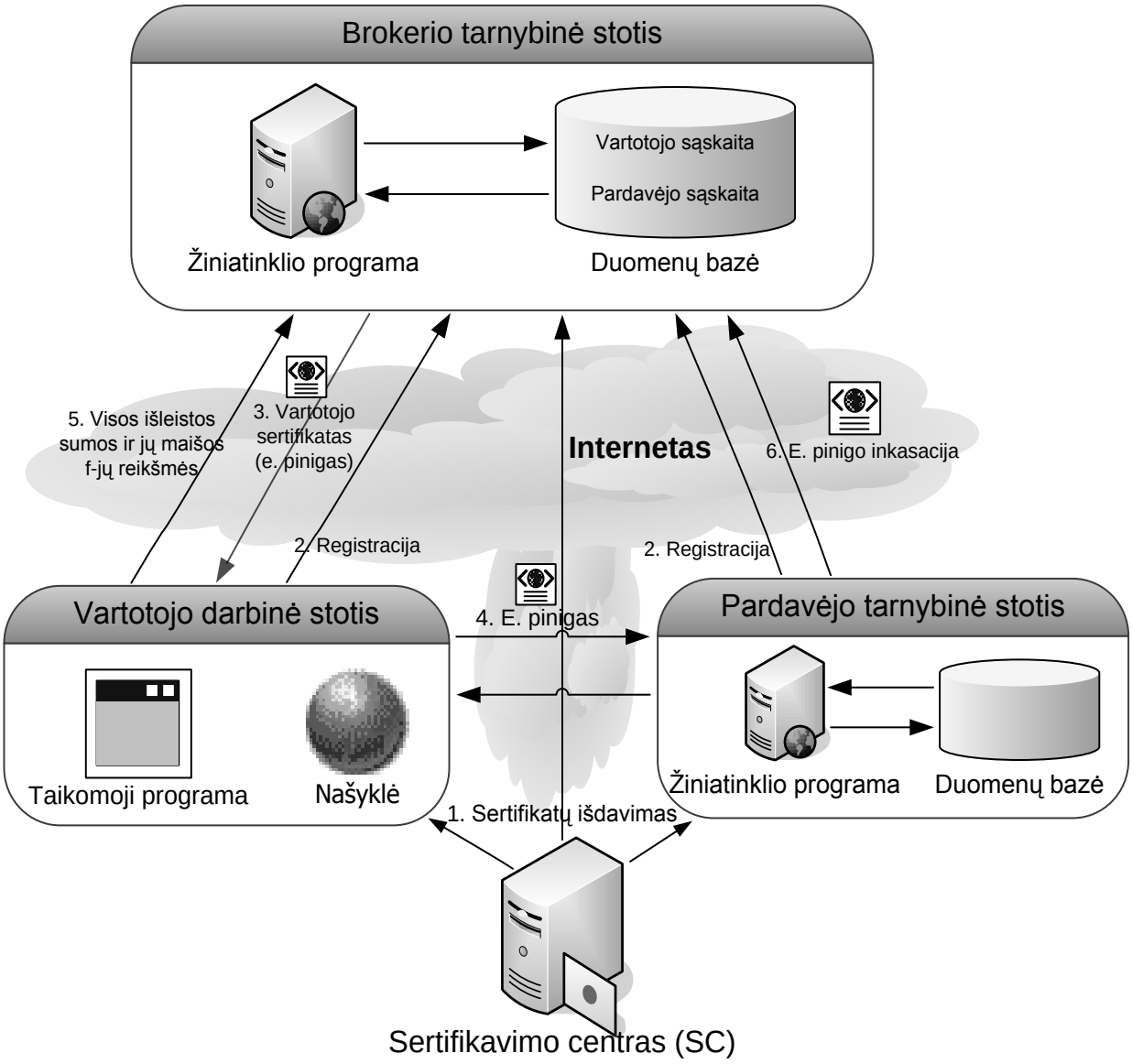
3. RIBOTOS SUMOS ELEKTRONINIŲ PINIGŲ CIRKULIACIJOS SISTEMOS PROJEKTAS

Šiame skyriuje pateikiamas ribotos sumos elektroninių pinigų cirkuliacijos sistemos projektas, sistemos konteksto schema, veikimo algoritmai ir reikalingos duomenų struktūros.

3.1. Sistemos konteksto schema

Sistemos konteksto schemą sudaro brokeris, pardavėjas ir vartotojas, kurie komunikuoja per interneto tinklą. Brokerio serveryje veikia žiniatinklio programa, kuri bendrauja su duomenų baze ir yra atsakinga už vartotojų ir pardavėjų aptarnavimą.

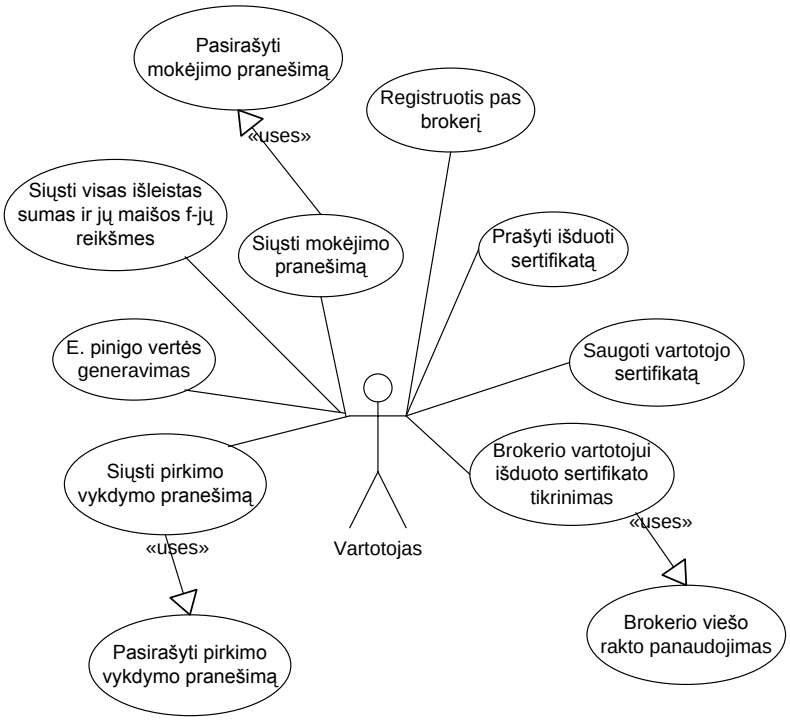
Vartotojo kompiuteryje veikia taikomoji programa skirta generuoti e. pinigą iš gautų šakninių reikšmių. Pardavėjo serveryje veikia žiniatinklio programa, kuri tikrina iš vartotojų gautus e. pinigus, renka informaciją apie pirkusius vartotojus ir saugo įrašus duomenų bazėje.



10 pav. Konteksto schema

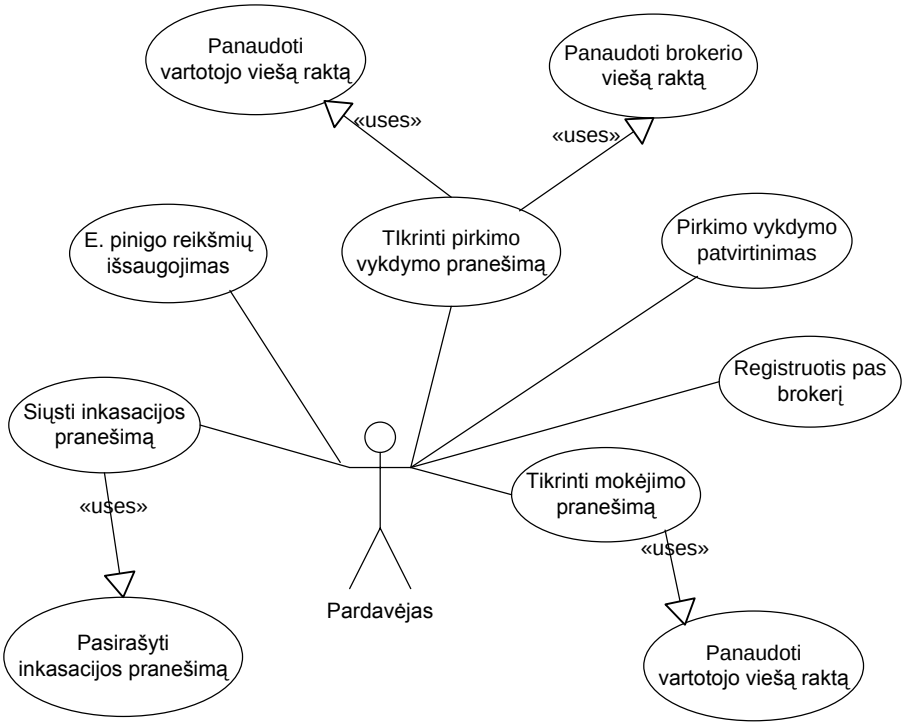
3.2. Panaudos atvejų diagramos

Sistemos panaudojimo atvejų diagramos pateiktos sekančiuose paveiksluose. Jose pavaizduoti sistemos aktoriai ir jų atliekamos funkcijos.



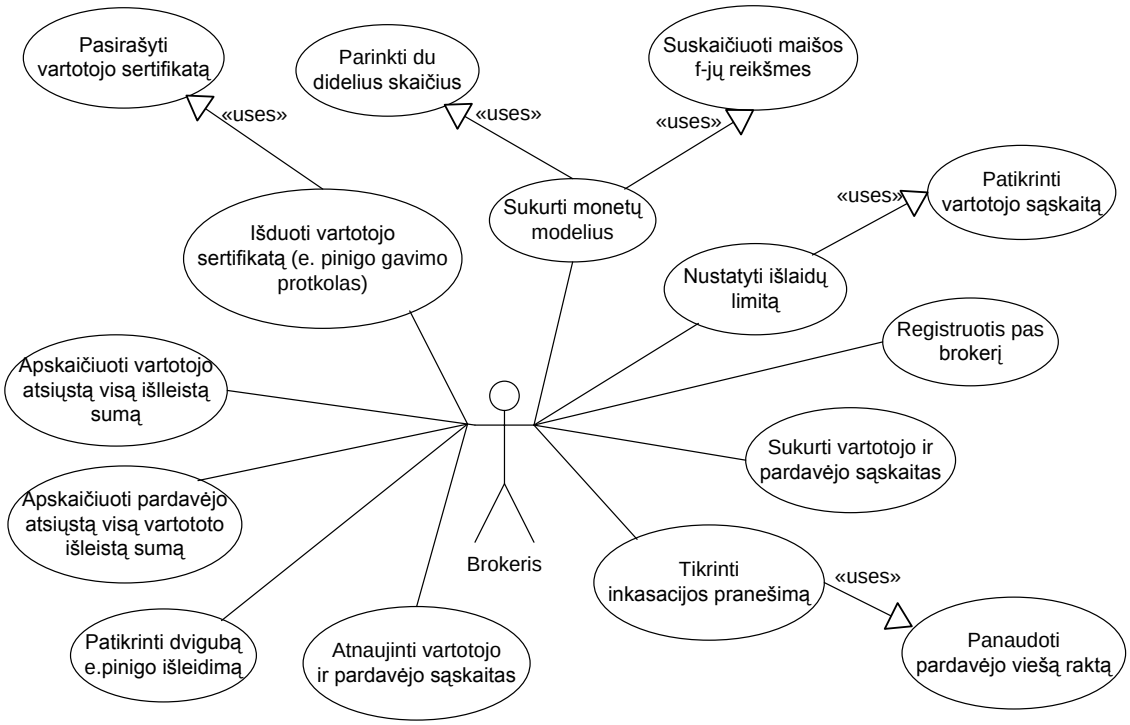
11 pav. Vartotojo panaudos atvejų diagrama

Vartotojas – tai sistemos dalyvis, kuris kreipiasis pas brokerį, prašo išduoti vartotojo sertifikatą, generuoja e. pinigo vertę, komunikuoja su pardavėju norėdamas atlikti pirkimą ir atsiskaito už prekes siųsdamas e. pinigą.



12 pav. Pardavėjo panaudos atvejų diagrama

Pardavėjo atliekami veiksmai pateikti 12 paveiksle. Pardavėjas – tai sistemos dalyvis, kuris turi savo sąskaitą pas brokerį, tikrina iš vartotojų gautus e. pinigus ir kreipiasi pas brokerį norėdamas įkelti turimus vartotojų mokėjimų pranešimus (e. pinigo inkasacija).

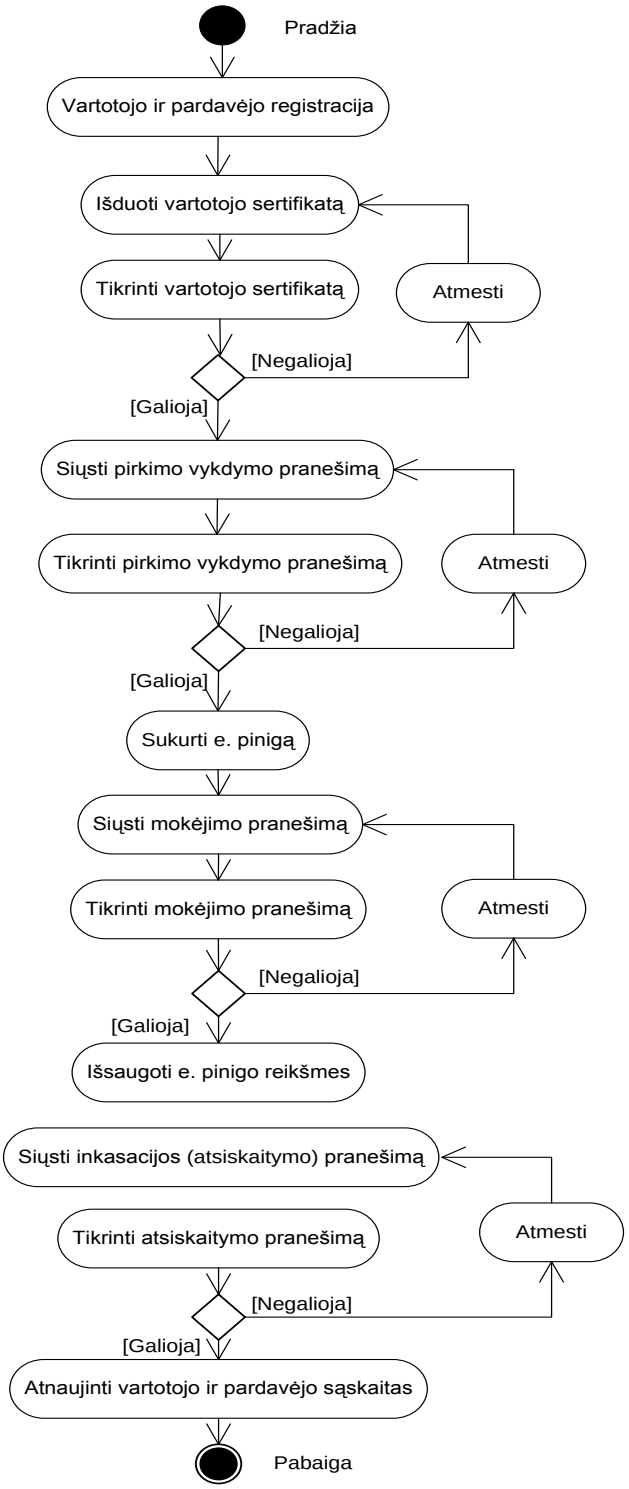


13 pav. Brokerio panaudos atvejų diagrama

Brokeris yra pagrindinis sistemos veikėjas. Jo atliekami veiksmai pavaizduoti 13 paveiksle. Jis atsakingas už vartotojų ir pardavėjų sąskaitų sukūrimą, vartotojų sertifikatų išdavimą, pradinės e. pinigo reikšmės sugeneravimą ir e. pinigo tikrumo patikrinimą, vartotojo ir pardavėjo sąskaitų atnaujinimą.

3.3. Veiklos diagramos

Veiklos diagramose galime matyti kokiu eiliškumu vyksta veiksmai ir kaip jie tarpusavyje susiję. Taip pat parodoma kokioje fizinėje aplinkoje atliekami veiksmai. Bendra sistemos veiklos diagrama pateikta sekančiame paveiksle.

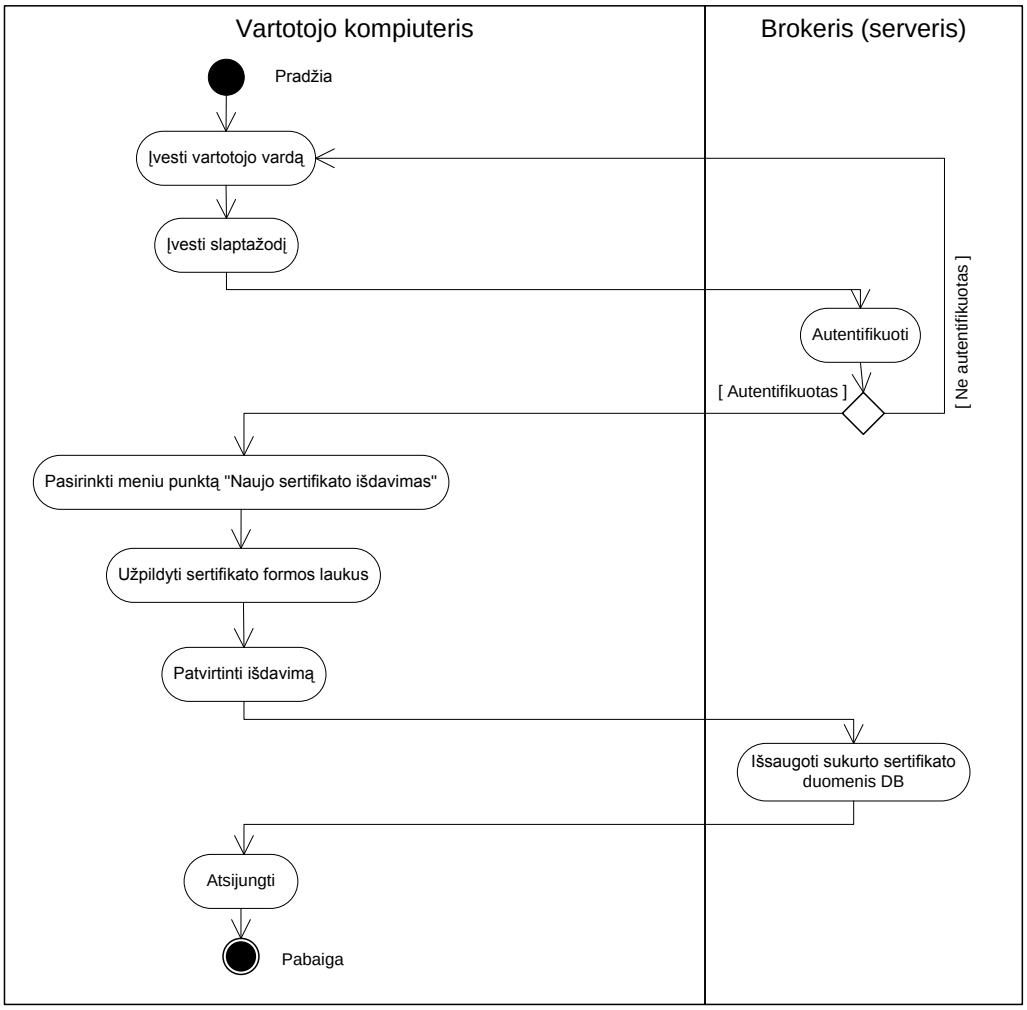


14 pav. Sistemos veiklos diagrama

Ši diagrama (14 pav.) skirta pavaizduoti, kokia tvarka vyksta vartotojo sertifikato išdavimas, kai vartotojas yra užsiregistravęs.

Kaip matome, iš pradžių vartotojas naršyklės pagalba turi prisijungti prie brokerio įvesdamas vartotojo vardą ir slaptažodį. Vartotojo autentifikacija atliekama brokerio serveryje.

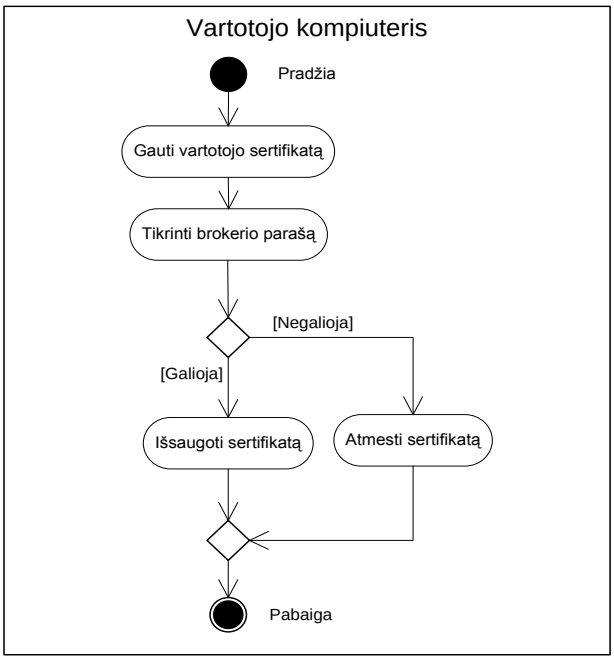
Kuomet vartotojas yra prisijungęs, jis užpildo sertifikato gavimui reikalingus formos laukus ir patvirtina sertifikato išdavimą. Duomenys apie išduotą sertifikatą išsaugomi brokerio duomenų bazėje.



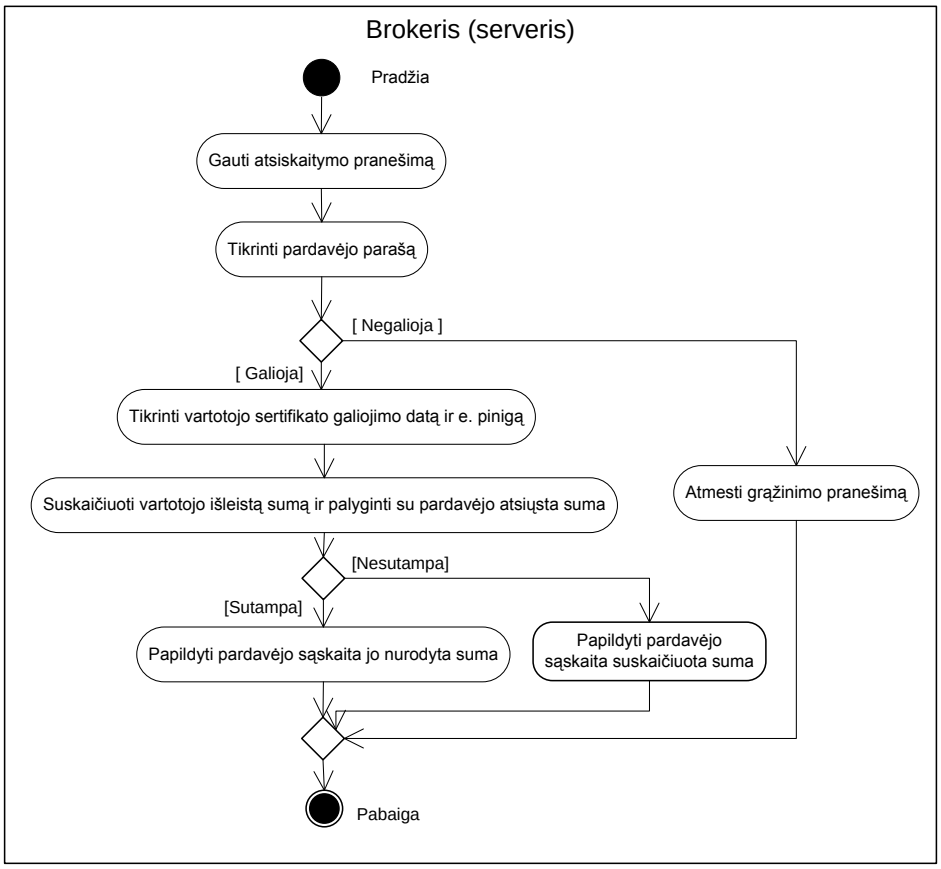
15 pav. Vartotojo sertifikato išdavimo veiklos diagrama

Vartotojui norint atlikti apmokėjimui reikalingą e. pinigo sukūrimą, jis pirma turi patikrinti iš brokerio gautą vartotojo sertifikatą (16 pav.).

Vykdant inkasacijos pranešimo tikrinimo procedūrą (17 pav.) iš pradžių patikrinamas pardavėjo e. parašas, toliau patikrinama pranešime esančio vartotojo sertifikato galiojimo data ir pats e. pinigas. Jei šie pranešimo parametrai pripažįstami galiojančiais, apskaičiuojama iš vartotojo gauta suma ir palyginama su pardavėjo atsiųsta. Jeigu sumos sutampa, pardavėjo sąskaita papildoma jo atsiųsta suma.



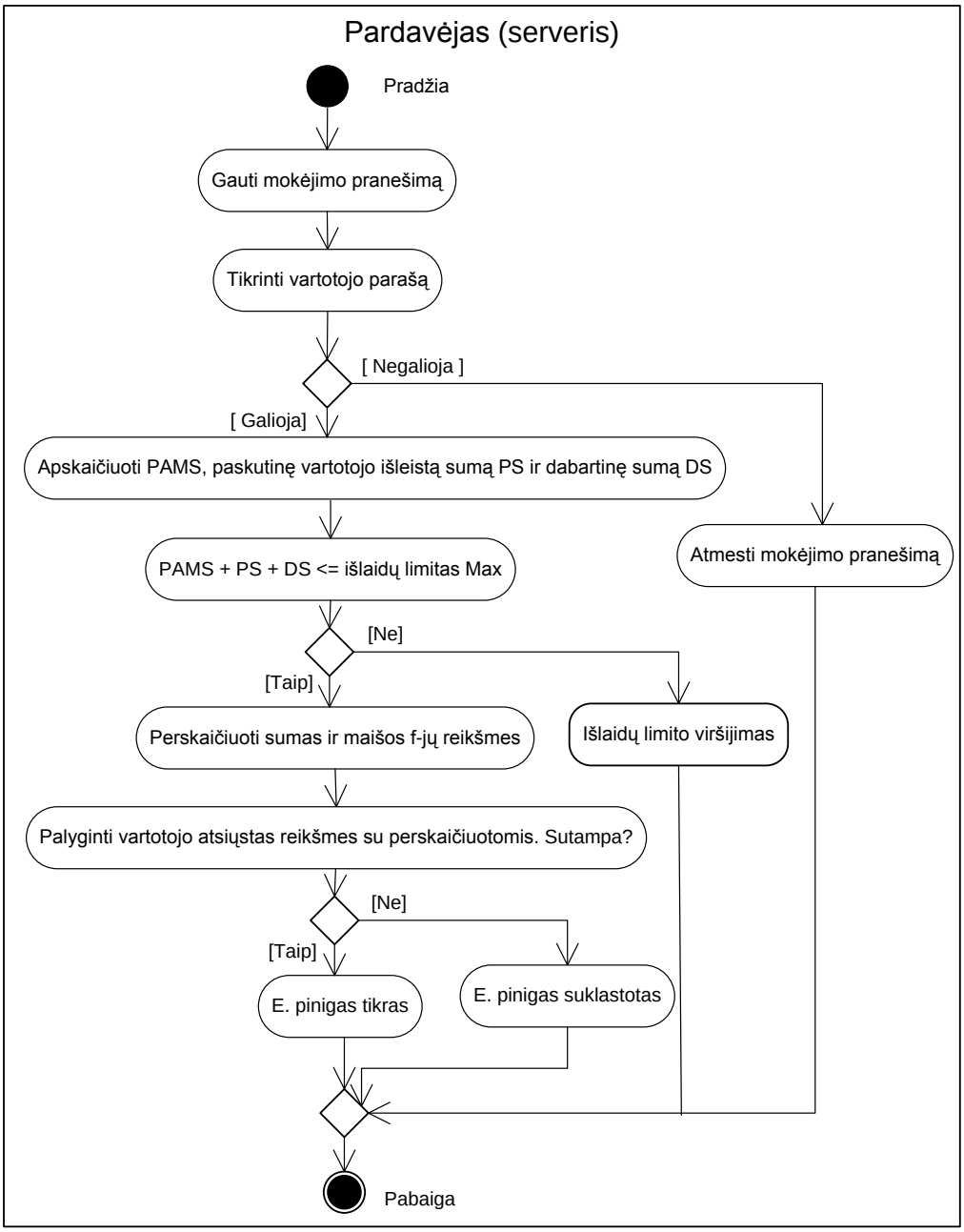
16 pav. Sertifikato tikrinimo veiklos diagrama



17 pav. Inkasacijos pranešimo veiklos diagrama

Iš pardavėjo brokeriui siunčiamas inkasacijos pranešimas yra skirtas vartotojų išleistų e. pinigų patikrinimui ir pardavėjo bei vartotojų sąskaitų balanso atnaujinimui (17 pav.).

Pardavėjui gavus vartotojo mokėjimo pranešimą yra vykdomas šio pranešimo tikrinimas, kurio algoritmo seka pateikta žemiau esančiame paveiksle.



18 pav. Mokėjimo pranešimo tikrinimo veiklos diagrama

Gavus mokėjimo pranešimą patikrinamas vartotojo e. parašas. Jeigu jis tikras, tuomet patikrinama, ar pranešime esanti prieš tai atliktų mokėjimų suma *PAMS*, apskaičiuota paskutinė vartotojo išleista suma PS ir dabartinė suma DS neviršija išlaidų limito Max. Neviršijus limito lyginamos vartotojo atsiųstos reikšmės su pardavėjo perskaičiuotomis. Joms sutapus e. pinigas laikomas tikru ir priimamas.

3.4. Pranešimų struktūros

Duomenų apsikeitimams tarp sistemos dalyvių naudojami XML formato pranešimai. Sekančiuose paveiksluose pateikiami šiuos pranešimus sudarantys duomenų laukai.

19 paveiksle matome brokerio išduotame sertifikate esančius duomenų laukus:

- B_{ID} – brokerio identifikacija
- V_{ID} – vartotojo identifikacija
- D_G – sertifikato galiojimo data
- C_0^1 – vieno cento vertės maišos funkcijos reikšmė
- C_0^{10} – dešimties centų vertės maišos funkcijos reikšmė
- Max – išleidžiamos sumos limitas
- H(Max) – išleidžiamos sumos limito maišos funkcijos reikšmė
- Brokerio e. parašo f-jos reikšmė – brokerio e. parašo funkcijos reikšmė visiems sertifikato laukams.

B_{ID}	V_{ID}	D_G	C_0^1	C_0^{10}	Max	Brokerio e. parašo f-jos reikšmė

19 pav. Vartotojo e. pinigo sertifikato duomenų laukai

Pirkimo vykdymo pranešimo struktūrą (20 pav.) sudaro tokie duomenų laukai:

- P_{ID} – pardavėjo identifikacija
- V_{ID} – vartotojo identifikacija
- S_B – brokerio išduoto sertifikato duomenys
- D – pirkimo data
- Vartotojo e. parašo f-jos reikšmė – vartotojo e. parašo funkcijos reikšmė visiems pirkimo vykdymo pranešimo laukams.

P_{ID}	V_{ID}	S_B	D	Vartotojo e. parašo f-jos reikšmė

20 pav. Pirkimo vykdymo pranešimo duomenų laukai

Mokėjimo pranešimą sudarantys duomenų laukai:

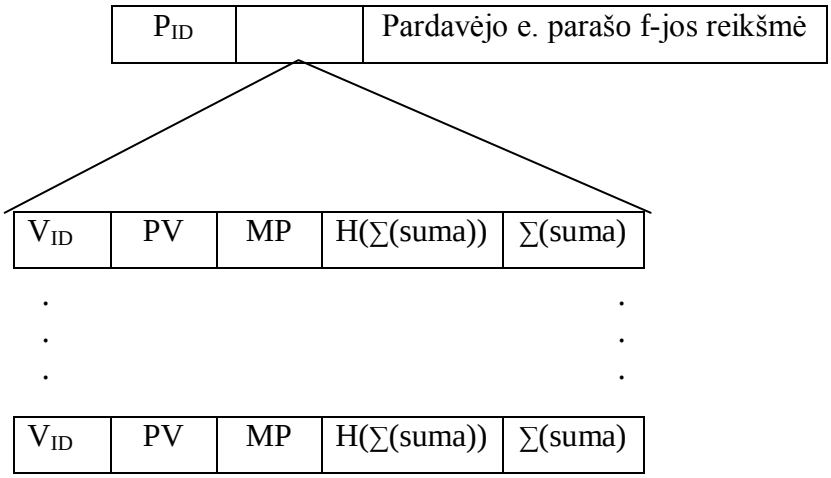
- V_{ID} – vartotojo identifikacija
- Σ_i^1 – iš vieno cento e. pinigo reikšmių sudaryta i-toji suma
- Σ_j^{10} – iš dešimties centų vertės e. pinigo reikšmių sudaryta j-toji suma
- h_j^1 – iš vieno cento vertės e. pinigo reikšmių sudarytos i-tosios sumos maišos funkcijos reikšmė
- h_j^{10} – iš dešimties centų vertės e. pinigo reikšmių sudarytos j-tosios sumos maišos funkcijos reikšmė
- n – vieno cento vertės e. pinigo reikšmės daugiklis
- m – dešimties centų vertės e. pinigo reikšmės daugiklis
- T – laiko žyma, kuri apsaugo nuo pakartotinio siuntimo
- PAMS – suma visų prieš tai atliktų mokėjimų
- H(PAMS) - suma visų prieš tai atliktų mokėjimų maišos funkcijos reikšmė
- Vartotojo e. parašo f-jos reikšmė – vartotojo e. parašo funkcijos reikšmė visiems mokėjimo pranešimo laukams.

V_{ID}	Σ_i^1	Σ_j^{10}	h_j^1	h_j^{10}	n	m	T	PAMS	H(PAMS)	Vartotojo e. parašo f-jos reikšmė

21 pav. Mokėjimo pranešimo duomenų laukai

Inkasacijos pranešimą sudarantys duomenų laukai:

- P_{ID} – pardavėjo identifikacija
- V_{ID} – vartotojo identifikacija
- PV – pirkimo vykdymo pranešimo duomenys
- MP – mokėjimo pranešimo duomenys
- ∑(suma) - visų vartotojo mokėjimų suma
- H(∑(suma)) - visų vartotojo mokėjimų sumos maišos funkcijos reikšmė
- Pardavėjo e. parašo f-jos reikšmė



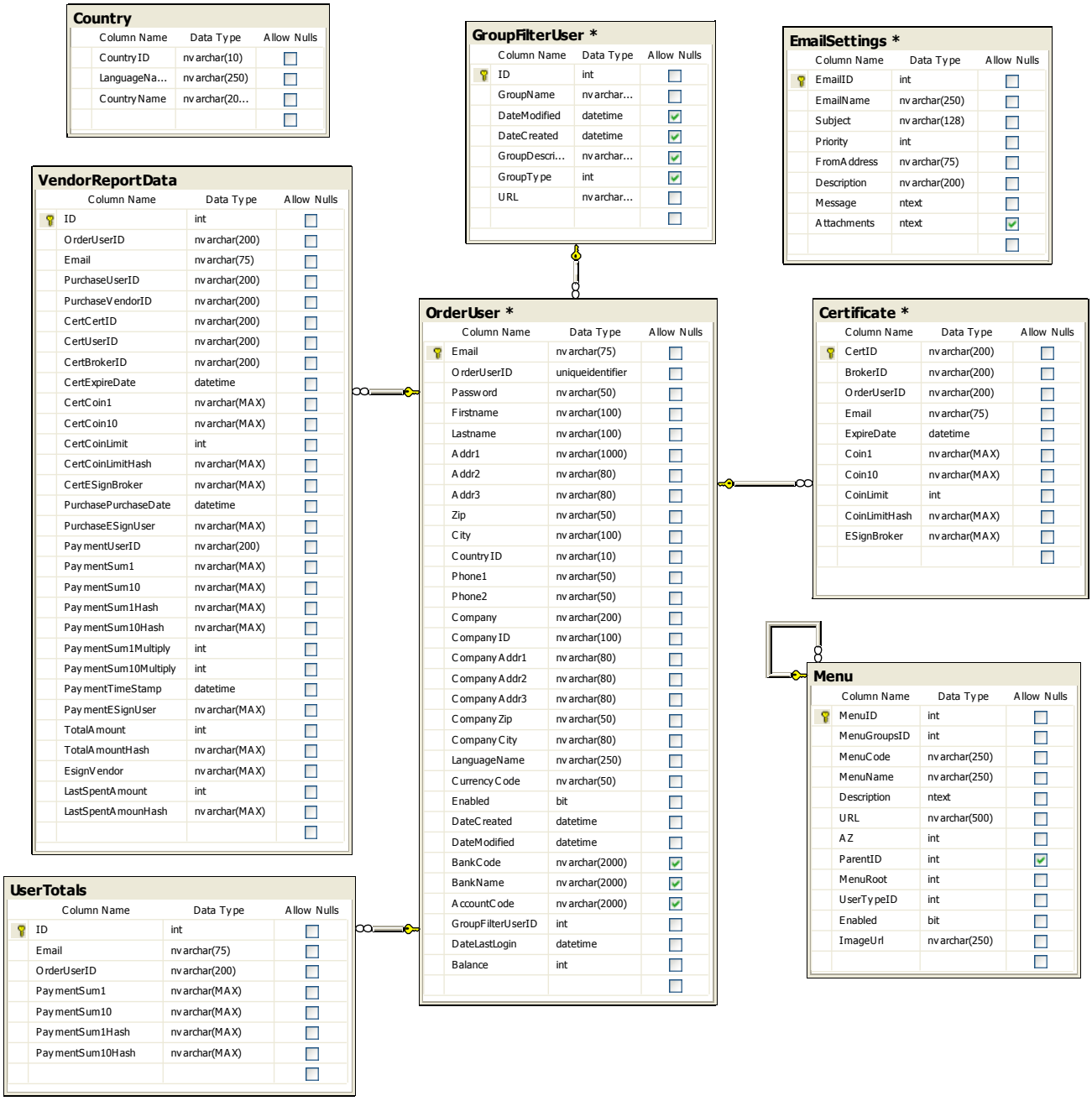
22 pav. Inkasacijos pranešimo duomenų laukai

3.5. Duomenų bazės loginė schema

Šiame skyriuje pateikiama brokerio duomenų bazės schema, skirta vartotojų informacijai saugoti. Taip pat nurodoma duomenų bazės lentelių paskirtis ir aprašymai.

3.5.1. Brokerio duomenų bazės schema

Pagrindiniams sistemos duomenims saugoti ir jais naudotis yra skirta 23 paveiksle pateikta duomenų bazė. Ši duomenų bazė veikia brokerio serveryje ir ja naudojasi žiniatinklio programa.



23 pav. Brokerio duomenų bazės schema

3.5.1.1. Duomenų bazės lentelių aprašymai

Šiame skyriuje pateikiami brokerio duomenų bazės lentelių aprašymai su trumpais paaiškinimais.

Lentelė „Country“. Šioje lentelėje saugoma informacija apie šalis įvairiomis kalbomis.

10 lentelė. „Country“ lentelės duomenų laukų aprašas

Lauko pavadinimas	Duomenų tipas(dydis)	Reikšmė pagal nutylėjimą	Komentaras
CountryID	nvarchar(10)		Raktas: šalies identifikatorius
LanguageName	nvarchar(250)	'LT'	Kalbos pavadinimas
CountryName	nvarchar(2000)		Šalies pavadinimas

Lentelė „EmailSettings“ skirta vartotojams siunčiamų elektroninio pašto laiškų informacijai saugoti. Elektroniniai laiškai vartotojams siunčiami jiems užsiregistravus sistemoje arba siunčiant slaptažodžio priminimą.

11 lentelė. „EmailSettings“ lentelės duomenų laukų aprašas

Lauko pavadinimas	Duomenų tipas(dydis)	Reikšmė pagal nutylėjimą	Komentaras
EmailID	int		Raktas: el. laiško identifikatorius
EmailName	nvarchar(250)		El. laiško pavadinimas
Subject	nvarchar(128)		El. laiško tema
Priority	int		Siuntimo prioritetas
FromAddress	nvarchar(75)		El. laiško siuntėjo e. pašto adresas
Description	nvarchar(200)	N''	El. laiško aprašymas
Message	ntext	N''	El. laiško turinys (žinutė)
Attachments	ntext	Galima palikti tuščią	Prisegti e. laiško failai

Lentelėje „GroupFilterUser“ saugoma vartotojų grupių informacija. Priklausomai nuo vartotojo grupės atidaromas skirtingas sistemos internetinis puslapis.

12 lentelė. „GroupFilterUser“ lentelės duomenų laukų aprašas

Lauko pavadinimas	Duomenų tipas(dydis)	Reikšmė pagal nutylėjimą	Komentaras
ID	int		Raktas: identifikatorius
GroupName	nvarchar(200)		Grupės pavadinimas
DateModified	datetime	getdate()	Įrašo keitimo data
DateCreated	datetime	getdate()	Įrašo sukūrimo data
GroupDescription	nvarchar(250)		Grupės aprašymas
GroupType	int	0	Grupės tipas
URL	nvarchar(500)	N''	Vartotojo nukreipimo URL adresas

Lentelėje „OrderUser“ saugoma sistemos vartotojų informacija. Joje saugoma registracijos metu vartotojo pateikti duomenys, kompanijos informacija, jei vartotojas registruojasi kaip pardavėjas, turimas sąskaitos balansas ir banko duomenys.

13 lentelė. „OrderUser“ lentelės duomenų laukų aprašas

Lauko pavadinimas	Duomenų tipas(dydis)	Reikšmė pagal nutylėjimą	Komentaras

Email	nvarchar(75)		Raktas: el. pašto adresas
OrderUserID	uniqueidentifier	newid()	Vartotojo identifikacija
Password	nvarchar(50)	N''	Vartotojo slaptažodis
Firstname	nvarchar(100)	N''	Vartotojo vardas
Lastname	nvarchar(100)	N''	Vartotojo pavardė
Addr1	nvarchar(1000)	N''	Vartotojo adresas (gatvė)
Addr2	nvarchar(80)	N''	Vartotojo adresas (namas)
Addr3	nvarchar(80)	N''	Vartotojo adresas (butas, jei yra)
Zip	nvarchar(50)	N''	Pašto kodas
City	nvarchar(100)	N''	Miestas
CountryID	nvarchar(10)	N''	Šalies identifikatorius
Phone1	nvarchar(50)	N''	Mobilus telefonas
Phone2	nvarchar(50)	N''	Telefonas
Company	nvarchar(200)	N''	Kompanija
CompanyID	nvarchar(100)	N''	Kompanijos identifikatorius
CompanyAddr1	nvarchar(80)	N''	Kompanijos adresas
CompanyAddr2	nvarchar(80)	N''	Kompanijos adresas
CompanyAddr3	nvarchar(80)	N''	Kompanijos adresas
CompanyZip	nvarchar(50)	N''	Kompanijos pašo kodas
CompanyCity	nvarchar(100)	N''	Miestas
LanguageName	nvarchar(250)	'LT'	Kalba
CurrencyCode	nvarchar(50)	'LTL'	Valiuta
Enabled	bit	1	Leisti vartotojui prisijungti
DateModified	datetime	getdate()	Įrašo keitimo data
DateCreated	datetime	getdate()	Įrašo sukūrimo data
BankCode	nvarchar(2000)	NULL	Banko kodas
BankName	nvarchar(2000)	NULL	Banko pavadinimas
AccountCode	nvarchar(2000)	NULL	Sąskaitos kodas
GroupFilterUserID	int	0	Vartotojų grupės identifikatorius
DateLastLogin	datetime	getdate()	Paskutinė prisijungimo data
Balance	nvarchar(500)	0	Vartotojo sąskaitos likutis

Lentelėje „UserTotals“saugomos vartotojų išleistos sumos ir jų maišos funkcijų reikšmės.

14 lentelė. „UserTotals“ lentelės duomenų laukų aprašas

Lauko pavadinimas	**Duomenų tipas(dydis)**	**Reikšmė pagal nutylėjimą**	**Komentaras**
ID	int		Raktas: identifikatorius
Email	nvarchar(75)		El. pašto adresas
OrderUserID	nvarchar(200)		Vartotojo identifikacija
PaymentSum1	nvarchar(MAX)	N''	Vartotojo išleistų vieno cento verčių suma
PaymentSum10	nvarchar(MAX)	N''	Vartotojo išleistų dešimties centų verčių suma
PaymentSum1Hash	nvarchar(MAX)	N''	Vartotojo išleistų vieno cento verčių sumos maišos funkcijos reikšmė
PaymentSum10Hash	nvarchar(MAX)	N''	Vartotojo išleistų dešimties centų verčių sumos maišos funkcijos reikšmė

Lentelė „VendorReportData“ skirta pardavėjų inkasacijos pranešimų laukams saugoti.

15 lentelė. „VendorReportData“ lentelės duomenų laukų aprašas

Lauko pavadinimas	**Duomenų tipas(dydis)**	**Reikšmė pagal nutylėjimą**	**Komentaras**
ID	int		Raktas: identifikatorius
OrderUserID	nvarchar(200)		Vartotojo identifikacija

Email	nvarchar(75)		El. pašto adresas
PurchaseUserID	nvarchar(200)		Pirkimo pranešimo vartotojo identifikacija
PurchaseVendorID	nvarchar(200)		Pirkimo pranešimo pardavėjo identifikacija
CertCertID	nvarchar(200)		Sertifikato identifikacija
CertUserID	nvarchar(200)		Išduoto sertifikato vartotojo identifikacija
CertBrokerID	nvarchar(200)		Išduoto sertifikato brokerio identifikacija
CertExpireDate	datetime		Sertifikato galiojima data
CertCoin1	nvarchar(MAX)		Vieno cento vertės maišos funkcijos reikšmė
CertCoin10	nvarchar(MAX)		Dešimties centų vertės maišos funkcijos reikšmė
CertCoinLimit	int		Išlaidų sumos limitas (centais)
CertCoinLimitHash	nvarchar(MAX)		Išlaidų sumos limito maišos funkcijos reikšmė
CertESignBroker	nvarchar(MAX)		Brokerio e. parašo reikšmė išduotam sertifikatui
PurchasePurchaseDate	datetime		Atlikto pirkimo data
PurchaseESignUser	nvarchar(MAX)		Vartotojo e. parašo reikšmė pirkimo pranešimui
PaymentUserID	nvarchar(200)		Mokėjimo pranešimo vartotojo identifikacija
PaymentSum1	nvarchar(MAX)		Vieno cento verčių suma
PaymentSum10	nvarchar(MAX)		Dešimties centų verčių suma
PaymentSum1Hash	nvarchar(MAX)		Vieno cento verčių sumos maišos funkcijos reikšmė
PaymentSum10Hash	nvarchar(MAX)		Dešimties centų verčių sumos maišos funkcijos reikšmė
PaymentSum1Multiply	int	1	Vieno cento vertės daugiklis
PaymentSum10Multiply	int	1	Dešimties centų vertės daugiklis
PaymentTimeStamp	datetime		Mokėjimo data (laiko žymė)
PaymentESignUser	nvarchar(MAX)		Vartotojo e. parašo reikšmė mokėjimo pranešimui
TotalAmount	int	0	Vartotojo išlaidų suma
TotalAmountHash	nvarchar(MAX)		Vartotojo išlaidų sumos maišos funkcijos reikšmė
EsignVendor	nvarchar(MAX)		Pardavėjo e. parašo reikšmė inkasacijos pranešimui
LastSpentAmount	int	0	Suma visų prieš tai atliktų mokėjimų
LastSpentAmounHash	nvarchar(MAX)		Visų prieš tai atliktų mokėjimų maišos f-s reikšmė

Lentelėje „Certificate“ saugoma vartotojams išduotų sertifikatų duomenys.

16 lentelė. „Certificate“ lentelės duomenų laukų aprašas

Lauko pavadinimas	Duomenų tipas(dydis)	Reikšmė pagal nutylėjimą	Komentaras
CertID	uniqueidentifier	newid()	Raktas: sertifikato identifikacija
BrokerID	nvarchar(200)		Išduoto sertifikato brokerio identifikacija
OrderUserID	nvarchar(200)		Vartotojo identifikacija
Email	nvarchar(75)		El. pašto adresas
ExpireDate	datetime		Sertifikato galiojima data
Coin1	nvarchar(MAX)		Vieno cento vertės maišos funkcijos reikšmė
Coin10	nvarchar(MAX)		Dešimties centų vertės maišos funkcijos reikšmė
CoinLimit	int		Išlaidų sumos limitas (centais)
CoinLimitHash	nvarchar(MAX)		Išlaidų sumos limito maišos funkcijos reikšmė
ESignBroker	nvarchar(MAX)		Brokerio e. parašo reikšmė išduotam sertifikatui

Lentelė „Menu“ skirta sistemos internetinės dalies meniu pasirinkų laukams saugoti.

17 lentelė. „Menu“ lentelės duomenų laukų aprašas

Lauko pavadinimas	Duomenų tipas(dydis)	Reikšmė pagal nutylėjimą	Komentaras
MenuID	int		Raktas: menu identifikatorius
MenuGroupsID	int		Meniu grupės identifiakcija

MenuCode	nvarchar(250)	N''	Meniu kodas
MenuName	nvarchar(250)		Meniu pavadinimas
Description	ntext	N''	Meniu aprašymas
URL	nvarchar(500)	N''	Puslapio nukreipimo adresas
AZ	int	0	Rikiavimas
ParentID	int		Šakniniam meniu priklausantys mazgai
MenuRoot	int	0	Tėviniai mazgai
UserTypeID	int	1	Vartotojo tipo identifikacija
Enabled	bit	1	Rodyti meniu mazgą
ImageUrl	nvarchar(250)	N''	Paveiksliuko adresas

3.6. Išvados

Atlikti darbai:

- Nurodyti ribotos sumos elektroninių pinigų cirkuliacijos sistemos dalyviai, išdėstytos kiekvieno jų atliekamos funkcijos.
- Pateikti esminiai sistemos veikimo algoritmai, atliekant sertifikato išdavimo, tikrinimo, mokėjimo ir inkasacijos pranešimų tikrinimo veiksmus.
- Apibrėžti sistemos dalyvių siunčiamus pranešimus sudarantys duomenų laukai.
- Suprojektuota brokerio duomenų bazė, skirta vartotojų informacijai saugoti.

4. RIBOTOS SUMOS ELEKTRONINIŲ PINIGŲ CIRKULIACIJOS SISTEMOS PROTOTIPO REALIZAVIMAS IR TYRIMAS

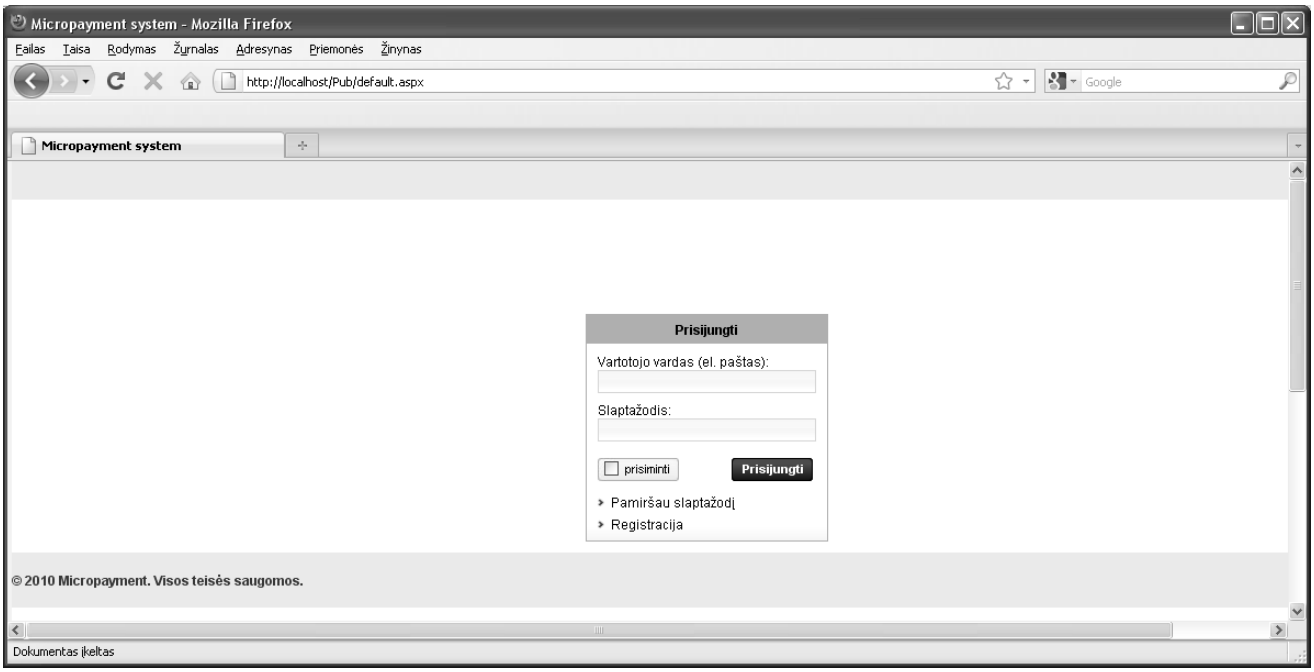
Šiame skyriuje aprašomas ribotos sumos elektroninių pinigų cirkuliacijos sistemos prototipo realizavimas ir tyrimas. Aptariami realizacijai naudoti programavimo įrankiai, pateikiami atliktos realizacijos ekranų vaizdai bei tyrimo rezultatai.

4.1. Sistemos prototipo realizavimo įrankiai ir realizacijos pavyzdžiai

Sistemos prototipo realizacijai įgyvendinti naudojami Microsoft Visual Studio 2005 ir Microsoft SQL Server 2008 programiniai paketai.

Viena iš sistemos prototipo dalių yra brokerio vaidmenį atliekanti žiniatinklio programa (angl. web application). Jos veikimui serveryje yra įdiegiama IIS (angl. Internet Information Services) žiniatinklio serveris ir .NET karkasas (angl. .NET Framework).

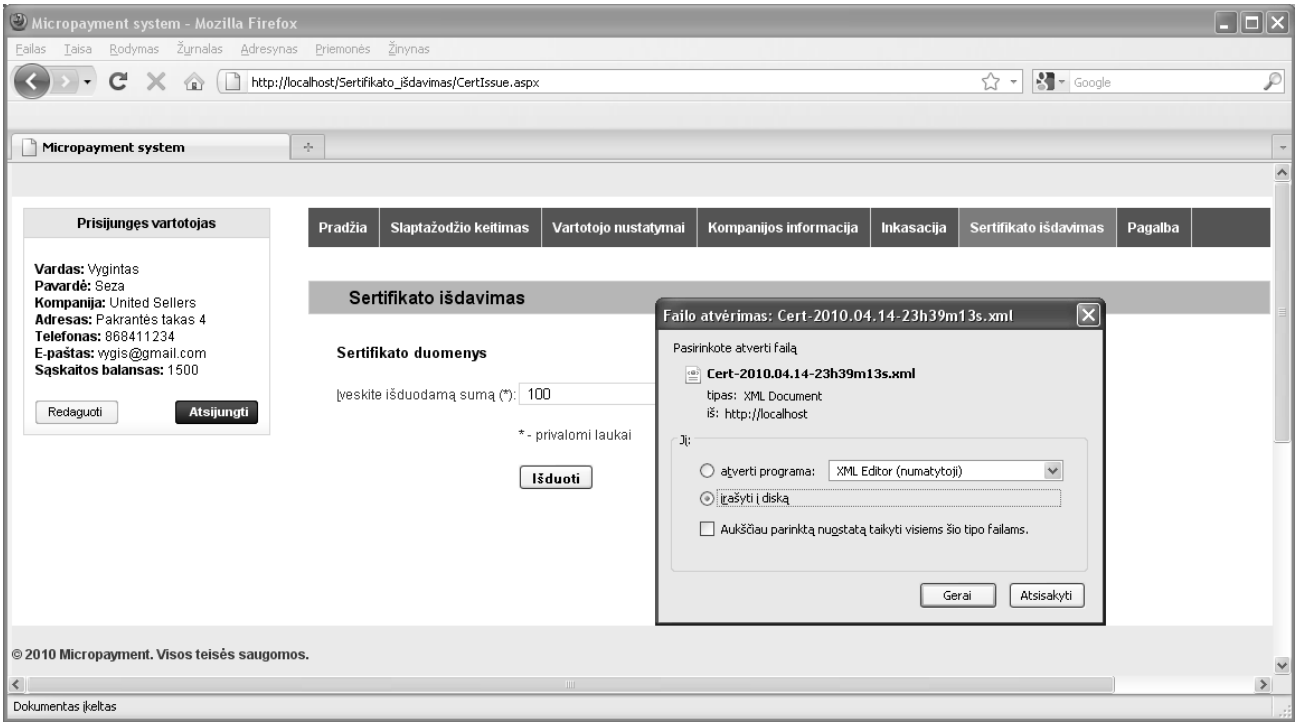
Norint prisijungti prie sistemos reikia įvesti vartotojo vardą ir slaptažodį į prisijungimo laukus. Brokerio internetinės programos prisijungimo langas pateiktas žemiau.



24 pav. Prisijungimo prie brokerio langas

Gauti prisijungimo duomenis galima registruojantis. Registracijos metu vartotojas užpildo būtinus laukus, tame tarpe įvedamas ir vartotojo prisijungimo vardas bei slaptažodis. Vartotojo registracijos forma iškviečiama paspaudus ant nuorodos „Registracija“. Tam panaudojamas „javascript“, kuris iškviečia „DevExpress ASPxPopupControl“ komponento iškylantį langą (angl. popup window). Jei vartotojas pamiršo slaptažodį, galima pasinaudoti slaptažodžio priminimo galimybe. Slaptažodis bus nusiųstas vartotojui elektroniniu paštu, kuris jį įveda į „DevExpress ASPxPopupControl“ komponento iškylantį langą.

Prisijungęs vartotojas turi teisę atlikti tam tikrus veiksmus sistemoje, tokius kaip savo informacijos keitimas, e. pinigo sertifikato išdavimas ar inkasacijos pranešimo įkėlimas. Prieš atliekant internetinį pirkimą, vartotojas privalo turėti brokerio išduotą e. pinigo sertifikatą. Sertifikato gavimui vartotojui sąskaitoje būtina turėti tam tikrą pinigų sumą. Prieš išduodant sertifikatą vartotojas turi įvesti pageidajamą gauti sumą (neviršijančią jo sąskaitos balanso), kuri bus išsaugota sertifikate. Paspaudus mygtuką „Išduoti“, patikrinama įvesta suma ir, jei viskas tvarkoje, leidžiama išsaugoti sertifikato failą XML formatu (25 pav.).



25 pav. E. pinigo sertifikato išdavimo langas

Sertifikato kūrimui naudojama *System.Xml* ir *System.Security.Cryptography* vardų srities (angl. namespace) iš .NET karkaso klasių bibliotekos. Kiekvienas sertifikatas turi unikalią identifikaciją „cert_id“, kuriai sukurti panaudojama *System.Guid* struktūra. Į sertifikatą patalpinama prisijungusio vartotojo unikali identifikacija ir brokerio identifikacija. Šakninės vieno ir dešimties centų vertės maišos funkcijų reikšmės sukuriamos *Random.Next* metodu sugeneruojant atsitiktinį didelį skaičių ir jį panaudojant *ComputeHash* metodui. Kadangi šakninės vertės yra maišos funkcijos reikšmės pavidalu, o ne įprastu skaičiumi, užtikrinamas didesnis saugumas.

Visi e. pinigo sertifikato laukai pasirašomi e. parašo reikšmę įterpiant į patį e. pinigo sertifikatą. Pasirašymui atlikti reikia iš sertifikatų saugyklos išgauti sertifikatą. Tam naudojama *X509Store* klasė, kurios pagalba iš visų saugykloje esančių sertifikatų pagal sertifikato *Thumbprint* atrenkamas pasirašymui reikalingas sertifikatas. Iš rasto sertifikato paimamas jame saugomas brokerio privatus raktas, kuris panaudojamas XML dokumento pasirašymui. Jeigu privatus raktas apsaugotas slaptažodžiu, pasirašymo metu bus paprašyta jį suvesti. Vartotojui išduotas e. pinigo sertifikatas pateiktas 26 paveiksle, kuriame matome tokius laukus kaip vartotojo identifikacija „user_id“, brokerio identifikacija „broker_id“, sertifikato galiojimo data „expire_date“, sukurtos vieno ir dešimties centų vertės šakninės reikšmės „coin_1“ „coin_10“,

išlaidų limitas „coin_limit“, išlaidų limito maišos funkcijos reikšmė „coin_limit_hash“ ir e. parašą sudaranti struktūra „Signature“.

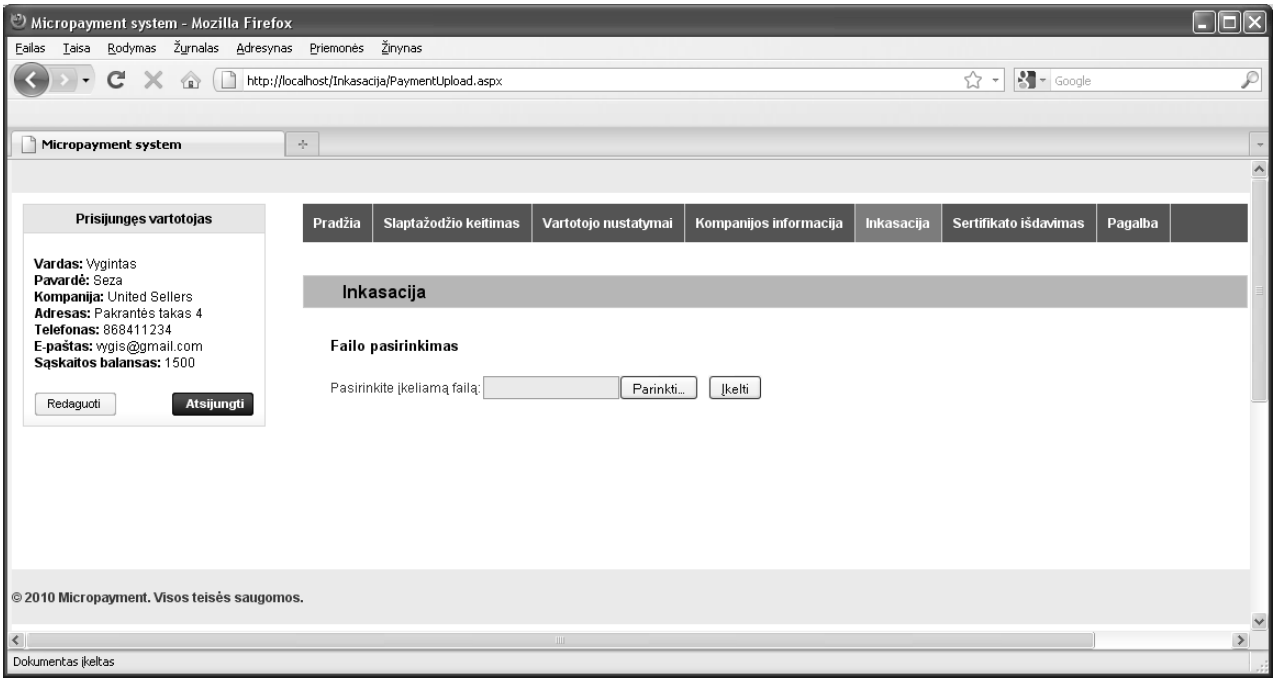
```
<?xml version="1.0" encoding="UTF-8"?>
<cert cert_id="f953c763-7462-4409-bb01-18f88f8e71a2">
  <user_id>4e13b5f4-d59d-49c7-8d54-9f09d4e0f1a7</user_id>
  <broker_id>BR-34bc90a5-7284-4513-92cf-740d443cd5a7</broker_id>
  <expire_date>2010.04.02 18:52:38</expire_date>
  <coin_1>6A701014AB7412272B96E09B8B1A6EFC7B226377</coin_1>
  <coin_10>133F7D667E571451C597098DD647DD39543A64A1</coin_10>
  <coin_limit>323</coin_limit>
  <coin_limit_hash>CB4DD52770E258826C4174C36202B18F649E262F</coin_limit_hash>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>WvQtRBnoSaYMkzk+HwuKksarn8o=</DigestValue>
      </Reference>
    </SignedInfo>
<SignatureValue>VnXdK+eHZWF5LEgOyM9ZzHOcHqxPdpiBKeR7ad4cr/1Z1LvMXRJwjdQJ+JAcbQOXoogrJ/AupE
HQhd5nWtlLEKNHo4HQtuIwutThPLCGljQGBsXwEVj9oXm9PZSI7HixZySPau2u1ig1tDSTnx4YILoQ8//eYsDx7TWx
gLomOSs=</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509IssuerSerial>
          <X509IssuerName>E=cert@ca.ktu.lt, CN=CERT CA 3, OU=Sertifikavimo centras,
O=Kauno technologijos universitetas, C=LT</X509IssuerName>
          <X509SerialNumber>5</X509SerialNumber>
        </X509IssuerSerial>
        <X509SubjectName>SERIALNUMBER=11223, E=brokeris@brokeris.lt, CN=Brokeris,
C=LT</X509SubjectName>
      </X509Data>
    </KeyInfo>
  </Signature>
</cert>
```

26 pav. Sukurto e. pinigo sertifikato turinys

Problemų pasirašymo metu iškyla dėl ASP.NET programos proceso (angl. worker process) teisių prieiti prie „Current User“ sertifikatų saugyklos, nes šis procesas veikia naudodamas ASPNET sąskaitą (angl. account), todėl negali pasiekti šios saugyklos. Norint pasinaudoti sertifikatais juos reikia perkelti iš „Current User“ saugyklos į „Local Machine“.

Pardavėjo surinkti vartotojų mokėjimai patalpinami į inkasacijos pranešimą, kurį pardavėjui prisijungus prie sistemos leidžiam įkelti nurodant jo buvimo vietą (27 pav.). Įkėlus pranešimą, patikrinamas pardavėjo e. parašas, patikrinami vartotojų e. parašai ant kiekvieno pirkimo vykdymo ir mokėjimo pranešimų ir perskaičiuojamos vartotojų sumokėtos e. pinigo

vertės.



27 pav. Inkasacijos pranešimų įkėlimo langas

Vartotojo e. pinigo generavimui skirta jo kompiuteryje veikianti taikomoji programa (28 pav.). Prisijungti prie programos galima įvedus registracijos pas brokerį metu pateiktus prisijungimo duomenis. Prisijungus leidžiama formuoti pirkimo vykdymo pranešimą, prieš tai pateikus galiojantį e. pinigo sertifikatą. Vartotojas pats nurodo pranešimo saugojimo vietą failų sistemoje.

28 pav. Pirkimo pranešimų formavimas

Į suformuotą pirkimo vykdymo pranešimo struktūrą (29 pav.) įtraukiamas vartotojo pateiktas e. pinigo sertifikatas „cert“, vartotojo ir pardavėjo identifikacijos „user_id“, „vendor_id“, pirkimo data „purchase_date“ ir vartoto e. parašas „e_sign_user“.

```
<?xml version="1.0" encoding="UTF-8"?>
<purchase_com>
  <cert cert_id="816e1dc5-7263-4a8d-8750-b4cf08e0b082">
  <user_id>4e13b5f4-d59d-49c7-8d54-9f09d4e0f1a7</user_id>
  <broker_id>BR-34bc90a5-7284-4513-92cf-740d443cd5a7</broker_id>
  <expire_date>2010.04.21 19:57:10</expire_date>
  <coin_1>770C69A14B632A288789D78100535707AE0483B8</coin_1>
  <coin_10>2F3250949A30FE182C9D81DFAD06ABC33D1C6E0D</coin_10>
  <coin_limit>232</coin_limit>
  <coin_limit_hash>4F0F5C96CA8457CCD84C30F91C0555BD7E615C81</coin_limit_hash>
  <e_sign_broker>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         .........
      </SignedInfo>
<SignatureValue>b6MAF0Ra5D+PaY44zOMNnnLFWdz5P+AYMqC5BH9ZiEnf6azgoTexTImuH35/Gn6kQupQnGz0qo
BkzqicFJHuwPN6l18FICBqEURw2lDBHOosQ1BBtjM3AdOrvhxEP8UJNNwpYlOq/L9m1QCDXL/V2AgzQ/kArq2tkgEA
oTlndWI=</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509IssuerSerial>
            <X509IssuerName>E=cert@ca.ktu.lt, CN=CERT CA 3, OU=Sertifikavimo centras,
O=Kauno technologijos universitetas, C=LT</X509IssuerName>
            <X509SerialNumber>5</X509SerialNumber>
          </X509IssuerSerial>
          <X509SubjectName>SERIALNUMBER=11223, E=brokeris@brokeris.lt, CN=Brokeris,
C=LT</X509SubjectName>
        </X509Data>
      </KeyInfo>
    </Signature>
  </e_sign_broker>
</cert>
  <user_id>4e13b5f4-d59d-49c7-8d54-9f09d4e0f1a7</user_id>
  <vendor_id>AB7412272B96E09B8B1A6EFC7B</vendor_id>
  <purchase_date>2010.04.20 15:24:07</purchase_date>
  <e_sign_user>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        .........
      </SignedInfo>
<SignatureValue>JjauNQ51Bk8Zt3mWi4H28sxGxPxqKKwij7BnTbR3VXCc1hbyZ9JBqKE4DAI3YrZyW0aZ90x0/B
65TETRR8b5p6jS+Ba6H+UIEcZ2zjooQ4wao9EEbn4l4fD6f1WcrL8O0iPZ45kpSYYOuiEeLgR5uIqTeQ8/mt+OZdMT
eUcQESc=</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509IssuerSerial>
            <X509IssuerName>E=cert@ca.ktu.lt, CN=CERT CA 3, OU=Sertifikavimo centras,
O=Kauno technologijos universitetas, C=LT</X509IssuerName>
            <X509SerialNumber>4</X509SerialNumber>
          </X509IssuerSerial>
          <X509SubjectName>SERIALNUMBER=83467, E=vygintas.seza@stud.ktu.lt, CN=Vygintas
Seza, G=Seza, SN=Vygintas, C=LT</X509SubjectName>
        </X509Data>
      </KeyInfo>
    </Signature>
  </e_sign_user>
</purchase_com>
```

29 pav. Sukurto pirkimo pranešimo turinys

Kuomet vartotojas pardavėjui pateikia pirkimo vykdymo pranešimą, toliau formuojamas mokėjimo pranešimas. Tam vartotojas įveda pageidaujamą sumą, neviršijančią e. pinigo sertifikate esančio išlaidų limito, ir spaudžia formavimo mygtuką. Žemiau pateiktame sukurtame mokėjimo pranešime saugoma vartotojo identifikacija, suformuotos sumos, jų maišos reikšmės, daugikliai, laiko žymė ir vartotojo e. parašas.

```
<?xml version="1.0" encoding="UTF-8"?>
<payment>
  <user_id>4e13b5f4-d59d-49c7-8d54-9f09d4e0f1a7</user_id>
  <sum_1>3538080A5587412272B96E09B8B1A6EFC7B226377</sum_1>
  <sum_1>603D730076571451C597098DD647DD39543A64A1</sum_1>
  <hash_sum_1>5980F5122141893476405701A6EFDF72D8077CA1</hash_sum_1>
  <hash_sum_10>84A0F169A1E751CFA2C58967C75DC71F79994D12</hash_sum_10>
  <sum_1_multiply>8</sum_1_multiply>
  <sum_10_multiply>5</sum_10_multiply>
  <time_stamp>2010.04.20 20:05:22</time_stamp>
  <e_sign_user>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
     <SignedInfo>
     <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <Reference URI="">
          <Transforms>
            <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          </Transforms>
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <DigestValue>fYNBUmRsQJBLTrr0omAMqLBxdm0=</DigestValue>
        </Reference>
      </SignedInfo>
<SignatureValue>jFrwD81UR2XXCcZ8uFnpMtDoQSkjGvT+EiCjHczWuM30XK1yBJB4x8dQlfqGE/C/f+If8eIIXfx
kj0CQWqbvxPjwYrRwHpSLjRyk/3uk9pPKAzy8MoTdp08AoZAvXPL3lw2ema7gukP5FfNBkSzKwXfbGrFV3cisk+A/zs
0KgFo=</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509IssuerSerial>
            <X509IssuerName>E=cert@ca.ktu.lt, CN=CERT CA 3, OU=Sertifikavimo centras,
O=Kauno technologijos universitetas, C=LT</X509IssuerName>
            <X509SerialNumber>4</X509SerialNumber>
          </X509IssuerSerial>
          <X509SubjectName>SERIALNUMBER=83467, E=vygintas.seza@stud.ktu.lt, CN=Vygintas
Seza, G=Seza, SN=Vygintas, C=LT</X509SubjectName>
        </X509Data>
      </KeyInfo>
    </Signature>
  </e_sign_user>
</payment>
```

30 pav. Sukurto mokėjimo pranešimo turinys

4.2. Ribotos sumos elektroninių pinigų cirkuliacijos sistemos prototipo tyrimas

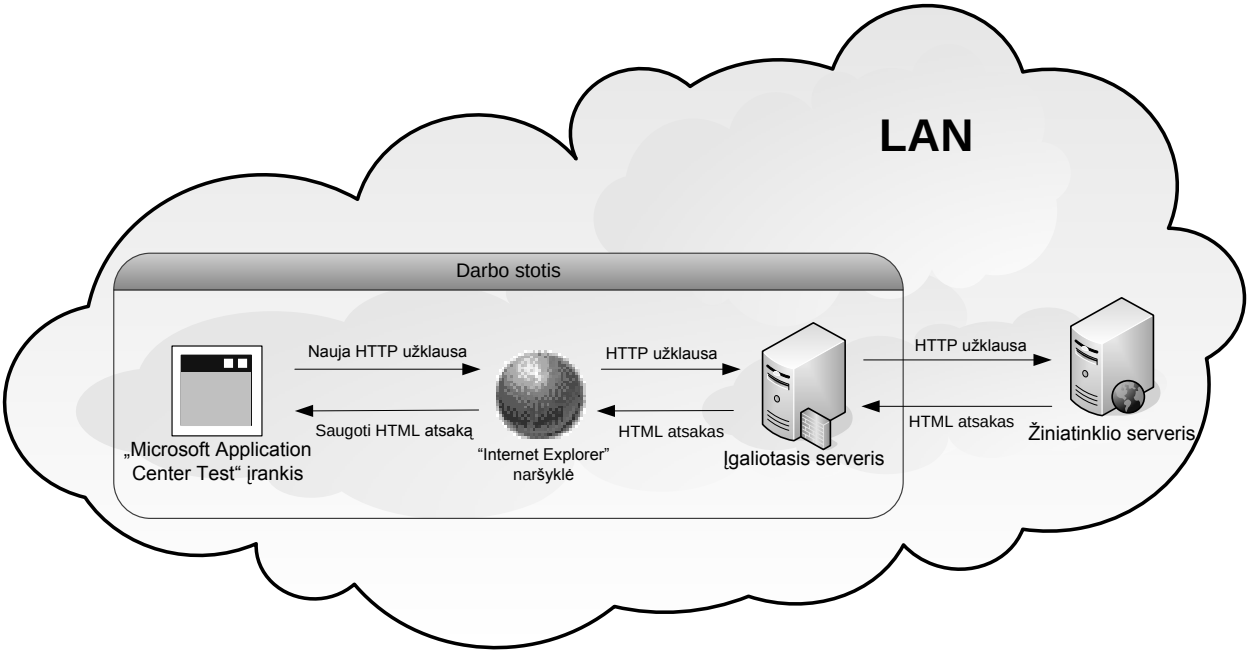
Sistemos saugumo konstrukcijų parinkimas įtakoja jos našumą ir išplečiamumą, tačiau saugumą ir našumą galima suderinti. Kuo saugesnė sistema, tuo labiau įtakojamas našumas ir

išplečiamumas.

Tyrimo metu siekiama išsiaiškinti sistemos prototipui tinkamą .NET karkase esantį maišos algoritmą ir elektroninio parašo algoritmą atsižvelgiant į našumą ir saugumą. Tam įvykdyti pagal našumą tarpusavyje lyginami MD5, SHA1, SHA512 maišos algoritmai bei DSA, RSA elektroninio parašo algoritmai.

Tyrimo rezultatams gauti naudojama 31 paveiksle pateikta schema. Bandymai atliekami lokaliame tinkle (angl. LAN), panaudojant jame esančią darbo stotį ir tarnybinę stotį. Darbo stotyje įdiegtas „Microsoft Application Center Test“ įrankis, „Internet Explorer“ naršyklė, kurioje įjungtas įgaliotasis serveris (angl. proxy server), veikiantis adresu 127.0.0.1 ir 8181 prievadu. Tarnybinėje stotyje įdiegtas žiniatinklio serveris (angl. web server), aptarnaujantis http užklausas. Taip pat tarnybinėje stotyje veikia žiniatinklio programa (angl. web application), generuojanti tyrimui reikalingas maišos funkcijų ir elektroninių parašų reikšmes.

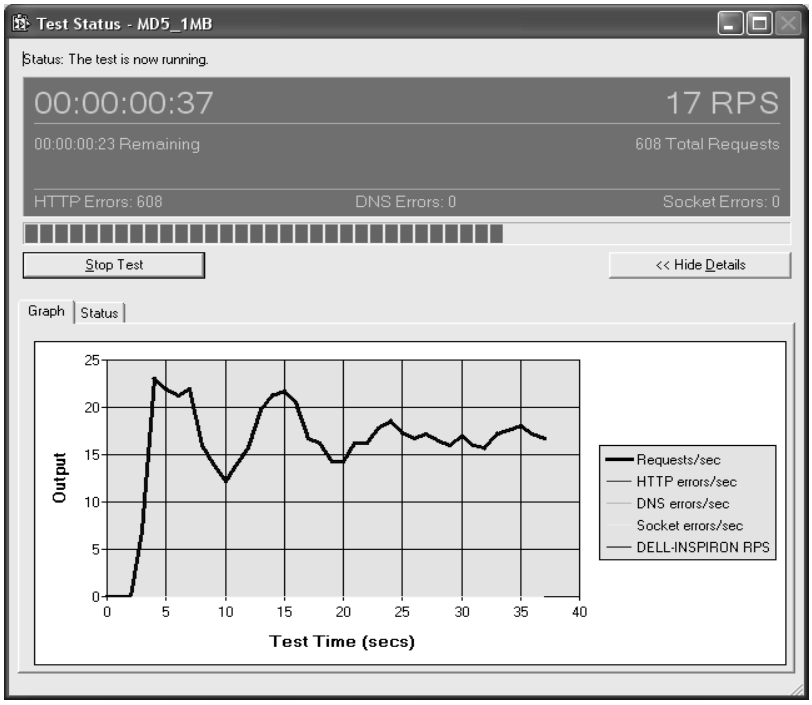
Verta paminėti, kad tyrimo rezultatams įtakos gali turėti lokalaus tinklo ir darbo stoties procesoriaus apkrovimas. Tarnybinės stoties įtaką galima atmesti dėl jos turimų techninių charakteristikų.



31 pav. Tyrimo schema

Našumo testams atlikti naudojamas „Microsoft Application Center Test“ (ACT) įrankis. Jo pagalba įrašomos HTTP užklausos, kurios vėliau testuojamos ir analizuojamos. Užklausoms fiksuoti „ACT“ įrankis naudoja įgaliotąjį serverį, per kurį vykdomi duomenų mainai su išoriniu tinklu. Iškvietus norimą puslapį ir užfiksavus užklausą, turimą įrašą galima testuoti, imituojant

vartotojų apkrovą, kurios metu atliekamas nurodytas skaičius lygiagrečių jungimusi. Vykdomo testo pavyzdys, kai URL adresu kreipiasi vienas vartotojas, pateiktas sekančiame paveiksle.

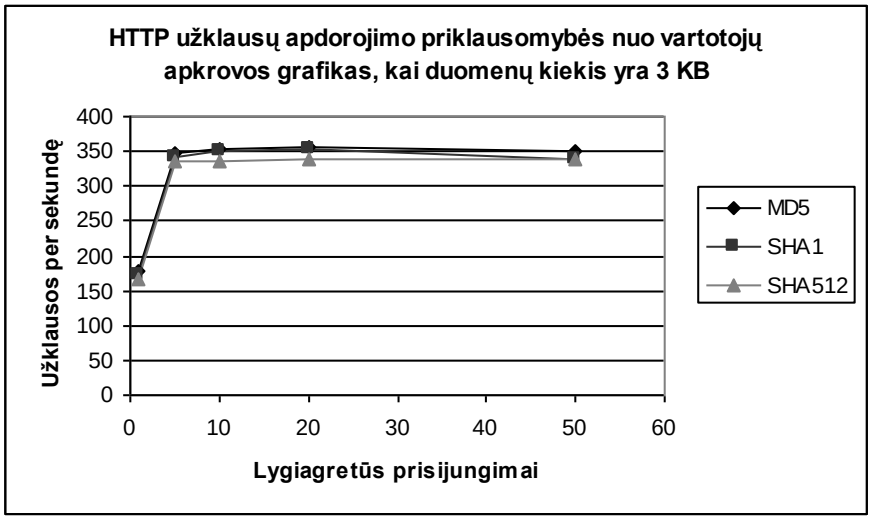


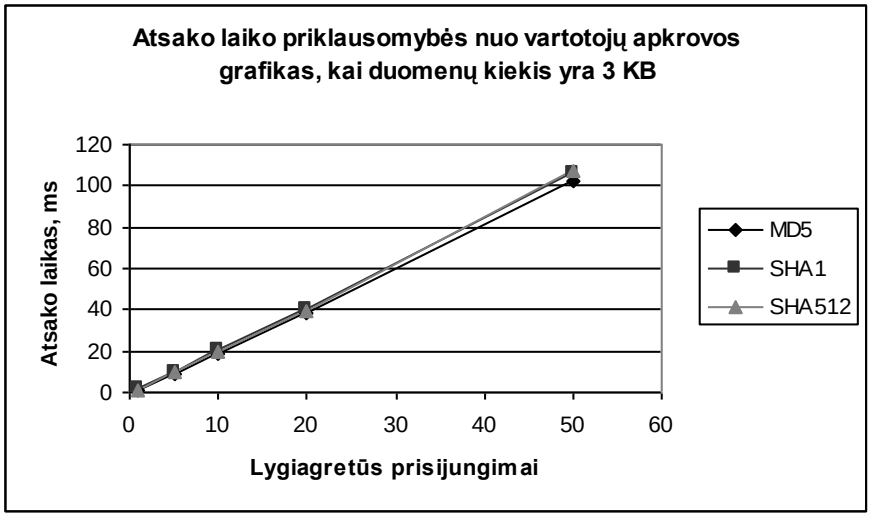
32 pav. Įrašytos užklausos testavimas

Taip imituojant lygiagrečius vartotojų prisijungimus ir baigus testavimus „ACT“ įrankis parodo kiekvieno atlikto testo rezultatų suvestinę. Testavimų metu interneto naršyklėje buvo užprašoma puslapio, kuris iš faile saugomų duomenų pateikia apskaičiuotą maišos reikšmę. Pasirinkti duomenų failų dydžiai: 3 KB, 141 KB ir 1 MB. Toliau pateikiami atliktų maišos algoritmų testavimų rezultatai, kai „ACT“ įrankio imituojamų lygiagrečių prisijungimų kiekiai yra 1, 5, 10, 20 ir 50.

Kaip parodyta 33 paveiksle, našumo atžvilgiu visi algoritmai yra panašūs. SHA512 pasižymi truputį mažesniu našumu.

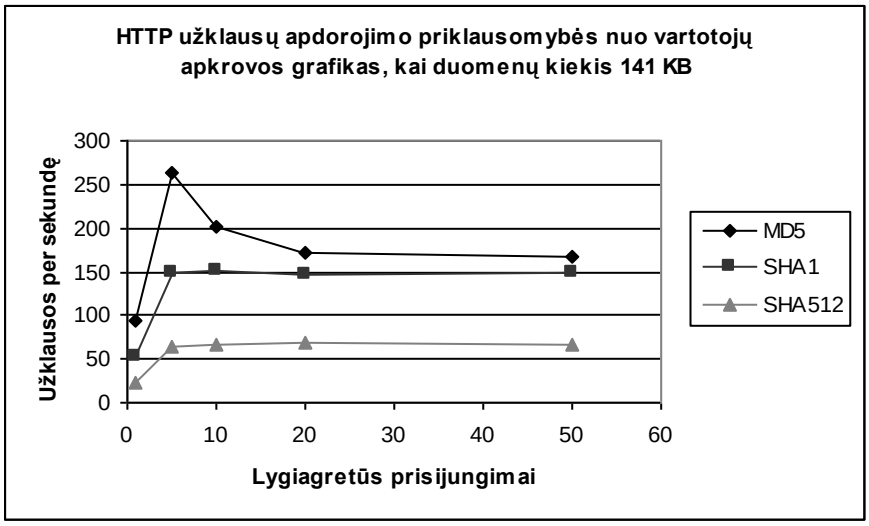
Sukuriant didesnes maišos reikšmes sunkiau panaudoti grubaus laužimo atakas (angl. brute force). Taigi tokia ataka sunkiau atliekama prieš SHA1 negu MD5, kadangi MD5 generuoja 128 bitų maišos reikšmę, o SHA1 160 bitų.

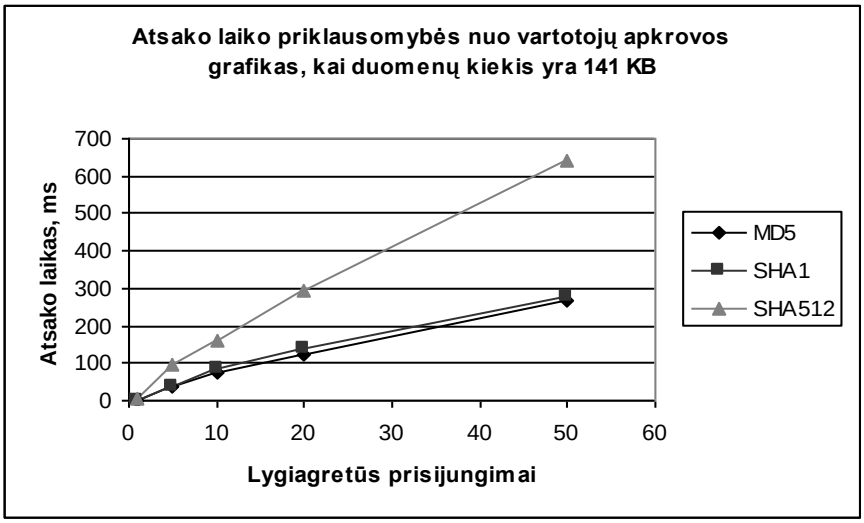




33 pav. Maišos algoritmų užklausų apdorojimo ir atsako laiko priklausomybės (3 KB)

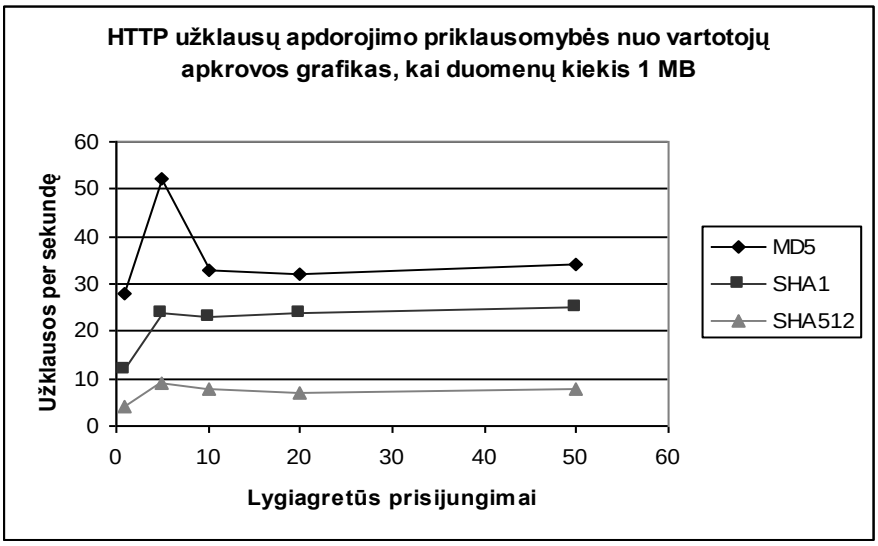
Galima pastebėti, kad padidėjus duomenų failui tarp maišos algoritmų atsirado didesni našumo skirtumai (34 pav.). Gauti duomenys rodo, kad esant penkiems lygiagretiems vartotojų prisijungimams MD5 algoritmas yra apie 42% greitesnis negu SHA1, o SHA1 57% greitesnis už SHA512.

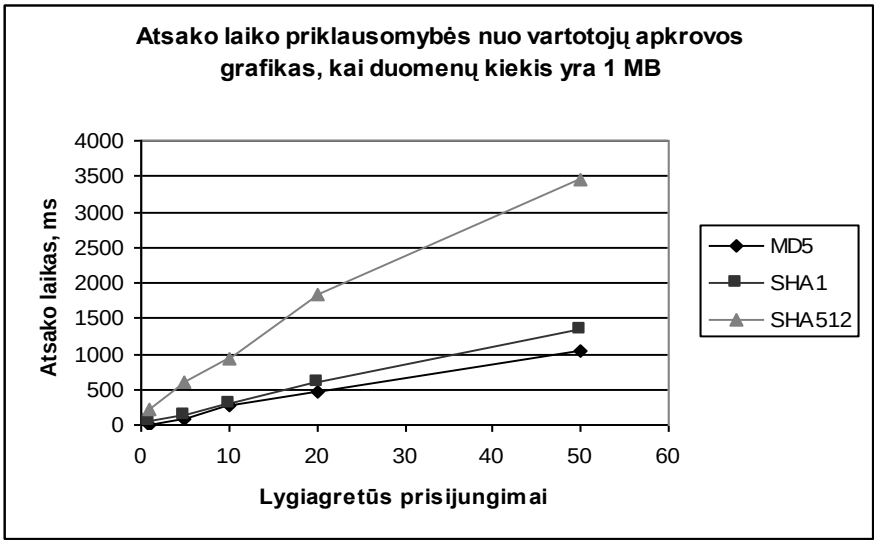




34 pav. Maišos algoritmų užklausų apdorojimo ir atsako laiko priklausomybės (141 KB)

Maišos algoritmų našumo skirtumai tampa dar didesni padidėjus duomenų dydžiui (35 pav.). MD5 yra apie 53% greitesnis negu SHA1, o SHA1 apie 63% greitesnis negu SHA512.





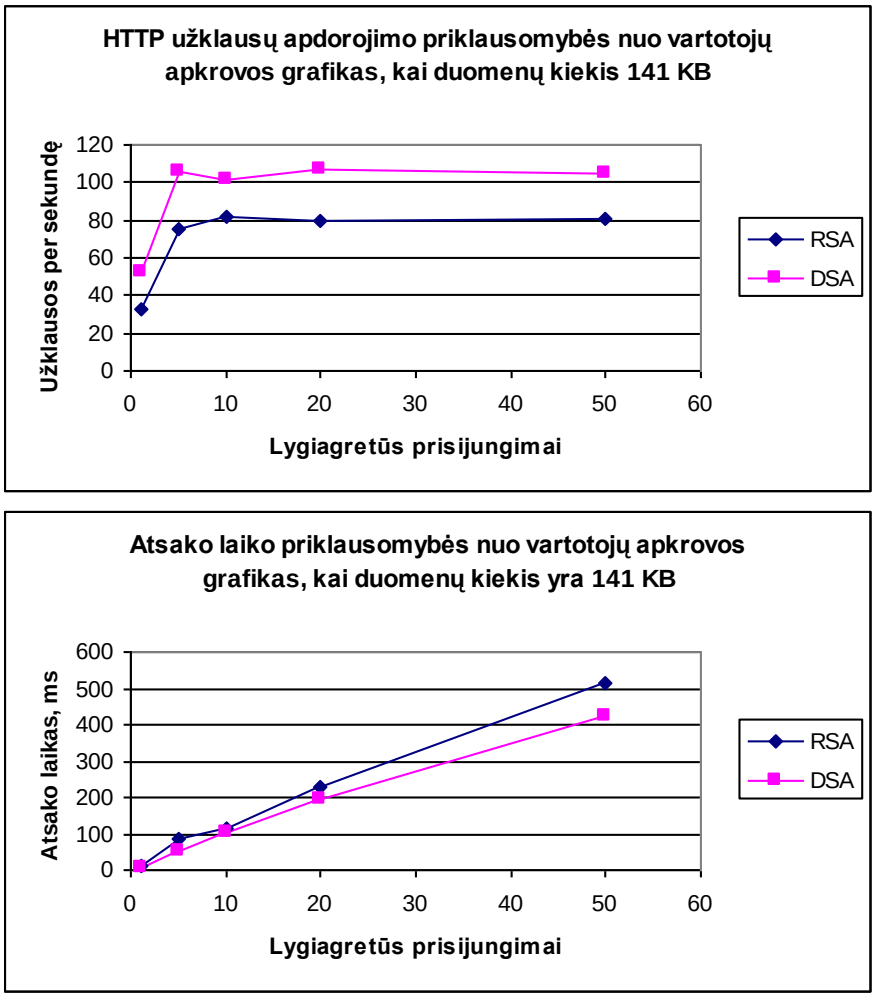
35 pav. Maišos algoritmų užklausų apdorojimo ir atsako laiko priklausomybės (1 MB)

Šifravimas naudojant asimetrinio rakto algoritmus yra labai lėtas, ypač esant dideliems duomenų kiekiams, todėl jie nėra naudojami, kai reikia šifruoti daug duomenų. Tam labiau tinka simetriniai algoritmai.

Vieni iš dažniausiai naudojamų asimetrinių algoritmų yra RSA ir DSA. RSA gali būti naudojamas tiek šifravimui, tiek parašo generavimui, o DSA tik parašo generavimui [16].

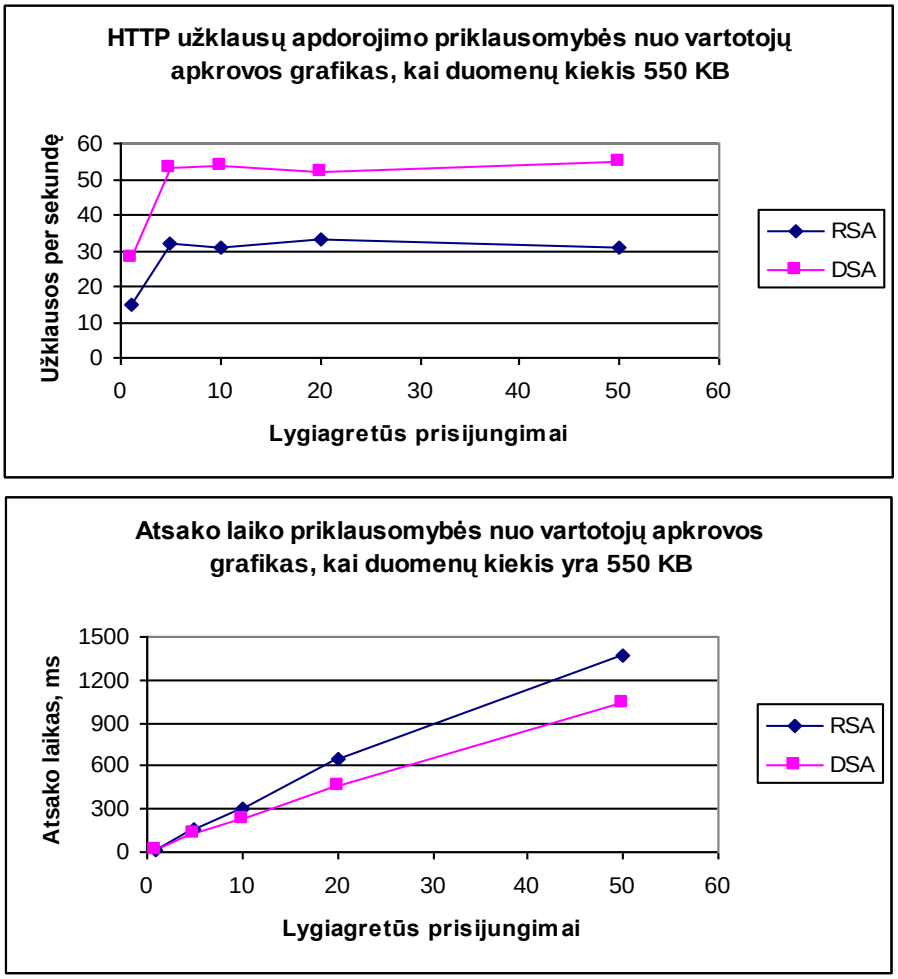
Žemiau esančiuose grafikuose pateikiami atliktų elektroninio parašo algoritmų testavimų rezultatai, kai „ACT“ įrankio imituojamų lygiagrečių prisijungimų kiekiai yra 1, 5, 10, 20 ir 50, lyginami RSA ir DSA algoritmai pagal tai kaip greitai sukuriamas ir kaip greitai patikrinamas elektroninis parašas.

Parašo sukūrimas. Abiejų algoritmų parašo sukūrimo priklausomybės esant 141 KB ir 550 KB dydžio failams pateiktos 36 ir 37 paveiksluose. RSA naudojamas rakto ilgis 1024 bitai, o DSA 512 bitų. Gauti rezultatai rodo, kad pasirašant DSA yra apie 30% spartesnis už RSA.



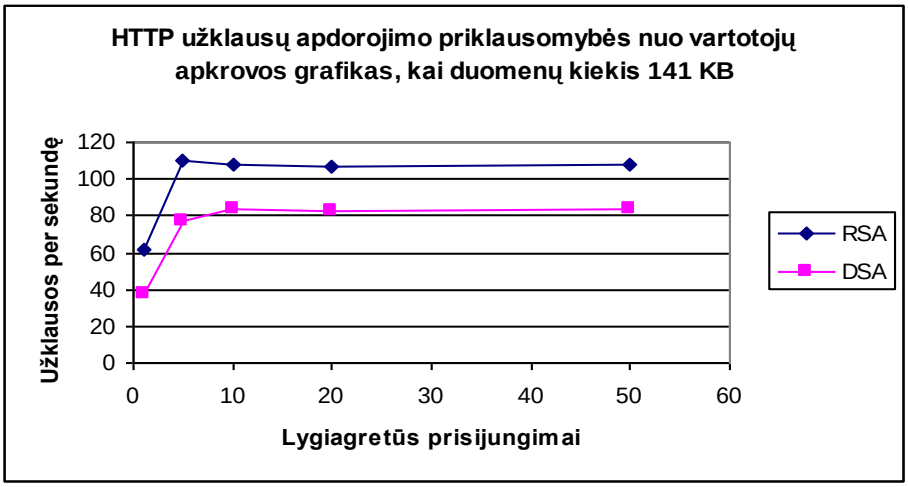
36 pav. Parašo algoritmų užklausų apdorojimo ir atsako laiko priklausomybės (141 KB)

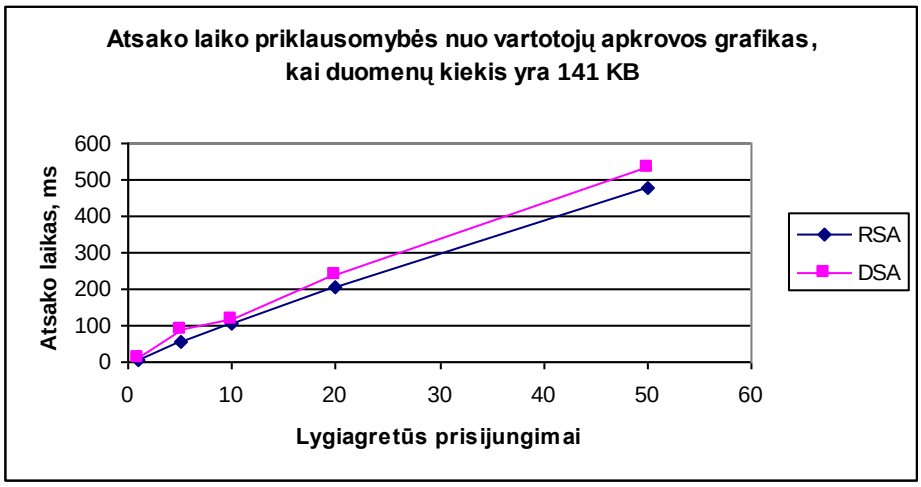
Padidinus pasirašomos informacijos kiekį DSA algoritmas išlieka spartesnis už RSA (37 pav.).



37 pav. Parašo algoritmų užklausų apdorojimo ir atsako laiko priklausomybės (550 KB)

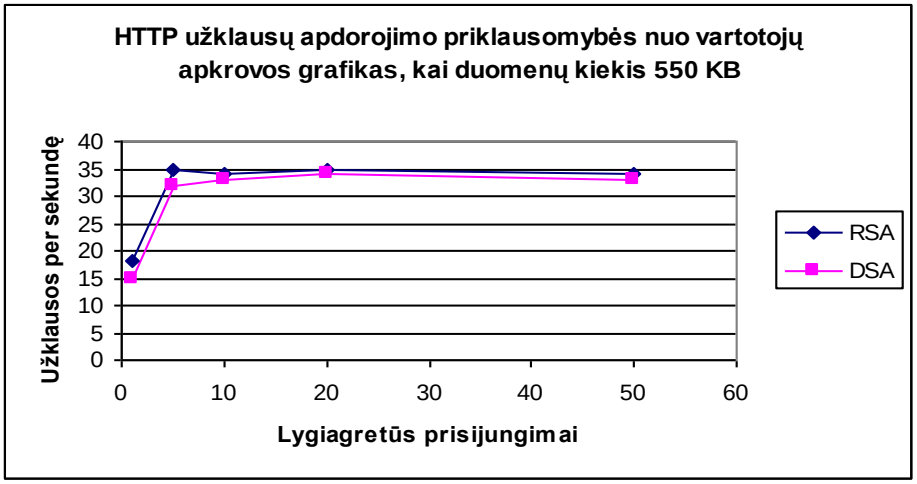
Parašo tikrinimas. Rezultatai pasikeičia priešingai atliekant elektroninio parašo tikrinimą (38 pav.). Šiuo atveju RSA yra apie 30% greitesnis už DSA.

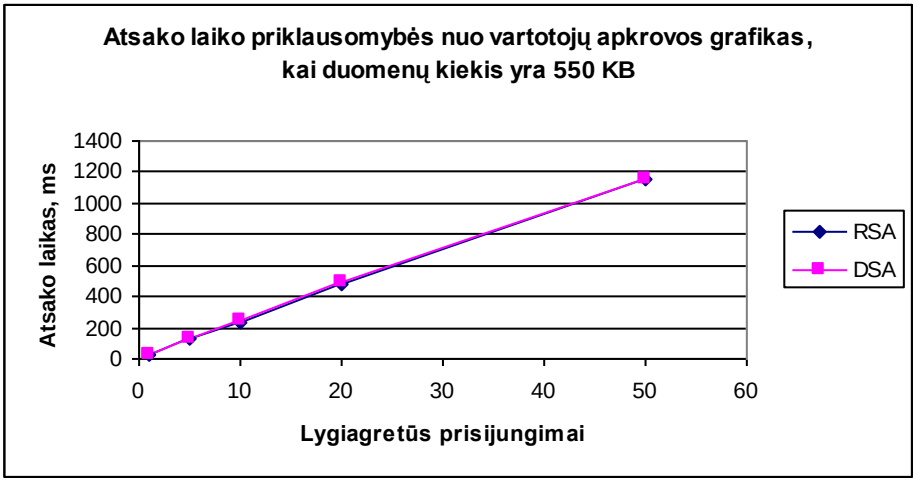




38 pav. Parašo algoritmų užklausų apdorojimo ir atsako laiko priklausomybės (141 KB)

Sekančiame paveiksle pateikti rezultatai rodo, kad atliekant e. parašo tikrinimą esant daugiau duomenų, našumo skirtumas tarp RSA ir DSA tampa nežymus.





39 pav. Parašo algoritmų užklausų apdorojimo ir atsako laiko priklausomybės (550 KB)

RSA elektroninio parašo formavimo procese privatus raktas naudojamas pranešimo santraukos šifravimui. Nors DSA yra panašus į RSA, tačiau DSA atveju pranešimo santrauka nėra šifruojama su privačiu raktu ar iššifruojama su viešu raktu. Vietoje to, e. parašui, sudarytam iš dviejų iš pranešimo santraukos ir privataus rakto gautų 160 bitų skaičių, generuoti DSA naudoja specialias matematines funkcijas [17].

RSA elektroninio parašo tikrinimui naudoja pranešimo siuntėjo viešą raktą. Tam iš gautų duomenų sukuriama pranešimo santrauka, siuntėjo viešu raktu iššifruojama gauta pranešimo santrauka ir palyginamos naujai sugeneruotos ir iššifruotos pranešimų santraukos. Jeigu jos sutampa, patvirtinamas siųsto pranešimo vientisumas.

DSA elektroninio parašo tikrinimui taip pat naudoja viešą raktą, tačiau tikrinimo procesas yra sudėtingesnis negu RSA.

4.3. Išvados

Įgyvendinta dalinė ribotos sumos elektroninių pinigų cirkuliacijos sistemos prototipo realizacija. Realizuotos sistemą sudarančios brokerio (žiniatinklio programa) ir vartotojo (taikomoji programa) dalys, reikalingos tyrimui atlikti.

Tyrimo metu lokaliame kompiuterių tinkle buvo atlikti maišos ir elektroninio parašo algoritmų našumo bandymai. Tarpusavyje palyginta .NET karkase esančių MD5, SHA1, SHA512 maišos algoritmų ir RSA, DSA elektroninio parašo algoritmų priklausomybė nuo apdorojamų duomenų kiekio.

Gauti rezultatai rodo, kad esant nedideliam (3KB) hešuojamų (angl. hashing) duomenų kiekiui našumo skirtumai tarp maišos algoritmų yra nedideli. Didinant duomenų kiekį kiekvieno iš algoritmų našumas skiriasi. Esant 141 KB dydžio duomenims ir penkiems lygiagretiems vartotojų prisijungimams MD5 algoritmas yra apie 42% greitesnis negu SHA1, o SHA1 57% greitesnis už SHA512.

Atlikti elektroninio parašo algoritmų našumo bandymai parodė, kad sukuriant e. parašą DSA yra apie 30% spartesnis už RSA, kai duomenų dydis 141 KB. Tuo tarpu tikrinant e. parašą RSA tai atlieka apie 30% sparčiau.

Remiantis atliktu tyrimu, galima teigti, kad atsižvelgiant į saugumo ir našumo santykį geriausiai naudoti SHA1 maišos algoritmą. Renkantis elektroninio parašo algoritmą patartina rinktis DSA, jeigu daugiau atliekama e. pasirašymo procedūrų, arba RSA, jeigu dažniau atliekamas e. parašo tikrinimas.

IŠVADOS

Pagrindiniai atlikti darbai ir pasiekimai:

1) Elektroninių pinigų cirkuliacijos schemų analizės dalyje apžvelgti elektroniniai pinigai, jų tipai, privalumai ir trūkumai. Aptarti elektroninių pinigų cirkuliacijos schemų modeliai ir pačiose cirkuliacijos schemose galimi naudoti saugumo mechanizmai. Išdėstyti schemoms keliami transakcijų ir saugumo reikalavimai. Atlikta mokėjimo schemų palyginamoji analizė, kurios metu išsiaiškinti jų veikimo principai ir pastebėta, kad atliekant vidutinės ir didelės vertės mokėjimus naudojami sudėtingi saugumo mechanizmai, kurie kartu padidina interneto tinklo apkrovą ir mokėjimo patvirtinimo sąnaudas. Tuo tarpu mažiems mokėjimams naudojami paprastesni saugumo užtikrinimo metodai, tokie kaip maišos funkcijos, slaptažodžiai, nereikalaujantys didelių sąnaudų.
2) Ribotos sumos elektroninių pinigų cirkuliacijos sistemos modelio dalyje apibrėžti reikalavimai, keliami siūlomam modeliui, ir pateiktas pats mažiems ir vidutiniams mokėjimams skirtas modelis, besiremiantis Payword mikromokėjimų sistemos koncepcija. Detaliai aptartas modelio protokolas ir naudojami saugumo mechanizmai, užtikrinantys našumą ir apsaugantys nuo e. pinigo klastojimo.
3) Sudarytas ribotos sumos elektroninių pinigų cirkuliacijos sistemos projektas, apibrėžiantis sistemos dalyvių funkcijas ir pagrindinius veikimo algoritmus. Struktūriškai nubraižyti sistemos dalyvių siunčiamus pranešimus sudarantys duomenų laukai. Suprojektuota brokerio duomenų bazė, skirta vartotojų informacijai saugoti.
4) Įgyvendinta dalinė sistemos prototipo realizacija panaudojant Microsoft Visual Studio 2005 ir Microsoft SQL Server 2008 programinius paketus. Realizuotos sistemą sudarančios brokerio (žiniatinklio programa) ir vartotojo (taikomoji programa) dalys, reikalingos tyrimui atlikti.
5) Lokaliame kompiuterių tinkle atliktas maišos ir elektroninio parašo algoritmų našumo tyrimas. Tarpusavyje palyginta .NET karkase esančių MD5, SHA1, SHA512 maišos algoritmų ir RSA, DSA elektroninio parašo algoritmų priklausomybė nuo apdorojamų duomenų kiekio. Remiantis atlikto tyrimo rezultatais, galima teigti, kad atsižvelgiant į saugumo ir našumo santykį geriausiai naudoti SHA1 maišos algoritmą. Renkantis elektroninio parašo algoritmą patartina rinktis DSA, jeigu daugiau atliekama e. pasirašymo procedūrų, arba RSA, jeigu dažniau atliekamas e. parašo tikrinimas.

LITERATŪRA

[1] Douglas Stebila, Uncloanable Quantum Money, Institute for Quantum Computing, University of Waterloo, CQISC, 2006, [žiūrėta 2009-01-19]. Prieiga per internetą: http://www.iqis.org/events/cqisc06/papers/Mon-1130-Stebila.pdf

[2] Dr. Andreas Schöter and Rachel Willmer,Digital Money Online, A Review of Some Existing Technologies, Intertrader Ltd., 1997,[žiūrėta 2009-01-18]. Prieiga per internetą: http://www.versaggi.net/ecommerce/articles/dmo.pdf

[3] E. Sakalauskas, et al. Kriptografinės sistemos. – Kauno technologijos universitetas, 2008, – 142 p.

[4] Hugo Godschalk, Malte Krueger, Why e-money still fails, Berlin, 2000 [žiūrėta 2009-01-03]. Prieiga per internetą: http://cnscenter.future.co.kr/resource/security/ecommerce/godschalk.pdf

[5] Jim Miller, E-money mini-FAQ (release 2.0), 2007 [žiūrėta 2009-01-03]. Prieiga per internetą: http://projects.exeter.ac.uk/RDavies/arian/emoneyfaq.html

[6] Juha Laine, ePayments, 2008.12.1, [žiūrėta 2008-12-27]. Prieiga per internetą: https://noppa.tkk.fi/noppa/kurssi/t-76.5762/luennot/lecture07.pdf

[7] M.Civilka, Elektroniniai atsiskaitymai, Vilniaus Universitas Teisės fakultetas Informatikos teisės centras, Vilnius, 2002, [žiūrėta 2009-01-12]. Prieiga per internetą: http://www.itc.tf.vu.lt/mokslas/E-atsiskaitymai.pdf

[8] Michelle Baddeley, Using E-cash in the new economy: an economic analysis of micropayment systems, Cambridge, UK, [žiūrėta 2009-01-03]. Prieiga per internetą: http://www.econ.cam.ac.uk/faculty/baddeley/ecash04.pdf

[9] OECD, The Future of Money, France, 2002, [žiūrėta 2009-01-19]. Prieiga per internetą: http://www.vwl.tuwien.ac.at/hanappi/Lehre/EMoney/FutoMoney.pdf#page=10

[10] Ricarda Weber, Chablis - Market Analysis of Digital Payment Systems, Version 1.5, 1999, [žiūrėta 2009-01-03]. Prieiga per internetą: http://purl.pt/282/1/v3d2/projects/chablis/pdf-documents/a-marketpay.pdf

[11] Pedro Isaias, Technology Issues ande Electronics Copyright Management Systems, [žiūrėta 2009-02-10]. Prieiga per internetą: http://www.ariadne.ac.uk/issue21/ecms/

[12] S. Kašėta, T. Adomkus. Telefonijos informacijos ir VoIP sauga. – Kauno technologijos universitetas, 2008, – 99 p.

[13] Stuart E. Weiner, Electronic Payments in the U.S., [žiūrėta 2009-01-19]. Prieiga per internetą: http://www.kc.frb.org/PUBLICAT/ECONREV/PDF/4q99wein.pdf

[14] T. Blažauskas, E. Sakalauskas, K. Lukšys. Elektroninių dokumentų ir duomenų sauga. – Kauno technologijos universitetas, 2008, – 155 p.

[15] CGI Group Inc., Public Key Encryption and Digital Signature: How do they work?, 2004, [žiūrėta 2010-02-10]. Prieiga per internetą: http://www.cgi.com/cgi/pdf/cgi_whpr_35_pki_e.pdf

[16] Ian Curry, Key Upadate and the Complete Story on the Need for Two Key Pairs, Entrust Technologies, 1998, [žiūrėta 2010-04-17]. Prieiga per internetą: http://www.firstvpn.com/papers/entrust/2keypairs10.pdf

[17] Rania Salah El-Sayed, Moustafa Abd El-Aziem, Mohammad Ali Gomma, An efficient signature system using optimized RSA algorithm, Egypt, [žiūrėta 2010-04-24]. Prieiga per internetą: http://eref.uqu.edu.sa/files/eref2/folder6/f69.pdf