KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Manvydas Milkus

Saugių tarpusavio atsiskaitymų sistemos sudarymas ir tyrimas panaudojant e.parašą

Magistro darbas

Darbo vadovas
prof. dr. E. Sakalauskas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

Manvydas Milkus

Saugių tarpusavio atsiskaitymų sistemos sudarymas ir tyrimas panaudojant e.parašą

Magistro darbas

Recenzentas

2010-05-

Vadovas

prof. dr. E. Sakalauskas

2010-05-

Atliko

IFN-8/3 gr. stud.
Manvydas Milkus

2010-05-

Kaunas, 2010

SUMMARY

Business subjects have been using different types of payments for many years. But some problems persists too. One of them is debt. It makes companies to have difficulties doing settlements with other companies, makes bad reputation for companies and bushiness on the whole. In nowadays many new technologies are raised, which can be used in many spheres. So in the business too.One of them is e-signature. But the research showed that most of payments systems still don‘t use it.

In this work safe inter-payments system was projected and suggested. It includes model of debt circles finding, identification and authority, circulation of e-documents. The examination of debt reseting module showed that this task needs much computers resources. Otherwise, the fact that such system can reduce contracts signing time is obvious too. In conclusion, similar systems could and should be developed in the future.

TURINYS

Paveikslų sąrašas

Lentelių sąrašas

ĮVADAS

Įvairaus pobūdžio atsiskaitymai versle naudojami jau tūkstančius metų ir yra seni, kaip ir pats verslas. Šiuo metu susiklosčius sudėtingai ekonominei situacijai, problemos užgriuvo ir ant verslininkų pečių. Lietuvoje, „Creditinfo“ duomenimis, kas antra įmonė turi pradelstų įsiskolinimų. Laiku nepadengiami įsiskolinimai daro nemažą žalą: trukdo įmonei vykdyti tiesioginę veiklą, kenkia tiek įmonės, tiek viso verslo įvaizdžiui [1].

Akivaizdu, kad plėtojantis informacinėms technologijoms, turi atsirasti naujų priemonių ir būdų, kurie padėtų verslui spręsti susidariusias problemas. Šiame darbe bus nagrinėjami įvairūs atsiskaitymo būdai, sudarytas saugių tarpusavio atsiskaitymų modelis, ištirtos jo realizavimo ir panaudojimo galimybės.

1 TARPUSAVIO ATSISKAITYMO MODELIŲ ANALIZĖ

1.1 Analizės tikslas

Apžvelgti esamus tarpusavio atsiskaitymo modelius, metodus ir būdus, esamas užskaitų ir e.pinigų sistemas, išnagrinėti e.parašo panaudojimo galimybes tarpusavio atsiskaitymams.

1.2 Tyrimo sritis, objektas ir problema

Sritis ir objektas

Įmonių tarpusavio skolų užskaitymas panaudojant internetą, e. parašą ir e.dokumentus

Sprendžiama problema

Verslo subjektai dažnai turi sudėtingus tarpusavio įsiskolinimus vieni kitiems, kuriuose dalyvauja kelios arba keliolika šalių. Todėl atsiranda galimybė įsiskolinimų duomenų bazės pagalba atsekti šiuos atsiskaitymus ir panaudojant internetinę technologiją bei e. parašą ir e. dokumentus atlikti tarpusavio skolų užskaitymą.

1.3 Įmonėse naudojamų atsiskaitymo būdų analizė

Visus piniginius atsiskaitymus galima suskirstyti į dvi pagrindines grupes:

- Atsiskaitymus grynaisiais pinigais
- Atsiskaitymus negrynaisiais pinigais

1.3.1 Atsiskaitymai grynaisiais pinigais

Atsiskaitymas grynaisiais pinigais yra itin seniai žmonijai žinoma ir naudojama atsiskaitymo forma. Tačiau nepaisant kai kurių privalumų (galimybė tuoj pat pinigus naudoti savo reikmėms), tokia atsiskaitymo forma turi ir ryškių minusų:

- Nepatogu mokėti didelias sumas;
- Tiksliam suskaičiavimui reikia atidumo ir laiko;
- Visada reali vagystės grėsmė;
- Visada egzistuoja galimybė gauti netikrus („padirbtus“) pinigus, kuriuos nelengva atskirti nuo tikrų;
- Atsiranda pajamų slėpimo galimybė;

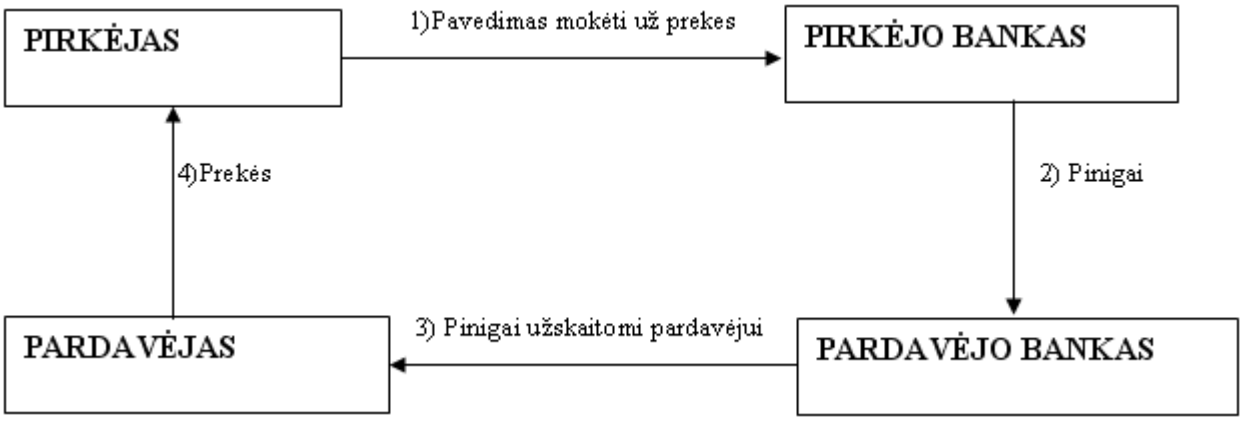
Atsiskaitymai grynaisiais pinigais populiariausi mažmeninėje prekyboje ir paslaugų sferoje, nors ir čia populiarumas mažėja, o tarp verslo bei valstybinių ir visuomeninių organizacijų jau senokai paplitęs atsiskaitymas negrynaisiais pinigais. Atsiskaitymai

negrynaisiais pinigais vykdomi perkeliant lėšas iš vienos įmonės atsiskaitomosios sąskaitos į kitos įmonės atsiskaitomąją sąskaitą. Grynųjų pinigų apyvarta pakeičiama bankų įrašais [2].

1.3.2 Atsiskaitymų negrynaisiais pinigais būdai

1.3.2.1 Mokėjimo pavedimas

Mokėjimo pavedimas yra įmonės nurodymas savo bankui pervesti tam tikrą sumą iš jos sąskaitos į gavėjo sąskaitą. 1 Paveiksle parodyta kokiu būdu, atsiskaitant mokėjimo pavedimais, pinigus gauna pardavėjas [2].



1 pav. Atsiskaitymo mokėjimo procedūra

Šis atsiskaitymo būdas - tai paprasčiausias mokėjimas iš einamosios sąskaitos. Pačioje prekybinėje operacijoje komerciniai dokumentai yra naudojami, tačiau jie nėra siunčiami per bankus. Tokio tipo atsiskaitymuose bankas neturi jokių papildomų įsipareigojimų. Čia jis veikia kaip paprasčiausias tarpininkas tarp mokėtojo ir pinigų gavėjo. Mokėjimo pavedimais galima atsiskaityti už prekes, paslaugas, grąžinti kreditą, mokėti palūkanas, mokesčius, atlikti kitus mokėjimus [2].

Mokėjimo pavedimas rašomas trim egzemplioriais, jei mokėtojas ir lėšų gavėjas turi sąskaitas tame pačiame banke. Pirmasis egzempliorius naudojamas kaip memorialinis orderis mokėtojo banke, antrasis įteikiamas lėšų gavėjui, trečiasis, patvirtintas banko darbuotojų parašais ir spaudu, grąžinamas mokėtojui [2].

Jei mokėtojo ir lėšų gavėjo sąskaitos yra skirtinguose bankuose, pildomi keturi pavedimo egzemplioriai. Pirmasis egzempliorius naudojamas kaip memorialinis orderis mokėtojo banke, antrasis ir trečiasis, nurašius lėšas, siunčiami lėšų gavėjo bankui. Čia antrasis egzempliorius naudojamas kaip memorialinis orderis lėšoms į gavėjo sąskaitą įskaityti ir lieka banke, o trečiasis įteikiamas lėšų gavėjui. Ketvirtasis egzempliorius grąžinamas mokėtojui. Atsiskaitant su keletu

gavėjų, turinčių sąskaitą tame pačiame banke, naudojamas suvestinis mokėjimo pavedimas. Jis skiriasi nuo paprastojo mokėjimo pavedimo tuo, kad čia į vieną dokumentą surašomi duomenys apie mokėtinas sumas keliems gavėjams [2].

Bankas, gavęs mokėjimo pavedimą, apmoka jį iš karto. Jeigu mokėtojo sąskaitoje nėra pakankamai pinigų, mokėjimas atidedamas, kol bus sukaupta reikiama suma. Jeigu pinigų trūksta, atsiskaitoma tokiu eiliškumu: mokesčiai, atlyginimai, mokėjimai bankui ir kt [2].

Mokėjimo pavedimas - labiausiai paplitusi Lietuvoje atsiskaitymo tarp ūkio subjektų forma, nes yra nesudėtingas jo vykdymas ir garantuojamas greitas pinigų gavimas. Pinigų gavimo terminas respublikos ribose yra viena darbo diena. Jei lėšų siuntėjo bankas pervedimą įvykdo iki 13^{00} valandos, lėšų gavėjo sąskaitoje pinigai parodomi tą pačią dieną. Pavedimai po 13^{00} valandos kliento sąskaitoje atsispindės kitą darbo dieną (kai kuriuose bankuose tą pačią dieną) [2].

Šio atsiskaitymo būdo privalumai:

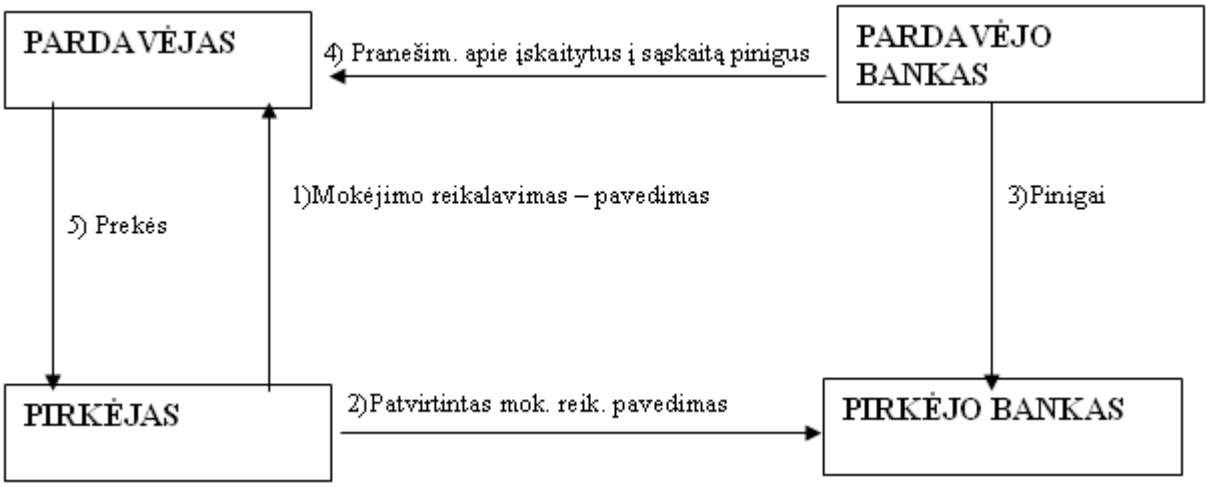
- Nereikia naudotis grynais pinigais;
- Galimybė vienu pavedimu sumokėti keliems gavėjams;
- Galimybė sumokėti dalimis;

Trūkumai:

- Nėra momentinis (reikia laiko, kol pinigai pasieks gavėjo sąskaitą)

1.3.2.2 Mokėjimo reikalavimas – pavedimas

Mokėjimų reikalavimas-pavedimas - tai prekių ar paslaugų tiekėjo, darbų atlikėjo išrašomas atsiskaitymų dokumentas už jo pateiktas prekes, suteiktas paslaugas, atliktus darbus [2].



2 pav. Atsiskaitymų mokėjimo reikalavimais – pavedimais procedūra

Nustatytos formos blanke išrašytą reikalavimą – pavedimą kartu su prekių pateikimo, paslaugų suteikimo ar darbų atlikimo sutartyje numatytais dokumentais pardavėjas siunčia mokėtojui arba pagal tarpusavio susitarimą mokėtojo bankui, kursi perduoda šiuos dokumentus mokėtojui. Pirkėjui ir pardavėjui susitarus, mokėjimų reikalavimus – pavedimus su atitinkamais prekių, paslaugų ar darbo atlikimo dokumentais mokėtojas gali atsiimti tiesiogiai iš prekių tiekėjo, paslaugų teikėjo ar darbų atilkėjo. Pirkėjas, sutikęs mokėti pagal pateiktą mokėjimų reikalavimą-pavedimą, įformina savo sutikimą atsakingų darbuotojų parašais ir antspaudu, perduoda jį savo bankui [2].

Mokėtojo bankas priima mokėjimų reikalavimus-pavedimus tik tuo atveju, jeigu mokėtojo sąskaitoje yra pakankamai pinigų pavedimui įvykdyti. Pirmasis mokėjimų reikalavimo-pavedimo egzempliorius, nurašius lėšas iš mokėtojo sąskaitos, lieka kaip memorialinis orderis banke. Antrasis siunčiamas tiekėjui, o trečiasis grąžinamas mokėtojui. Jeigu mokėtoją ir lėšų gavėją aptarnauja skirtingi bankai, pirmasis dokumento egzempliorius lieka mokėtojo banke, antrasis ir trečiasis, nurašius lėšas, siunčiami lėšų gavėjo bankui. Čia antrasis egzempliorius panaudojamas kaip memorialinis orderis, o trečiasis įteikiamas lėšų gavėjui. Ketvirtasis egzempliorius, patvirtintas banko darbuotojo, grąžinamas mokėtojui [2].

Jeigu pirkėjas dėl tam tikrų priežasčių atsisako sumokėti visą mokėjimų reikalavimo-pavedimo sumą arba jos dalį, apie tai jis tiesiogiai praneša pardavėjui. Tokiu atveju rašomas atsisakymas nuo akcepto, kurį gavęs bankas (nuo 3 iki 7 dienų) mokėjimo operaciją sulaiko.
Mokėjimų reikalavimus-pavedimus šiuo metu Lietuvoje daugiausia naudoja komunalinius patarnavimus teikiančios įmonės, turinčios nuolatinius klientus ir žinančios jų finansines galimybes [2].

1.3.2.3 Įmonių tarpusavio įskaitiniai atsiskaitymai

Įmonės tarpusavyje gali atsiskaityti įskaitymų būdu. Tokiu atveju mokėtojas privalo turėti lėšų ne visai įsiskolinimo sumai, o tik jo skirtumui. Tarpusavio reikalavimų įskaitymai gali būti nuolatiniai tarp dviejų įmonių arba tarp daugelio įmonių taip pat fiksuoti konkrečiai datai. Tuo tikslu kiekvienai įmonei įskaitos dalyvei atidaroma speciali sąskaita, kurioje iki įskaitymo dienos įrašomos visos įmonės, skolingos tai įmonei, ir surašomi jos pačios įsiskolinimai. Įskaitymo dieną palyginamos galutinės sumos ir nustatomas likutis [2].

Lietuvoje įskaitas rengia Lietuvos bankas, paskelbdamas visos respublikos mastu, kada bus vykdoma skolų įskaita per Atsiskaitymų centrą (suteikiant kreditus arba ne). Tačiau tokios respublikos mastu atliekamos skolų įskaitos nepasiteisina, nes esama daug nemokių įmonių, įmonių skolininkių grandinė nutrūksta, kadangi daug skolininkų yra užsienyje [2].

Overdraftas

Overdraftas suteikia teisę įmonei naudoti pinigų sumas, viršijančias banko sąskaitos likutį iki nustatytos maksimalios overdrafto sumos. Overdraftas – efektyvus trumpalaikio kreditavimo būdas, padedantis subalansuoti įmonės pinigų srautus ir patenkinti einamųjų lėšų poreikį. Overdrafto laikotarpio metu įmonė bet kada gali pasinaudoti overdraftu, o palūkanos yra mokamos tik už panaudotą sumą. [3]

Overdrafto privalumai:

- galimybė subalansuoti įmonės pinigų srautus;
- įmonė nėra apribota pinigų išėmimo ir grąžinimo grafiku;
- palūkanos mokamos tik už panaudotą overdrafto sumą; [3]

Čekis

Viena iš banko teikiamų paslaugų - galimybė atsiskaityti banko čekiais (Lietuvos komerciniuose bankuose šie čekiai dar vadinami vardiniais). Šia paslauga klientas gali pasinaudoti, kai nežino gavėjo banko sąskaitos numerio arba moka nedidelę sumą, arba kai negali atsiskaityti kitomis priemonėmis, pavyzdžiui, mokėjimo pavedimu, arba kai jo apsisprendimą atsiskaityti banko čekiais veikia kitos priežastys. Kai kuriais atvejais banko čekiai yra patogesni už kitas atsiskaitymo priemones. Atsiskaitymo banko čekiais tarpininkas yra bankas. .Jame automatiškai nurašomos iš kliento sąskaitos pinigų sumos pervedamos į čekį pateikusio asmens sąskaitą. Tai supaprastina atsiskaitymus, daro juos patogesnius ir patikimesnius [2].

Čeki*s* yra vertybinis popierius - tam tikra teisine forma sudarytas čekio davėjo pavedimas bankui, kad jis besąlygiškai apmokėtų (pervestų) arba išmokėtų jame įrašytąją sumą. Čekis yra vertybinis popierius, pavedimas bankui, kuris turi būti sudarytas pagal tam tikrą teisinę formą, pagrįstą čekio rekvizitais. Šie rekvizitai yra vieningi visame pasaulyje, jie išvardyti LR čekių įstatyme, kuris savo ruožtu parengtas remiantis 1931 m. Ženevos konvencijos Vieningų čekių įstatymu [2].

Vekselis

Vekselis – tai vertybinis popierius, kuris išrašomas įstatymo nustatyta tvarka ir kuriuo jį išrašęs asmuo įsipareigoja be sąlygų, tiesiogiai ar netiesiogiai sumokėti tam tikrą pinigų sumą nurodytam vekselyje asmeniui pats ar įsako tai padaryti kitam. Tokiu būdu vekseliai yra skirstomi į dvi rūšis: paprastąjį ir įsakomąjį. Paprastasis vekselis yra vekselis, kuriuo davėjas pats įsipareigoja besąlygiškai sumokėti vekselio turėtojui vekselyje įrašytą sumą. Įsakomasis vekselis – kuriuo davėjas įsako kitam asmeniui sumokėti vekselyje įrašytą sumą vekselyje nurodytam asmeniui [4].

Atsiskaitymai vekseliais turi daug pranašumų prieš kitas atsiskaitymų formas. Vekselį išrašęs asmuo besąlygiškai pasižada grąžinti skolą sutartu laiku. Be to vekselis gali būti laiduotas (laidavimas garantuojamas laiduotojų turtu) gali būti perduotas kitam asmeniui. Taipogi vekselį gali išpirkti kreditinės įstaigos, sumokėdamos šiek tiek mažesnę pinigų sumą [2].

Dokumentinis akredityvas

Dokumentinis akredityvas - tai atsiskaitymo būdas, kai pirkėjo prašymu bankas išleidžia dokumentą, kuriuo įsipareigoja pardavėjui (akredityvo gavėjui) sumokėti už išsiųstas prekes, atliktus darbus ar suteiktas paslaugas, kai pastarasis pateikia bankui akredityvo terminus ir sąlygas atitinkančius dokumentus. Akredityvu rekomenduojama atsiskaityti, kai prekybos partneriai nepažįsta vienas kito, abejojama partnerio mokumu, sudaromos sutartys su politiškai ar ekonomiškai nestabiliomis šalimis arba kai to reikalauja įstaymai [5].

Akredityvo privalumai pardavėjui

- pardavėjas turi pirkėjo banko įsipareigojimą sumokėti už išsiųstas prekes/atliktas paslaugas;
- pirkėjas negali atsisakyti apmokėti, jei bankui pateikiami akredityvo sąlygas ir terminus atitinkantys dokumentai;
- pardavėjas gali apskaičiuoti išsiųstų prekių apmokėjimo datą [5].

Akredityvo privalumai pirkėjui

- bankas apmokės pardavėjui už išsiųstas prekes su sąlyga, kai jis pateiks bankui akredityvo sąlygas ir terminus atitinkančius dokumentus;
- pirkėjui suteikiama galimybė kontroliuoti prekių išsiuntimo terminus;
- išleisdamas akredityvą, pirkėjas įrodo savo mokumą (kas ypatingai svarbu sudarant naujus prekybinius sandėrius) ir gali tikėtis lengvatų iš pardavėjo ateityje;
- išleidžiant akredityvą su atidėtu mokėjimu, pirkėjui suteikiama galimybė parduoti gautas prekes, o po to atsiskaityti su pardavėju, t.y. pardavėjas kredituoja pirkėją [5].

1.3.2.4 Elektroniniai pinigai

E.pinigai – tai e.dokumentai, turintys realių pinigų vertę ir pripažįstami jų vartotojų tarpusavio atsiskaitymuose. Šiuo metu naudojami dviejų tipų e.pinigai: veikiantys prijungties rėžimu (online) ir veikiantys atjungties rėžimu (offline) [6].

Elektroniai atsiskaitymai internete labai dažnai vykdomi naudojantis kreditinėmis kortelėmis. Pirkėjas išsirenka prekes ar paslaugas ir nurodo savo vardą, pavardę, kreditinės kortelės numerį ir kortelės saugos kodą (CVV2), kuris būna parašytas kitoje kreditinės kortelės pusėje ir kurį žinoti gali tik kortelės savininkas. Gavęs šiuos duomenis pardavėjas gali kreiptis į pirkėjo banką ir nuskaityti pinigus. Čia kyla daug grėsmių: nesąžiningas pardavėjas gali nuskaityti daugiau pinigų nei jam priklauso, kažkada vėliau atlikti pakartotinį nuskaitymą siekiant pasipelnyti taip pat neturėdamas tokios teisės išsisaugoti pateiktus duomenis duomenų bazėje, kuri vėliau gali būti specialiai perduota kitiems asmenims arba nulaužta piktavalių tinklo vartotojų. Nesirūpinant perduodamos informacijos sauga, svarbūs ir slapti duomenys gali būti perimti pakeliui pas pardavėją. Dėl šių priežasčių buvo sukurtas ir sėkmingai pradėtas naudoti SET protokolas [7].

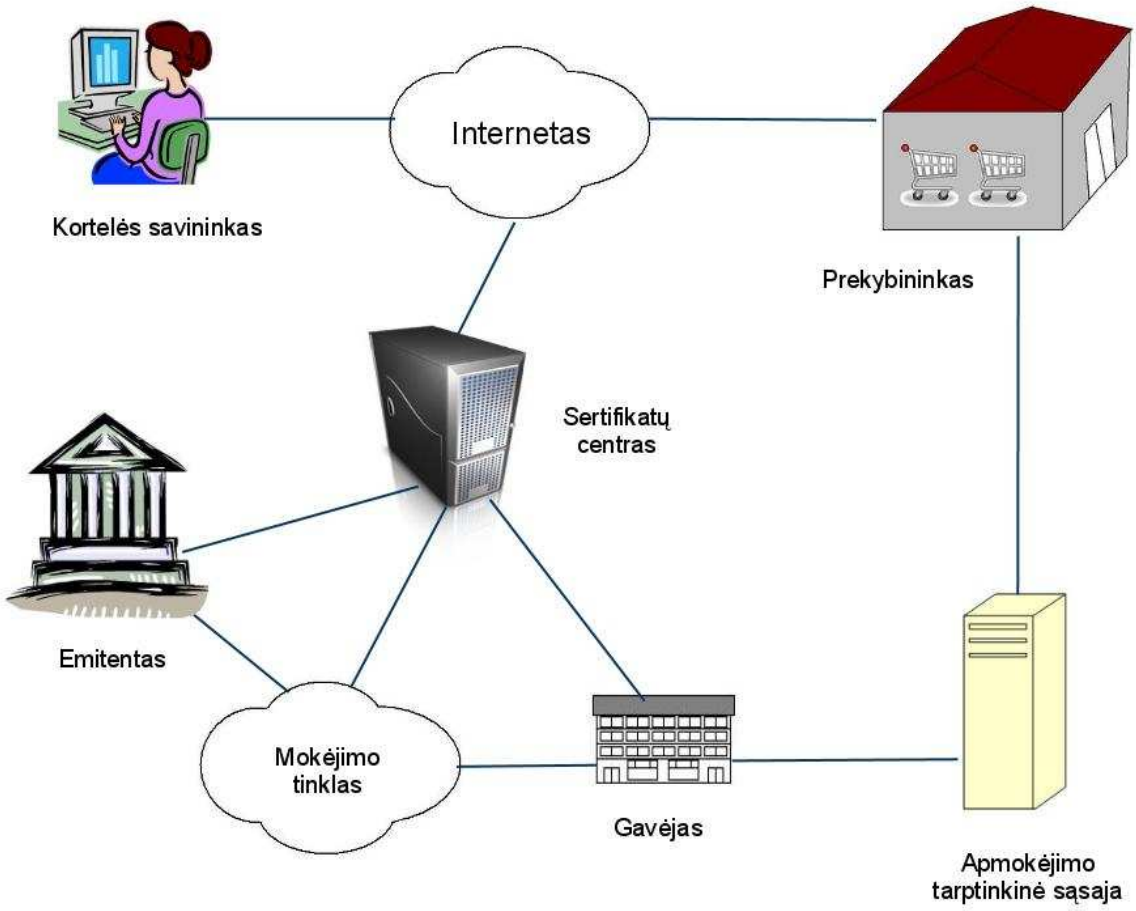
Atsiskaitymas kreditinėmis kortelėmis naudojantis SET

SET – saugos protokolų ir formatų rinkinys, kuris sudaro sąlygas vartotojams saugiu būdu internete veikiančia kredito kortelių mokėjimo infrastruktūra. SET teikiamos paslaugos:

- Informacijos konfidencialumas. Tuo metu, kai kortelės savininko mokėjimo informacija keliauja tinklais, užtikrinamas jos saugumas. Svarbus SET bruožas yra tas, kad protokolas pardavėjui neparodo kredtinės kortelės numerio, jį sužino tik bankas. Konfidencialumui užtikrinti naudojamas standartinis DES šifravimo algoritmas.

- Duomenų vientisumas. SET užtikrina, kad tarp prekybininko ir vartotojo perduodamos informacijos turinys nebus modifikuotas trečiosios šalies. Pranešimo vientisumą garantuoja RSA skaitmeninis parašas. Informacijos apsaugai taip pat pasitelkiami HMAC ir SHA-1 algoritmai.
- Kortelės savininko sąskaitos autentifikavimas. SET leidžia prekybinkui patikrinti, ar kortelės savininkas yra teisėtas šios kortelės sąskaitos numerio vartotojas. Šiam tikslui SET naudoja X.509v3 skaitmeninį serftifikatą su RSA skaitmeniniu parašu.
- Prekybininko autentifikavimas. SET suteikia kortelės savininkui galimybę patikrinti, ar prekybininkas turi ryšį su finansine institucija, galinčia priimti mokėjimo korteles. Šiam tikslui SET naudoja X.509v3 skaitmeninį sertifikatą su RSA skaitmeniniu parašu [7].

SET dalyvių schema



3 pav. SET dalyvių schema

SET dalyviai:

- Kortelės savininkas. Elektroninėje aplinkoje tiek privatūs vartotojai, tiek organizacijos per asmeninius kompiuterius su prekybininkais bendrauja internetu. Kortelės savininkas yra legalus mokėjimo kortelės, kurią išdavė emitentas, turėtojas.
- Prekybininkas. Tai asmuo ar organizacija, galinti kortelės savininkui parduoti reikamų prekių ar paslaugų. Paprastai šios prekės ir paslaugos siūlomos per elektroninius tinklus ar elektroniniu paštu. Prekybininkas, kuris priima mokėjimo korteles, privalo turėti ryšį su gavėju.
- Emitentas. Finansinė istitucija (pvz bankas), kuris sieja kortelės savininką su mokėjimo kortele.
- Gavėjas. Finansinė institucija, sukurianti ryšį tarp prekybininko, mokėjimo kortelės legalumo ir paties mokėjimo. Prekybinkai paprastai priima daugiau nei vieną kreditinės kortelės tipą, tačiau nenori bendrauti su keliomis bankų kortelių saugos tarnybomis ar su keliais skirtingais emitentais. Gavėjas prekybininkui patvirtinina, kad duotos kortelės sąskaita yra aktyvi, o pasiūlytas pirkinys neviršija kredito limito. Gavėjas taip pat atlieka elektroninį mokėjimo pervedimą į prekybininko sąskaitą. Po to emitentas per mokėjimo tinklą gavėjui iš pirkėjo sąskaitos perveda pinigus.
- Mokėjimo tinklas. Tai dažniausiai tinklu vykdoma funkcija, kurią valdo gavėjas ar nustatyta trečioji šalis. Ji tikrina, ar vykstantys procesai atitinka mokėjimo pranešimus. Naudodamas SET protokolą mokėjimo tinklas stebi, ar kortelės savininkų ir prekybinkų legalumas nustatomas teisingai.
- Sertifikatų centras. Jo paskirtis kortelių savininkams, prekeiviams ir mokėjimo tinklams išduoti X.509v3 viešojo rakto sertifikatus [7].

SET Dvigubas parašas

SET protokolas pasižymi labai svarbia savybe – dvigubu parašu. Dvigubo parašo tikslas – sujungti du pranešimus, skirtus dviem skirtingiems gavėjams. Pavyzdžiui, tuo atveju, kai pirkėjas nori nusiųsti informaciją apie ketinamą įsigyti prekę pardavėjui ir mokėjimui informaciją bankui. Šiuo atveju 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 [7].

Skaitmeniniai piniginiai čekiai

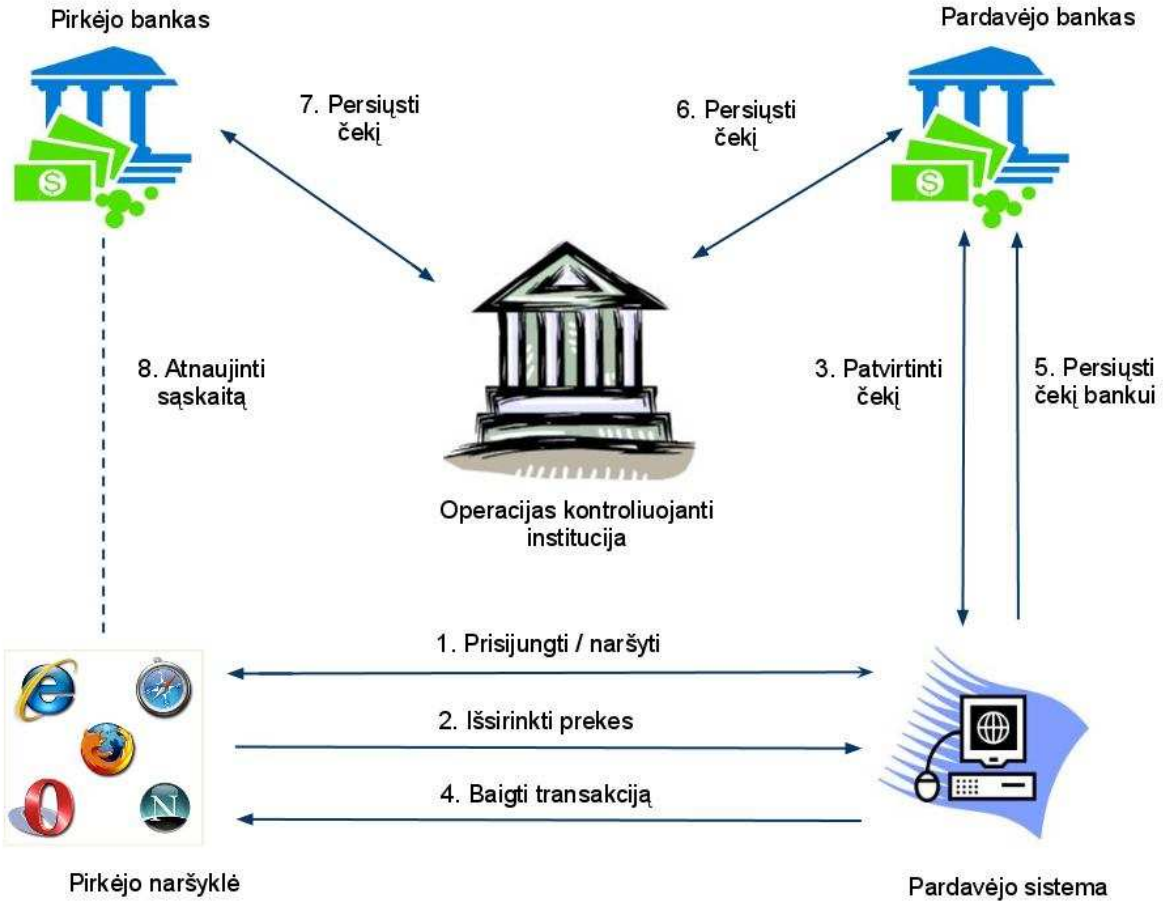
Skaitmeninis piniginis čekis yra popierinio čekio skaitmeninis variantas. Tai dokumentas, kuriame yra nurodymas mokėtojo bankui apie pinigų pavedimą. Elektroninėje komercijoje lėšos, naudojant skaitmeninius piniginius čekius, yra persiunčiamos iš mokėtojo banko sąskaitos į gavėjo banko sąskaitą. Kaip ir įprastiniu variantu, kartu su skaitmeniniu piniginiu čekiu yra pateikiama instrukcija mokėtojo bankui, kad turi būti atliekamas tam tikros sumos mokėjimas identifikuotam gavėjui. Elektroninių piniginių čekių teikiami privalumai:

- Yra galimybė tuoj pat patikrinti lėšas;
- Naudojant skaitmeninį parašą galima užtikrinti saugumą;
- Paprasčiau apiforminamas užsakymas ir sąskaitų apmokėjimas[8].

Atsiskaityme skaitmeniniu čekiu dalyvauja 3 veikėjų grupės:

- Klientas ir pardavėjas;
- Kliento ir pardavėjo bankai;
- Operacijas tvarkanti institucija, kuri vykdo bankinių operacijų tarp skirtingų bankų kontrolę. Funkcijos, kurios priskiriamos operacijas tvarkančiai institucijai, gali būti kontroliuojamos atskiro objekto arba pačių bankų [8].

Vartotojas, naudodamasis naršykle, gali matyti įvairias parduotuves ir jų puslapius. Naršyklėje yra galimybė yra galimybė matyti įvairius skaitmeninio piniginio čekio formatus. Atsiskaitymo trazankcija atliekama keliomis fazėmis. Pirmoje fazėje vartotojas perka. Antroje – pirkėjas siunčia skaitmeninį piniginį čekį savo bankui, kurį jis grąžina pardavėjui. Trečioje fazėje pardavėjo bankas kreipiasi į operacijas tvarkančia instituciją arba į vartotojo banką, kad ji atliktų skaitmeninį atsiskaitymo patikrinimą. Detalesni veiksmai pateikiami 4 paveiksle.



4 pav. Skaitmeninio piniginio čekio veikimo schema

1.4 Veikiančių atsiskaitymo sistemų analizė

1.4.1 Pinigų pervedimų sistemos

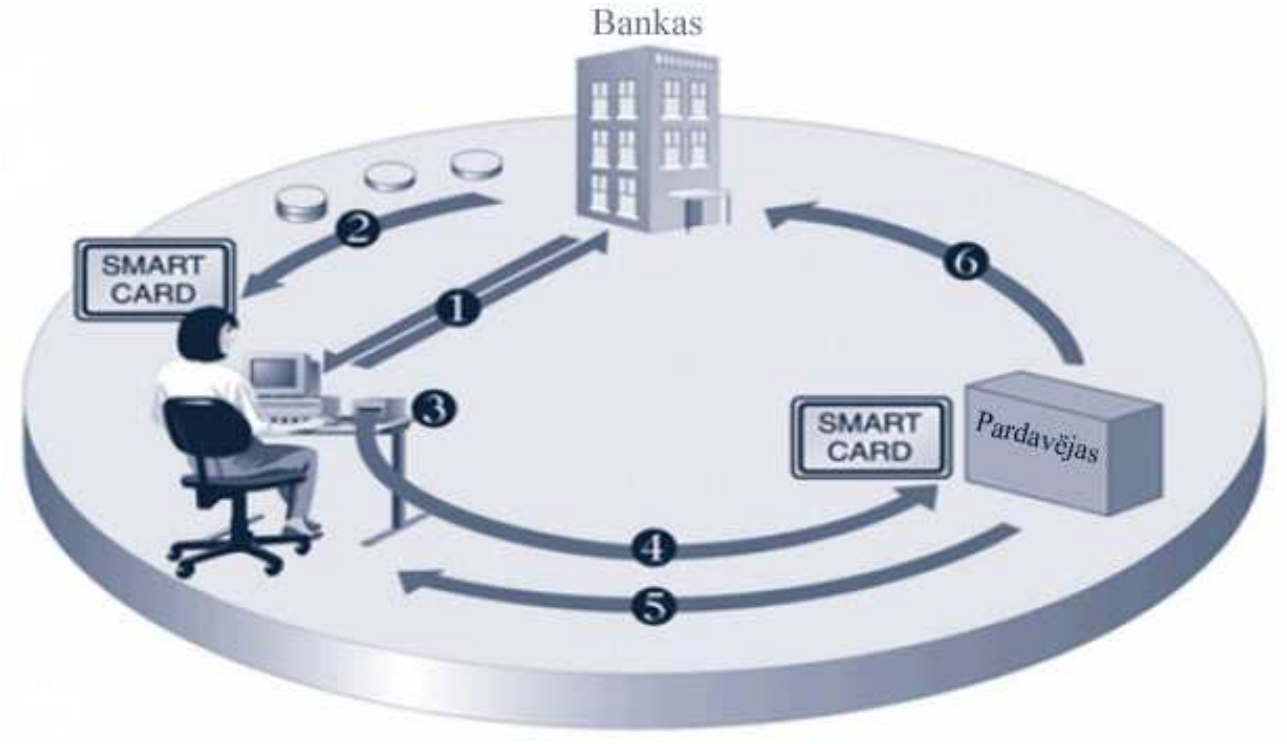
1.4.1.1 Mondex sistema

Mondex sistema yra dalis MasterCard pasaulinio tinklo, leidžianti kortelės turėtojams pernešti, laikyti ir leisti pinigus naudojantis mokėjimų kortele. Tai yra greitesnis būdas atsiskaityti nei tradicinė valiuta ir dažnai saugesnis. Šis būdas yra panašus į mokėjimą grynais pinigais, leidžiantis atsiskaityti nedelsiant, bet kartu nereikalaujant PIN kodų ar pervedimo autorizacijos. Unikali Mondex platforma leidžia naudotis tokiose terpėse, kur įprasti pinigai negalimi:

- Internetas;
- Mobilūs telefonai;
- Interaktyvi televizija;

Mondex sistema pinigus laiko elektronine forma mikroshemoje. Vykstant atsiskaitymui, dalis pinigų vertės perkeliama iš mikroschemos kortelėje į mikroschemą terminale(kortelės skaitytuve) [9].

Veikimo schema



5 pav. Mondex veikimo schema

1) Vartotojas atsidaro sąskaitą ir gauna smart card kortelę;
2) Vartotojas parsisiunčia iš banko pinigus ir įrašo į kortelę;
3) Vartotas įdeda kortelę į skaitytuvą;
4) Atsiskaitant už prekes ar paslaugas, pinigų suma iš kortelės nusiunčiama pardavėjui;
5) Pardavėjas pristato prekes ar suteikia paslaugas;
6) Pardavėjas nusiunčia pinigus į savo sąskaitą banke [6].

Mondex schemos elementai

- Kortelės, užprogramuotos gauti ir kaupti vertę;
- Prietaisai, sugebantys išsiųsti vertę į kortelę;
- Prietaisai, sugebantys gauti vertę parsiųstą iš kortelės;
- Programinė įranga ir kiti prietaisai;

Mondex atsiskaitymuose naudojami prietaisai

- Specialūs kasos aparatai (Electronic cash register);
- Elektroninės piniginės (Electronic wallet);
- Likučio skaitytuvai (Key fob balance reader);
- Mondex telefonai (Mondex telephone);
- Pinigų perkėlimo terminalai (Value transfer terminal);
- Kortelių skaitytuvai (IC card reader/writer);

Sistemos saugumas

Kiekvieną kartą naudojantis Mondex kortele, mikroprocesorius kortelėje sukuria unikalų skaitmeninį parašą, kuris gali būti pripažintas kitos Mondex kortelės su kuria atliekamas sandoris. Kortele nesinaudojant, ją galima užrakinti, o prieš naudojant atrakinti įvedus asmeninį vartotojo numerį (PCN). PCN numeris gali būti pakeistas tik pasinaudojus Mondex pinigine ar asmeniniu Mondex telefonu [9].

Pagrindiniai privalumai

- Patogumas. Sistema leidžia vartotojui atlikti mokėjimą neieškant bankomato ar gaištant laiką autorizuojantis. Atsiskaityti galima netik su pardavėjais ar paslaugų tiekėjais, bet ir kitais kortelės naudotojais (fiziniais asmeninimis);
- Saugumas. Kortelėje įdiegta jos užrakinimo (lock) funkcija, kuri gali apsisaugoti nuo neleistino panaudojimo. Užrakinimo kodas yra parenkamas kortelės savininko ir gali būti bet kuriuo metu pakeistas;
- Lankstumas. Sistema gali atsiskaityti už betką ir praktiškai betkokia realia pinigų suma. Vienu metu kortelėje gali būti laikomi 5 skirtingų valiutų pinigai;
- Kontrolė. Kortelės savininkas gali išleisti tik tiek, kiek pinigų yra kortelėje, todėl negresia skolos ar limito pereikvojimai.

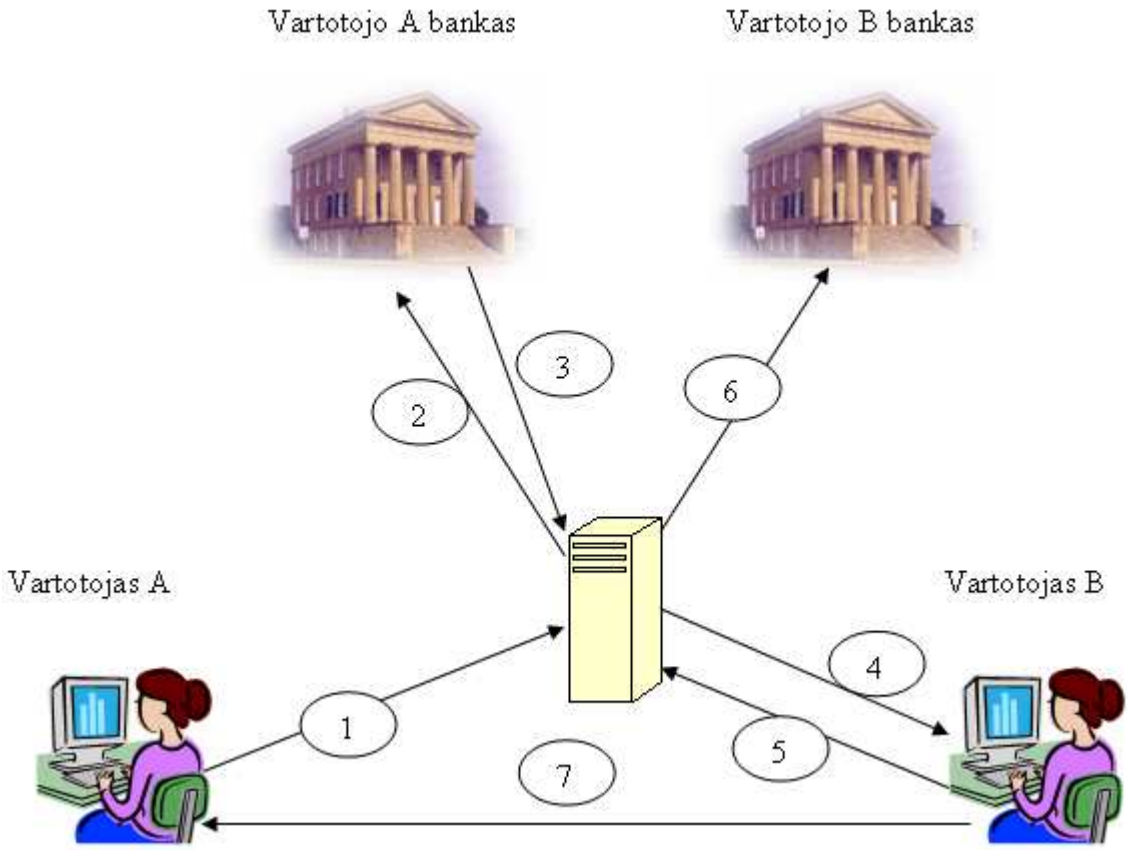
Pagrindiniai trūkumai

- Reikia turėti specialią įrangą;
- Sandoriai nėra visiškai anoniminiai;
- Pametus kortelę pinigai prarandami (nebent ji būtų rasta ir grąžinta į banką);
- Po daugelio sandorių gali įvykti perpildymas dėl kortelės atminties ribotumo [9].

1.4.1.2 PayPal sistema

PayPal - pirmoji pasaulyje elektroninių pinigų sistema, sukurta JAV 1993 m. Ši sistema atlieka tarpininko, patikimos trečiosios šalies vaidmenį tarp pardavėjo ir pirkėjo, o dažnai ir tarp klientų. Paypal supaprastina atsiskaitymus kreditinėmis kortelėmis, suteikia daugiau anonimiškumo ir saugumo, o vartotojus patraukia paprastumu ir prieinamumu (viskas valdoma per internetinio puslapio sąsają). Vartotojas registruodamasis sistemoje turi pateikti tikrą vardą, pavardę, gimimo datą, gyvenamosios vietos adresą, elektroninį paštą. Asmens tapatybė užtikrinama įvedant kreditinės kortelės numerį ir jos saugos kodą (CVV2), kurį žinoti turi tik kortelės savininkas. Gavusi šiuos duomenis, PayPal atlieka nedidelės vertės pervedimą į kliento kreditinės kortelės sąskaitą, prašydama nurodyti pervestą sumą. Tikslią sumą gali sužinoti tik asmuo, kuriam priklauso sąskaita. Tokiu būdu įsitikinama, kad tam tikras asmuo, tikrai yra tas, kuriuo dedasi. Tokiam sistemos nariui suteikiamas statusas „patvirtintas“ (verified) ir jis gali naudotis visais sistemos privalumais [10].

Atsiskaitymų Paypal sistemoje schema



6 pav. Atsiskaitymų schema PayPal sistemoje

1) Vartotojas A atlieka pervedimą sistemoje tam tikra suma vartotojui B
2) Paypal sistema siunčia prašymą vartotojo A bankui nurodytai sumai
3) Vartotojo bankas perveda pinigus paypal sistemai
4) Vartotojas B informuojamas apie gautas įplaukas
5) Vartotojas B paprašo pervesti pinigus į jo banko sąskaitą
6) Paypal sistema perveda pinigus į vartotojo B banko sąskaitą
7) Vartotojas B suteikia vartotojui A prekes ar paslaugas

Pervedimai sistemoje įskaitomi akimirksniu, todėl po pirmo žinsgnio seka ketvirtas ir iškart gali sekti septintas, o antras trečias ir šeštas žingsniai atliekami vėliau, prisitaikant prie bankų darbo laiko ir specifikos. Vartotoju B gali būti tiek pardavėjas (nuolat užsiemantis šia veikla), tiek fizinis asmuo parduodantis tam tikrą daiktą vieną kartą, tiek paprastas asmuo pinigus gaunantis kaip paramą ar dovaną (pvz šeimos narys, giminaitis esantis užsienyje), todėl septintas punktas gali ir negzistuoti [10].

Paypal sistema yra ganėtinai lanksti, todėl vartotojas B neprivalo iškart persivesti pinigų į savo banko sąskaitą (penktas ir šeštas žingsniai) ir gali juos kiek nori laiko laikyti sistemoje, juos pervesti kitiems asmenims, o bet kada panorėjus – persivesti į savo banko sąskaitą. Lygiai taip pat vartotojas A gali turėti pakankamą sumą Paypal balanse ir iš jo atlikti pervedimą (tuomet antras ir trečias žingsniai nevykdomi) [10].

Sistemos saugumas

PayPal sistemoje internetiniai puslapiai ir perduodami duomenys apsaugomi naudojant Secure Sockets Layer (SSL) protokolą. Tapatumą patvirtina kompanija „Verisign“, informacija šifruojama 3DES algoritmu, 168 bitų raktu. Vartotojas atpažįstamas pagal įvestą elektronio pašto adresą ir slaptažodį. Slaptažodį turi sudaryti bent 8 simboliai [10].

Sistemos privalumai

- Paslauga prieinama daugiau kaip 180 pasaulio šalių
- Paprasta gauti ir siųsti pinigus
- Pirkėjams visiškai nemokama paslauga
- Užtikrinama kreditinių kortelių ir bankų sąskaitų slaptumas
- Visi pervedimai yra momentiniai (nereikia laukti)

Sistemos trūkumai

- Dėl populiarumo tarp vartotojų, PayPal yra pamėgta kreditinių kortelių vagių ir kitų piktavalių

1.4.2 Užskaitų sistemos

1.4.2.1 Užskaitų sistema „eBuhalteris.lt“

eBuhalteris.lt – internetinė tarpusavio užskaitų sistema (ITUS). Tai specializuota duomenų bazė, skirta gauti informaciją apie galimus debitorinius atsiskaitymus. Projekto tikslas – efektyvesnė kompanijų aspkaita. ITUS naudotojai turi galimybę sumažinti pradelstų gautinų apmokėjimų skaičių bei sutrumpinti laukiamų apmokėjimų terminą [11].

Sistemos veikimo principas

- Įmonė užsiregistruoja sistemoje;
- Įmonė pateikia informaciją apie savo debitorius;
- Įmonė atlieka paiešką sistemoje ir savo el.paštą gauna pranešimą apie galimą užskaita ir šalių kontaktinis duomenis;

- Šalims pasirašius dokumentus įvykdoma užskaita [11].

Pagrindiniai privalumai

- Paprasta naudotis. Norint pradėti naudotis, įmonei tereikia suvesti savo duomenis ir palaukti, kol administratorius juos patvirtins;
- Integracija su buhalterinėmis programomis. Sistema suteikia galimybę debitorių sąrašą importuoti iš tokią funkciją palaikančių apskaitos programų („Centas“, „Būtent“, „Paulita“, „Stekas“, „Pragma“, „Tėja“) [11].

Pagrindiniai trūkumai

- Nėra naudojamas centralizuotas e.parašas. Gautų dokumentų pasirašymą įmonės turi inicijuoti pačios (tiek elektroniniu, tiek įprastu būdu). Todėl vieningo e.parašo nenaudojimas gali sukelti papildomų problemų;
- Standartinis prisijungimas. Prie sistemos prisijungiama tradiciniu būdu – vartotoju vardu ir slaptažodžiu, kas įpareigoja vartotoją įsiminti papildomų duomenų ir neskatina perėjimo prie pažangesnių e.parašų.

1.4.2.2 Debitorinių įsiskolinimų valdymo sistema debitoriai.lt

Debitoriai.lt - tai kompleksinis sprendimas efektyviam debitorinių įsiskolinimų valdymui. Sprendimas apima debitorinių įsiskolinimų prevenciją, klientų stebėseną, skolų susigrąžinimą, nesikreipiant į skolų išieškojimo bendroves ar teismą, trišales skolų užskaitas, skolų perleidimą tretiems asmenims [12].

Kreditorių galimi atlikti veiksmai

- Registruoti debitorinių įsiskolinimų informaciją iš karto po to, kai yra išrašoma sąskaita faktūra už patiektas prekes ar suteiktas paslaugas.Tai atliekama periodiškai įkeliant į sistemą neapmokėtų sąskaitų sąrašą;
- Periodiškai priminti savo klientams apie neapmokėtas sąskaitas. Sistema pagal neapmokėtų sąskaitų sąrašą tikrina, kada kokia sąskaita turi būti apmokėta ir pagal įmonės individualius nustatymus siunčia el.paštu debitoriui priminimus apie pradelstus mokėjimus;
- Stebėti savo klientų mokumo būklę. Tuo tikslu projekto dalyvis sudaro jį dominančių įmonių sąrašą. Stebėjimo metu fiksuojami įmonių debitorinių įsiskolinimų pasikeitimai ir apie juos kartą į savaitę yra informuojama el.paštu;

- Ieškoti informacijos apie tam tikros įmonės skolų apmokėjimo praktiką. Susipažinti su įmonės kredito istorija yra būtina prieš suteikiant jai kredito limitą ar tam tikros trukmės atidėjimo terminus;
- Paviešinti delsiančias ar vengiančias apmokėti skolą įmones tam skirtame informaciniame skolininkų portale. Paviešinimas atliekamas automatiškai jei debitorius nesureaguoja į raginimus atsiskaityti. Per kiek dienų po apmokėjimo termino pradelsimo debitorius įtraukiamas į skolininkų sąrašus ir viešai paskelbiamas kiekvienas projekto dalyvis nustato individualiai;
- Atlikti trišales užskaitas. Sistema periodiškai pagal esamus duomenis tikrina trišalių užskaitų galimybę ir apie jas informuoja projekto dalyvius el.paštu.
- Parduoti debitorinius įsiskolinimus [12].

Debitorių galimi atlikti veiksmai

- Matyti, kas ir kokius Jūsų debitorinius įsiskolinimus yra užfiksavę sistemoje ir pasirūpinti laiku padengti įsiskolinimą, kad Jūsų įmonės kredito istorija išliktų švari;
- Nesutikti su viena ar kita Jūsų įmonei pareikšta pretenzija dėl įsiskolinimo;
- Ieškoti galimų trišalių užskaitų savo debitoriniams įsiskolinimams padengti. Tuo tikslu turite patalpinti į sistemą ne tik savo skolininkus, bet ir įmones kurioms yra skolinga Jūsų įmonė (jei apie Jūsų skolą kreditorius jau yra įvedęs informaciją, tai antrą kartą įvedinėti nereikia). Jūsų pačių įvesti įsiskolinimai kitoms įmonėms bus naudojami tik galimom užskaitom rasti [12].

Pagrindiniai privalumai

- Galimybė užsisakyti priminimus apie esamus įsiskolinimus;
- Galimybė nepripažinti skolos;
- Nėra viešai atskleidžiami kreditoriaus tapatybė;
- Galima intergracija su buhalterinėmis programomis.

Pagrindiniai trūkumai

- Nėra naudojamas centralizuotas e.parašas;
- Standartinis prisijungimas. Prie sistemos prisijungiama tradiciniu būdu – vartotoju vardu ir slaptažodžiu, kas įpareigoja vartotoją įsiminti papildomų duomenų ir neskatina perėjimo prie pažangesnių e.parašų.

1.5 e. parašo panaudojimo galimybės

1.5.1 e. parašo veikimo principas

e.parašas (dar vadinamas skaitmeniniu parašu) yra apibrėžiamas kaip saugumo mechanizmas, įtrauktas kito skaitmeninio įrašo viduje, kuris įgalina įrašo kūrėjo identifikavimą ir taip pat leidžia nustatyti, ar įrašas nebuvo modifikuotas. [13] Skaitmeniniai parašai patvirtinina, kad dokumentą sukūrė būtent ta organizacija ar asmuo, kurį reprezentuoja skaitmeninis parašas. Skaitmeninis parašas yra duomenų rinkinys, gaunamas iš pasirašomo pranešimo arba dokumento ir pasirašančio asmens privataus rakto, panaudojant parašo šifravimo algoritmą. Skaitmeniniai parašai būna pridėti prie pranešimo, kad pagal jį būtų galima identifikuoti siuntėją. Gavėjas patikrina skaitmeninį parašą, iššifruodamas jį siuntėjo viešuoju raktu. Tokiu būdu yra užtikrinama, kad bendraujama tikrai su tuo, kuo reikia.[8]

Viešojo rakto infrastruktūra

Viešojo rakto infrastruktūra yra viena iš pagrindinių technologijų, leidžiančių laikytis saugumo reikalavimų. Ši technologija yra skaitmeninių sertifikatų ir sertifikuojančių įstaigų sistema, patvirtinanti šalių dalyvaujančių tam tikrame procese teisėtumą. Viešojo rakto infrastruktūros funkcijos leidžia sukurti ir valdyti viešuosius ir privačius raktus, kurie reikalingi sistemų funkcionavimui. Ši technologija yra pagrindas, pagal kurį sukuriami visi kiti sistemų ir tinklų saugumo komponentai. Tai leidžia užtikrinti konfidencialumą, vientisumą, nepaneigiamumą ir autentiškumo nustatymą.[8]

Pagrindiniai viešojo rakto infrastruktūros komponentai:

- Sertifikavimo įstaiga, kurianti ir pasirašanti skaitmeninius sertifikatus. Ji taip pat prižiūri sertifikatų atšaukimo sąrašus, viešai pateikia sertifikatus, bedradarbiauja su administratoriais;
- Registravimo įstaiga, tikrinanti organizacijų ir asmenų pateikiamus dokumentus, norint nustatyti, ar būtent ta organizacija ar asmuo nori gauti sertifikatą;
- PKIX standartas, apibrėžiantis viešųjų raktų sertifikatų turinįir nustatantis standartus, leidžiančius sukurti tarpusavio sąryšį tarp skirtingų sertifikavimo įstaigų sukurtų skaitmeninių sertifikatų.[8].

Viešojo rakto infrastruktūra tampa labai svarbi kilus sukčiavimo atvejui, kai kai pakeičiamas dokumentų turinys arba atskleidžiamas siunčiamų tinklu duomenų turinys arba kai yra būtinas asmens ar organizacijos identiteto patvirtinimas. Dėl šių priežasčių organizacijoms,

dirbančioms verslo, elektroninės vyriausybės ar finansų srityse yra ypač tinkslinga naudoti viešojo rakto infrastruktūrą.[8]

Viešojo rakto infrastruktūros privalumai:

- Mažesni tranzakcijų kaštai;
- Mažesnė ir labiau išskaidyta rizika;
- Pasiekiamas didesnis efektyvumas ir geresnės sistemos bei tinklo charakteristikos;
- Mažesnis saugumo sistemų sudėtingumo laipsnis [14].

1.5.2 E. Parašo juridinis pagrindas

LR seimas 2000-07-11 priemė „Elektronio parašo įstatymo“, kuriuo remiantis visi e.parašu pasirašyti dokumentai gali turėti tokią pačią juridinę galią kaip ir ranka pasirašyti dokumentai. Toliau pateikiamos esminės šio įstatymo ištraukos.

LR Elektroninio parašo įstatymas

Publikavimas: Valstybės žinios, 2000-07-26, Nr. 61-1827

2000-07-11 Priėmė - Lietuvos Respublikos Seimas

Statusas: Įsigalioja nuo 2000-07-26

Ištraukos:

2 straipsnis. Pagrindinės šio įstatymo sąvokos

4. **Elektroninis parašas** (toliau - **parašas**) - duomenys, kurie įterpiami, prijungiami ar logiškai susiejami su kitais duomenimis pastarųjų autentiškumui patvirtinti ir (ar) pasirašančiam asmeniui identifikuoti.

5. **Saugus elektroninis parašas** - elektroninis parašas, kuris atitinka visus šioje dalyje nurodytus reikalavimus:

1) yra vienareikšmiškai susietas su pasirašančiu asmeniu;

2) leidžia identifikuoti pasirašantį asmenį;

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

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

11. **Saugi parašo formavimo įranga** - parašo formavimo įranga, kuri atitinka visus šioje dalyje nurodytus reikalavimus:

1) parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, praktiškai įmanoma gauti tik vienintelį kartą, ir užtikrinamas jų slaptumas;

2) parašo formavimo duomenų, naudojamų elektroniniam parašui sukurti, atkurti praktiškai neįmanoma, ir nuo elektroninio parašo klastočių apsaugo esamos technologijos;

3) parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, pasirašantis asmuo gali patikimai apsaugoti nuo kitų asmenų;

4) parašo formavimo įranga, kuriant elektroninį parašą, nekeičia pasirašomų duomenų ir netrukdo pasirašančiam asmeniui stebėti tuos duomenis prieš pasirašant.

8 straipsnis. Elektroninio parašo galia

1. Saugus elektroninis parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu, elektroniniams duomenims turi tokią pat teisinę galią kaip ir parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme.

2. Elektroninis parašas negali būti laikomas negaliojančiu dėl bet kurios iš žemiau išvardytų priežasčių:

1) kad yra elektroninis;

2) kad nėra paremtas kvalifikuotu sertifikatu;

3) kad nėra paremtas akredituoto sertifikavimo paslaugų teikėjo išduotu kvalifikuotu sertifikatu;

4) kad nėra sukurtas saugia parašo formavimo įranga [15].

1.6 e. parašo sistemos

1.6.1 KTU akademinė e.parašo sistema

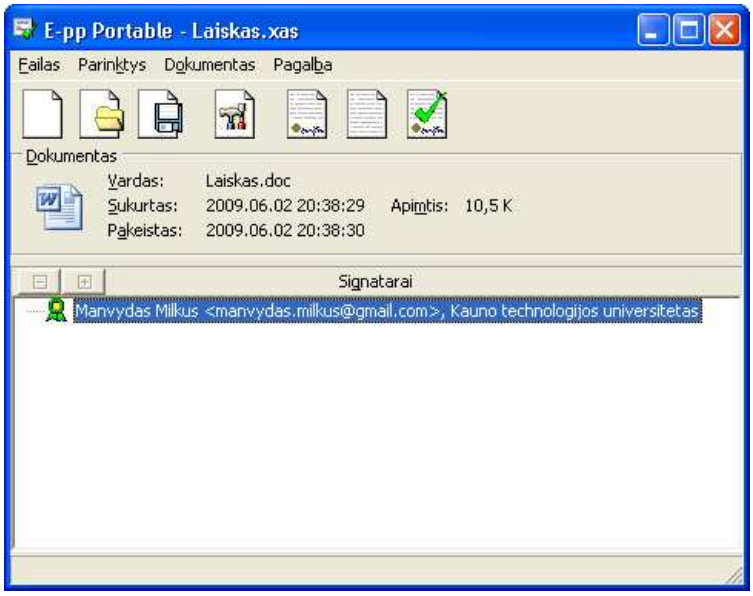
KTU akademinė e.parašo sistema (dar vadinama „a-sign“) susideda iš e.parašo programinės įrangos ir e.parašo infrastruktūros. Naudojimasis sistema yra nemokamas ir atviras visiems. Norint naudotis akademiniu parašu reikia:

- atsisiųsti ir įdiegti raktų generavimo programą
- susigeneruoti viešą ir privatų raktus
- gauti a-sign sertifikatą

- įsirašyti viešą, privatų raktus ir sertifikatą į USB atmintinę (papildomai galima įdiegti juos kompiuteryje)
- atsisiųsti ir įdiegti parašo formavimo bei tikrinimo programinę įrangą. [16]

e.parašo programinė įranga „epp Portable“

Naudojantis šia programa vartotojas gali pasirašyti kompiuteryje laikomus įvairių formatų dokumentus ir failus, patikrinti seniau pasirašytų ar iš kitų asmenų gautų dokumentų parašus, iš pasirašyto dokumento išgauti dokumento originalą. Programa nesudėtinga naudoti, sąsaja lietuvių kalbą. Žemiau pateikiamas programos darbo langas (pav. 7):



7 pav. Programos epp Portable darbo langas

Akademiniame paraše naudojamas rsa-sha1 algoritmas parašo formavimui, xmldsig parašo struktūra, informacija koduoja base64 kodavimu.

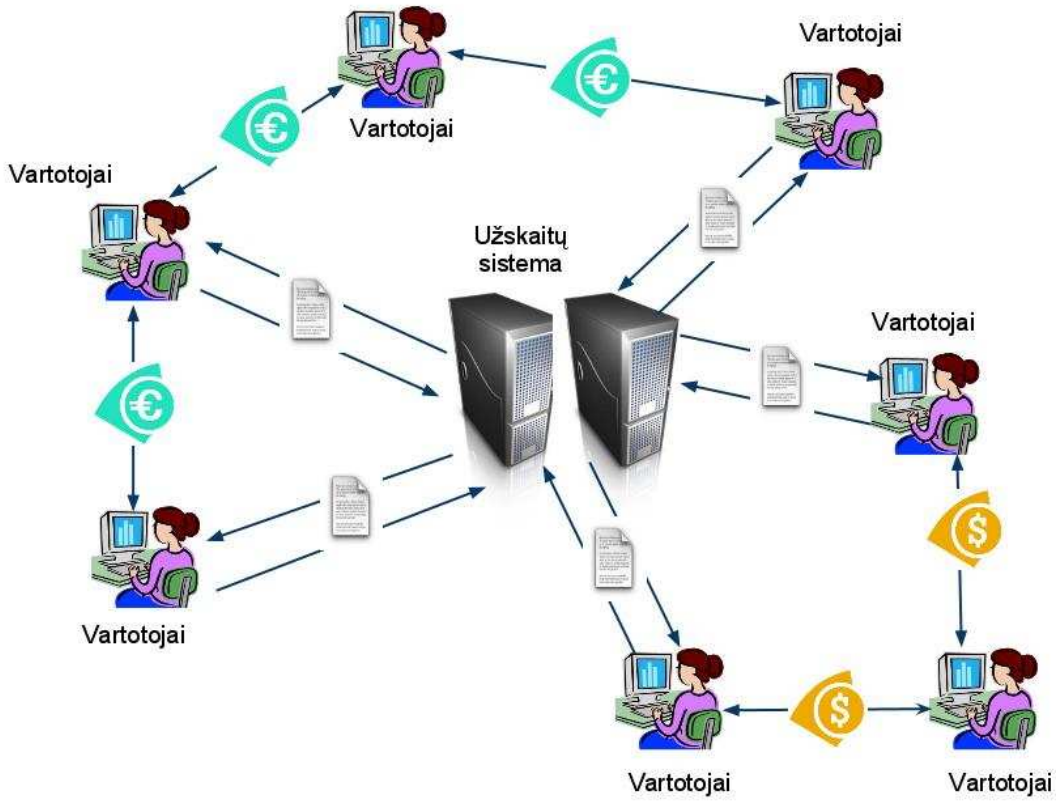
1.7 Analizės išvados

Analizės dalyje apžvelgti įmonių naudojami tarpusavio atsiskaitymo būdai ir po dvi elektroninių perdvedimų bei užskaitų sistemos, išskirti jų trūkumai ir privalumai. Surastos užskaitų sistemos, leidžia teigti, jog tarpusavio užskaitų sistemos yra daugiau ar mažiau aktualios šių laikų vartotojams. Pastebėta, kad atsiskaitymuose vis dar nenaudojamas e.parašas. Įsigilinus į e.parašo panaudojimo galimybes, nustatyta, kad tai tinkama technologija.

2 SAUGIŲ TARPUSAVIO ATSISKAITYMŲ SISTEMOS PROJEKTINĖ DALIS

2.1 Sistemos koncepcija

Verslo subjektai tarpusavyje vykdo su verslu susijusią veiklą (perka, parduoda, gauna ir priima apmokėjimus), o apie nepadengtus įsiskolinimus informuoja sistemą, siųsdami e.dokumentus, pasirašytus e.parašu (taip pat ir patvirtina esamus įsiskolinimus kitiems vartotojams). Atsiradus skolų minimizavimo poreikui, sistemos vartotojai atlieka paiešką duomenų bazėje ir esant skolų užskaitymo galimybei, ją įvykdo, atsiųsdami tokius užskaitymus patvirtinančius, e.parašu pasirašytus, dokumentus (pav. 8).



8 pav. Sistemos koncepcijos schema

2.2 Iškelti reikalavimai

2.2.1 Reikalavimai sistemai

Sistemai keliami reikalavimai:

- Jei įmanoma, sistema vartotojui turi būti prienama 24 valandas per parą, 7 dienas per savaitę;
- Sistema turi identifikuoti ir autentifikuoti vartotojus pagal jų e.parašą;
- Sistema turi turėti savo e.parašą ir galėti juo pasirašyti dokumentus;
- Sistema turi galėti patikrinti pasirašytų dokumentų teisingumą;
- Sistema visus duomenis turi talpinti duomenų bazėje, ir esant poreikiui, informaciją iš jos nuskaityti;
- Sistema turi turėti galimybę ieškoti skolas anuliuojančių ciklų kiekvienam vartotojui;
- Apie svarbiausius įvykius sistema vartotojus turi informuoti e.paštu;
- Sistema turi galėti generuoti konkrečios struktūros dokumentus;
- Sistema turi priimti ir apdoroti konkrečios struktūros dokumentus;
- Dokumentams turi būti naudojama XML žymėjimo kalba;
- Vartotojui ir iš vartojo siunčiami/gaunami duomenys turi būti siunčiami saugiu kanalu.

2.2.2 Reikalavimai vartotojo sąsajai

Vartotojo sąsajai keliami reikalavimai;

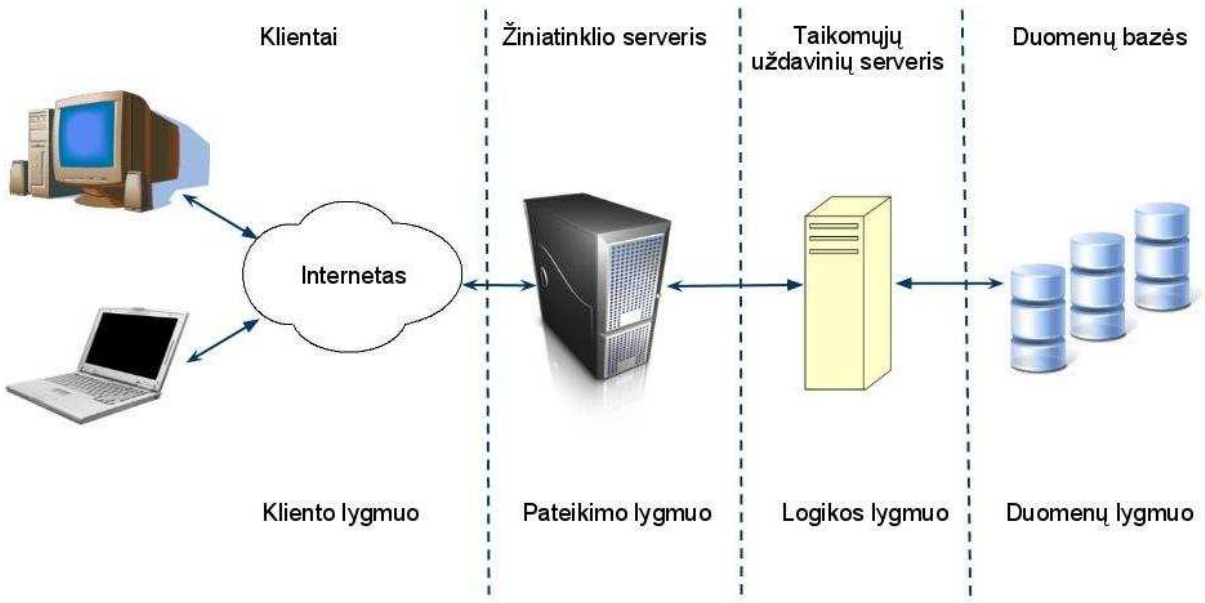
- Vartotojo sąsaja turi būti paremta žiniatinklio technologija ir prieinama per internetą naudojantis interneto naršykle;
- Prisijungimas prie sistemos turi būt galimas visomis populiariausiomis naršyklėmis, nepriklausomai nuo operacinės sistemos;
- Vartotojas prisijungti per sistemos turi tik naudojantis e. Parašu;
- Visi vartotojui galimi veiksmai turi būti pasiekiami per grafinius meniu punktus (nenaudojamos komandinės eilutės, programavimų kalbų);
- Vartotojas turi galėti peržiūrėti įvykdytų užskaitymų įstoriją, ieškoti naujš galimų užskaitymų, juos inicijuoti, įvesti ir anuliuoti savo bei kitų vartotojų skolas.

2.3 Sistemos lygmenys

Visą sistemą galima padalinti į 4 lygmenis (pav. 9):

- Kliento lygmenį, kuriame vyksta informacijos mainai tarp sistemos ir vartotojų;
- Pateikimo lygmenį, kuriame iš apdorotų rezultatų generuojamas dinamiškai besikeičiantis turinys;

- Taikomųjų uždavinių lygmenį, kuriame atliekami skaičiavimai;
- Duomenų lygmenį, kuriame saugoma visa reikalinga informacija.



9 pav. Sistemos lygmenys

2.3.1 Informacijos mainų modelis

Informacijos mainų modulio pagrindinės funkcijos:

- Informacijos įvedimas į sistemą;
- Dokumentų formavimas;
- Informacijos išvedimas;
- Informacijos perdavimo tarp sistemos vartotojų ir sistemos.

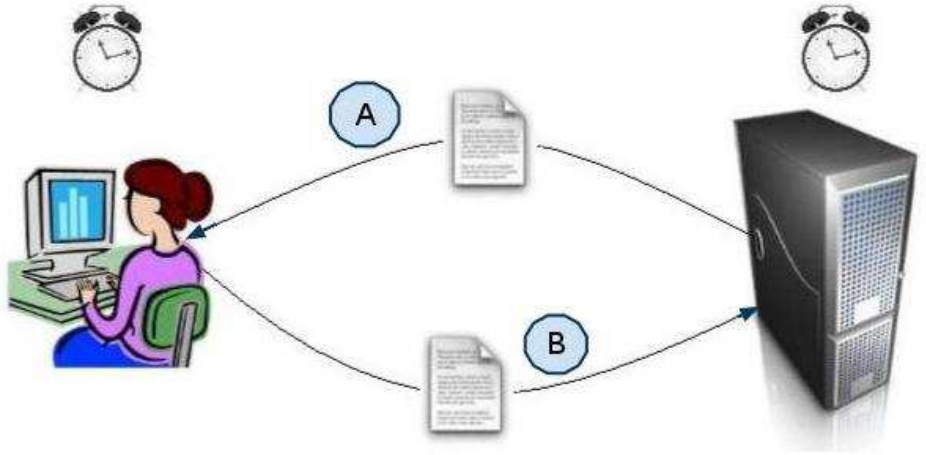
Informacijos įvedimas į sistemą

Informacijos įvedimas į sistemą susideda iš:

- Identifikacijos ir autentifikacijos;
- Parašo patikros;
- Dokumento sintaksės kontrolės;
- Informacijos logikos kontrolės;
- Informacijos įrašymo į duomenų bazę;

2.3.2 Identifikacijos ir autentikacijos modelis

Visi vartotojai, norintys prisijungti prie sistemos turi sėkmingai įvykdyti identifikaciją ir autentifikaciją. Tai atliekama vartotojui atsidarius prisijungimo puslapį ir paprašius prisijungimo failo. Sistema sukuria failą, jį pasirašo ir pateikia vartotojui (pav. 10 A dalis). Vartotojas turi 10 minučių suformuota failą pasirašyti ir vėl grąžinti sistemai (pav. 10 B dalis). Sistema, gavusi iš vartotojo failą, patikrina vartotojo parašą, savo parašą ir pasirašymų laikus. Jei parašai autentiški, o laiko tarpas, praėjęs tarp pirmo pasirašymo ir dokumento pateikimo nėra didesnis nei leidžiama, vartotojas identifikuojamas pagal jo sertifikato informaciją ir jam suteikiamas priėjimas prie sistemos. Pagrindinis tokio idenfikavimo ir autentifikavimo metodo privalumas yra tai, kad vartotojui nereikia žinoti jokio papildomo prisijungimo vardo ir atsiminti dar vieno slaptažodžio.



10 pav. Identifikacijos ir autentifikacijos schema

2.3.3 Dokumento sintaksės kontrolė

Kadangi pasirašyti dokumentai yra pateikiami XML formatu, o šis formatas pasižymi griežta dokumento tvarka, todėl įmanoma patikrinti, ar failas neturi XML sintaksės klaidų. Pagrindinė taisyklė yra tai, kad dokumente visada turi būti uždaranti žyma jeigu yra atidaranti arba pabaigos ženklas turi būti toje pačioje žymoje (jei naudojama tik viena).

Pasirašytame dokumente naudojamos žymos:

`<SignedDoc>` - naudojamas aprašyti sukurtą dokumentą;

`<DataFile>` - naudojamas aprašyti pasirašytą dokumentą;

`<Signature>` - naudojamas parašui aprašyti;

`<SignatureMethod>` - naudomas parašo metodui nuskayti;

`<Transform>` - naudojamas informacijos transformavimui aprašyti;

<DigestMethod> - naudojamas santraukos metodui aprašyti;

<DigestValue> - naudojamas santraukos vertei nurodyti;

<X509Data> - naudojamas X.509 standarto sertifikato informacijai nurodyti;

<X509Certificate> - naudojamas sertifikatui pateikti;

<SigningTime> - naudojamas pasirašymo laiko nurodyti;

<Signer> - naudojamas pasirašusiam asmeniui nurodyti;

<Name> - naudojamas pasirašusio asmens tapatybei nurodyti;

Papildomai dokumentuose naudojamos žymos:

<dokumentas> </dokumentas> su atributu nr - dokumento pradžiai ir pabaigai žymėti;

<subjektas></subjektas> - atskiriems subjektais atskirti su atributu id;

<data> </data> - datai žymėti;

<vardas> </vardas> - subjekto vardui žymėti;

<pavarde> </pavarde> - subjekto pavardei žymėti;

<pavadinimas> </pavadinimas> - įmonės pavadinimui žymėti;

<suma></suma> - skolos sumai žymėti;

<adresas></adresas> - subjekto adresui žymėti;

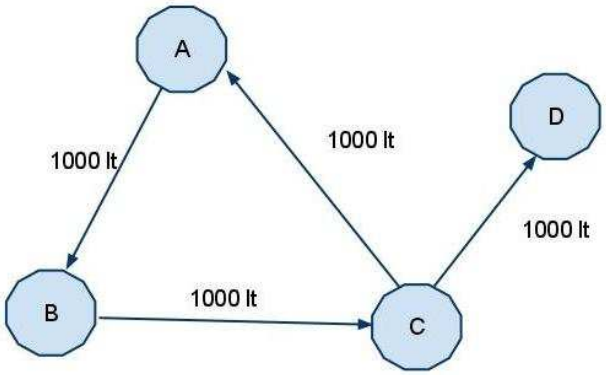
<saskaita> </saskaita> - subjekto sąskaitos numeriui žymėti;

<banko_kodas></banko_kodas> - subjekto naudojamo banko kodui žymėti;

<swift></swift> - subjekto sąskaitos swift kodui žymėti;

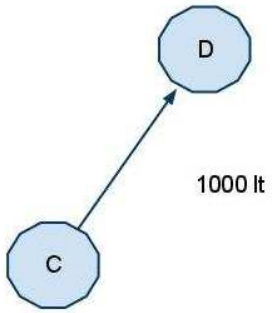
2.4 Skolų užskaitymo modelis

Norint geriau suprasti tarpusavio skolų užskaitymo principą panagrinėkime nesudėtingą pavyzdį: Tarkime, kad Jonas Jonaitis (pavadinkime jį vartotoju A) yra skolingas 1000 litų Petrui Petraičiui (jį pavadinkime vartotoju B), šis savu ruoštu skolingas 1000 litų Giedriui Giedraičiui (vartotojas C), o pastarasis skolingas po 1000 lt Jonui Jonaičiui ir Tadui Tadauskui (vartotojas D). Tai schematiškai pavaizduota 11 paveiksle:



11 pav Vartotojų skolų schema

Iš paveikslo akivaizdžiai matome, jog vartotojai A, B ir C gali susitarti ir anuliuoti skolas vienas kitam nenaudodami grynų pinigų ar pervedimų ir taip gerokai sumažindami įsipareigojimų vienas kitam skaičių. Po įvykdyto užskaitymo, C vartotojo skola vartotojui D išliks, nes D nebuvo įmanoma įtraukti į skolų grandinę (12 pav).



12 pav. Vartotojų skolų schema po įvykdytos užskaitos

Pavyzdyje naudota schema matematikoje yra vadinama grafu. Grafas – tai tai tam tikrų objektų (grafo viršūnių) sujungtų lankais, rinkinys. Taigi matematiškai, įsiskolinimų grandinėse dalyvaujančius subjektus, laikysime grafo viršūnėmis, pačius įsiskolinimus vadinsime lankais, o surastą skolų grandinę - ciklu. Ciklas – tai gretimų lankų seka, kurios pirma ir paskutinė viršūnė sutampa. Ciklų radimas ir jų eliminavimas yra svarbus tuo, kad tokiu būdu galima sumažinti ar eliminuoti visų ciklo subjektų skolas neatliekant jokių tarpusavio atsiskaitymų [17].

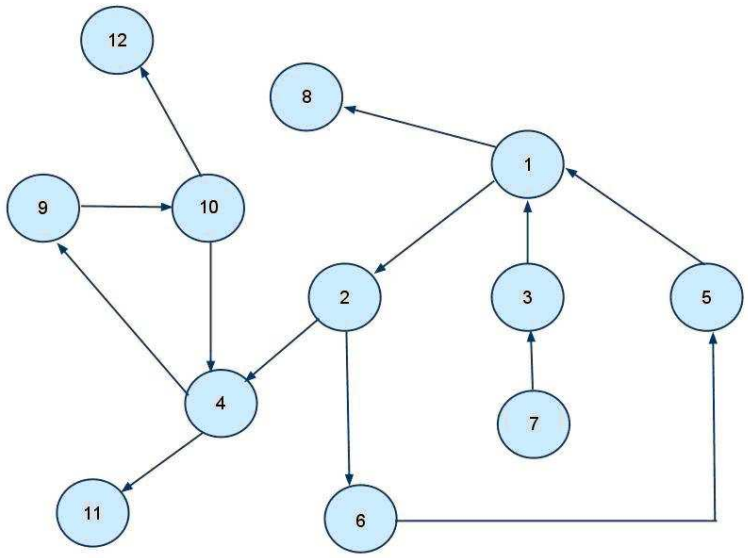
Ciklų paieškai pasirinktas paieškos gilyn (angl. Depth first search) algoritmas. Algoritmo esmė: Pradžioje sakome, kad visos grafo viršūnės yra naujos (neaplankytos). Tarkime, kad paieška pradedama iš viršūnės v_0. Viršūnė v_0 tampa nenauja, ir išrenkame viršūnę u, kuri yra gretima viršūnei v_0. Jei viršūnė u yra nauja, peržiūros procesą tęsiame iš viršūnės u. Tarkime, kad esame viršūnėje v. Jei yra nauja dar neaplankyta viršūnė u, gretima viršūnei v, tai nagrinėjame viršūnę u (ji tampa nenauja) ir paiešką tęsiame iš viršūnės u.Jei nėra nei vienos naujos viršūnės, gretimos viršūnei v, tai sakome, kad viršūnė v išsemta, grįžtame į viršūnę, iš kurios patekome į

viršūnę v, ir paiešką tęsiame iš šios viršūnės. Patekę į viršūnę, kurioje jau buvome užfiksuojame ciklą. Paiešką baigiame, kai pradinė paieškos viršūnė v_0 tampa išsemta viršūne [18].

2.4.1 Skolų užskaitymo modelio realizacija

Norint kompiuteriu vykdyti ciklų paiešką naudojantis grafų teorijos metodais, skolų informaciją patogiausia laikyt matematine forma. Tam buvo pasirinkta gretimumo struktūra. Gretimumo struktūra – tai viršūnėms gretimų viršūnių aibių šima [18].

Panagrinkime konkretų grafą (pav. 13) :



13 pav. Grafas

Šiam grafui sudaryta gretimumo struktūra pateikiama 1 lentelėje. Čia pateiktą informaciją reiktų suprasti taip: iš pirmos viršūnės galima pateikti į viršūnes 8 ir 2, iš antros į 4 ir 6 ir t.t.

Lentelė Nr. 1 Grafo gretimumo struktūra

1	8	2
2	4	6
3	1	
4	9	11
5	1	
6	5	
7	3	
8		
9	10	
10	4	12
11		
12		

Kadangi prieš tai aptartas paieškos gilyn algoritmas buvo sukurtas visoms grafo viršūnėms apeiti, o ne specialiai ciklams ieškoti, duotasis algoritmas šiek tiek modifikuojamas, panaudojant lankų matricą M, kurioje eilutės i-tasis numeris atitinka viršūnę iš kurios yra išeinantis lankas, o stulpelio j-tasis numeris atitinka viršūnę, į kurią yra įeinantis lankas. Eilutės ir stulpelio susikirtime yra fiksuojama, ar jau buvo eita iš i viršūnės į j viršunę (reikšmė „1“ jei buvo ir „0“ jei nebuvo).

Be anksčiau minėtų duomenų masyvų, paieškos metode taip pat yra naudojami masyvai I ir K atitinkamai išsemtom viršūnėm ir nueitam keliui saugoti. Viršūnė laikoma „išsemta“ jei visos viršūnės, į kurias galima iš jos patekti, yra aplankytos arba jei tai yra aplankyta viršūnė, neturinti išeinančių lankų. Nueitas kelias, tai viršūnių seka, per kurią einant, buvo ateita iki dabar nagrinėjamos viršūnės.

Veikimo algoritmas

Viršūnė, iš kurios pradedama ieškoti ciklo, įrašoma į masyvą K. Iš gretimumo struktūros imama pirma viršūnė, gretimai esamai, ir patikrinama, ar ji nėra išsemta, ir ar nebuvo seniau aplankyta (tam naudojamas masyvas M), jei abi sąlygos neigiamos, viršūnė įrašoma į masyvą K ir vėl kartojama procedūra. Jei kuri nors iš salygų tenkinama, viršūnė praleidžiama ir imama kita viršūnė iš gretimumo struktūros. Pasiekus viršūnę, iš kurios visos pasiekiamos viršūnės yra aplankytos arba ji neturi išeinančių lankų, viršūnė įrašoma į masyvą I ir ištrinama iš kelio masyvo K (grįžtama atgal). Algoritmo vykdymas baigiamas aplankius visas viršunes ir ištuštinus masyvą K (ciklas nerastas) arba patekus į viršūnę, kuri jau yra kelio masyve K (ciklas surastas).

2.4.2 Skolų užskaitymo modelio realizacijos testavimas

Išmėginkime anskčiau minėtą pavyzdį, testuojant šio modulio veikimą. Gauti tokie rezultatai:

Algoritmo suskaičiuota gretimumo struktūra:

```
-----
| 1 | 8 2
| 2 | 4 6
| 3 | 1
| 4 | 9 11
| 5 | 1
| 6 | 5
| 7 | 3
| 8 |
| 9 | 10
| 10| 4 12
| 11|
| 12|
----
```

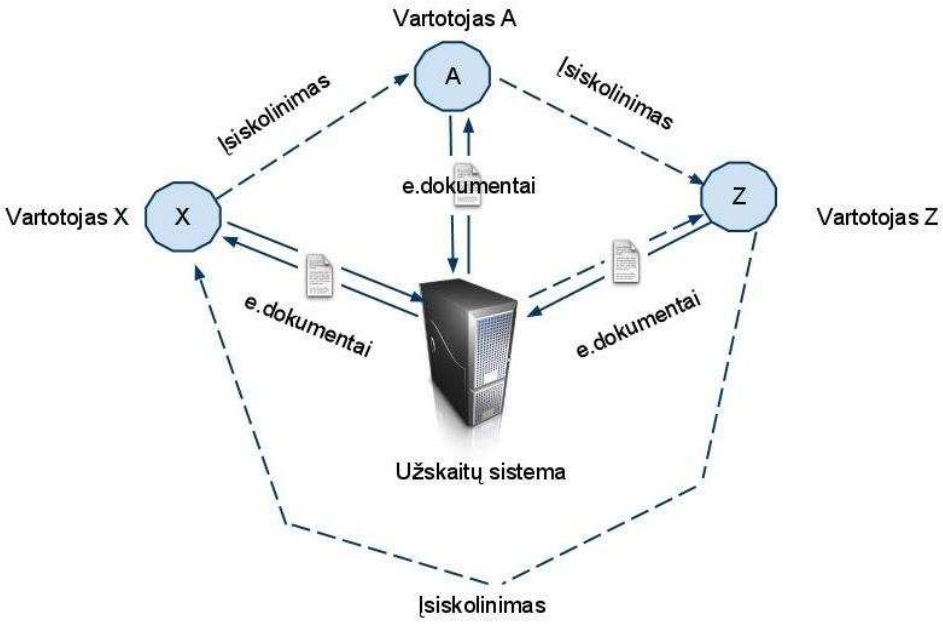
Ciklų paieškos rezultatai ieškant ciklų iš kiekvienos viršūnės:

```
Paieška is viršūnės: 1. Panaudota operacijų: 18. Ciklas: 1 2 6 5
Paieška is viršūnės: 2. Panaudota operacijų: 18. Ciklas: 2 6 5 1
Paieška is viršūnės: 3. Panaudota operacijų: 25. Ciklo nebuvo
Paieška is viršūnės: 4. Panaudota operacijų: 3. Ciklas: 4 9 10
Paieška is viršūnės: 5. Panaudota operacijų: 18. Ciklas: 5 1 2 6
Paieška is viršūnės: 6. Panaudota operacijų: 18. Ciklas: 6 5 1 2
Paieška is viršūnės: 7. Panaudota operacijų: 27. Ciklo nebuvo
Paieška is viršūnės: 8. Panaudota operacijų: 1. Ciklo nebuvo
Paieška is viršūnės: 9. Panaudota operacijų: 3. Ciklas: 9 10 4
Paieška is viršūnės: 10. Panaudota operacijų: 3. Ciklas: 10 4 9
Paieška is viršūnės: 11. Panaudota operacijų: 1. Ciklo nebuvo
Paieška is viršūnės: 12. Panaudota operacijų: 1. Ciklo nebuvo
```

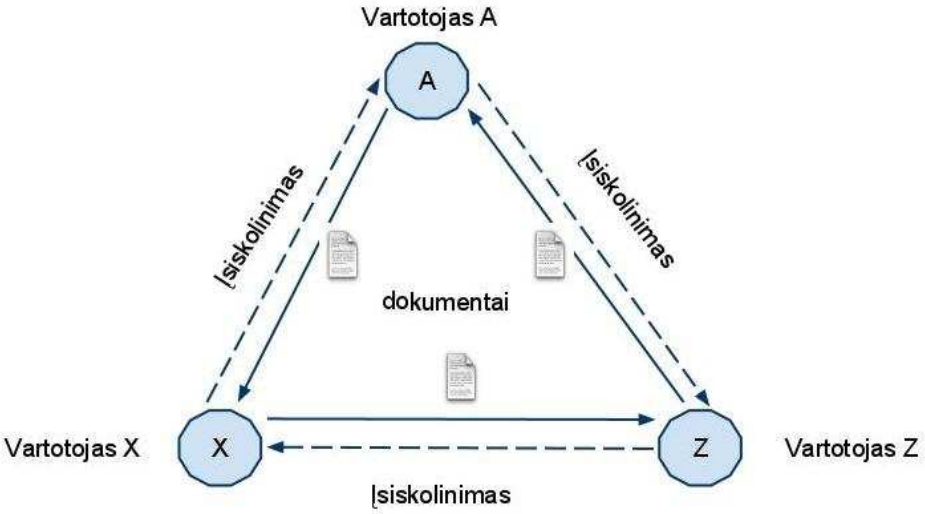
Kaip matome 13 pav. grafas turi du ciklus (viršūnės 4, 9,10 ir 1, 2, 6, 5). Tą patį grąžino ir skolų užskaitymo modelis. Seka 9, 10, 4 atitinka tą patį ciklą kaip ir 10, 4, 9 arba 4, 10, 9, skirtinga išsidėstymo tvarka atsiranda dėl skirtingos paieškos viršūnės ir nekeičia prasmės.

2.5 e.dokumentų cirkuliacijos modelis

e.dokumentais sistemoje laikomi elektroniniai dokumentai pasirašyti e.parašu. Sistemai radus galimą įvykdyti užskaitų grandinę ir vartotojui inicijavus šį užskaitymą, vartotojas pasirašo dokumentą sistemos sugeneruotą, jog sutinka anuliuoti skolą subjekto X naudai, jei jam pačiam skolą anuliuos subjektas Y. Tarpusavio užskaita įgauna pilną juridinę galią, kuomet visi grandinėje esantys subjektai e.parašu pasirašo sutikimą anuliuoti skolas ir sistemai pateikia tai įrodančius dokumentus. Sistema informuoja vartotojus apie sėkmingai įvykdytą užskaitą, pateikdama tai patvirtinantį dokumentą su sistemos e.parašu. Tokiu būdu įvairaus dydžio skolų grandinių užskaitymai gali būti įvykdyti per 1 darbo dieną, nes visi subjektai gali pasirašyti dokumentą atskirai vienas nuo kito tuo pačiu metu (pav. 14). Tai yra daug greičiau nei standartinės daugiašalės sutartys, kurias parašais turi patvirtinti visi sandoryje dalyvaujantys subjektai (pav. 15)



14 pav. Dokumentų cirkuliacija



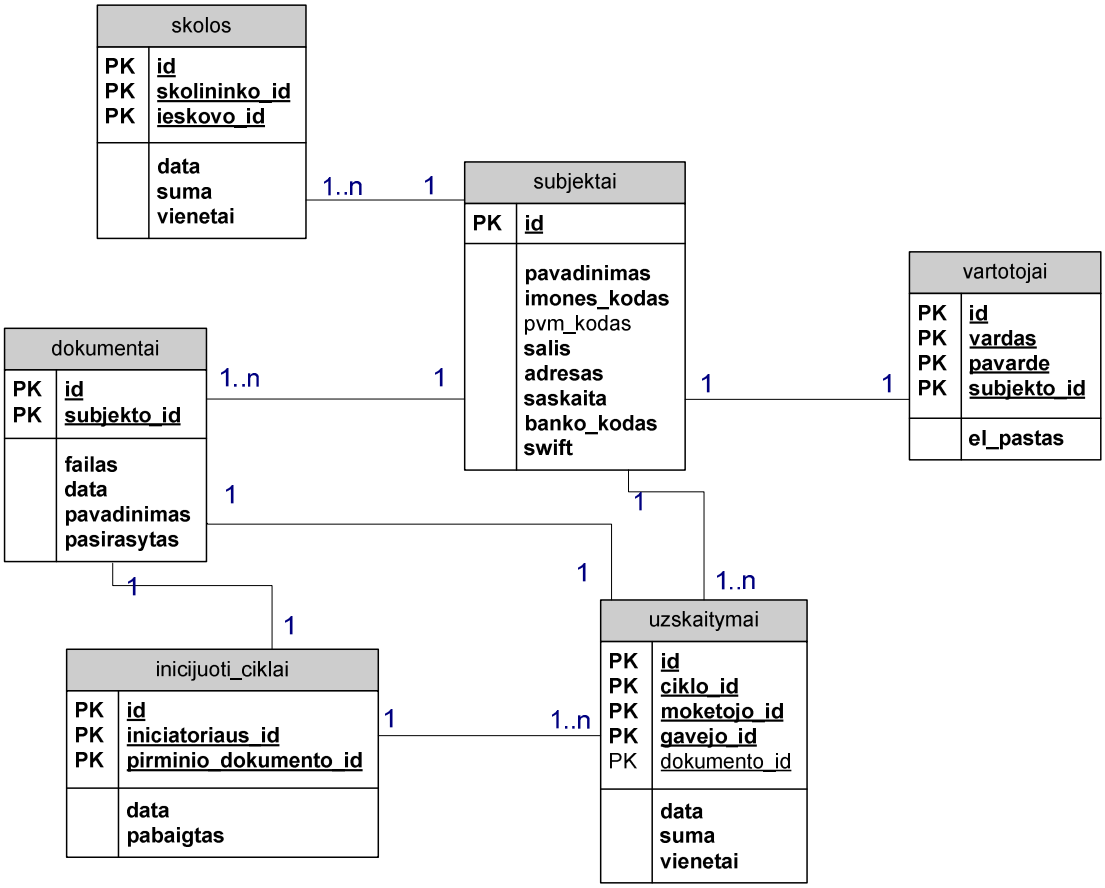
15 pav. Tradicinių dokumentų cirkuliacija

2.6 Duomenų bazės prototipas

Duomenų bazės pagrindinė užduotis saugoti visą reikalingą informaciją, o atsiradus poreikiui - ją pateikti ar keisti.

2.6.1 Duomenų bazės schema

16 paveiksle pateikiama suprojektuotos duomenų bazės schema



16 pav. Duomenų bazės schema

2.6.2 Duomenų bazės lentelių laukų tipai

Lentelė „subjektai“

Lentelė Nr. 2 „subjektai“

id	int
pavadinimas	varchar(128)
imones_kodas	varchar(16)
pvm_kodas	varchar(16)
salis	varchar(32)

adresas	varchar(128)
saskaita	varchar(20)
swift	varchar(16)

Laukas „id“ yra skirtas unikaliam eilutės indentifikatoriui saugoti.

Laukelyje „pavadinimas“ saugomas įmonės ar organizacijos pavadinimas (jei juridinis asmuo) arba vardas ir pavardė (jei fizinis asmuo).

Laukas „imones_kodas“ skirtas saugoti įmonės kodui (jei juridinis asmuo) arba asmens kodui(jei fizinis asmuo).

Laukas „pvm_kodas“ nurodo subjekto pvm mok4tojo kodą.

Lauke „salis“ nurodoma šalis, kurioje subjektas vydo veiklą.

Lauke „adresas“ nurodomo subjekto tikslus adresas.

Lauke „saskaita“ nurodomoa subjekto banko sąskaitos numeris.

Lauke „swift“ nurodoma subjekto banko sąskaitos swift kodas.

Lentelė „skolos“

Lentelėje „skolos“ laikoma informacija apie kitiems skolingus subjektus.

Lentelė Nr. 3 „skolos“

id	int
skolininko_id	int
ieskovo_id	int
data	int
suma	float
vienetai	varchar(16)

Laukas „id“ yra skirtas unikaliam eilutės indentifikatoriui saugoti.

Laukas „skolininko_id“ nurodo skolininko identifikacijos numerį lentelėje „subjektai“.

Laukas „ieskovo_id“ nurodo asmens, kuriam yra skolinga identifikacijos numerį lentelėje „subjektai“.

Laukas „data“ skirtas saugoti skolos sukūrimo datą.

Laukas „suma“ saugo konkretų skolos dydį tam tikrais vienetais.

Laukas „vienetai“ nurodo, kokiais vienetais (valiuta) matuojama skola.

Lentelė „uzskaitymai“

Lentelėje „uzskaitymai“ saugomi įvykdyti skolų anuliavimai arba skolų sumažinimai.

Lentelė Nr. 4 „uzskaitymai“

id	int
ciklo_id	int
moketojo_id	int
gavejo_id	int
dokumento_id	int
suma	float
vienetai	varchar(16)
data	int

Laukas „id“ yra skirtas unikaliam eilutės indentifikatoriui saugoti.

Laukas „ciklo_id“ skirtas nurodyti, kuriam vykdomam ciklau priklauso užskaitymas.

Laukas „mokėtojo_id“ nurodo identifikacinį numerį lentelėje „subjektai“.

Laukas „gavejo_id“ nurodo skolos ieškovo identifikacinį numerį lentelėje „subjektai“.

Laukas „suma“ saugo anuliuotos sumos vertę tam tikrais vienetais.

Laukas „vienetai“ nurodo, kokiais vienetais (valiuta) buvo atliktas užskaitymas.

Laukas „data“ skirtas saugoti užskaitymo įvykdymo datai.

Lentelė „vartotojai“

Lentelėje „vartotojai“ saugomi subjektų prisijungimo prie sistemos duomenys.

Lentelė Nr. 5 „vartotojai“

id	int
subjekto_id	int
vardas	varchar(64)
pavarde	varchar(64)
el_pastas	varchar(64)

Laukas „id“ yra skirtas unikaliam eilutės indentifikatoriui saugoti.

Laukas „subjekto_id“ nurodo sistemos vartotojo identifikacijos numerį lentelėje „subjektai“.

Laukas „vardas“ skirtas subjektą atstovaujančio asmens vardui saugoti.

Laukas „pavarde“ skirtas subjektą atstovaujančio pavardei saugoti.

Laukas „el_pastas“ skirtas subjekto naudojamo elektroninio pašto adresui saugoti.

Lentelė „dokumentai“

Lentelėje „dokumentai“ saugomi sistemos sugeneruoti ir vartojų pateikti failai.

Lentelė Nr. 6 „dokumentai

id	int
subjekto_id	int
pavadinimas	varchar(128)
failas	mediumblob
data	int
pasirasytas	tinyint

Laukas „id“ yra skirtas unikaliam eilutės indentifikatoriui saugoti.

Laukas „subjekto_id“ nurodo dokumento kūrėjo/savininko identifikacijos numerį lentelėje „subjektai“.

Laukas „pavadinimas“ nurodo patalpinto failo vardą.

Lauke „failas“ saugomas pats dokumentas.

Laukas „data“ skirtas saugoti dokumento pateikimo datai.

Laukas „pasirasytas“ nurodo požymį, ar pateiktas dokumentas yra pasirašytas.

Lentelė „inicijuoti_ciklai“

Lentelėje „inicijuoti_ciklai“ saugoma informacija apie vykdytus ir vykdomus ciklus.

Lentelė Nr. 7 „inicijuoti_ciklai“

id	int
iniciatoriaus_id	int
pirminio_dokumento_id	int
data	int
pabaigtas	tinyint

Laukas „id“ yra skirtas unikaliam eilutės indentifikatoriui saugoti.

Laukas „iniciatoriaus_id“ nurodo ciklą iniciavusiu subjekto identifikacijos numerį lentelėje „subjektai“.

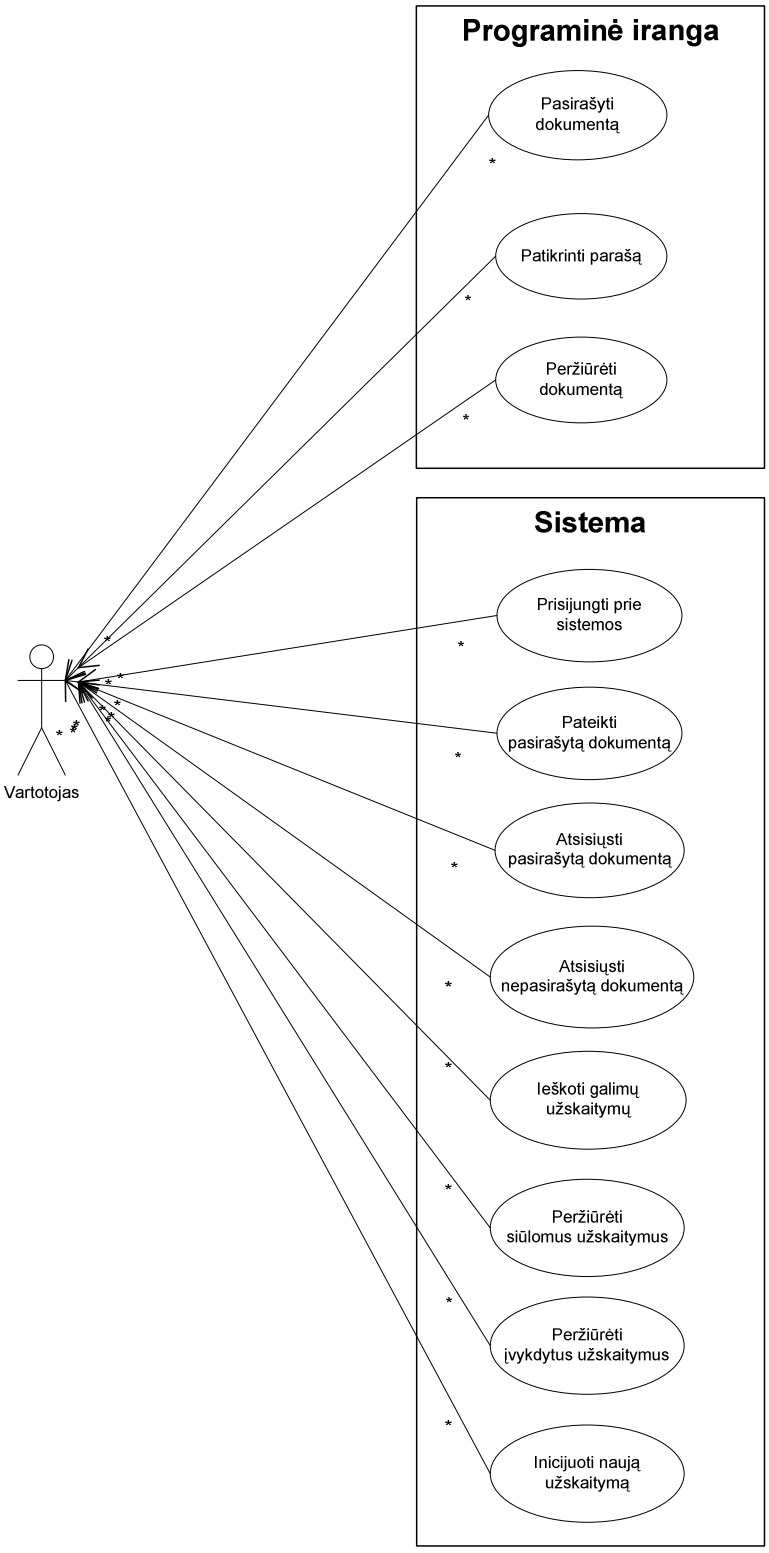
Laukas „pirminio_dokumento_id“ skirtas nurodyti sistemos sugeneruoto dokumento identifikacijos numerį lentelėje „dokumentai“.

Laukas „data“ skirtas saugoti ciklo_iniciavimo datai.

Laukas „pabaigtas“ nurodo požymį, ar ciklas yra pilnai įvykdytas.

2.7 UML diagramos

2.7.1 Vartotojo panaudojimo atvejų diagrama



17 pav. Vartotojų panaudojimo atvejų diagrama

Vartotojų panaudojimo atvejų diagrama parodo, kokius veiksmus galima atlikti vartotojo atžvilgiu. Trys pirmieji atvejai (dokumentų pasirašymas, parašo tikrinimas, dokumento peržiūra) atliekami pasinaudojant specializuota pasirašymo programine įranga, kuri įdiegta vartotojo kompiuteryje (epp portable pasirašymo programa). Likę atvejai (prisijungimas prie sistemos, pasirašyto dokumento pateikimas, pasirašyto dokumento atsisiuntimas, nepasirašyto dokumento atsisiuntimas, galimų užskaitymų paieška, siūlomų užskaitymų peržiūra, įvykdytų užskaitymų peržiūra, naujo užskaitymo iniciavimas) atliekami prisijungus prie sistemos.

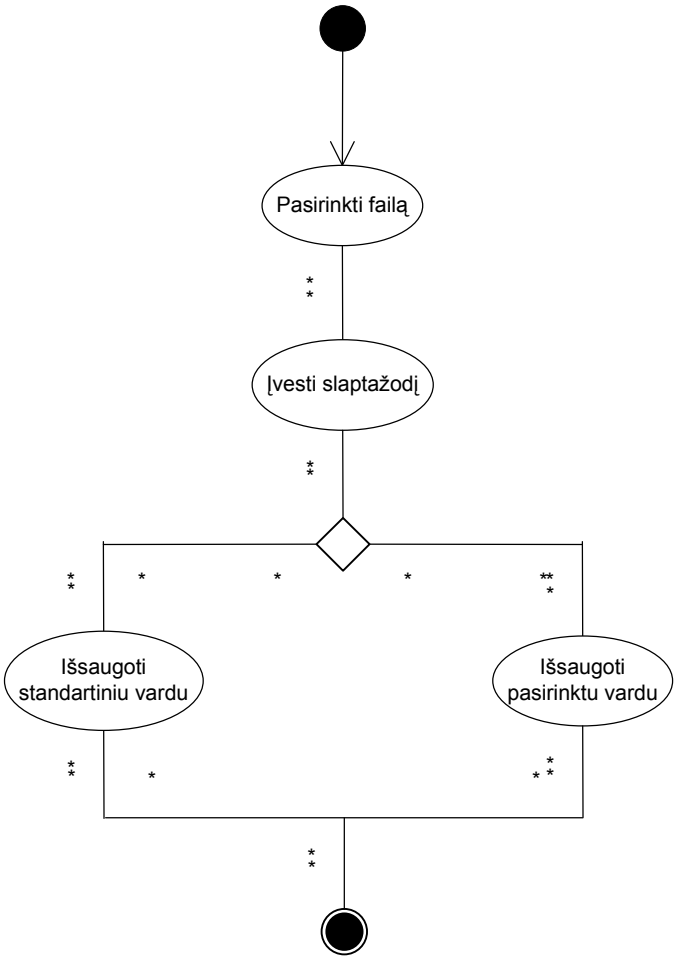
2.7.2 Veiklos diagramos kiekvienam panaudojimo atvejui

Prisijungimo prie sistemos

18 pav. Prisijungimo prie sistemos veiklos diagrama

Vartotojas norėdamas prisijungti prie sistemos turi išsisaugoti specialiai jam sugeneruotą prisijungimo failą ir jį pasirašyti epp portable programa. Pasirašytą failą vartotojas turi grąžinti sistemai.

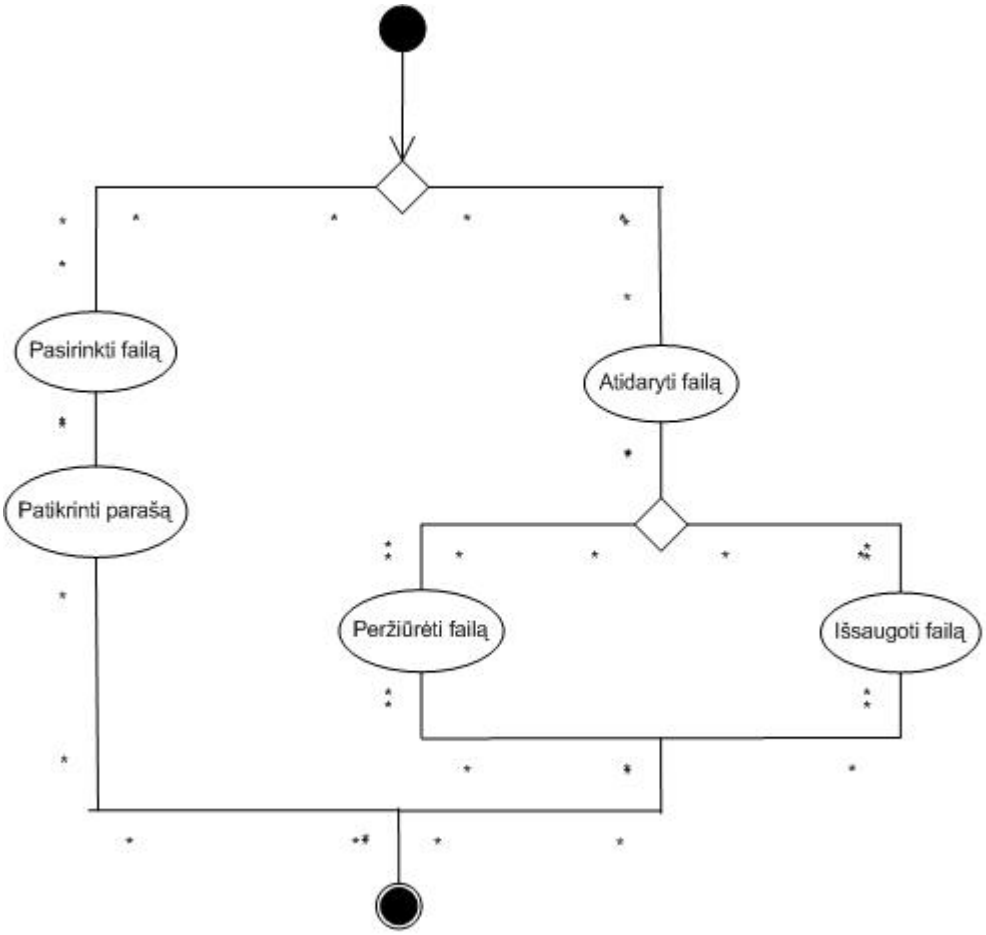
Dokumento pasirašymo



19 pav. Dokumento pasirašymo veiklos diagrama

Vartotojas norėdamas pasirašyti dokumentą turi epp portable programoje pasirinkti norimą failą, meniu susirasti punktą „Dokumentas“ ir išskleidusiame meniu paspausti „dokumento pasirašymas“. Programa paprašys įvesti slaptažodį. Tai teisingai atlikus, vartotojas pasirašytą failą gali išsaugoti standartiniu vardu (pagal pirminį failą) arba pats parinkti norimą vardą.

Dokumento peržiūros ir parašo tikrinimo

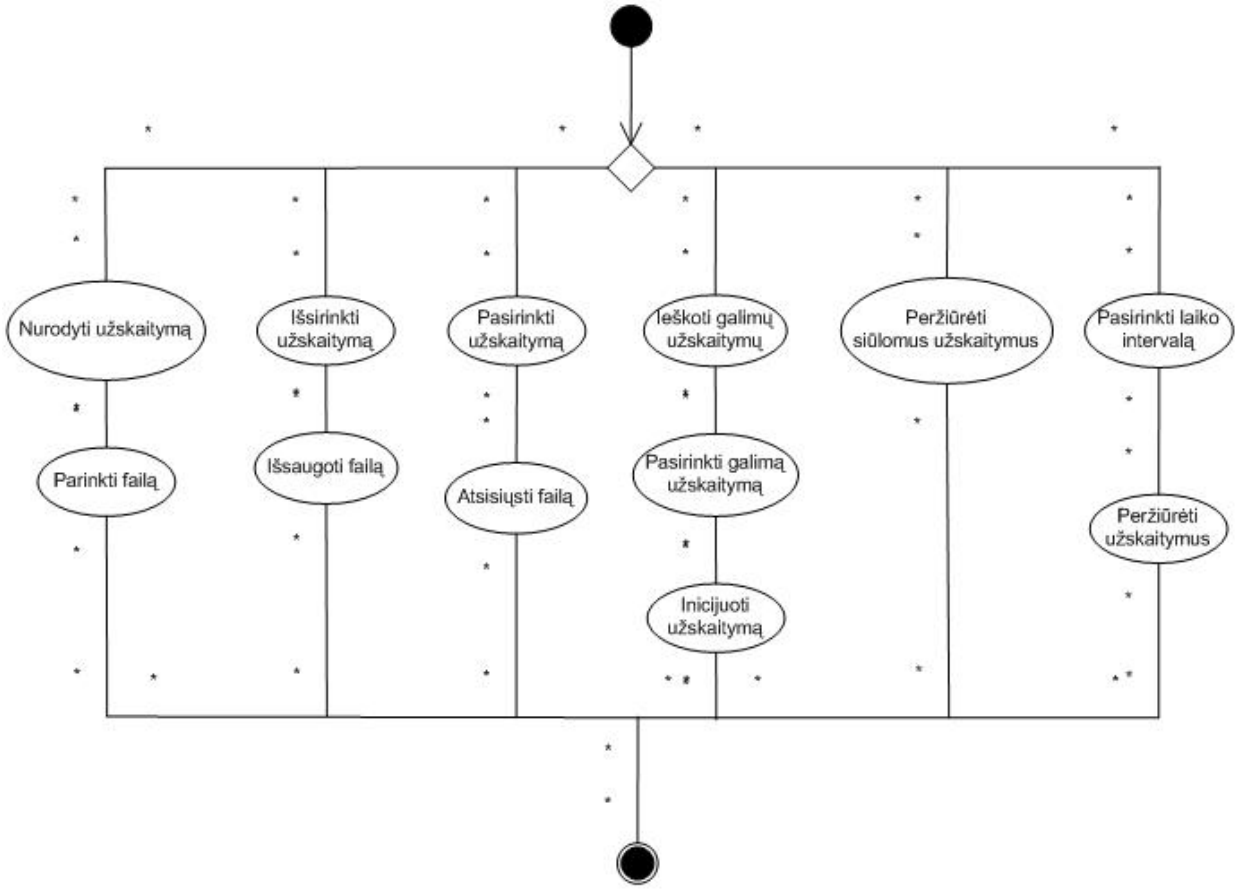


20 pav. Dokumento peržiūros ir parašo tikrinimo veiklos diagrama

Vartotojas norėdamas patikrinti dokumento parašą turi epp portable programoje atidaryti norimą failą, meniu susirasti punktą „Dokumentas“ ir išsiskleidusiame meniu paspausti „Tikrinti“. Programa išmes pranešimą apie patikrintus parašus, o pagrindiniame lange atsiras dokumente panaudoti parašai ir validumas

Vartotojas norėdamas peržiūrėti pasirašytą dokumentą turi atsidaryti dokumentą programa epp portable, meniu susirasti punktą „Dokumentas“ ir išsiskleidusiame meniu paspausti „Peržiūrėti“. Automatiškai pasileis atitinkama failo peržiūros programa, o joje norimas dokumentas. Kitas variantas meniu „Failas“ pasirinkti punktą „Išsaugoti dokumentą“. Išsaugojus dokumentą, jį galima peržiūrėti ir vėliau.

Pasirašyto dokumento pateikimo, pasirašyto dokumento atsisiuntimo,nepasirašyto dokumento atsisiuntimo, galimų užskaitymų paieškos, įvykdytų užskaitymų peržiūros, naujo užskaitymo iniciavimo



21 pav. Pasirašyto dokumento pateikimo, pasirašyto dokumento atsisiuntimo,nepasirašyto dokumento atsisiuntimo, galimų užskaitymų paieškos, įvykdytų užskaitymų peržiūros, naujo užskaitymo iniciavimo veiklos diagrama

Vartotojas norėdamas pateikti sistemai pasirašytą dokumentą turi pasirinkti kokį užskaitymą (jei jų daugiau nei vienas) jis sutinka vykdyti ir nurodyti failą iš savo kompiuterio. Nurodytas failas bus įkeltas.

Vartotojas norėdamas atsisiųsti į savo kompiuterį pasirašytą dokumentą, turi pasirinkti vieną iš įvykdytų ar vykdomų užskaitymų ir, radęs reikiamą nuorodą, išsaugoti failą savo kompiuteryje.

Vartotojas norėdamas atsisiųsti į savo kompiuterį nepasirašytą dokumentą, turi pasirinkti vieną iš siūlomų užskaitymų ir, radęs reikiamą nuorodą, išsaugoti failą savo kompiuteryje.

Vartotojas norėdamas rasti tuo metu galimus užskaitymus turi pasirinkti meniu punktą “Galimų užskaitymų paieška” ir atsidariusiame lange įvykdyti paiešką.

Vartotojas norėdamas peržiūrėti kitų vartotojų inicijuotus užskaitymus turi pasirinkti meniu punktą “Peržiūrėti siūlomus užskaitymus” ir atsidariusiame lange peržiūrėti rezultatus.

Vartotojas norėdamas peržiūrėti seniau įvykdytus užskaitymus turi paspausti ant meniu punkto “Įvykdyti užskaitymai”, nustatyti kada įvykdytus užskaitymus jis nori matyti ir peržiūrėti jam pateiktus rezultatus.

Vartotojas norėdamas inicijuoti naują užskaitymą, turi pasirinkti meniu punktą “Galimų užskaitymų paieška” ir atsidariusiame lange įvykdyti paiešką. Esant rezultatams, vartotojas turi pasirinkti vieną užskaitymą (jei variantų daugiau nei vienas) ir paspausti mygtuką “Inicijuoti”.

2.8 Projektinės dalies išvados

Šiame darbe etape buvo suformuluoti reikalavimai sistemai, nusakyta jos koncepcija, įvardyti sistemos lygmenys, aprašyti informacijos mainų, identifikacijos ir autentikacijos modeliai. Daugiau dėmesio skirta skolų užskaitymo modeliui nagrinėjimui, algoritmo sukūrimui ir išbandymui. Pateiktas duomenų bazės prototipas, vartotojas galimybes nusakančios UML diagramos.

3 SAUGIŲ TARPUSAVIO ATSISKAITYMŲ SISTEMOS TYRIMAS

Suprojektuota sistema buvo tiriama dviem požiūriais:

- Tarpusavio skolų suradimo laiko sąnaudų įvertinimas;
- Tarpusavio atsiskaitymų įvykdymo laiko sąnaudų įvertinimas;

3.1 Tarpusavio skolų suradimo laiko sąnaudų įvertinimas

3.1.1 Testavimo aplinka ir pradiniai duomenys

Visi testavimo veiksmai buvo atlikti darbo kompiuteryje, kuriame įdiegta Windows XP operacinė sistema, Apache žiniatinklio serveris, PHP5 programavimo kalba, MySQL duomenų bazė.

Kompiuterio techniniai duomenys:

- AMD Athlon3800 procesorius;
- 1 GB 667 Mhz spartos RAM atmintis;
- 160 GB kietasis diskas;

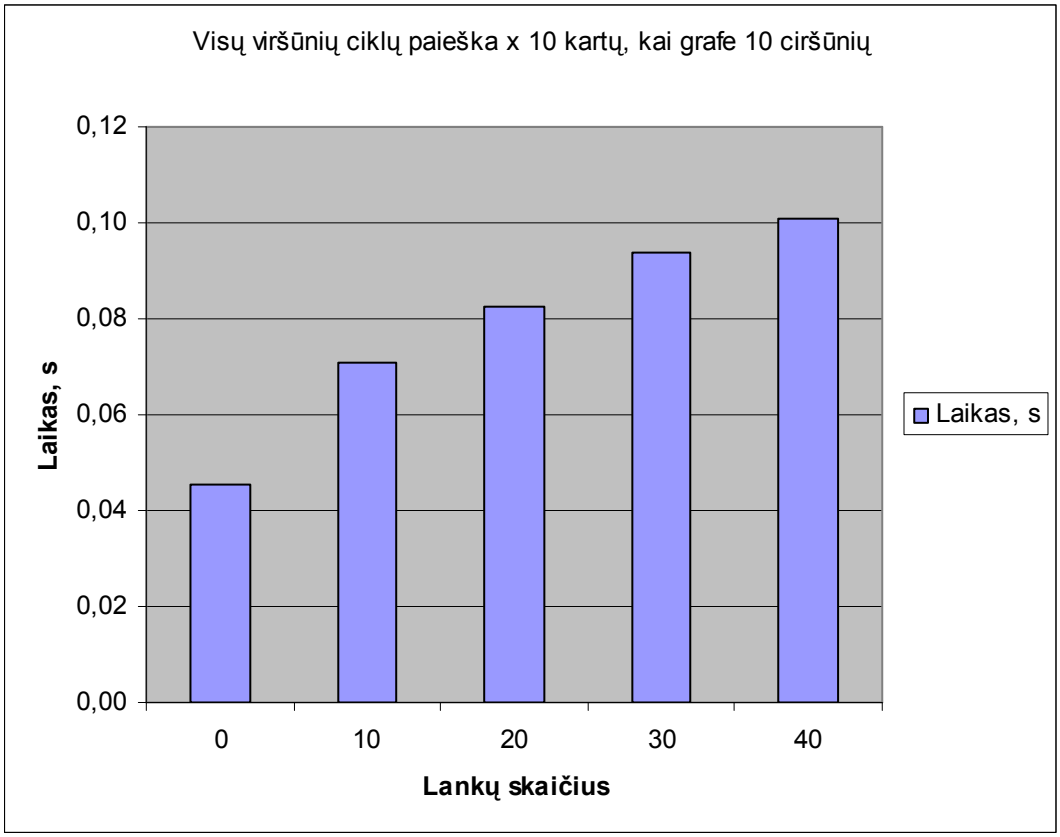
Testams naudojami duomenys buvo sugeneruoti naudojantis PHP integruota atsitiktinių skaičių generavimo funkcija.

3.1.2 Testas Nr.1

Šiame teste, buvo matuojamas visų grafo viršūnių ciklų suradimo laikas, kuomet grafe egzistuoja 10 viršūnių, testą pakartojant 100 kartų, norint gauti tikslesnius rezultatus. Gauti rezultatai matomi 8 lentelėje ir 22 paveiksle.

Lentelė Nr. 8 „Testo Nr. 1 rezultatai“

0	10	20	30	40
0,04546	0,07096	0,08258	0,09395	0,10076



22 pav. Testo Nr.1 stulpelinė diagrama

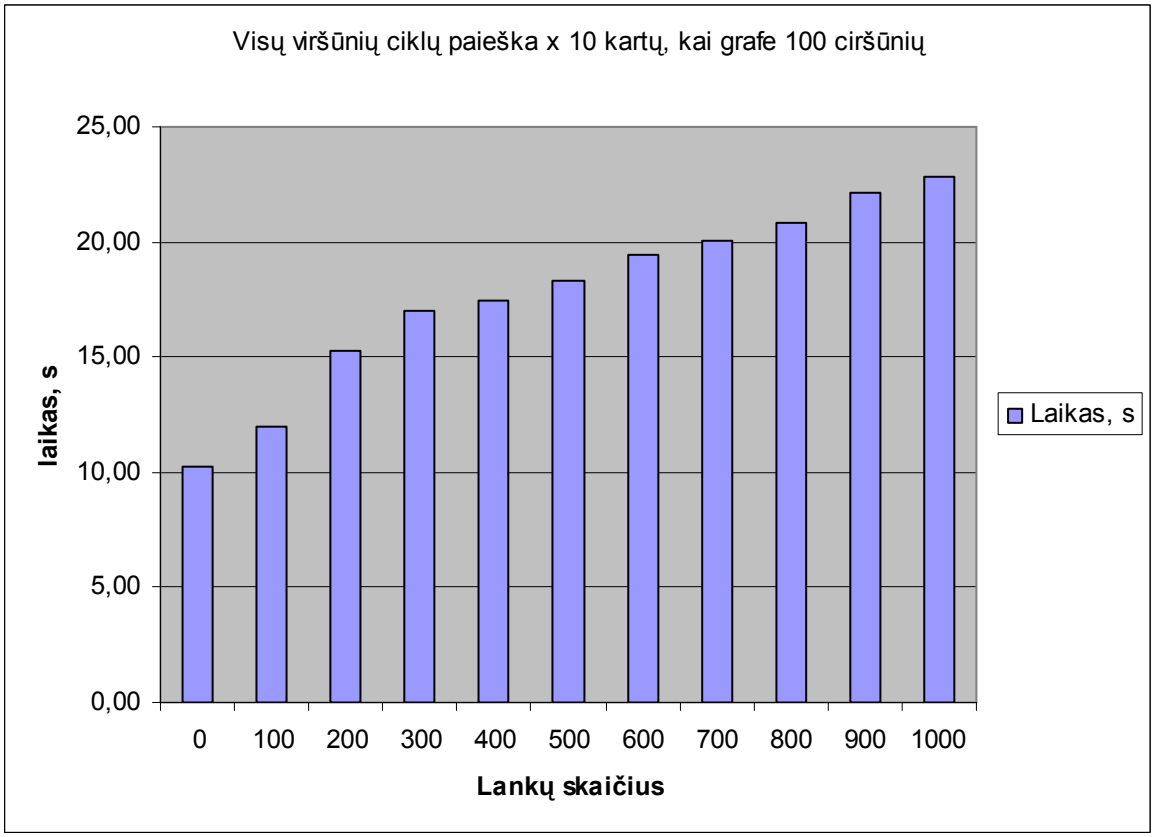
Vidutinis testo vienos viršūnės patikrinimo laikas: 0,000787 s.

3.1.3 Testas Nr.2

Šiame teste, buvo matuojamas visų grafo viršūnių ciklų suradimo laikas, kuomet grafe egzistuoja 100 viršūnių, testą pakartojant 10 kartų. Gauti rezultatai matomi 9 lentelėje ir 23 paveiksle.

Lentelė Nr. 9 „Testo Nr. 2 rezultatai“

0	100	200	300	400	500	600	700	800	900	1000
10,260	11,959	15,274	16,979	17,446	18,316	19,456	20,016	20,848	22,140	22,800



23 pav. Testo Nr.2 stulpelinė diagrama

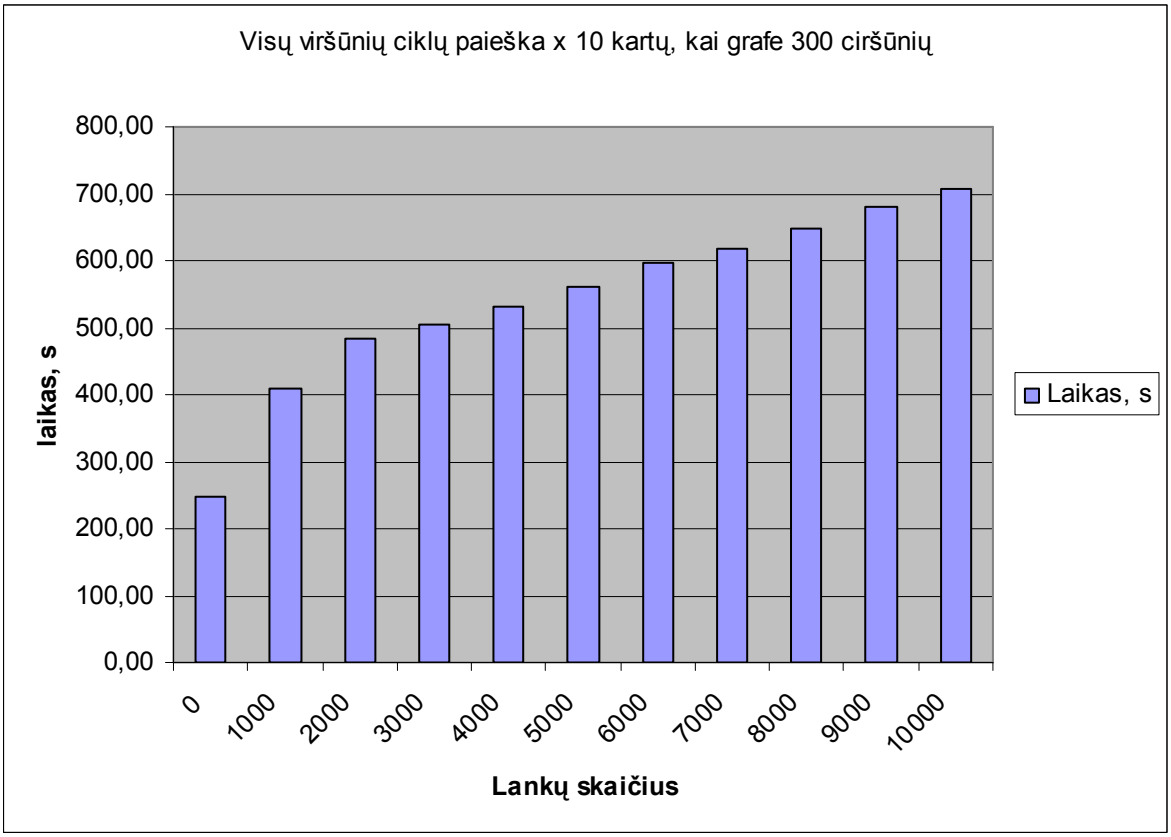
Vidutinis testo vienos viršūnės patikrinimo laikas: 0,0177723 s

3.1.4 Testas Nr.3

Šiame teste, buvo matuojamas visų grafo viršūnių ciklų suradimo laikas, kuomet grafe egzistuoja 1000 viršūnių, testą pakartojant 10 kartų. Gauti rezultatai matomi 10 lentelėje ir 24 paveiksle.

Lentelė Nr. 10 „Testo Nr. 3 rezultatai“

0	1000	2000	3000	4000	5000	6000	7000	8000	9000	10000
548,61	410,32	482,80	504,72	532,36	562,42	596,48	617,68	647,75	679,51	708,34



24 pav. Testo Nr.2 stulpelinė diagrama

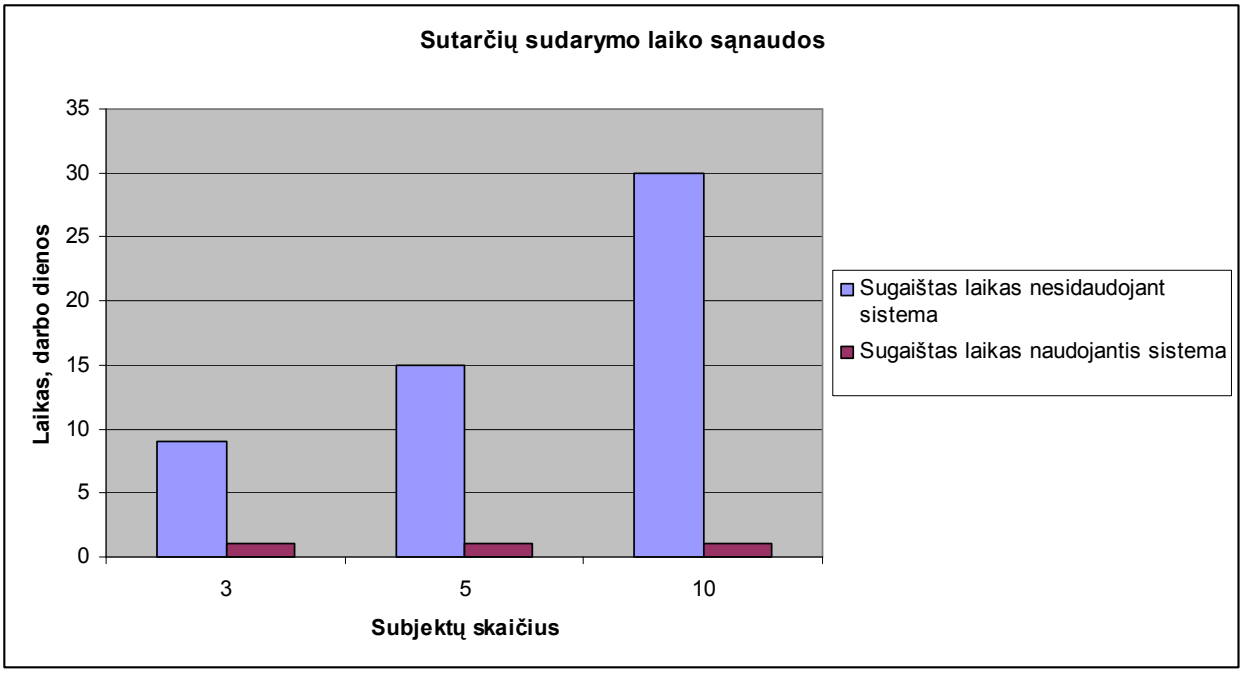
Vidutinis testo vienos viršūnės patikrinimo laikas: 0,18155 s.

3.2 Tarpusavio atsiskaitymų įvykdymo laiko sąnaudų įvertinimas

Prieš pradedant laiko sąnaudų įvertinimą, tarkime, jog subjektas prisijungti prie sistemos turi galimybę bent per kartą per darbo dieną, o registruotas laiškas keliauja 3 darbo dienas. Kadangi sistema suprojektuota taip jog kiekvienas vartotojas gali patvirtinti savo dalyvavimą užskaitoje nelaukiant kitų subjektų patvirtinimo (apie tai plačiau 2.5 skyriuje) iš to išplaukia, kad sistemai normaliai funkciojonuojant ir subjektams dirbant įprastu ritmu, užskaita gali būti įvykdyta per vieną darbo dieną, kai standartinis sutarčių pasirašymas užtruks daug ilgiau (priklausomai nuo subjektų skaičiaus). Teoriniai skaičiavimai pateikiami 10 lentelėje ir 22 paveiksle lyginant su teoriniu sutarčių sudarymo laiku nesinaudojant sistema.

Lentelė Nr. 11 „Tarpusavio atsiskaitymų ir tradicinių sutarčių pasirašymo laiko sąnaudos“

Subjektų skaičius	3	5	10
Laikas (darbo dienomis) nesinaudojant sistema	9	15	30
Laikas (darbo dienomis) naudojantis sistema	1	1	1



25 pav. Sutarčių sudarymo laiko sąnaudų diagrama

Čia pateikiami skaičiavimai yra orientacinio pobūdžio, nes realus sutarčių sudarymo laikas gali šiek tiek skirtis naudojimosi sistema atveju (pvz vienas vartotojas vieną dieną nerado laiko ar neturėjo galimybės pateikti systemai pasirašytą dokumentą) ir gerokai skirtis sudarant standartines sutartis (pvz subjektai gali susitikti ir visikartu pasirašyti sutartis, sutartis siųsti per greitesnius kurjerius ir kiti variantai).

3.3 Eksperimento rezultatai

Eksperimento metu nustatyta, kad pasirinkto ciklų paieškos algoritmo veikimo laikas yra tiesiogiai proporcingas ciklo viršūnių ir lankų skaičiui ir gali būti kritinis esant dideliam duomenų kiekiui ar dažnam užklausų pasikartojimui. Kita vertus, ciklų paieškos laikus būtų galima sumažinti naudojant optimalesnį paieškos algoritmą ir skaičiavimui atliekant specialiai tam paruoštame serveryje, turinčiame daugiau resursų.

Nustatyta, kad normaliai funkcionuojančios sistemos naudojimas, laiko atžvilgiu, yra gerokai pranešesnis prieš standartinį sutarčių sudarymo modelį. Realus pranašumas labai priklauso nuo subjektų skaičiaus, jų bendravimo pobūdžio ir skirtingais atvejais gali smarkiai skirtis.

IŠVADOS

Įmonėse naudojamų atsiskaitymo būdų analizės dalyje aptarti populiariausi atsiskaitymo variantai apimant grynuosius pinigus, negrynuosius pinigus, elektronines lėšų pervedimo sistemas, tarpusavio užskaitų sistemas. Pastebėta, kad mokėjimo sistemose vis dar nelabai aktyviai panaudojamas e.parašas. Išanalizuotos techninės bei teisinės jo panaudojimo galimybės ir padaryta išvada, kad tai atsiskaitymams tinkama technologija.

Saugių tarpusavio užskaitymų sistemos projektinėje dalyje aprašyta sistemos koncepsija, iškelti reikalavimai. Aprašyti sistemos informacijos mainų, idetifikacijos ir autorizacijos modeliai. Detaliau išnagrinėtas skolų užskaitymo modelis, paiškinta ir išbandyta jo realizacija. Pateiktas e.dokumentų cirkuliacijos modelis ir projekte naudotas duomenų bazės prototipas. Galimi vartotojo veiksmai nusakyti UML diagramomis.

Esperimentinėje darbo dalyje ištirtas skolų paieškos modulio veikimas. Nustatyta, kad tai pakankamai imlus resursam procesas, todėl kuriant realią sistemą turėtų būti maksimaliai optimizuotas. Taip pat šioje dalyje pateikiami teoriniai dokumentų pasirašymo ir cirkuliavimo laiko sąnaudų skaičiavimai, lyginant juos su standartiniu dokumentų pasirašymu. Gauti rezultatai byloja apie e.dokumentų sistemos pranašumą ir galimybę toliau vystyti šią sferą.

LITERATŪRA

[1] Creditinfo Lietuva [interaktyvus] [žiūrėta 2010-05-23]. Prieiga per internetą <http://www.creditinfo.lt/?PageID=623&NewsID=2588>

[2] VAŠKELAITIS, V. Piniginai atsiskaitymai. Teorija ir praktika. Vilnius, 2001

[3] nordea.lt [interaktyvus] [žiūrėta 2010-05-09]. Prieiga per internetą <http://www.nordea.lt/lt/pages/overdraftas>

[4] Mokesčių žinios [interaktyvus]. Specializuotas savaitraštis Lietuvos mokesčių mokėtojams, 2006 [žiūrėta 2010-05-09]. Prieiga per internetą: <http://www.mzinios.lt/lt/2006-01-11/straipsniai/patarimai/vekselis_bukite_budrus.html>

[5] swedbank.lt [interaktyvus] [žiūrėta 2010-05-09]. Prieiga per internetą <http://www.swedbank.lt/lt/pages/verslo/dokumentiniai_akredityvai>

[6] O'Mahony, M; Peirce, M; Tewari, H. Electronic Payment System for E-Commerce. 2002. ISBN 1580534635

[7] KAŠĖTA, S.; ir ADOMKUS, T. Telefonijos informacijos ir VoIP sauga. Kaunas

[8] KIAULEIKIS, Valentinas, et al. Elektroninio verslo sauga. Mokomoji knyga. Kaunas, 2008. ISBN 978-9955-737-18-6

[9] mondex.com [interaktyvus] [žiūrėta 2009-01-16]. Prieiga per internetą <http://www.mondex.com>

[10] paypal.com [interaktyvus] [žiūrėta 2009-01-03]. Prieiga per internetą <http://www.paypal.com>

[11] ebuhalteris.lt [interaktyvus] [žiūrėta 20010-03-12]. Prieiga per internetą <http://www.ebuhalteris.lt>

[12] debitoriai.lt [interaktyvus] [žiūrėta 20010-03-12]. Prieiga per internetą <http://www.debitoriai.lt>

[13] KULCU, O. Evolution of e-records management practices in e-government. The Electronic Library, 2009, Nr. 27. ISSN 0264-0473

[14] WEISE, J. Public Key Infrastructure Overview. Palo Alto, 2001.

[15] Valstybės žinios, 2000-07-26, Nr. 61-1827

[16] KriptoGama [interaktyvus] [žiūrėta 2009-06-02]. Prieiga per internetą <http://a-sign.ktu.lt>

[17] WEISSTEIN, Eric, Graph. [interaktyvus] [žiūrėta 2010-05-23]. Prieiga per internetą <http://mathworld.wolfram.com/Graph.html >

[18] PLUKAS, Kostas, et al. Taikomoji diskrečioji matematika, Kaunas, 2004, ISBN 9955-09-031-6

1 PRIEDAS. PILNI TESTO NR.1 REZULTATAI

Testas Nr.1

```
Gretimumo struktūra:
-----
| 1 |
| 2 |
| 3 |
| 4 |
| 5 |
| 6 |
| 7 |
| 8 |
| 9 |
| 10|
----

Testas x 10 kartų
Viršūnių: 10
Grafo lankų: 0
-------------------------------------------------------
Laukiami rezultatai:
Paieška is viršūnės: 1 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 2 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 3 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 4 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 5 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 6 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 7 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 8 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 9 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 10 .Panaudota operacijų 1. Ciklo nebuvo
-------------------------------------------------------
Skaičiavimai atlikti per: 0.045459985733 sekundžių

Gretimumo struktūra:
-----
| 1 | 10
| 2 |
| 3 | 5 6
| 4 | 1
| 5 |
| 6 | 9 7
| 7 | 1 5
| 8 |
| 9 |
| 10| 2 8

Testas x 10 kartų
Viršūnių: 10
Grafo lankų: 10
-------------------------------------------------------
Laukiami rezultatai:
Paieška is viršūnės: 1 .Panaudota operacijų 7. Ciklo nebuvo
Paieška is viršūnės: 2 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 3 .Panaudota operacijų 17. Ciklo nebuvo
Paieška is viršūnės: 4 .Panaudota operacijų 9. Ciklo nebuvo
Paieška is viršūnės: 5 .Panaudota operacijų 1. Ciklo nebuvo
```

```
Paieška is viršūnės: 6 .Panaudota operacijų 15. Ciklo nebuvo
Paieška is viršūnės: 7 .Panaudota operacijų 11. Ciklo nebuvo
Paieška is viršūnės: 8 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 9 .Panaudota operacijų 1. Ciklo nebuvo
Paieška is viršūnės: 10 .Panaudota operacijų 5. Ciklo nebuvo
------------------------------------------------------
Skaičiavimai atlikti per: 0.0709648132324 sekundžių

Gretimumo struktūra:
-----
| 1 | 10 3 9
| 2 | 7
| 3 | 5 6 10
| 4 | 1 2 10
| 5 | 4
| 6 | 9 7
| 7 | 1 5
| 8 | 7
| 9 | 7 2
| 10| 2 8

Testas x 10 kartų
Viršūnių: 10
Grafo lankų: 20
------------------------------------------------------
Laukiami rezultatai:
Paieška is viršūnės: 1 .Panaudota operacijų 4. Ciklas: 1 10 2 7
Paieška is viršūnės: 2 .Panaudota operacijų 4. Ciklas: 2 7 1 10
Paieška is viršūnės: 3 .Panaudota operacijų 8. Ciklas: 3 5 4 1 10 2 7 1
Paieška is viršūnės: 4 .Panaudota operacijų 8. Ciklas: 4 1 10 2 7 1 3 5
Paieška is viršūnės: 5 .Panaudota operacijų 8. Ciklas: 5 4 1 10 2 7 1 3
Paieška is viršūnės: 6 .Panaudota operacijų 13. Ciklas: 6 9 7 1 10 2 7 5 4 1 3
Paieška is viršūnės: 7 .Panaudota operacijų 4. Ciklas: 7 1 10 2
Paieška is viršūnės: 8 .Panaudota operacijų 21. Ciklas: 8 7 1 10 2 7 5 4 1 3
10
Paieška is viršūnės: 9 .Panaudota operacijų 13. Ciklas: 9 7 1 10 2 7 5 4 1 3 6
Paieška is viršūnės: 10 .Panaudota operacijų 4. Ciklas: 10 2 7 1
------------------------------------------------------
Skaičiavimai atlikti per: 0.0825769901276 sekundžių

Gretimumo struktūra:
-----
| 1 | 10 3 9
| 2 | 7 8
| 3 | 5 6 10 7
| 4 | 1 2 10
| 5 | 4 1
| 6 | 9 7 2 5
| 7 | 1 5 10
| 8 | 7
| 9 | 7 2 4 3
| 10| 2 8 5 6

Testas x 10 kartų
Viršūnių: 10
Grafo lankų: 30
------------------------------------------------------
Laukiami rezultatai:
Paieška is viršūnės: 1 .Panaudota operacijų 4. Ciklas: 1 10 2 7
```

```
Paieška is viršūnės: 2 .Panaudota operacijų 4. Ciklas: 2 7 1 10
Paieška is viršūnės: 3 .Panaudota operacijų 8. Ciklas: 3 5 4 1 10 2 7 1
Paieška is viršūnės: 4 .Panaudota operacijų 8. Ciklas: 4 1 10 2 7 1 3 5
Paieška is viršūnės: 5 .Panaudota operacijų 8. Ciklas: 5 4 1 10 2 7 1 3
Paieška is viršūnės: 6 .Panaudota operacijų 22. Ciklas: 6 9 7 1 10 2 7 5 4 1 3
5 1 9 2 8 7 10
Paieška is viršūnės: 7 .Panaudota operacijų 4. Ciklas: 7 1 10 2
Paieška is viršūnės: 8 .Panaudota operacijų 15. Ciklas: 8 7 1 10 2 7 5 4 1 3 5
1 9 7 10
Paieška is viršūnės: 9 .Panaudota operacijų 12. Ciklas: 9 7 1 10 2 7 5 4 1 3 5
1
Paieška is viršūnės: 10 .Panaudota operacijų 4. Ciklas: 10 2 7 1
-----------------------------------------------------
Skaičiavimai atlikti per: 0.0939548015594 sekundžių


Gretimumo struktūra:
-----
| 1 | 10 3 9 8
| 2 | 7 8 3
| 3 | 5 6 10 7 8 4
| 4 | 1 2 10 8 6
| 5 | 4 1
| 6 | 9 7 2 5 8 1
| 7 | 1 5 10 4
| 8 | 7 9
| 9 | 7 2 4 3
| 10| 2 8 5 6


Testas x 10 kartų
Viršūnių: 10
Grafo lankų: 40
-----------------------------------------------------
Laukiami rezultatai:
Paieška is viršūnės: 1 .Panaudota operacijų 4. Ciklas: 1 10 2 7
Paieška is viršūnės: 2 .Panaudota operacijų 4. Ciklas: 2 7 1 10
Paieška is viršūnės: 3 .Panaudota operacijų 8. Ciklas: 3 5 4 1 10 2 7 1
Paieška is viršūnės: 4 .Panaudota operacijų 8. Ciklas: 4 1 10 2 7 1 3 5
Paieška is viršūnės: 5 .Panaudota operacijų 8. Ciklas: 5 4 1 10 2 7 1 3
Paieška is viršūnės: 6 .Panaudota operacijų 23. Ciklas: 6 9 7 1 10 2 7 5 4 1 3
5 1 9 2 8 7 10 8 9 4 2 3
Paieška is viršūnės: 7 .Panaudota operacijų 4. Ciklas: 7 1 10 2
Paieška is viršūnės: 8 .Panaudota operacijų 15. Ciklas: 8 7 1 10 2 7 5 4 1 3 5
1 9 7 10
Paieška is viršūnės: 9 .Panaudota operacijų 12. Ciklas: 9 7 1 10 2 7 5 4 1 3 5
1
Paieška is viršūnės: 10 .Panaudota operacijų 4. Ciklas: 10 2 7 1
-----------------------------------------------------
Skaičiavimai atlikti per: 0.100757837296 sekundžių
```

2 PRIEDAS. DARBE NAUDOTAS SERTIFIKATAS

KTU sertifikavimo centro išduotas sertifikatas

26 pav. Darbo autoriaus sertifikatas