KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Raimondas Butauskas

E-parduotuvės lojalumo sistema panaudojant e-pinigus

Magistro darbas

Darbo vadovas

Prof. Eligijus Sakalauskas

Kaunas, 2012

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

KOMPIUTERIŲ KATEDRA

E-parduotuvės lojalumo sistema panaudojant e-pinigus

Magistro darbas

Recenzentas

Doc. dr. Saulius Japertas

2012-05-29

Vadovas

Prof. Eligijus Sakalauskas

2012-05-29

Atliko

IFN-0/3 gr. stud.

Raimondas Butauskas

2012-05-23

Kaunas, 2012

Turinys

LENTELĖS

PAVEIKSLAI

SUMMARY

Loyalty program is a marketing effort by the merchant to keep customers loyal to their stores. It tries to keep track of the purchasing-behavior of a customer by recording customer's purchase information, including his credit card number, as akey identifier to the customer. While it may benefit the customer, the drawback is that the privacy of the customer is intruded. If the customer is using an anonymous payment system such as electronic cash / digital coins, his privacy is protected, but he will not get any benefit from the loyalty program which tries to record his payment information. This paper suggests several solutions to this problem.

Among the solutions, we present the idea of *blindly signed pseudo digital certificates,* whichsatisfies our requirement for a loyalty program scheme with an anonymous payment system. We have shown in this paper that it is possible for the merchant to conduct a customer loyalty program although the customers are using an anonymous payment system. Several solutions exist, such as using cookies, least authentic type of digital certificates (pseudo digital certificates), linkable anonymous payment system, and blindly signed pseudo Digital certificates.

Amongst those solutions, the blindly signed pseudo digital certificates satisfies all of our requirements and the most versatile. Three of the solutions basically relies on an additional 'authentication token', which might be considered 'external' or not inherent in the payment protocol. Despite several requirements which are not addressed, the solution to use linkable anonymous payments still make use the inherent design of the payment protocol itself.

We also acknowledge several limitations. One of the most obvious limitation is that the merchants still do not have the ability to gather maximum information it can get, such as customer's mailing address. Of course, the customers can fill those information, only if they are willing to do so and know the consequences. The second limitation is, especially with the blindly signed pseudo digital certificate, that these solution may require the customer to willingly join the loyalty program. From a practical point of view, probably the setup can be awkward for the customers, if not well designed. On the other hand, this limitation may also be an advantage, since law in several states.

Anotacija. Lojalumo sistema skirta rinkodaros pastangomis išlaikyti ištikimus klientus savo parduotuvėse. Lojalumo sistema stebi kliento elgesį perkant prekes įrašo kliento pirkimo informaciją, įskaitant jo kreditinės kortelės numerį, kaip raktą atpažinti vartotojui. Nors ši sistema yra naudinga pirkėjui, tačiau trūkumas yra tai, kad pažeidžiamas kliento privatumas. Jei vartotojas naudojasi anonimiškai mokėjimo sistema, elektroniniais pinigais, tokiu būdu vartotojas išsaugo savo privatumą, tačiau tokiu atveju vartotojas negaus jokios naudos iš lojalumo programos, kuri bando įrašyti jo mokėjimo informacija. Šiame straipsnyje apžvelgsime ir aptarsime keletą šios problemos sprendimo būdų. Kaip šios problemos sprendimą, pristatome idėją aklai pasirašant pseudo skaitmeninius sertifikatus, kurie atitinka mūsų reikalavimus lojalumo programai su anoniminio mokėjimo sistemą.

1 Įvadas

Paskutiniu metu pasirodė keletas straipsnių, kuriuose aiškiai paminėtos problemos susijusios su duomenų rinkimu, kuomet bankai ir pardavėjai renka ir kaupia informaciją apie vartotojus. Nors jų tikslas panaudojant tokius sukauptus duomenis, yra kaip galima geriau aptarnauti klientus, tačiau šiuo atveju išlieka vienas tas pats trūkumas, kaip ir lojalumo programos tai, kad yra pažeidžiamas kliento privatumas.

Žinoma, jeigu klientai naudojasi anonimine mokėjimo sistema, kur klientų tapatybė yra slepiama, jų privatumas yra garantuotas. Bet, kita vertus, klientai praranda jo poreikius atitinkančių prekybinių pasiūlymų nauda, nes prekybininkai negalės susekti kiekvieno kliento pirkimo-elgesio.

Šiame straipsnyje mes siūlome keletą būdų, kaip galima prekybininkams sekti klientų pirkimo-elgesį, net jei vartotojas naudojasi anoniminio mokėjimo sistema, pavyzdžiui elektroniniais pinigais. Taigi, atrodo, kad du priešingi interesai, kurie yra kliento privatumas ir pirklio poreikis rinkti statistinius duomenis apie kliento elgesį, gali būti išspręsti.

Mes apibūdinsime lojalumo programą, arba kitaip tariant klientų išlaikymo programą, kartu ir jos svarbą. Mes taip pat išnagrinėsime kaip prekybininkai gali surinkti reikiamą informaciją klientų lojalumui užtikrinti.

Mes apibūdinsime lojalumo programą, arba kitaip sakant klientų išlaikymo programą. 2 skirsnyje mes taip pat išnagrinėsime, kaip prekybininkai gali surinkti reikiamą informacija lojalumo programai. 2 skirsnyje, mes aptarsime įvairias anoniminio mokėjimo sistemas kartu ir motyvaciją. Šiuo metu, mes matome, nesuderinamumą lojalumo programos ir anoniminio mokėjimo sistemos.

1.1 Analizės tikslas

Apžvelgti esamas elektroninio mokėjimo sistemas jų modelius, metodus ir būdus, išnagrinėti e.parašo panaudojimo galimybes e.parduotuvės atsiskaitymo sistemose. Apžvelgti esamas lojalumo sistemas ir jų panaudojimo galimybes e.parduotuvės sistemoje.

Prašome atkreipti dėmesį, kad mes savo darbe sutelkiame visa dėmesį kliento registracijos ir atpažinimo protokolui, bei lojalumo sistemai. Taigi mes nenagrinėjame kitų saugumo klausimų tokių kaip informacijos perdavimo privatumo, tai yra kita problema.

1.2 Tyrimo sritis, objektas ir problema

Sritis ir objektas

E.parduotuvės lojalumo sistema panaudojant e.pinigus.

Sprendžiama problema

1. Problemos susijusios su duomenų rinkimu, kuomet bankai ir pardavėjai renka ir kaupia informaciją apie vartotojus yra pažeidžiamas kliento privatumas.
2. Lojalumo sistemos veiksmingumas kai vartotojas naudojasi anoniminio mokėjimo sistema, pavyzdžiui elektroniniais pinigais.
3. Kaip perduoti kortelės duomenis ir perkamų prekių duomenis saugiai Internete?
4. Pirkėjo ir pardavėjo autentifikavimas.

2. ANALITINĖ DALIS

2.1 Lojalumo programos apibrėžimai ir reikšmės

Lojalumo programa apibrėžiama, kaip struktūrinės rinkos pastangos skatinančios lojalų kliento elgesį, kuris atneša prekybinę naudą. Dar vienas terminas *„klientų išlaikymo programa*“, kuria Harris[8] apibūdina, kaip nuolatines pastangas stengiantis išlaikyti esamus ir dar būsimus klientus, aktyviai jiems teikiant verslo pasiūlymus.

Programos tikslas yra išlaikyti esamų klientų pirkimus ir padidinti jų pirkimo lojalumą, taip pat pritraukti naujų klientų. Lojalumo tikslas sumažinti galimybę klientui įsigyti kitą konkurencingą prekę ar paslaugą. Boltonn[8] ir Bramlelet[8] lojalumo stebėjimo tyrimai su kreditinėmis kortelėmis parodė, kad klientai esantys lojalumo programoje yra kur kas mažiau jautrūs į kai kuriuos klausimus, kurie tuo metu kitiems būtų aktualūs, tokie kaip prastesnė kokybė, šiek tiek aukštesnė kaina.

Glaudūs santykiai tarp pardavėjo ir kliento yra labai svarbus aspektas kliento lojalumui. Kiekvienas pardavėjas privalo suprasti kliento poreikius ir išsaugoti kliento ištikimybę, pasitikėjimą ir atsidavimą, nes pardavėjas yra tiesiogiai susijęs su kliento pirkimu. Todėl tiksliai žinant ko vartotojas nori - kokia jis nori matyti parduotuvę, kurioje jis apsipirkinės yra labai svarbus veiksnys kliento lojalumui ir jo pirkimams. Pagrindinis Harris [8] argumentas yra tas, kad turi būti sukurta aplinka kur būtų tenkinami esamų klientų poreikiai, bet ištirti nauji klientų poreikiai.

Finansinę lojalumo svarbą pabrėžė William[4], nes lojalumo programa suteikia garantuotas ateities pajamas. Žemas klientų lojalumo lygis reiškia, kad ateityje gali iškilti grėsmė būsimų pajamų sumažėjimui, ar net visiškam praradimui.

2.2 Intelektuali lojalumo programos duomenų analizė

Tarp keletos informacijos gavimo metodų apie kliento poreikius yra kliento pirkimų istorija. Reikia pabrėžti, kad yra keletas būdų kaip galima gauti šiuos duomenis. Pardavėjas gali peržvelgti kliento pirkimo modelį atliekant apsipirkimą. Pavyzdžiui pardavėjas žino, kada pirkėjas perka grūdų, taip pat jis žino kokias prekes pirko kiti klientai kartu su šia preke, taigi pardavėjas šiam apsipirkimui taip pat pasiūlo kitų klientų pirktas prekes perkant grūdų. Gali būti, kad yra žinoma, jog visi klientai kurie pirko grūdus, kartu su jais pirko ir pieną.

Be to pardavėjas gali turėti kiekvieno kliento apsipirkimo struktūrą ir laikas nuo laiko gali sudaryti konkrečius pasiūlymus konkrečiam klientui, priklausomai nuo jo ankstesnių apsipirkimų. Pavyzdžiu jei vartotojas dažniai perka grūdus pardavėjas gali pasiūlyti nuolaidą šiai prekei ir pasiūlyti pabandyti naujas šios rūšies prekės. Pardavėjas taip pat parodo, kurios javų rūšys yra geriausios ir perkamiausios, taip pat pirkėjas gali pasiūlyti kartu prie jo perkamu prekių ir sausus pusryčių dribsnius. Pardavėjas gali ir nesiūlyti šių prekių įsigyti, jei jis mato kad vartotojas retai perka šias perkės.

Boltonas ir Bramlett[8] tyrimai parodo kad yra dar vienas geras pavyzdys kreditinės lojalumo kortelės. Jie pastebėjo, kad lojalumo kortelėse galima saugoti kiekvieno kliento apsipirkimo modelį. Lojalumo programos nariai gali kaupti lojalumo taškus su kiekvienu išleistu piniginiu vienetu. Vėliau šios taškus bus galima iškeisti į automobilių nuomą, atostogų pasirinkimo galimybes ir kitas mažesnes dovanas. Verta pastebėti, kad kai kurios tokios kreditinės kortelės yra mokamos ir jei vartotojas ją nori įsigyti už ja tenka sumokėti pinigus.

Prekybos požiūriu naudoti kreditinės kortelės numerį kliento atpažinimui atrodo visiškai normaliai. Tuomet pardavėjui nereikia klausinėti kliento ar jis dalyvauja lojalumo programoje. Jis tiesiog įrašo kiekviena kliento apsipirkimą į kortelę. Taip pats patogiausias lojalumo variantas ir iš karto klientui pritaikoma lojalumo programa. Žinoma daugelis kreditinių kortelių kompanijų turi partnerystės ryšius su pardavėjais ir šios kompanijos gali surinkti daug vertingos informacijos apie klientą. Debetinės kortelės taip pat įgauna pripažinimą kuriose kiekvienas sandėris gali būti atsektas.

Prekybininkų siūlomos lojalumo sistemos apima, ne tik lojalumo korteles. Pirkėjams yra dalinami įvairus lipdukai kuriuos jie turi klijuoti ant specialaus aplanko. Po to už atitinkama surinktų lipdukų kiekį siūloma įsigyti įvairių prekių padengiant dali prekės vertės surinktais lipdukais.

Atsiskaitant klientui už įsigytas prekes grynaisiais pinigais pardavėjas negali atsekti kliento. Taip pat galime sakyti, kad atsiskaitymas grynaisiais pinigais gali būti prilyginamas anoniminio atsiskaitymo sistemai.

2.3 E-parduotuvės anonimiškumo motyvai

Labai svarbu yra gauti informacija apie kliento nupirktas prekes. Trečios šalys tokios kaip pardavėjai turėdami tokio pobūdžio informaciją gali stebėti savo klientų poreikius, bei jų apsipirkimo elgesį. Be to visi surinkti duomenys gali būti susiję. Surinktus duomenis būtų galima pavadinti taip, kad jie yra vienas bendras didelis duomenų rinkinys ir pagal juos būtų galimą , beveik viską pasakyti apie kliento asmeninį gyvenimo būdą. Vartotojas gali pageidauti, kad jo privatūs duomenys ir buvimo vieta išliktų privatūs.

Chaum‘s [8] propagavo anoniminio mokėjimo sistemą. Nesenai atlikto tyrimo GVU WWW Surveying Team, technologijos universiteto komandos vykdyta apklausa parodė, kad daugiau kaip pusė apklaustųjų norėtų atsiskaityti už prekes, bei paslaugas anonimiškai.

2.4 E-parduotuvės dvi anonimiškumo kryptys.

Savo darbe apžvelgsime dvi anonimiškumo kryptis. Pirma kryptis tai apie kurią jau kalbėjome aukščiau, pagal kuria pardavėjas negali atsekti kliento pirkimų ir nustatyti ryšius tarp pirkėjo ir pardavėjo. Šiuo būdu vartotojas išsaugo pilną pirkimo privatumą. Šio pirkimo būdo negali atsekti ir finansinės institucijos bankas.

Antroji dar viena anoniminio mokėjimo kryptis yra elektroninis pinigas, kurio privalumas yra tas, kad niekas negali atsekti kas jį išleido ir koks tai buvo pirkėjas ar visi išleisti pinigai buvo vieno ir to paties kliento ar skirtingų klientų. Tisounis pastebėjo, kad netgi keletą pirkimų turint norą, nors jie ir anoniminiai juos taip pat galima atsekti pačiais paprasčiausiais būdais, pagal pirkimo vietą, apsipirkimo laiką, apsipirkimo kiekį arba ieškant pagal išleistą pirkėjo apsipirkimo sumą.

Pirmoji elektroninio anoniminio mokėjimo sistema buvo pasiūlyta elektroninių pinigų sistema, elektroniniai grynieji pinigai. Ši elektroninių pinigų sistemos savybė yra universali. Kai kurie šiuos pinigus vadina elektroninėmis monetomis, nes tikrieji pinigai yra nežinia kur.

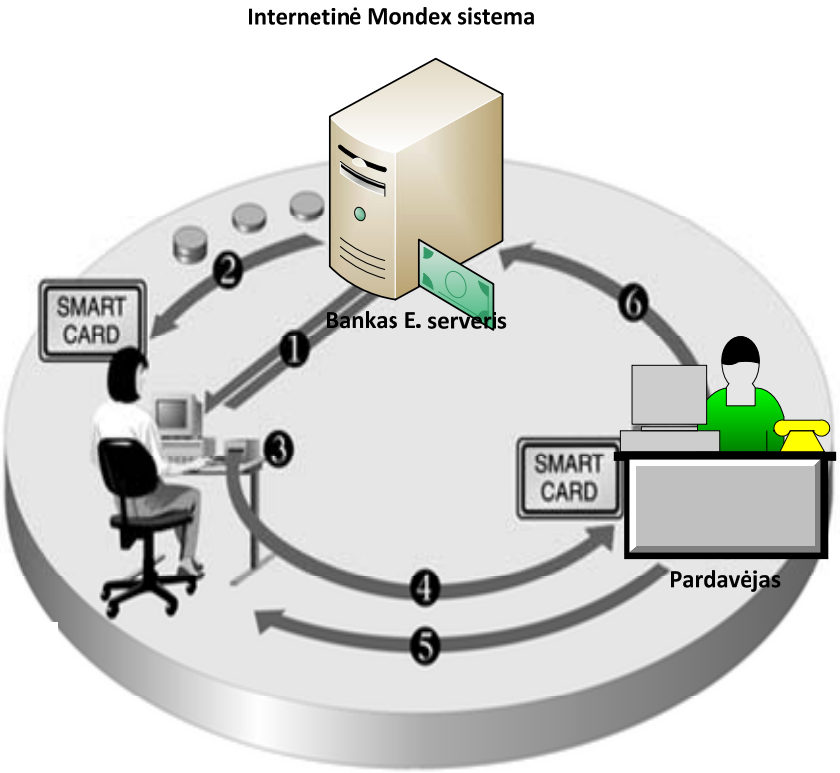
2.5 Veikiančių e-atsiskaitymo sistemų analizė

2.5.1 Esamos pinigų pervedimų sistemos

Mondex sistema

Mondex[6] sistema yra dalis MasterCard pasaulinio tinklo, leidžianti kortelės turėtojams pernešti, laikyti ir leisti pinigus naudojantis mokėjimų kortele. Šis atsikaitymo būdas yra kurkas geresnis ir saugesnis, nei atsiskaitymas grynaisiais pinigais. Tačiau šis metodas yra panašus į atsiskaitymą grynaisiais pinigais, jis leidžia atsiskaityti nedelsiant, bet kartu nereikalaujant PIN kodų ar pervedimo autorizacijos. Mondex sistema leidžia vykdyti atsikaitymus kur įprastiniai pinigai negalimi.

- Interaktyvi televizija;
- Internetas;
- Mobilūs telefonai;



1. Pav. internetinė mondex sistema.

Mondex[6] sistemoje pinigai saugomi elektronine forma. Vykstant atsiskaitymui, dalis pinigų vertės perkeliama iš mikroschemos kortelėje į mikroschemą terminale (kortelės skaitytuve) .

1) Vartotojas atsidaręs sąskaitą 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; 21

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 [6].

Pagrindiniai privalumai:

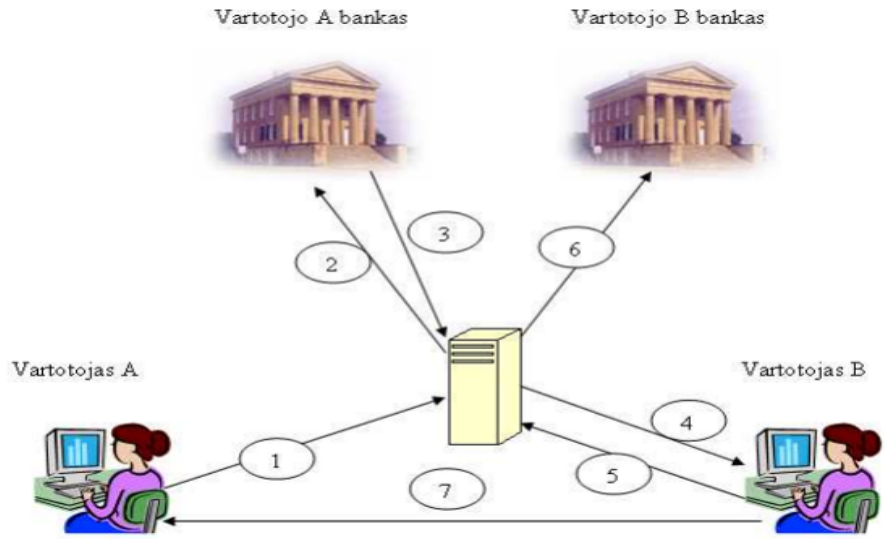
- Patogumas. Sistema leidžia vartotojui atlikti mokėjimą neieškant bankomato ar gaištant laiką autorizuojantis. Atsiskaityti galima netik su pardavėjais ar paslaugų tiekėjais, bet ir kitais kortelės naudotojais (fiziniais asmenimis);
- Saugumas. Kortelėje įdiegta jos užrakinimo (lock) funkcija, kuri gali apsisaugoti nuo neleistino panaudojimo. Užrakinimo kodas yra parenkamas kortelės savininko ir gali būti bet kuriuo metu pakeistas;
- Lankstumas. Sistema gali atsiskaityti už bet ką ir praktiškai bet kokia 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]

PayPal sistema:

PayPal [7] - 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 [7].



2. 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 žingsnio 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 užsiimantis 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 neegzistuoti [7].

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) [7].

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 [7].

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

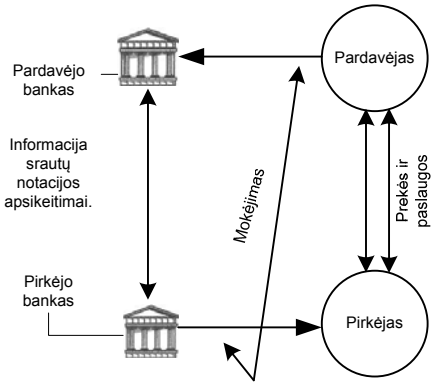
• Visi pervedimai yra momentiniai (nereikia laukti)

Sistemos trūkumai

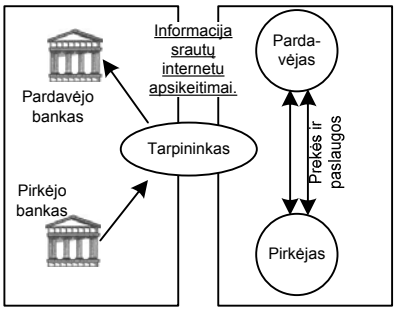
• Dėl populiarumo tarp vartotojų, PayPal yra pamėgta kreditinių kortelių vagių ir kitų piktavalių

2.6 Užduoties iškėlimas

Šiuo metu, mes galime pastebėti lyg ir nesuderinamus interesus. Bankai ar pardavėjai nori rinkti statistinius duomenis apie klientų elgseną ir kliento mokėjimo informaciją, tačiau klientai gali ir nori naudotis anoniminio apmokėjimo sistema. 3 paveiksle yra supaprastinta operacijų schema grynaisiais ir negrynaisiais pinigais. Pinigai juda iš pirkėjų bankų pardavėjų bankams. Jei pirkėjas atsiskaito ne grynaisiais pinigais, mokėjimo informaciją, o ne pinigų srautus iš pirkėjo pardavėjui, ir galutinis mokėjimas įvyksta tarp pirkėjo ir pardavėjo bankų koreguojant ataskaitas, grindžiamas mokėjimo informaciją.



3. pav. Tradicinė mokėjimo sistema.



4. pav. Elektroninio mokėjimo sistema.

Tam tikros atsiskaitymo sistemos susiję su surenkamu dideliu asmeninės informacijos kiekiu. Off-line pasaulyje pati anonimiškiausia mokėjimo/atsiskaitymo priemonė yra grynieji pinigai. 4 paveikslas rodo elektroninio mokėjimo sistemą, kurioje tarpininkas veikia kaip elektroninis bankas kuris keičia pinigus į elektroninę formą, kuri toliau yra siunčiamą į bankus interneto kanalu. Taip pat kaip ir kasdieniai pinigai, e-pinigai gali būti plačiai naudojami kasdieniniame gyvenime su kur kas didesniu pirkimo sandorio efektyvumu. Kadangi pinigų vertė yra aiški ir neginčijama, jų gavėjai nereikalauja papildomo autentiškumo užtikrinimo. Kitos mokėjimo priemonės – kreditinės kortelės, dažnai reikalauja asmeninės informacijos atskleidimo, siekiant užtikrinti mokėtojo autentiškumą. Priemonės,

kurios įgalintų ir OL aplinkoje naudoti ‘grynuosius’ pinigus, labai padidintų anonimiškumo laipsnį ir apribotų header informacijos apie vartotoją/mokėtoją rinkimą. Keletas kompanijų jau yra įdiegusios ir plėtoja ‘e-grynųjų’ pinigų mechanizmus pasauliniuose tinkluose. E-grynieji pinigai (EGP) encryption sistemos pagalba mokėtojui suteikia anonimiškumą. Iš esmės, pinigai iš banko sąskaitos gali būti paversti e-monetomis, kurios savo ruožtu paverčiamos e-pinigine vartotojo kompiuteryje. Iš čia e-monetos gali būti pervedamos kitiems ūkio subjektams, on-line vykdantiems veiklą. Kiekviena e-moneta turi unikalų serijinį numerį ir yra patvirtinama e-parašu, kuris įgalina įvertinti sandorių autentiškumą ir užkerta kelią tos pačios e–monetos pakartotinam išleidimui. Siekiant apsaugoti vartotojo anonimiškumą, vartotojo kompiuteris (o ne bankas) gali randomo pagalba (atsitiktinai) monetai suteikti unikalų serijinį numerį, kuris specialiame e-voke yra persiunčiamas bankui. Bankas prie voko prideda ‘aklą skaitmeninį parašą’, debituoja vartotojo sąskaitą banke ir e-monetą grąžina, net nesužinodamas jos serijinio numerio. Po to vartotojas gali išleisti e-monetą, ir apmokėjimas yra įvykdomas, netgi jeigu jis taip ir nesužino mokėtojo tapatybės.

Šis įvertinimo procesas labiau panašus į elektroninio parašo tikrinimo procesą – jo metu negalima nustatyti tikrųjų pasirašiusiojo asmens duomenų ar tuo labiau parašo formavimo duomenų. Tokio patikrinimo metu tėra nustatoma, ar sąskaitoje pateikti duomenys iš tiesų yra to konkretaus naudotojo, kurio vardu užpildyta sąskaita, ir kuris atlieka mokėjimą, duomenys.

Prieš formuojant mūsų problema mums visų pirma reikėtų suprasti esančias problemas realiame pasaulyje. Turime pastebėti, kad bankai (arba pas mus tekste minimos kreditų bendrovės) vargu ar galės apsaugoti klientų privatumą, kuomet bankų sistemos laikas nuo laiko papildomos įvairiomis šiuolaikiškomis naujomis sistemomis. Egzistuoja mažiausiai keturi pagrindinai aspektai, kurie neužtikrina pilnos apsaugos klientų privatumui.

- Informacijos perdavimas internetu.
- Trečiųjų šalių santykiai (pvz. Santykiai su pardavėjais)
- Kompiuterizuotas kredito vertinimas
- Duomenų santykių su klientais valdymas (lojalumo programos)
- Mokėjimo ir užsakymo konfidencialumas
- Informacija turi būti matoma tik tam, kam ji skirta
- Naudojamas šifravimas
- Perduodamų duomenų integralumas

- Užtikrinti kortelės turėtojo autentifikavimą
- Naudojami skaitmeniniai sertifikatai ir parašai
- Užtikrinti pardavėjo autentifikavimą
- Protokolas turi nepriklausyti nuo saugaus transporto protokolo (SSL/TLS, VPN, SSH) naudojimo (ar nenaudojimo)
- Informacijos konfidencialumas
- Pardavėjas negali sužinoti pirkėjo kreditinės kortelės duomenų. Jie pateikiami tik bankui emitentui. Naudoja DES.
- Duomenų integralumas
- Užsakymo ir mokėjimo duomenys pasirašomi naudojant SHA-1 maišos funkciją. Kai kurios dalys naudoja HMAC su SHA-1
- Pirkėjo autentifikavimas
- X.509v3 skaitmeniniai sertifikatai
- Pardavėjo autentifikavimas
- X.509v3 skaitmeniniai sertifikatai
- Skirtingai nei IPSec ar SSL/TLS, SET palaiko tik po vieną kriptografinį algoritmą kiekvienai funkcijai

Taip pat esame pastebėję, kad daugumas komercinių internetinių puslapių norint juose naršyti- pirkti reikalauja kliento registracijos, informacijos apie klientų turimas kreditines korteles, jų gyvenamą vietą, arba kitaip jie nepristatys prekių. Iš vienos pusės žiūrint tai paprasčiausia saugumo priemonė leidžianti apsisaugoti nuo kreditinių kortelių klastojimo. Bet nėra jokios garantijos, kad pardavėjas nerenka informacijos apie klientą ir apie jo atliekamus pirkimus.

2.6.1 Saugumo problemos:

Dabar mes formaliai apibrėžiame mūsų problemą:

1. Kadangi sistemos klientai naudojasi anoniminio mokėjimo sistema, mums reikia rasti sprendimą, kaip pardavėjai galės sekti savo klientų pirkimo elgesį.
2. Saugi registracija, bei prisijungimas prie e-parduotuvės.
3. Sudėtingas lojalumo sistemos administravimas.

4. Galimas lojalumo informacijos padirbinėjimas.
5. Neteisėta registracija. (kurios paskirtis daryti žalą tretiems asmenis ar platinti netinkamo pobūdžio informaciją)

2.7 Analitinės dalies išvados.

1. Nustatėme lojalumo sistemos svarbą vartotojui.
2. Susidūrėme su vartotojų anonimiškumo problema, teikiant lojalumo programos pasiūlymus.
3. Atlikus analizę išryškėjo vartotojų saugios registracijos ir prisijungimo problema prie e-parduotuves sistemos.
4. Susidūrėme su galimu neteisėtu lojalumo sistemos panaudojimu, dėl kurio pardavėjai gali patirti papildomų išlaidų.

3. PROJEKTINĖ DALIS

3.1 Siūlomas kriptografinis saugumo sprendimas.

Taip kaip mes šiuo metu atlikome elektroninių pinigų tyrimus, mes iš pradžių mastėme apie pinigų sukūrimą lojalumo palaikymui. Matomai taip pat, kaip ir eilinis pirkimas grynaisiais pinigais turi keletą aspektų, mes manėme, kad bus kur kas lengviau, jeigu turėsime elektroninį anoniminį pinigą, kuris saugo kliento privatumą. Tada mes įrodysime, kad elektroniniai pinigai yra tas pats kas ir pirkimas grynais pinigais.

Paaiškėjo, kad anoniminiai elektroniniai pinigai yra labai svarbūs mūsų tyrime. Elektroninis pinigas yra paruoštas lygiai taip pat kaip ir kiti, naudojant aklas pasirašymo protokolų schemas, bet be monetos vertės. Pasirašant elektroninius pinigus mes panaudojame slapyvardį tapatybę, kuris yra sukuriamas pasirašant protokolą. Parašas su pseudo tapatybe reiškia, kad tokia tapatybė yra patikima. *Todėl pagrindinis mūsų sprendimas remiasi aklu pasirašymu ant vartotojo sugeneruoto pranešim.*. Mes nustatome asmens slapyvardį kaip asmens vardą, kuris nėra tikras asmens vardas.

Padetalizuosime aklą sertifikatų centro parašą paremtą RSA kriptosistema, ant vartotojo atsitiktinio pranešimo.

1. Raktų generavimas

$n=pq$, p-pirm. Generuojami pirminiai skaičiai turi tenkinti FIPS-140 pseudo atsitiktinių skaičių generatoriaus savybes.

Vartotojo viešasis ir privatusis raktai

$VrK_V=(e,n)$ $PrK_V=d$

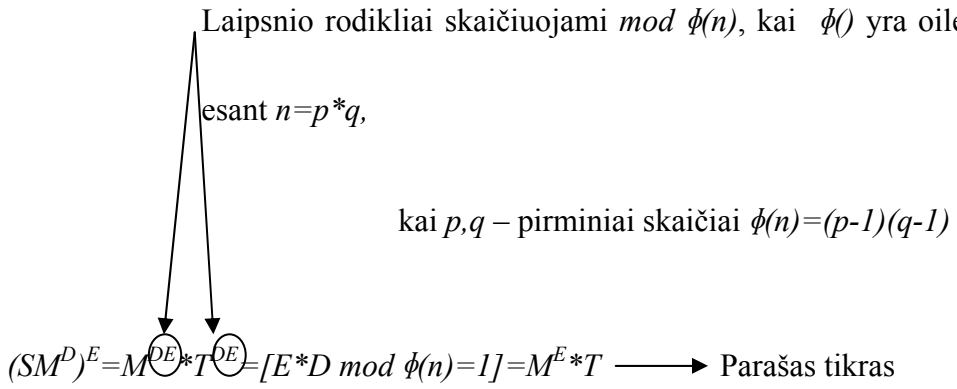
Sertifikatų centro viešasis ir privatusis raktai

$VrK_C=(E,N)$ $PrK_C=D$

2. Parašo maskavimas atsitiktiniu skaičiumi M<n

$SM=M^E*T$ ⟶ $SM^D=(M^E*T)^D$

3. Parašo tikrinimas ⟵ SM^D



5. Parašo tikrinimas ir Demaskavimas

$SM^D=M^{ED}*T^D*mod(n)=M^1*T^D$

$M^{-1}*SM^D=M^{-1}*M^1*T^D=T^D$

Dabar apibrėšime siūlomo lojalumo sistemos protokolo reikalavimus. Siūlomas sprendimas turėtų turėti tokias savybes:

- Protokolas turėtų leisti prekybininkams susieti keletą mokėjimų vietų, laiką konkretaus kliento pirkiniams.
- Protokolas turi užtikrinti dalinį anonimiškumą su pardavėju.
- Mokėjimams vykdyti naudosime SET protokolą.
- Kliento slapyvardis negali būti naudojamas kito kliento. Slapyvardis turi būti unikalus kiekvienam klientui.
- Kliento slapyvardis yra sukuriamas tik paties kliento ir niekas negali jo pakeisti ir redaguoti.
- Protokolas gali būti naudojas tik po to kai buvo patvirtinta kliento tapatybė autentiškumas pardavėjui. Po to vartotojas susikuria savo slapyvardį toki, kad bet kuri kita šalis negalėtų jo susieti su tikrąja kliento tapatybe.
- E-parašu paremtas saugumas.

SET[3] Standartas sukurtas kompanijų Visa ir MasterCard (kartu su Microsoft, IBM, Netscape, RSA, VeriSign) 1996 metais. Specialiai projektuotas apsaugoti kreditinių kortelių transakcijas. Standartas kurtas norint užtikrinti:

- Privatumą (prieinama tik reikiama informacija)

- Konfidencialumą (visi pranešimai šifruojami)
- Pasitikėjimą (visos šalys turi skaitmeninius sertifikatus)

3.1.1 E-parašo saugumas

Dokumentų pasirašymas elektroniniu būdu

Dokumentų pasirašymui elektroniniu būdu naudojamas skaitmeninis sertifikatas. Tai virtualus dokumentas – asmens tapatybės nustatymo priemonė, vienareikšmiškai ir saugiai identifikuojanti sertifikato savininką, turinti realiam parašui prilygstančią juridinę galią. Naudodami skaitmeninį sertifikatą galite įrodyti savo tapatybę atlikdami operacijas internetu, patogiai gauti priėjimą prie jums reikalingos asmeninės informacijos. Siųsdami elektroniniu būdu pasirašytą informaciją verslo partneriams ar draugams garantuosite, jog duomenys gaunami iš jūsų yra tikri.

Skaitmeninių sertifikatų veikimas pagrįstas asimetrinio šifravimo technologija. Verta paminėti, kad šifravimo metu informacija pakeičiama į specifinę formą, iš kurios duomenis paversti atgal į pradinę formą galima tik žinant duomenų pakeitimo algoritmą. Raktas yra tokio algoritmo parametras. Tokiam asimetriniam šifravimui, dar vadinamam viešojo rakto kodavimu, naudojama matematiškai tarpusavyje susijusių raktų pora – privatus (angl. *private key*) ir viešasis (angl. *public key*) raktai.

Viešasis raktas paprastai laisvai pasiekiamas asmenims, kuriems norima saugiai siųsti informaciją, o privatųjį raktą paslaptyje saugo jo savininkas. Pastarasis, prieš siųsdamas duomenis gavėjui, juos užšifruoja savo privačiu raktu. Tokį pranešimą gavėjas gali iššifruoti tik tos pačios raktų poros viešuoju raktu. Galimas ir atvirkščias variantas: siuntėjas duomenis šifruoja gavėjo viešuoju raktu, o gavėjas juos gali iššifruoti tik savo privačiu raktu. Kitaip sakant, viešojo ir privataus rakto pora funkcionuoja tik naudojama kartu. Šį šifravimo būdą išrado JAV Masačiusetso Technologijos Instituto profesoriai R. Rivest, A. Shamir, ir L. Adleman. Iš kūrėjų pavardžių kilo algoritmo pavadinimas – RSA[10].

Nors viešasis ir privatus raktai yra skirtingi, tačiau jie gali atlikti tiktai vienpusį kodavimą – užkoduoti pranešimą taip, kad jį atkoduotų tik kitas tos pačios poros raktas. Kitaip tariant raktai koduoja „priešingomis kryptimis“. Ši technologija sukuria pagrindą elektroninio parašo atsiradimui. Jei gavėjas gali atkoduoti pranešimą viešojo rakto pagalba, tai ši žinutė yra užkoduota siuntėjo privataus rakto pagalba. Kadangi privatus raktas yra tik vienas ir yra gerai apsaugotas, tai jis tampa tam tikru elektroniniu parašu – dokumentu, kurio

niekas kitas negali sukurti. Naudojant skaitmeninį sertifikatą yra galimybė patikrinti vartotojo teises į konkretų raktą, o tai užkerta kelią neteisėtam privačiojo rakto naudojimui.

Dėl minėtų priežasčių skaitmeniniai sertifikatai suteikia galimybę patikimai identifikuoti elektroninius veiksmus atliekančių asmenų tapatybę.

Esminės viešojo rakto infrastruktūros (*Public Key Infrastructure – PKI*), kurioje viešojo rakto kodavimui naudojamas skaitmeninis sertifikatas, funkcijos yra šios:

autentifikavimas – naudojamas abiejų dalyvaujančių asmenų tapatybės įrodymui;

integralumas – galimybė įsitikinti, kad siuntimo metu duomenys nebuvo pakeisti;

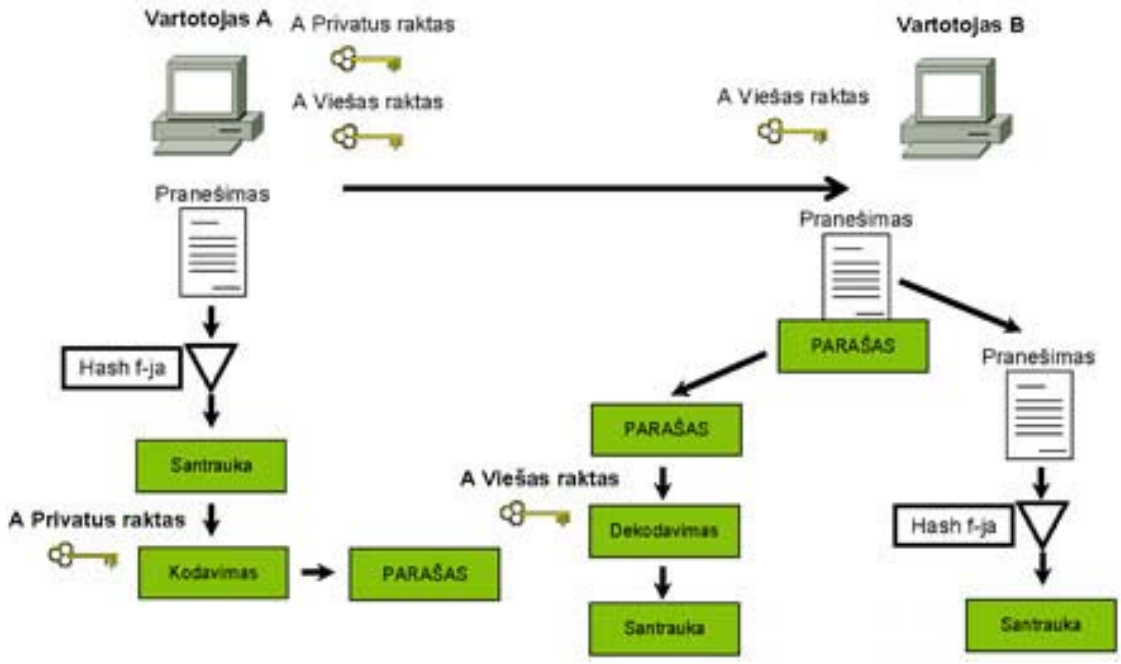
konfidencialumas – siunčiama informacija gali būti koduojama siekiant užtikrinti jos saugumą nuo trečiųjų asmenų;

neatskiriamumas – viešojo rakto infrastruktūra leidžia abiems dalyvaujančioms pusėms saugiai patekti į tinklą ir pasirašyti siunčiamus duomenis.

Skaitmeninį sertifikatą sudaro ir skiria sertifikavimo paslaugas teikianti organizacija (*Certification Authority – CA*), pasirašanti jį savo privačiu raktu. Ji taip pat teikia sertifikatų duomenis parašo naudotojams elektroniniams parašams tikrinti.

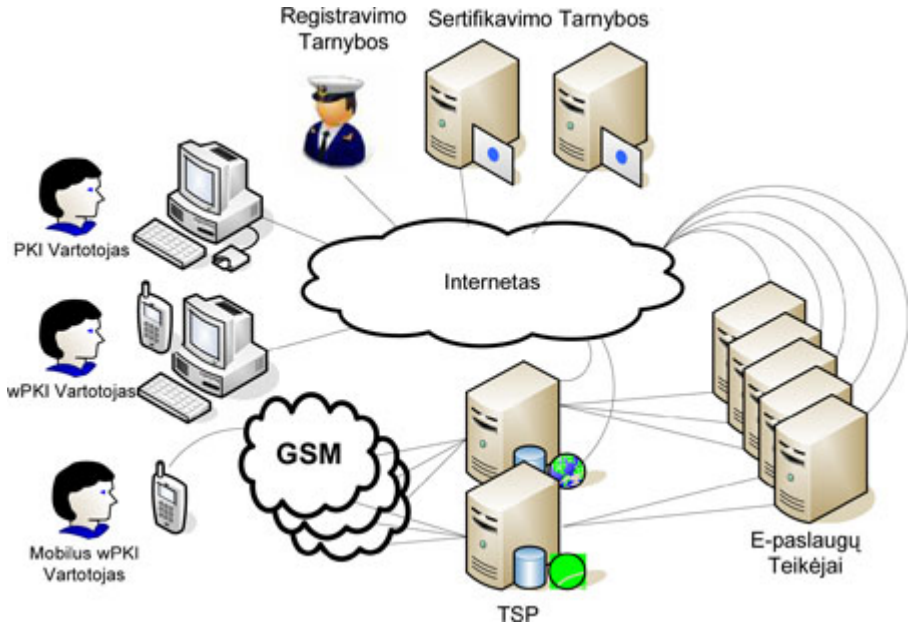
Skaitmeninis sertifikatas paprastai susideda iš:

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



5. pav. Pranešimo pasirašymas E-parašu šifravimo algoritmas

Skaitmeninis parašas turi būti patvirtintas oficialiai. Taigi, asmeniniai duomenys (pvz., vardas ir pavardė, ar slapyvardis) kartu su viešuoju raktu turi būti perduoti oficialioms institucijoms. Duomenis ir viešąjį raktą skaitmeniniu parašu pasirašo autoritetingas asmuo (sertifikatų centras) ir jie perduodami atgal savininkui. Skaitmeninis sertifikatas - tai duomenys apie asmenį ir jo viešąjį raktą, pasirašyti skaitmeniniu nepriklausomos įstaigos - sertifikatų centro - parašu. Norint įsitikinti, kad sertifikatas nesuklastotas, tereikia žinoti viešąjį sertifikatų centro raktą. 6 paveiksle pateikta sertifikavimo tarnybos schema.



6. pav. Sertifikatų registravimo išdavimo tarnybos.

Skaitmeniniame sertifikate be informacijos apie asmenį ir jo viešąjį raktą, būtinai turi būti nurodytas sertifikato galiojimo laikas, sertifikato serijos numeris, informacija apie sertifikatą išdavusią įstaigą ir jos skaitmeninis parašas. Galima nurodyti ir kitokius papildomus duomenis, pvz., nurodyti vartojimo teises, ir taip pasiekti tinkamą duomenų naudojimo vietiniame tinkle apsaugos lygmenį. Skaitmeninio sertifikato pavyzdys: Unikalus sertifikato numeris certificate serial number: 0065933 Sertifikatų centro atributai issuer of certificate: C=LT L=Vilnius O=VĮ Infostruktūra (Elpasas) OU=Elpaso 1 klasė - tikslinis asmens sertifikatas Šifravimo rakto savininko atributai subscriber name: C=LT O=VĮ Infostruktūra (Elpasas) L=Vilnius OU=Valstybinė duomenų apsaugos inspekcija CN=Vyr. inspektorius Jonas Jonaitis E=jojo@is.lt Viešasis šifravimo raktas public key: 235687387…...…..…46646445 Sertifikato galiojimo pradžia valid since: 2011 08 28 Sertifikato galiojimo pabaiga valid until: 2011 11 28 Skaitmeninio parašo algoritmas signature algorithm RSA(1024 bits) Skaitmeninis sertifikatų centro, išdavusio šį sertifikatą, parašas Digital Signature of the issuer VĮ Infostruktūra (Elpasas) 453a089f3….....….4 æ *$56 Sertifikato formatas yra aprašytas tarptautiniu standartu X.509, todėl jį gali perskaityti ar kurti programos, pripažįstančios X.509 standartą. Prie pranešimo ar transakcijos gali būti prijungti keli sertifikatai, kurių kiekvienas tvirtina pirmesniojo tikrumą. Paskutinysis sertifikatas turi būti pasirašytas pripažinto sertifikatų centro. 4 paveiksle Sertifikatų centras Prie siunčiamo dokumento prijungus informaciją apie siuntėjo viešąjį raktą, jį tokiu būdu galima perduoti gavėjui. Tačiau iškyla klausimas, kas paliudys, kad tas viešasis raktas (t.y. šifravimo raktų pora) priklauso tam asmeniui, kurio vardu pasirašomas elektroninis pranešimas. Todėl šį vaidmenį turi atlikti sertifikatų centras (CA - Certification Authority). Sertifikatų centras - nepriklausoma patikima trečioji šalis, kuri registruoja vartotoją ir jo viešąjį šifravimo raktą, išduoda ribotą laikotarpį galiojantį liudijimą - skaitmeninį sertifikatą, to centro skaitmeniniu parašu patvirtinantį unikalaus viešojo rakto priklausomybę tam vartotojui, tvarko ir seka sertifikatų galiojimą, suteikia informaciją apie vartotojų sertifikatus. Taigi skaitmeninis sertifikatas yra lyg ir asmens pasas, patvirtintas nepriklausomos įstaigos, įrodantis siuntėjo tapatybę. Dėl kokių nors priežasčių gali prireikti panaikinti sertifikato galiojimą (pvz., asmuo prarado privataus rakto failą, pasikeitė asmens įgaliojimai - darbuotojas pakeitė darbą ir pan.). Todėl nepriklausomas tarpininkas - sertifikatų centras - turi suorganizuoti savo veiklą taip, kad asmuo nedelsdamas galėtų pranešti apie sertifikato panaikinimą, laikiną jo galiojimo sustabdymą ar galiojimo pratęsimą. Sertifikatų centras yra centrinė skaitmeninio parašo infrastruktūros dalis (žr. 6 schemą). Šiuo metu veikiantys sertifikatų centrai (VeriSign, BelSign, GNS.CA, Netrust, mTrust) savo pareigas, taisykles ir atsakomybę aprašo savo nuostatuose (angl. CPS - certification practices statement), kurie yra

pagrindinis sertifikatų centro veiklą ir santykius su savo abonentais - sertifikatų gavėjais - reguliuojantis dokumentas. Asmuo gauna tokiame sertifikatų centre skaitmeninį sertifikatą, kurį įsidiegęs į savo naršyklę ar atitinkamą programinę įrangą, gali pasiekti saugaus darbo su duomenimis lygmenį. Sertifikatų centras gali būti ir vidinis, tenkinantis vienos organizacijos reikmes. Tada organizacija pati tvarko sertifikatų bazę, dažniausiai ją tiesiogiai sujungdama su personalo duomenų baze. Viešasis sertifikatų centras teikia savo paslaugas visiems to pageidaujantiems (asmenims ir organizacijoms, kurios neturi resursų saugiam sertifikatų tvarkymui).

3.1.2 Viešojo rakto sertifikatas

Skaitmeninis sertifikatas, kitaip vadinamas *viešojo rakto sertifikatas* tai saugos priemonė kurios pagalba gali būti perduodama informaciją per nesaugius žiniatinklio kanalus. Skaitmeniniai sertifikatai dažniausiai naudojami, kaip priemonės perduoti informacija ir užtikrinti autentiškumą naudojantis nesaugiais interneto kanalais. Iš esmės jos padeda mums įsitikinti, kad asmuo rašantis pranešimą prisistato kaip „Aldona“ ir iš tikrųjų ji yra „Aldona“. Tai padeda nustatyti asimetrinis kriptografijos šifravimo algoritmai tokie, kaip RSA El-gmal, PSI ir t.t.

Norint sukurti skaitmeninį sertifikatą pačioje pradžioje vienas asmuo sukuria viešųjų raktų porą, jis pasilieka saugoti savo privačius raktus, tada siunčia savo viešąjį raktą su savo asmenine informacija sertifikavimo institucijai (CA). CA sukuria sertifikatą kurį pasirašo viešuoju raktu. Tačiau paprastai jis apima ir kitą būtina informaciją tokia, kaip asmens informacija, adresas, asmens kodas, gyvenama vieta, galiojimo laikas ir t.t. Bet kuris kitas asmuo norėdamas patikrinti informaciją turi turėti CA viešąjį raktą.

Skaitmeniniai sertifikatai gali turėti skirtingus „autorizacijos“ lygius. Pirmos klasės lygis yra pats žemiausias, kuo aukštesnis lygis tuo geresnė autorizacija. Pirmai klasei priklauso sertifikavimo centro išduoti sertifikatai be subjekto asmenybės tikrinimo. Tik saugumo priemonė, verčia, kad ūkio subjektas įvestų savo elektroninio pašto adresą registracijos metu, nes paprastai vartotojas gaus jo prašomą CA pažymą į pašto dėžutė. Tačiau Aldona, gali pretenduoti ir į Bronius sertifikatą, pateikdama Broniaus duomenis, jo asmeninę informaciją ir *jai* bus (naujai sukurtas) e-mail adresas *bronius@e-mail.com* CA registracijos metu.

Norint gauti aukščiausio lygio saugumo sertifikatą toki kokį naudoja WEB – serveriai yra kur kas sudėtingesnė procedūra. Norėdami gauti aukščiausio lygio sertifikatą, reikia asmeniškai atvykti į sertifikavimo centrą ir ten užsiregistruoti, pateikus asmenybe

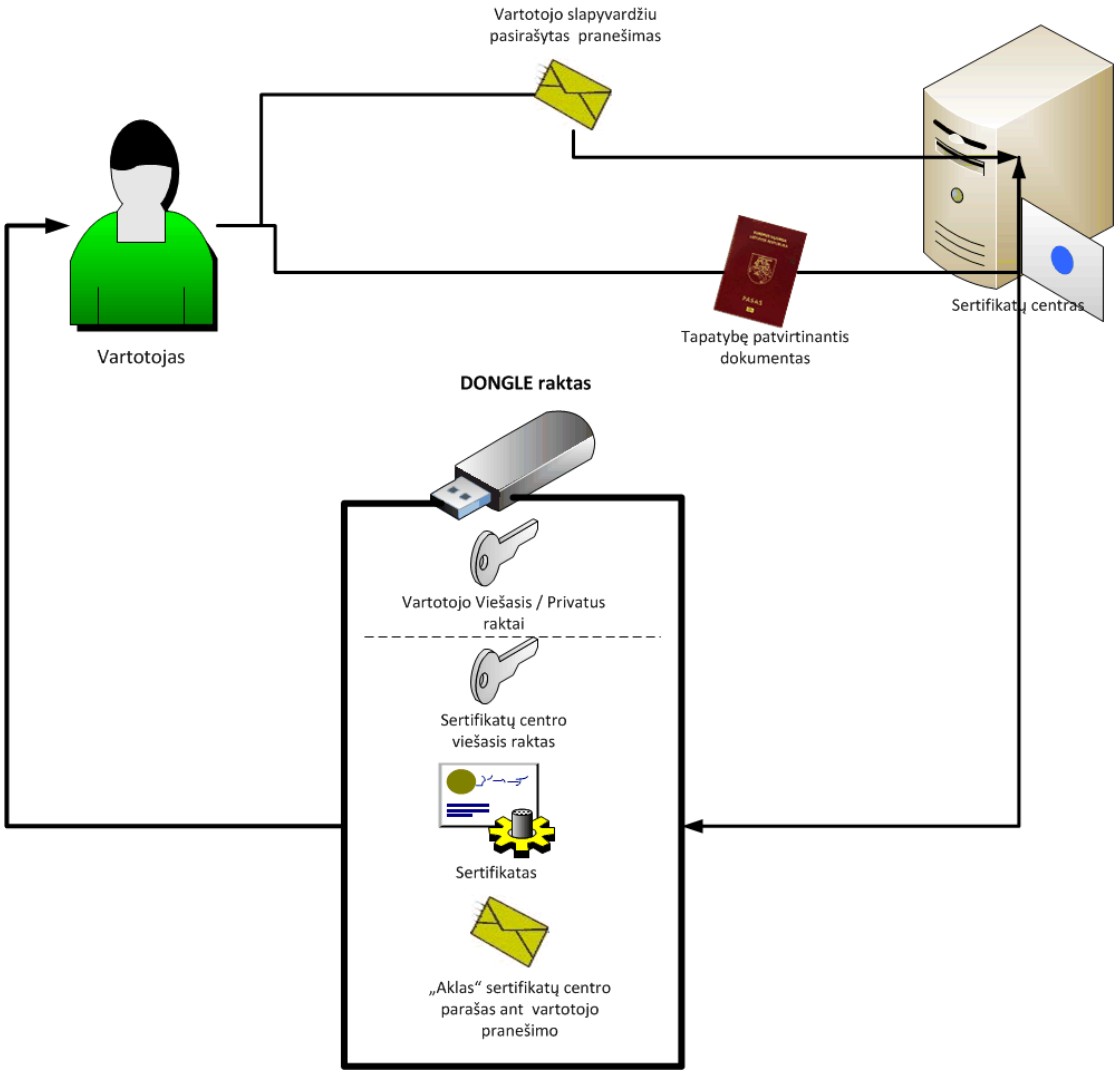
patvirtinančius dokumentus. Tokio lygio sertifikatas iš CA garantuoja, kad sertifikatas Broniaus Bronislovo yra tikrai Broniaus Bronislovo.

Mūsų nagrinėjamoje situacijoje mums pilnai pakanka ir pačio paprasčiausio pirmos klasės sertifikato. Mums visikai nėra svarbu kokį slapyvardį pasirinks pats vartotojas. Jei sertifikavimo centras nenustatinėja kliento tapatybės išduodamas pirmo lygio sertifikatą ir išduoda tik autorizuota skaitmeniniu parašu šis sertifikatas tenkina visus mūsų keliamus reikalavimus išskyrus šeštąjį reikalavimą, nes nebuvo galimybės patikrinti pirkėjo asmenybės.

3.1.3 Aklu parašu sertifikatų centro pasirašomas pranešimas.

Pagrindinė šio sprendimo idėja yra aklai slapyvardžius pasirašomas skaitmeninis pranešimas kiekvienam klientui (7 paveikslas). Atkreipkime dėmesį, kad šis sprendimas yra toks pat kaip ir ankščiau aprašytas. Tik šiuo atveju pardavėjas gali patikrinti kliento tapatybę. Aklasis parašas reiškia, kad aklai pasirašęs asmuo neturi jokių žinių kokį tekstą jis pasirašė. Kaip tai veikia:

1. Patikima šalis patvirtina prieiga prie kliento tam tikru būdu, pavyzdžiui naudojantis skaitmeniniais liudijimais ar kitais fiziniais įrodymais. Šis žingsnis yra labai svarbus tinkamai identifikuoti klientą, nes po to jį turės atpažinti lojalumo sistema. Primename jei protokolas bus atliekamas per viešąjį nesaugų tinklą tai apsikeičiami pranešimai turi būti pasirašyti, kad būtų galima patvirtinti autentiškumą.
2. Vartotojas su tapatybę patvirtinančiu dokumentu kreipiasi į sertifikatų centrą. Generuoja viešųjų ir privačiųjų raktų poras. Privačiuosius raktus pasilieka pas save. Paruošia ir pasirašo slapyvardžiu pranešimą.
3. Vartotojas panaudoja savo viešąjį raktą ir atlieką pranešimo pasirašymą, sertifikatų centras pasirašo savo viešuoju raktu. Abu vartotojas ir sertifikatų centras atliko būtinus žingsnius vykdydami pasirašymo protokolą.
4. Galiausiai vartotojas gauna sertifikatų centro parašą savo pranešimui (t.y. sertifikatų centras aklai pasirašė vartotojo slapyvardžiu sugeneruotą pranešimą).
5. Po protokolo įvykdymo vartotojas gauna pasirašytą pranešimą viešąjį sertifikato centro raktą ir skaitmeninį sertifikatą, savo sugeneruotų raktų porą.
6. Visi šie duomenys vartotojui įrašomi ir perduodami DONGLE rakte sertifikatų centre. Kadangi pranešimas buvo pasirašytas aklai todėl niekas negali nustatyti pasirašiusiųjų tapatybės.



7. pav., Aklasis parašas ant slapyvardžius sugeneruoto pranešimo.

Tik gavęs vartotojas sertifikatų centro parašą ant savo sugeneruoto pranešimo galės registruotis ir prisijungti e-parduotuvėje. Visi šie duomenys sertifikatų centre vartotojui įrašomi į aparatinį įrenginį DONGLE raktą.

DNGLE raktų paskirtis apsaugoti duomenis pritaikius aparatinį metodą, pagrįstą apsaugos rakto naudojimu. Apsaugos raktas – aparatinis įrenginys, kuris jungiamas prie kompiuterio, ir be kurio atitinkama taikomoji programa neveiks [7, 13] arba praras dalį funkcijų. Dalis programų apsaugotos apsaugos raktais, kuriuose įrašytas identifikacinis numeris, todėl programa patikrina programoje įrašyta ID su rakte įrašytu ID.

Dalis apsaugos raktų susideda iš mikroprocesoriaus ir atminties, taip raktas atlieka funkcijų skaičiavimus ir kriptografinius šifravimus, todėl raktą sunkiau dublikuoti ar generuoti [15].

Programa siunčia duomenų kiekį į modulį, kuriame duomenys apdorojami ir gautas rezultatas siunčiamas atgal programai [16]. Jei rezultatas tinkamas – programa veiks. Tai leidžia apsaugoti programą nuo neautorizuoto naudojimo.

Apsaugos raktai skiriasi keliais parametrais: prie kompiuterio jungiamu prievadu, taikomosios programos ir įrenginio komunikavimo algoritmu, šifravimo sudėtingumu, pritaikymo galimybėmis ir kaina. Modulių skaičius dažniausiai apsprendžiamas kai apsprendžiamas programų kopijų skaičius [15].

Apsaugos raktų įrenginiai

Universalios nuoseklios magistralės (angl. USB – Universal Serial Bus) modulis 1 pav. USB prievado moduliai yra populiariausi, nes kiekvienas kompiuteris turi kelis USB prievadus. Kompiuteryje įdiegtos kelios taikomosios

programos gali būti apsaugomos atskirais USB moduliais. Pasinaudojus USB komutatoriumi prie vieno kompiuterio prievado galima prijungti kelis USB modulius [14]

8. pav. USB modulis [17]

3.2 E-parduotuvei keliami reikalavimai.

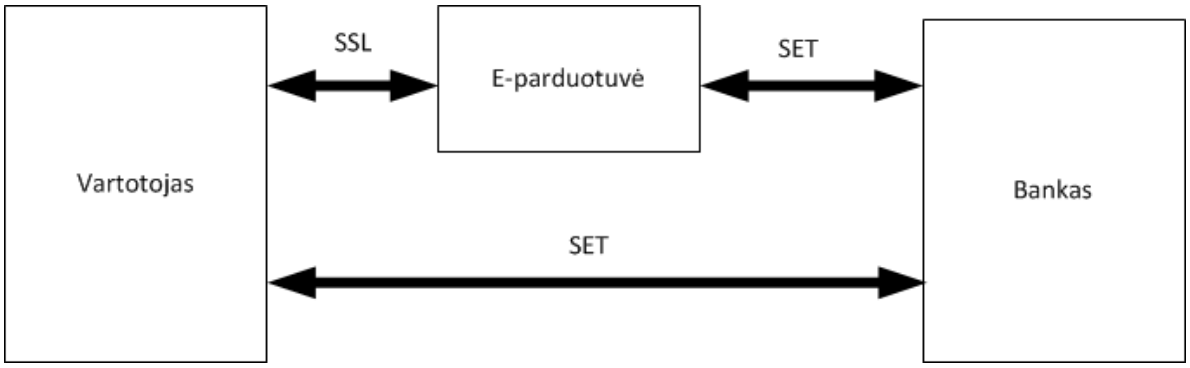
E.pinigai – tai e.dokumentai, turintys realių pinigų vertę ir pripažįstami jų vartotojų tarpusavio atsiskaitymuose. Šiuo metu naudojami dviejų tipų e.pinigai: veikiantys prijungties rėžimu (online) ir veikiantys atjungties rėžimu (offline) [9]. Elektroniai atsiskaitymai internete labai dažnai vykdomi 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 [3]. Mokėjimams atlikti naudosime SET protokolą.

Elektroninei parduotuvei yra keliami šie reikalavimai:

- Elektroninė parduotuvė skirta Windows ir Linux operacinėms sistemoms.
- Privalo būti realizuota duomenų kaupimo sritis, kurioje duomenys būtų įrašomi, trinami, redaguojami;
- Vartotojui turi būti suteikta galimybė peržiūrėti prekes, įtraukti jas į savo prekių vežimėlį, nusipirkti norimas prekes;
- Elektroninės parduotuvės priežiūrai turi būti sukurta administratoriaus sritis, kurios pagalba būtų galima įkelti naujas prekes, redaguoti informaciją apie prekes ir pan.
- Elektroninė parduotuvė turi turėti lojalumo sistemą. Lojalumo sistema turi būti sudaryta iš apsipirkimo nuolaidos, bei skelbiamų akcijų prekėms ar prekių rinkiniams.
- Lojalumo sistema turi skatinti pirkėja apsipirkti sekantį kartą.
- Elektroninėje parduotuvėje visi vykdomi pirkimai turi būti pasirašomi el,. Parašu ir pridedamas sertifikatas.

- Tarp vartotojo ir elektroninės parduotuvės naudojamas saugus SSL ryšys.
- Visi vartotojai registracijai ir prisijungimui prie elektroninės parduotuvės privalo įsidiegti papildomą programinę įrangą („epp portable“ dokumento pasirašymo programą)[15].
- Naujų vartotojų registracijos patvirtinimui neturi būti naudojamas el., paštas.
- Prisijungiant prie e-parduotuvės sistemos, nereikalingas prisijungimo vardas ir slaptažodis.

3.2.1 Elektroninės parduotuvės struktūra ir naudojami ryšio protokolai.



9. Pav., elektroninės parduotuvės struktūra ir naudojami ryšio protokolai.

Saugiųjų jungčių lygmuo (angl. SSL) – tai duomenų, perduodamų iš žiniatinklio naršyklės į žiniatinklio serverį ir atgal šifravimo technologija. Ši technologija paprastai naudojama internetinės bankininkystės ir el. prekybos svetainėse. Tam tikrose kitų svetainių dalyse taip pat gali būti naudojama SSL, pvz., įvedant prisijungimo informaciją nurodomiems slaptažodžiams apsaugoti.

Žiniatinklio adresai, apsaugoti SSL, pradedami `https:`, o ne `http:`, taigi šios sąvokos dažnai vartojamos kaip lygiavertės. Naudojant SSL užtikrinamas didesnis privatumas ir sauga negu naudojant neužšifruotą žiniatinklio ryšį. Taip sumažinama grėsmė, kad trečioji šalis perims ir netinkamai naudos informaciją. Daugelis lankytojų, bendrindami mokėjimo ir kitą asmeninę informaciją, jaučiasi saugiau, jei svetainėje naudojamas SSL ryšys.

Yra dvi SSL naudojimo sritys:

1. Užtikrinti bendravimo saugumą tarp naršyklės bei Web serverio. Įdiegtas mūsų Web serveryje skaitmeninis sertifikatas yra savotiškas elektroninis svetainės dokumentas, leidžiantis mūsų lankytojams nustatyti jos tapatumą, bei saugumą. Ši paslauga yra būtina norint atlikti bet kokias elektroninės komercijos operacijas, susijusias su apmokėjimu už prekes ir paslaugas.

2. Užtikrinti bendravimo saugumą tarp serverio ir serverio. Daugiau ir daugiau kompanijų naudoja SLL sertifikatus užtikrinant bendravimo saugumą tarp serverio ir serverio. Šiuo metu SLL sertifikatas naudojamas užtikrinti bendravimą tarp elektroniės parduotuvės serverio. Be to, yra galimybė apsaugoti ftp tinklalapius, duomenų bazes ir kt.

SET (Secure Electronic Transaction) transakcijų šifravimas

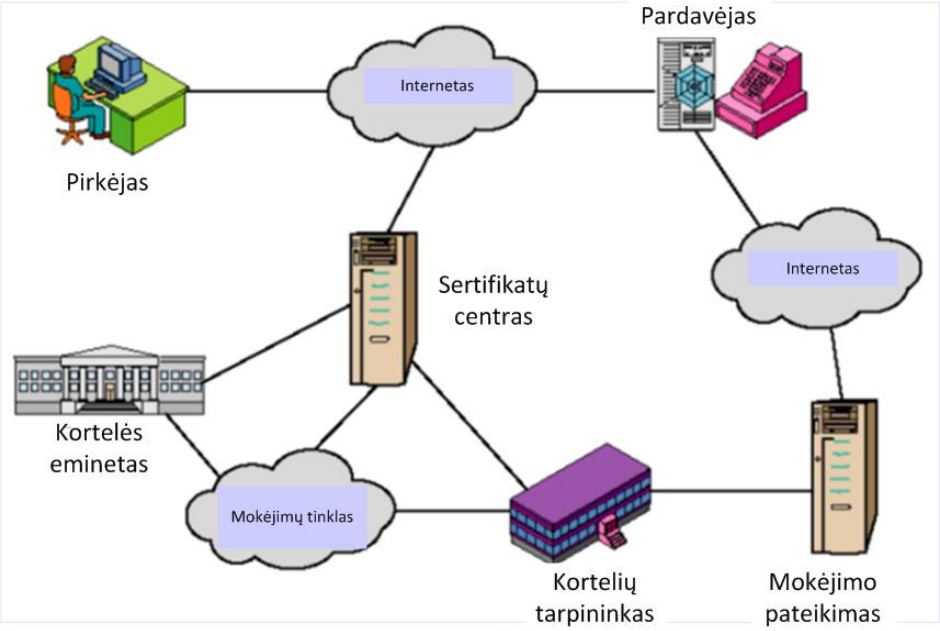
SET šifruoja mokėjimo kortelių duomenis ir užtikrina, kad abi dalyvaujančios pusės – mokėtojas ir pardavėjas – yra unikalios. Ši technologija yra dviejų kortelių gamintojų – „MasterCard“ ir VISA – bendradarbiavimo vaisius. SET laikoma patikima technologija, nes ji sertifikuota kortelių gamintojų. Siunčiant užklausą ji užkoduojama taip, kad tik bankas gali ją iššifruoti. Naudojamas dvigubas vartotojo parašas, kurį gali patikrinti tik banko įranga. Apmokestinimo informacija siunčiama pardavėjui, o kortelės ir papildoma informacija – apmokestinimo serveriui. Apmokestinimo informacija siunčiama atviru tekstu, o visa kita – šifruotai. Vien pavogtų kortelės duomenų šiuo atveju nepakaks, nes elektroninį parašą turi kortelės savininkas.

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 kreditinės kortelės numerio, jį sužino tik bankas. Konfidencialumui užtikrinti naudojamas standartinis DES šifravimo algoritmas. 16

- 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 sertifikatą 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 [3].



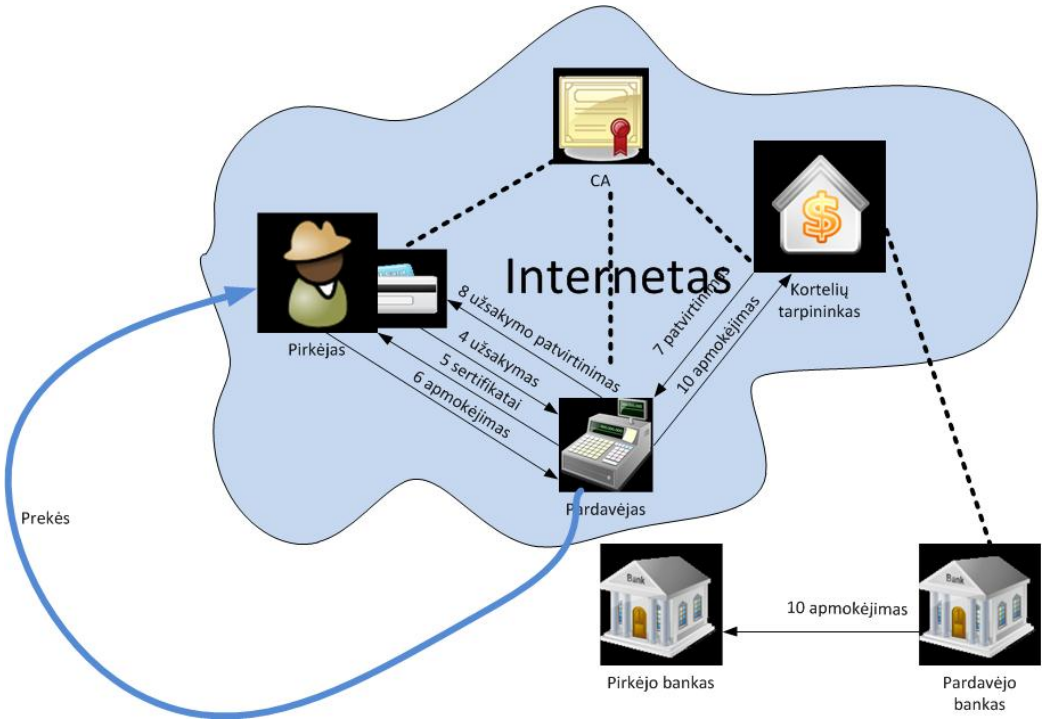
10. pav., SET atsiskaitymo protokolo schema.

1. Pirkėjas atsidaro sąskaitą. Pirkėjas įsigyja kreditinę kortelę (Visa ar MasterCard) banke, kuris palaiko SET
2. Pirkėjas gauna sertifikatą. Patikrinus tapatybę banke pirkėjas gauna X.509v3 sertifikatą (ir RSA raktų porą), pasirašytą banko. Bankas garantuoja jog sertifikatas atitinka realią kortelę
3. Pardavėjas turi reikiamus sertifikatus

Pardavėjas priimantis tam tikro tipo kortelę (Visa) turi du sertifikatus Vieną – pranešimų pasirašymui, antrą – raktų apsikeitimui. Pardavėjas turi kortelių tarpininko (acquirer payment gateway) sertifikatą su jo viešuoju raktu. (11pav. SET protokolo veikimo algoritma).

1. Pirkėjas pateikia užsakymą. Prekės krepšelyje. Pirkėjas nusiunčia krepšelį pardavėjui, kuris suformuoja ir pateikia užsakymo dokumentą (prekės, kainos, suma, užsakymo nr.)

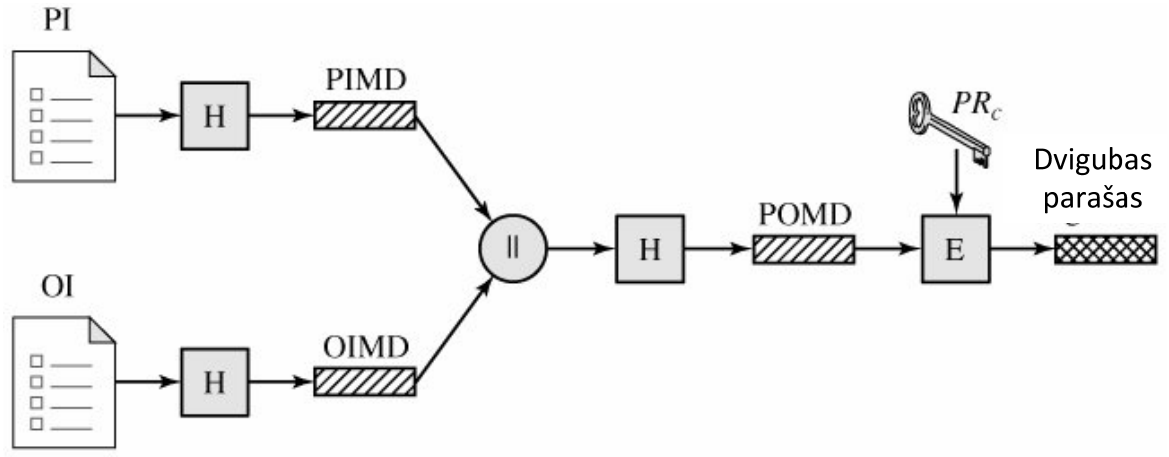
1. Autentifikuojamas pardavėjas. Pardavėjas pirkėjui papildomai atsiunčia savo sertifikatą atitinkantį pasirinktą kortelės tipą, bei kortelių tarpininko sertifikatą. Duomenis patikrina ir pasirašo spec. programa (wallet application) kuria naudojasi pirkėjas
2. Pirkėjas siunčia užsakymą ir apmokėjimą. Pirkėjas užšifruoja užsakymą, prideda apmokėjimo informaciją ir siunčia ją pardavėjui kartu su savo sertifikatu Naudojamas dvigubas parašas. Pirkėjo sertifikatas leidžia pardavėjui autentifikuoti pirkėją
3. Pardavėjas paprašo apmokėjimo patvirtinimo. Pardavėjas nusiunčia šifruotą mokėjimo informaciją kortelių tarpininkui, Kuris patvirtina (ar paneigia) jog pirkėjas turi pakankamai lėšų kortelėje apmokėti sąskaitą.
4. Pardavėjas patvirtina užsakymą. Pardavėjas nusiunčia užsakymo patvirtinimą pirkėjui
5. Pardavėjas pateikia prekes ir/ar paslaugas pirkėjui
6. Pardavėjas gauna apmokėjimą. Pardavėjas nusiunčia apmokėjimo prašymą kortelių tarpininkui (acquirer payment gateway), kuris perveda pinigus iš pirkėjo banko į pardavėjo banką



11. pav. SET protokolo veikimo algoritmas.

- Tarkime pirkėjas nusiunčia pardavėjui du atskirus pranešimus:
- Pasirašytą pirkimo užsakymą (OI)
- Pasirašytą mokėjimo informaciją (PI)
- Papildomai pirkėjas nusiunčia mokėjimo informaciją (PI) bankui

- Jei pardavėjas turi kitą užsakymą iš to paties pirkėjo, jis gali teigti jog apmokėjimo informacija skirta tam kitam užsakymui
- Būtina susieti abu pranešimus, be to
- pardavėjas neturi matyti mokėjimo informacijos,
- bankas neturi matyti užsakymo informacijos, bet turi būti galimybė įsitikinti, jog mokėjimas skirtas būtent tam užsakymui
- Apskaičiuojamas maišos (SHA-1) rezultatas pirkimo ir mokėjimo informacijai OIMD ir PIMD
- Rezultatai sujungiami [H(PI) || H(OI)] ir apskaičiuojamas rezultato maišos rezultatas POMD
- Pirkėjas užšifruoja (RSA) galutinį rezultatą savo sertifikatu (PRc) ir gaunamas dvigubas parašas DS (12pav. dvigubo parašo algoritmas).



12. pav. dvigubo parašo algoritmas

PI- mokėjimo informacija

OI- Užsakymo informacija

H- h- maišos f-ja (SHA-1)

PIMD – mokėjimo pranešimas

OIMD- užsakymo pranešimas

II – kontetanacija

POMD-mokėjimo pranešimas

E- parašo šifravimo algoritmas (RSA)

PR_c –kliento privatus raktas.

Pardavėjas

- Turi pirkėjo viešąjį raktą PUc iš jo sertifikato, turi DS
- Turi pilną OI pranešimą ir maišos rezultatą PIMD=H(PI)
- Gali apskaičiuoti:
- H(PIMD || H(OI)) ir D(PUc, DS)
- Gautos reikšmės turi būti lygios

Bankas

- Turi pirkėjo viešąjį raktą PUc iš jo sertifikato, turi DS
- Turi pilną PI pranešimą ir maišos rezultatą OIMD=H(OI)
- Gali apskaičiuoti:
- H(H(PI) || OIMS) ir D(PUc, DS)

Gautos reikšmės turi būti lygios

- Pirkėjui reikalingi pardavėjo pasirašymo ir kortelių tarpininko (acquirer gateway) raktų apsikeitimo sertifikatai
- Pirkėjas paprašo šių sertifikatų siųsdamas Initiate Request pranešimą pardavėjui
- Pranešimo turinys:
- Kortelės tipas (Visa)
- ID kurį pirkėjas priskyrė šiam apsikeitimui pranešimais (Initiate Request/Initiate Response)
- Nonce1

Pardavėjas sugeneruoja atsakymą:

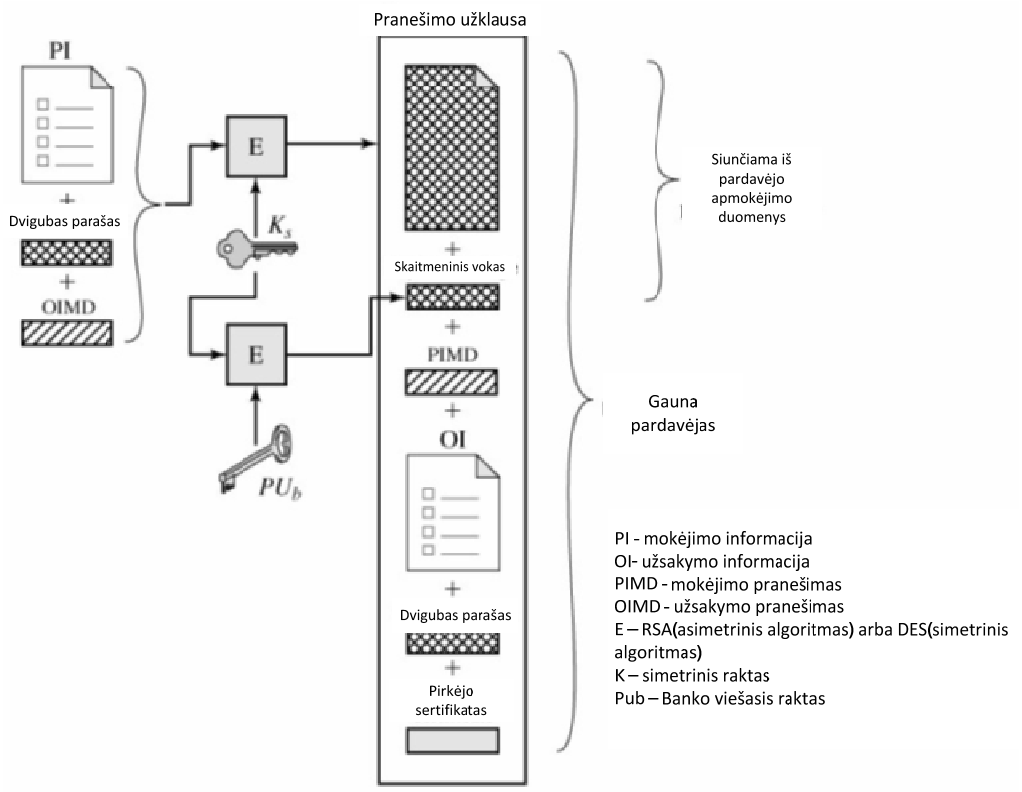
- Atsakymą pasirašo naudodamas savo sertifikatą skirtą pasirašymui
- Prideda pirkėjo Nonce1
- Prideda pardavėjo Nonce2 (Kurį pirkėjas turi grąžinti per kitą apsikeitimą pranešimais)
- Transakcijos ID, vienareikšmiškai identifikuojantį šią tranzakciją

- Papildomai prie pasirašytos dalies prideda:
- Pardavėjo sertifikatą skirtą pasirašyti
- Kortelių tarpininko (acquirer) raktų pasikeitimo sertifikatą
- Pirkėjas patikrina du sertifikatus panaudodamas CA
- Paruošia OI ir PI
- Pardavėjo priskirtas transakcijos ID pridedamas prie OI ir PI
- OI neturi visų duomenų apie užsakymą (prekių sąrašo su kainomis). Jis turi tik užsakymo numerį, kurį sugeneravo pardavėjas prieš tai buvusiose tranzakcijos fazėse
- Sukuria Purchase Request pranešimą:
- Sugeneruoja vienkartinį simetrinį raktą Ks
- Apmokėjimo informacija
- PI, DS, OIMD. Viskas užšifruojama Ks.

Skaitmeninis vokas (angl. digital envelope), kuris gaunamas Ks užšifruojant kortelių tarpininko (acquirer gateway) raktų apsikeitimo sertifikatu.

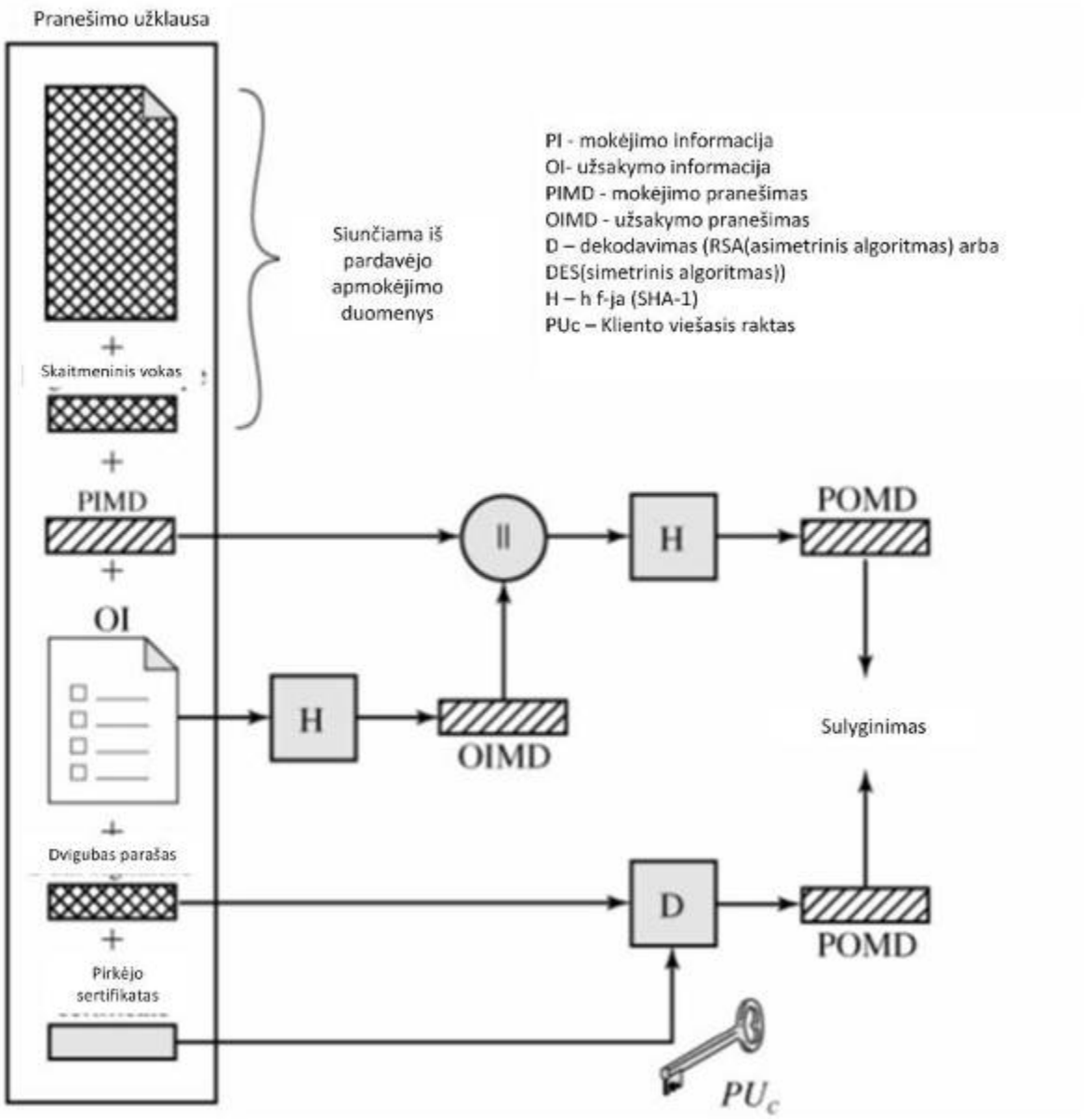
Užsakymo informacija(13pav. Užsakymo užklausos formavimas.***)***

- OI, DS, PIMD
- Pirkėjo sertifikatas



13. pav. Užsakymo užklausos formavimas.

- Patikrina pirkėjo sertifikatą CA
- Patikrina DS naudodamas pirkėjo sertifikatą. Tai užtikrina jog užsakymas nebuvo pakeistas persiuntimo metu ir jį tikrai pasirašė pirkėjas
- Persiunčia apmokėjimo informaciją kortelių tarpininkui (acquirer gateway) apmokėjimo patvirtinimui
- Po patvirtinimo (įvykdęs Payment Authorization tranzakciją) siunčia Purchase response pranešimą pirkėjui



14. pav. Pardavėjas patikrina pirkimo užklausą algoritmas.

- Atsakymo blokas, kuris patvirtina užsakymą, turi nuorodą į atitinkamą transakcijos ID
- Šis blokas Pasirašomas pardavėjo sertifikatu
- Blokas ir parašas siunčiamas pirkėjui kartu su pardavėjo pasirašymo sertifikatu
- Pirkėjo programa (wallet) gavusi pranešimą:
- Patikrina pardavėjo sertifikatą
- Patikrina parašą ir atsakymo bloką
- Imasi atitinkamų veiksmų (parodo pranešimą ekrane)

- Pardavėjas patikrina apmokėjimo galimumą siųsdamas (14pav. Pardavėjas patikrina pirkimo užklausą algoritmas.) Authorization Request pranešimą kortelių tarpininkui (acquirer payment gateway):
- Su Pirkimu susieta informacija (gauta iš pirkėjo)
- PI, OIMD
- Dvigubas parašas DS.
- Pirkėjo skaitmeninis vokas (digital envelope)
- Pardavėjo suformuota mokėjimo tikrinimo informacija:
- Blokas su transakcijos ID, pasirašytas pardavėjo pasirašymo privačiuoju raktu ir užšifruotas pardavėjo sugeneruotu vienkartiniu simetriniu raktu Km
- Skaitmeninis vokas. Vienkartinis simetrinis raktas Km užšifruotas kortelių tarpininko (acquirer gateway) raktų pasikeitimo viešuoju raktu
- Sertifikatai
- Pirkėjo pasirašymo, pardavėjo pasirašymo ir pardavėjo raktų pasikeitimo sertifikatai

Kortelių tarpininkas :

- Patikrina visus gautus sertifikatus CA
- Išsišifruoja mokėjimo tikrinimo informacijos bloką. Pirma sužino simetrinį raktą Km, po to ir visą informaciją
- Patikrina pardavėjo parašą
- Išsišifruoja PI. Pirma išsišifruoja voką, suranda simetrinį raktą Ks, o po to ir visą apmokėjimo informaciją
- Patikrina PI dvigubą parašą
- Patikrina ar pardavėjo tranzakcijos ID sutampa su pirkėjo nurodyta informacija
- Paprašo ir gauna apmokėjimo patikrinimo informaciją iš kortelę išdavusios finansinės institucijos

Patikrinęs apmokėjimo galimybę kortelių tarpininkas siunčia pardavėjui Authorization Response pranešimą:

Patvirtinimo informacija (atsakymas).

- Patvirtinimo rezultatų blokas, pasirašytas tarpininko pasirašymo sertifikatu ir užšifruotas vienkartiniu simetriniu raktu Kg, kurį sugeneruoja tarpininkas
- Skaitmeninis vokas, kuriame Kg raktas užšifruotas pardavėjo raktų apsikeitimo sertifikatu Capture Token
- Naudojamas vėlesnėse transakcijose, realiam pinigų pervedimui. Turi būti grąžinamas nepakeistas.
- Kortelių tarpininko pasirašymo sertifikatas

Paprasčiausia pirkimo transakcija reikalauja:

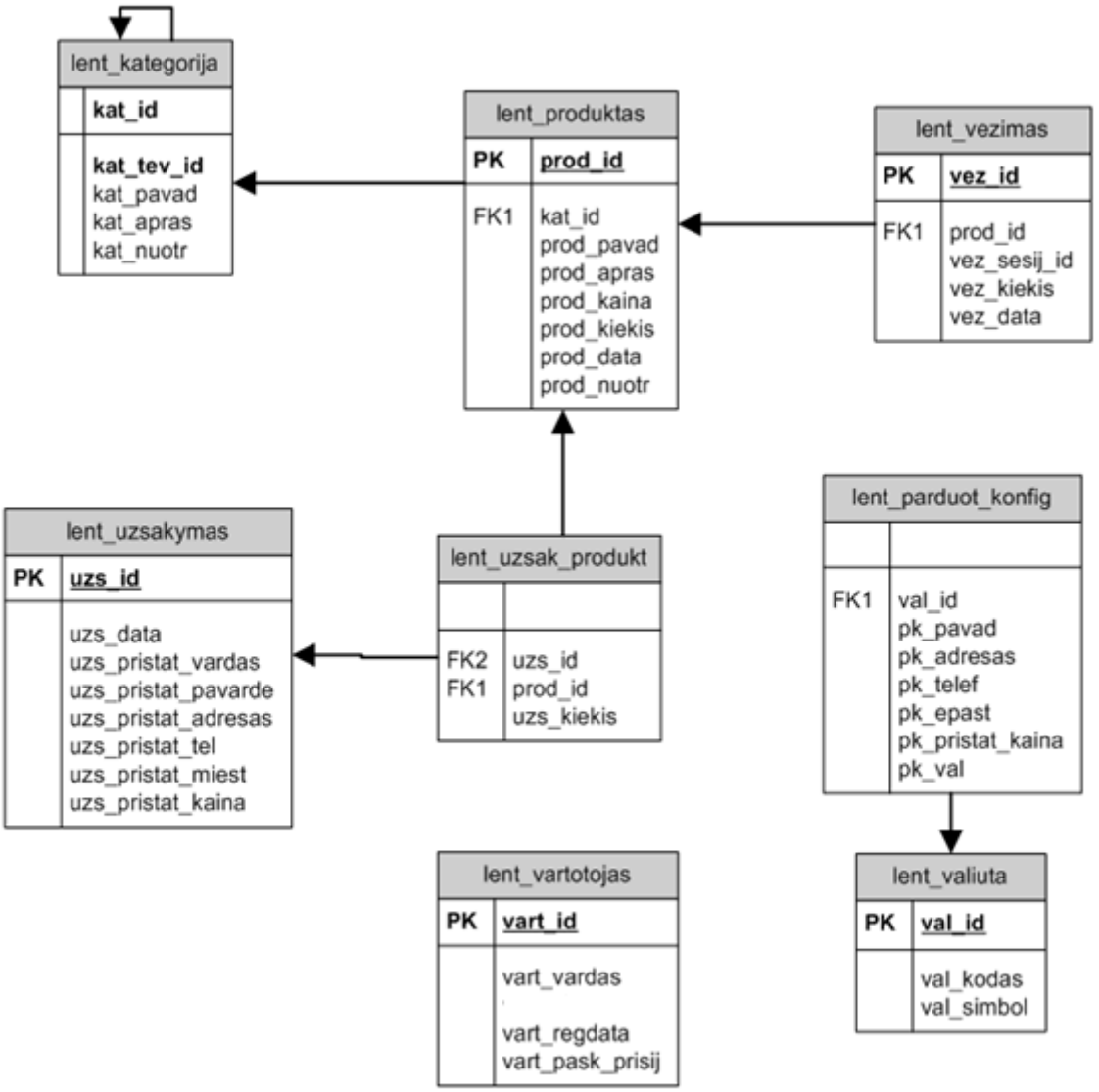
- Keturių pranešimų tarp pirkėjo ir pardavėjo.
- Du pranešimai tarp pardavėjo ir kortelių tarpininko.
- 6 skaitmeniniai parašai.
- 9 RSA užšifravimo/iššifravimo ciklai.
- 4 DES užšifravimo/iššifravimo ciklai.
- 4 sertifikatų patikrinimai.
- Naudojama skaitmeninio voko technika.
- Raktas generuojamas vienašališkai.
- Naudoja SHA-1 160 bitų santraukas.
- Autentifikavimui naudoja skaitmeninius sertifikatus.
- Kiekviena šalis turi po du sertifikatus, pasirašymui ir raktų apsikeitimui.
- Statistiškai globaliai unikalius ID.
- Dvigubas parašas.

SET trūkumai

- Sudėtinga schema, daug šalių.
- Geriausiai tenkina kortelių institucijas, nes sutaupo jiems pinigus.
- Lėtas, tranzakcijos trunka iki 50 sek.
- Neportabilus.
- Reikia sertifikatų bei spec. programos (SET wallet) pirkėjo kompiuteryje.

- Nepakankamai saugus (Sertifikatai saugomi pirkėjo kompiuteryje).
- Nepopuliarus tarp pardavėjų.

3.2 Projektuojamos sistemos duomenų bazės lentelių struktūra.



15. pav. duomenų bazės modelis

Trumpai apžvelgsime kokie duomenys saugomi lentelėse. (15pav. duomenų bazės modelis).

1. Lentelė.Kkategorija

Lentelės pavadinimas	Aprašymas
lent_kategorija	Visos kategorijos ir su jomis susiję duomenys.
lent_uzsakymas	Informaciją apie užsakymas, kurį padarė vartotojas.
lent_produktas	Produktai ir su jais susijusi informacija.
lent_vezimas	Kai vartotojas įsideda prekę į vežimėlį, duomenys saugomi šioje lentelėje.
lent_uzsak_produkt	Saugomi užsakyti produktai.
lent_vartotojas	Parduotuvės administratoriaus prisijungimo duomenys.
lent_parduot_konfig	Parduotuvės nustatymų duomenys.
lent_valiuta	Valiutos sąrašas.

Toliau smulkiau aptarsime kiekvienoje lentelėje saugomus duomenis:

Šioje lentelėje saugoma informacija apie kategorijas. Mūsų prekės saugomos pirmo lygio kategorijose (t.y. Kategorija1->Prekė1), tačiau galimas ir gilesnis kategorijų lygis (Kategorija1->Kategorija1.1->..->Kategorija1.x.x.x->Prekė1). Lentelėje saugomi tokie duomenys:

- kat_id – tai unikalus kiekvienos kategorijos ID;
- kat_tev_id – tai yra tėvinės kategorijos ID, kai naudojamas gilesnis kategorijų lygis;
- kat_pavad – kategorijos pavadinimas, matomas parduotuvėje;
- kat_apras – kategorijos aprašymas;
- kat_nuotr – nuotrauka, iliustruojanti kategoriją.

2. Lentelė. Užsakymas

kat_id	kat_tev_id	kat_pavad	kat_apras	kat_nuotr
21	0	Spausdintuvai	Lazeriniai spausdintuvai	printer.jpg
20	0	Nešiojami kompiuteriai	Kompaktiški ir galingi kompiuteriai	nesiojami.jpeg
19	0	Staliniai kompiuteriai	Pilnos komplektacijos stacionarūs kompiuteriai	stacionarus.jpeg
24	0	Monitoriai	Dideli monitoriai Jums	monitors.jpeg
25	0	Kietieji diskai	Įvairūs kietieji diskai	hdd.jpeg
26	0	Procesoriai	Jūsų kompiuterio "jėga"	cpu.jpeg
27	0	Atmintis	Atminties komponentai	atmintis.jpeg

Vartotojui išsirinkus prekių ir atlikus užsakymą, informacija saugoma šioje lentelėje:

- uzs_id – užsakymo ID;
- uzs_data – data, kada buvo atliktas užsakymas;
- uzs_pristat_vardas – užsakovo vardas;
- uzs_pristat_pavarde – užsakovo pavardė;
- uzs_pristat_adresas – adresas, kuriuo bus pristatytos prekės;
- uzs_pristat_tel – užsakovo telefono numeris;
- uzs_pristat_miest – miestas į kurį bus pristatyta prekė;
- uzs_pristat_salis – valstybė į kurią bus pristatyta prekė;
- uzs_pristat_kaina – užsakymo kaina.

lent_produktas

Saugomi visi produktai. Vienas produktas gali turėti vieną didelę nuotrauką bei vieną mažytę nuotrauką (thumbnail). Lentelėje yra tokie laukai:

- prod_id – produkto ID (kiekvieno unikalus);
- kat_id – kategorijas, kuriai priklauso produktas ID;
- prod_pavad – produkto pavadinimas;
- prod_apras – produkto aprašymas;
- prod_kaina – produkto kaina;
- prod_kiekis – koks kiekis produktų yra prekyboje;
- prod_data – produkto patalpinimo data;
- prod_nuotr – produkto nuotrauka.

3. Lentelė. Produktas

prod_id	kat_id	prod_pavad	prod_apras	prod_kaina	prod_kiekis	prod_data	prod_nuotr
30	27	DDR2	pTekstas1	485,00		Data1	atmintis3a.jpg
9	7	DDR	Tekstas2	19,00	3	ata2	atmintis2a.jpg
8	7	DIMM	Tekstas3	25,00	5	ata3	atmintis1a.jpg
32	25	HDD1	Tekstas4	259,00	9	Data4	hdd1a.jpg
33	25	HDD2	Tekstas5	584,00	3	Data5	hdd2a.jpg
34	25	HDD3	Tekstas6	859,00	0	Data6	hdd3a.jpg
35	24	LCD	Tekstas7	1845,00	2	Data7	monit1a.jpg
36	24	LCD	Tekstas8	1025,00	5	Data8	monit2a.jpg
37	20	IBM	Tekstas9	5897,00	2	Data9	lapt1a.jpg
38	20	Mac Book	Tekstas10	6874,00	2	Data10	lapt2a.jpg

prod_id	kat_id	prod_pavad	prod_apras	prod_kaina	prod_kiekis	prod_data	prod_nuotr
39	20	Vaio	Tekstas11	5421,00	1	Data11	lapt3a.jpg
40	26	Intel	Tekstas12	450,00	2	Data12	cpu1a.jpg
41	26	Intel	Tekstas13	256,00	1	Data13	cpu2a.jpg
42	26	AMD	Tekstas14	358,00	2	Data14	cpu3a.jpg
43	26	AMD	Tekstas15	400,00	4	Data15	cpu4a.jpg
44	19	IBM	Tekstas16	4521,00	3	Data16	pc1a.jpg
45	19	iMac	Tekstas17	7999,00	1	Data17	pc2a.jpg
46	21	Lazerinis spausdintuvas	Tekstas18	452,00	5	Data18	print1a.jpg
47	21	Daugiafunkcinis aparatas	Tekstas19	875,00	3	Data19	print2a.jpg

lent_vezimas

Saugomi duomenys apie produktus, kuriuos pirkėjas įsideda į pirkinių vežimą:

- vez_id – prekių vežimėlio ID;
- prod_id – prekių ID, kurias įsidėjęs pirkėjas;
- vez_kiekis – išsirinktų prekių kiekis;
- vez_data – įdėjimo į prekių vežimą data.

lent_uzsak_produkt

Visi užsakyti produktai saugomi šioje lentelė.

- uzs_id – užsakymo ID;
- prod_id – užsakyto produkto ID;
- uzs_kiekis – užsakymų kiekis;

lent_vartotojas

Saugomi duomenys prisijungimui prie administratoriaus srities. Ateityje galima būtų modifikuoti parduotuvę, kad tik užsiregistravę vartotojai galėtų apsipirkinėti. Šioje lentelėje yra tokie laukai:

- vart_id – užsiregistravusio vartotojo ID;
- vart_vardas – užsiregistravusio vartotojo prisijungimo vardas (pseudonims);
- vart_regdata – registracijos data;
- vart_pask_prisij – informacija apie paskutinį prisijungimą.

4. Lentelė. Vartotojas

vart_id	vart_vardas	vart_regdata	vart_pask_prisij
1	Ešalonas	2012 03 02 17:32:15	2012 05 23 20:34:41

5 lentelė parduot_konfig

Saugoma informaciją apie parduotuvę. Visa konfigūracija prieinama iš parduotuvės administratoriaus srities:

- pk_pavad – parduotuvės pavadinimas;
- pk_adresas – parduotuvės adresas;
- pk_telef – parduotuvės telefonas;
- pk_epast – parduotuvės elektroninis paštas;
- pk_pristat_kaina – pristatymo kaina;
- pk_val – valiutos sąrašas;

Lentelėje saugomi duomenys:

5. lentelė. Parduot_konfig

pk_pavad	pk_adresas	pk_telef	pk_epast	pk_pristat_kaina	pk_val
TR E-parduotuvė	Interneto platybės	123456	anonimas@gmail.com	5,00	3

pk_val reikšmė 3 reiškia, jog pasirinkta valiuta, kurios ID – 3, tai yra Lietuvo s Litas.

lent_valiuta

Saugomas sąrašas valiutos, kuria galima atsiskaityti parduotuvėje.

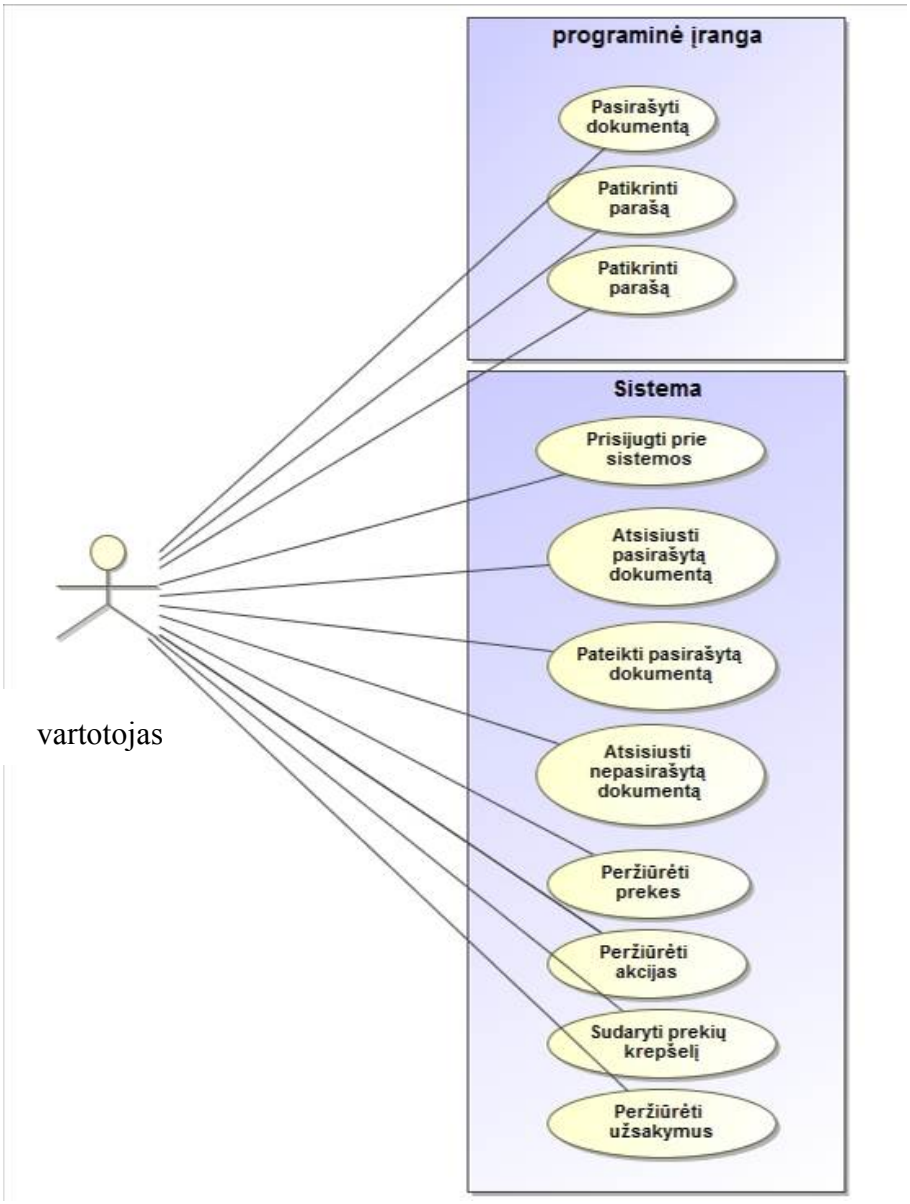
- val_id – valiutos ID;
- val_kodas – valiutos kodas (pvz. LTL);
- val_simbol – valiutos simbolis (pvz. €).

6. Lentelė. Lent_valiuta

val_id	val_kodas	val_simbol
1	EUR	€
3	LTL	lt

val_simbol reikšmė € yra – Euro simbolis (€).

3.4.2.4 Vartotojo panaudojimo atvejų diagrama



16. pav. Vartotojų panaudojimo atvejų diagrama.

Vartotojų panaudojimo atvejų diagrama parodo, kokie veiksmai atliekami vartotojo atžvilgiu. Pirmiausiai yra pasirašomas dokumentas ir patikrinamas parašas. Dokumento pasirašymas ir parašo patikrinimas atliekamas pasinaudojus papildoma progrmine įrangą vartotojo kompiuteryje („epp portable“ pasirašymo programa). Likę atvejai tai prisijungimas prie sistemos, pasirašyto dokumento pateikimas, prekių peržiūra, užsakymo paruošimas, užsakymų peržiūra, užsakymo pateikimas.

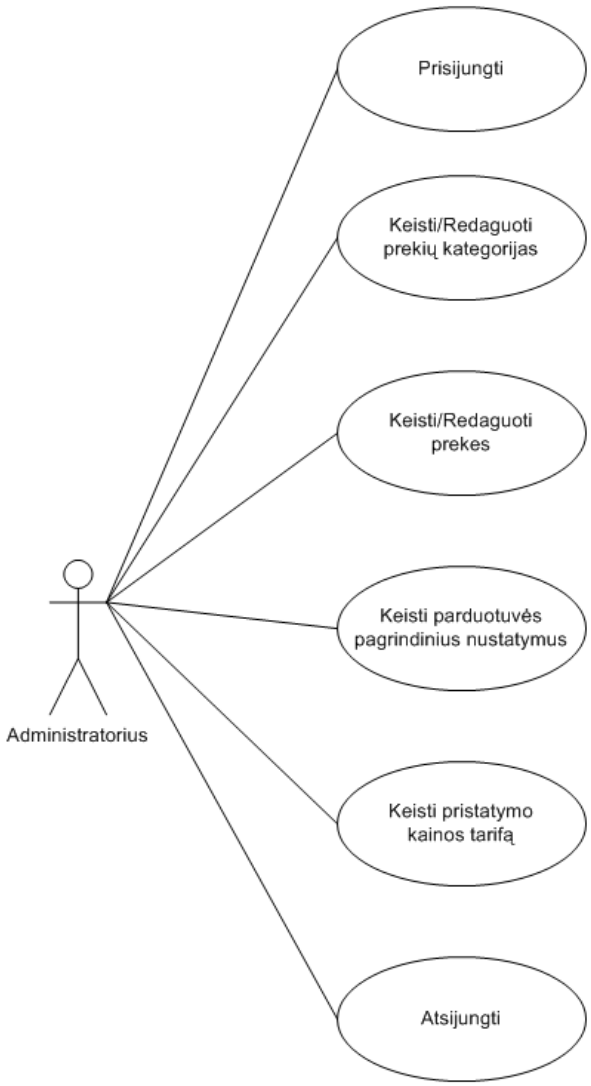
3.4.2.1 Pirkėjo funkcijos

Pirkėjas apsilankęs elektroninėje parduotuvėje gali pasirinkti prekių kategoriją. Pasirinkęs prekę ją gali įkelti į savo prekių vežimėlį;

- Gali peržiūrėti prekių vežimėlio turinį, pašalinti norimas prekes arba atnaujinti kiekį;
- Pirkėjas atsiskaito už prekes užpildydamas pristatymo formą. Ją užpildžius prašoma patvirtinti užsakymą.

3.4.2.2 Administratoriaus funkcijos

Administratoriaus atliekamos funkcijos yra pateiktos žemiau esančiame panaudos atvejų (angl. Use-case) diagramoje:



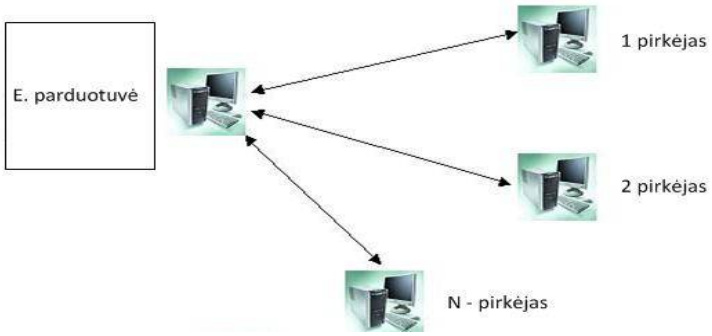
17. pav. Administratoriaus f-jų PA

3.3 Lojalumo sistema.

3.3.1 E-parduotuvės lojalumo sistemos f-jos

- Lojalumo sistema skirta pritraukti pirkėjus juos skatinti apsipirkti sekantį kartą.
- Lojalumo sistema turi suteikti pirkėjams nuolaidas, bei siūlyti įsigyti akcijos prekes.
- Sistema apima net tik nuolaidų taikymą, bet ir pirkėjo perkamo krepšelio didinimą (akcijų modulis)

Sistema skatina nuolatini apsipirkimą (pav., spausdinamas dovanų kuponas sekančiam apsipirkimui.



18. pav. E-parduotuvės lojalumo sistemos schema.

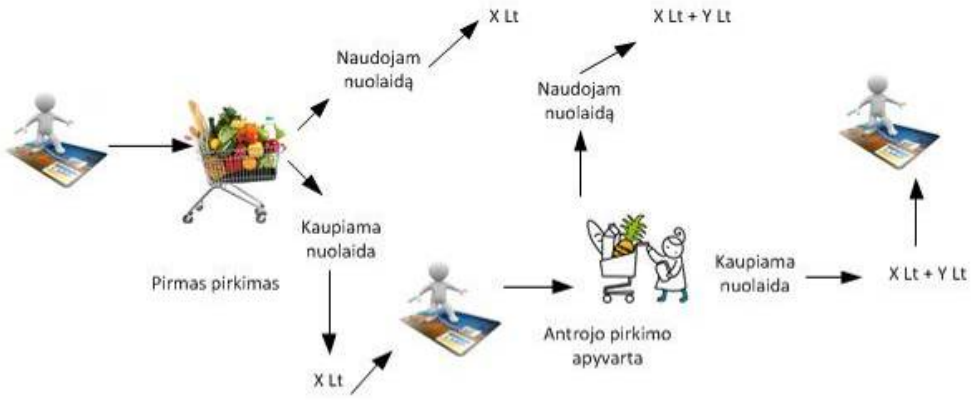
- Įvedami pirkėjų duomenys (17 pav.)
- Suteikiama bazinė nuolaida
- Lojalumo sistemos valdymas
- Lojalumo ataskaitų gavimas

19. pav. Nuolaidos steikimo pirkėjui schema.

- Standartinė nuolaida priskiriama pirkėjui (18 pav.). Kiekvieną kartą taikoma e. apsipirkimo sumai.

20. pav. Bazinės nuolaidos taikymas pasiekus apyvartą Y.

- X – bazinė nuolaida, pasiekus apyvartą Y (19 pav.) klientui taikoma nuolaida – Z



21. pav. Galimybė pasirinkti ar naudoti nuolaidą ar ją toliau kaupti

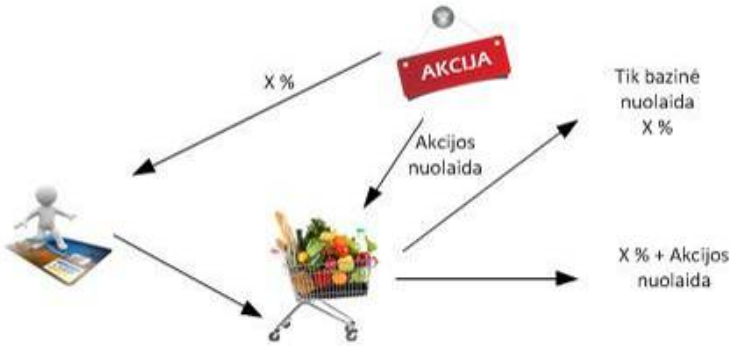
- Apsiperkant už tam tikrą sumą (21 pav. Galimybė pasirinkti ar naudoti nuolaidą ar ją toliau kaupti) pirkėjas gali pasirinki ar toliau kaupti nuolaidą, ar ją pasinaudoti iš karto.

3.3.2 E-parduotuvės lojalumo sistemos akcijų modulis.

Lojalumo sistemos akcijų modulis skirtas ne tik suteikti pirkėjams geras nuolaidas, bet ir padidinti jų pirkimo krepšelių turinį.

Čia yra teikiami įvairūs pasiūlymai sumuojamos akcijos nuolaidos ir siūloma įsigyti papildomas prekes už patrauklią kainą. Akcijų modulyje galima pasirinkti kam bus taikomos akcijos:

- Tik lojaliems klientams.
- Visiems klientams.

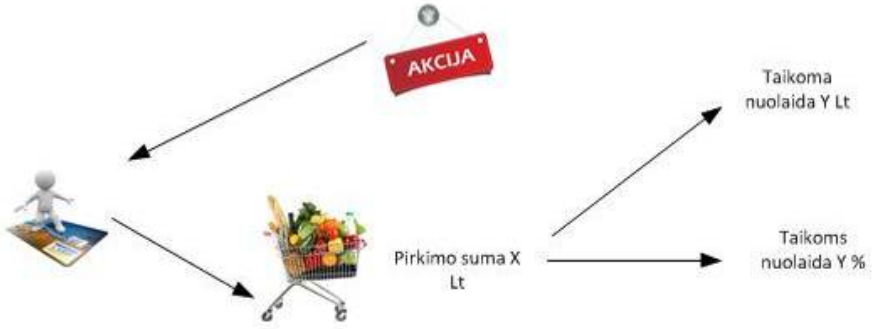


22. pav. Lojalumos sistemos akcijų modulis.

Pasirenkame ar lojalaus kliento nuolaidą sumuosime su akcijos metu teikiamomis nuolaidomis (21 pav.).

Nustatomas E. Parduotuvėje akcijos laikotarpis

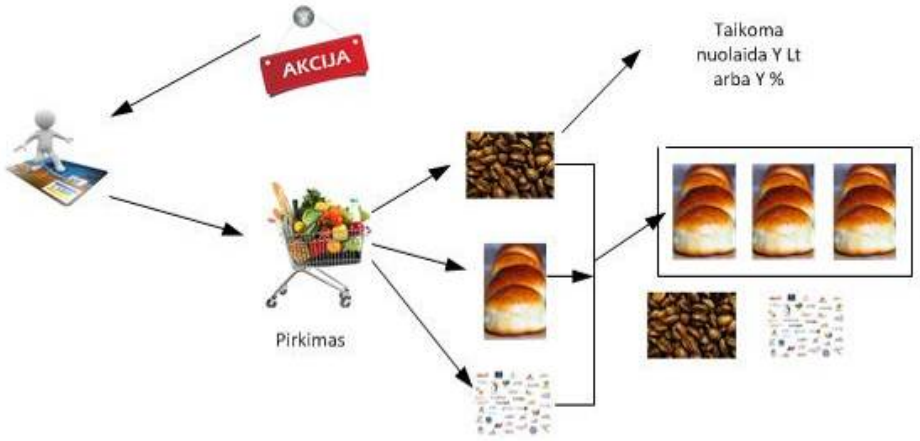
- Akcija taikoma yyyy mm dd – yyyy mm dd
- Nustatomos akcijos savaitės dienos P, A, T, K, P, Š, S.
- Nustatoma akcijos laikas valandomis hh:ss – hh:ss



23. pav. Pasirinkimas kokią nuolaidą taikyti.

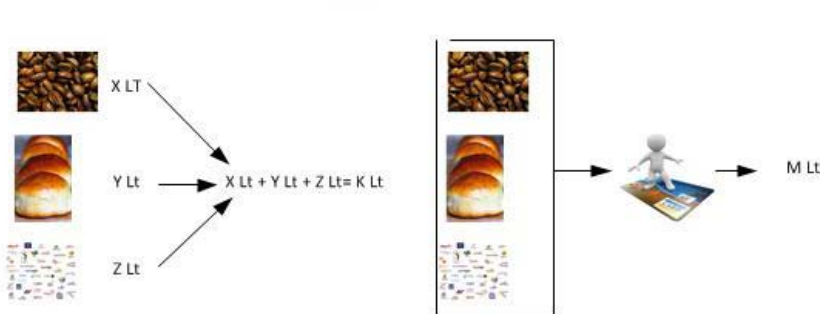
Galimybė pasirinkti kokia nuolaidą taikyti (22 pav.):

- Taikoma procentinė nuolaida Y % .
- Taikoma nuolaida sumai Y Lt.



24. pav. Taikomos procentinės arba suminės nuolaidos.

- Taikoma procentinė arba suminė nuolaida prekių komplektui arba atitinkamas prekių kiekis iš komplekto (23 pav).



25. pav. Fiksuotos kainos prekių pasirinkimas.

- Taikyti fiksuota kaina prekei iš komplekto (24 pav)
- Perkant komplektą gauti prekę iš komplekto pasirinktinai, nesvarbu ar tai brangiausia prekė ar pigiausia.

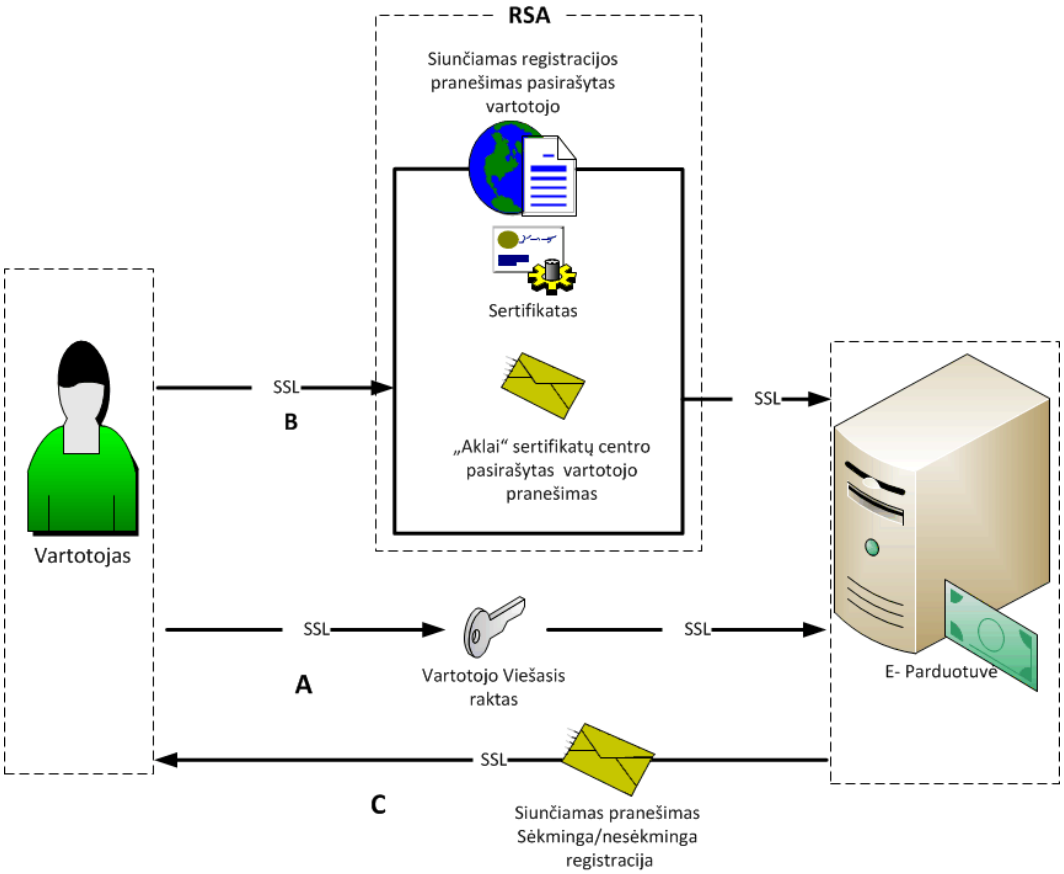
Informacijos apdorojimas ir pateikimas pardavėjui:

- Pirkimų dažnumas
- Pirkimų suma.
- Regionas iš kurio buvo perkama.
- Pirkėjo dažniausiai perkamos prekės.
- Informacijos teikimas pirkėjams El. Paštu.

3.4.1 Kriptografiškai saugios registracijos prie e-parduotuvės sistemos modelis.

Visi vartotojai, norintys prisiregistruoti sistemoje turi sėkmingai įvykdyti registracijos procedūrą. Tai atliekama vartotojui jungiantis saugiu prisijungimu naudojant SSL atsidarius registracijos puslapį ir pasirinkus registracija. Sistema paprašo vartotojo įkelti vartotojo viešąjį raktą (25 pav. A dalis). Vartotojas perduoda sistemai savo viešąjį raktą kuris jam yra įrašytas sertifikatų centre. Po sėkmingo rakto perdavimo sistema paprašo vartotoją perduoti sertifikatų centro pasirašytą vartotojo pranešimą ir sertifikatų centro sertifikatą (25 pav. B dalis). E-parduotuvės sistema patikrina vartotojo turimą sertifikatų centro sertifikatą, perduotą vartotojo pranešimą, panaudodama viešąjį sertifikatų centro raktą. Jeigu visi duomenys teisingi tuomet registruojamas vartotojas sistemoje, o vartotojui siunčiamas pranešimas apie sėkmingą registraciją. Jei duomenyse randama neatitikimų, vartotojas apie tai yra įspėjamas siunčiant vartotojui pranešimą (25pav. C dalis).

Kaip matome registracijos metu nėra naudojami jokie papildomi slaptažodžiai ir jokių slaptažodžių, bei vartotojo vardų jungiantis prie sistemos prisiminti nereikės.

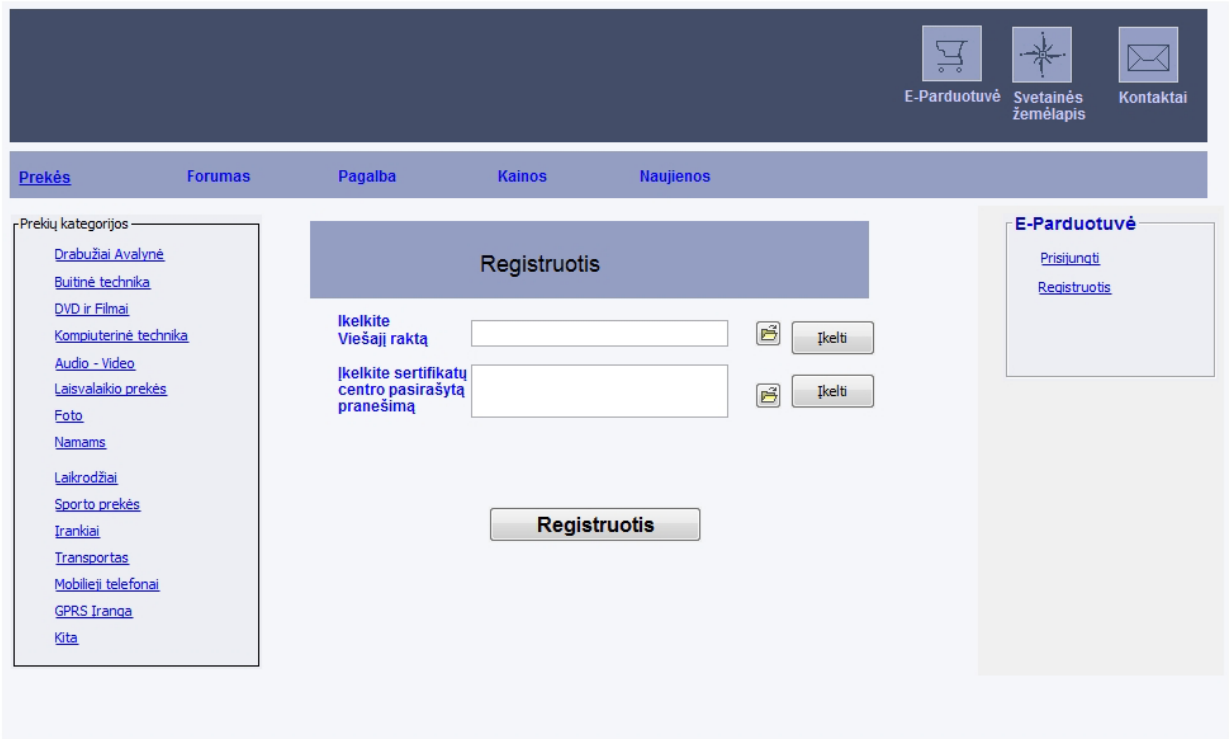


26. Pav., vartotojo registracija e-parduotuvės sistemoje.

Vartotojui pradedant registracija pirmiausiai yra nustatomas saugus SSL ryšio kanalas. Vartotojas saugiu ryšio kanalu jungiasi prie e-parduotuvės sistemos. Pirmajai registracijai e-parduotuvės sistemoje vartotojas privalo turėti sertifikatų centro pasirašytą pranešimą, sertifikatą,, bei savo viešąjį raktą, kuris jam buvo išduotas sertifikatų centre kartu su visais prieš tai išvardintais duomenimis (25 pav.).

Vartotojui skirtingai, nei šiuo metu paplitusiose e-komercijos sistemose yra atveriama registracijos forma*, kurioje nereikalaujama įvesti prisijungimo vardo, slaptažodžio. Neprašoma vartotojo kartoti slaptažodį n kartų, įvedinėti įvairias apsaugos frazes iš piešinėlių ir t.t. (26 pav.)*

Tai pat ši sistema yra apsaugota nuo neteisėtos registracijos, kurios paskirtis būna platinti netinkamo pobūdžio informacija, bei daryti žalą tretiesiems asmenims.

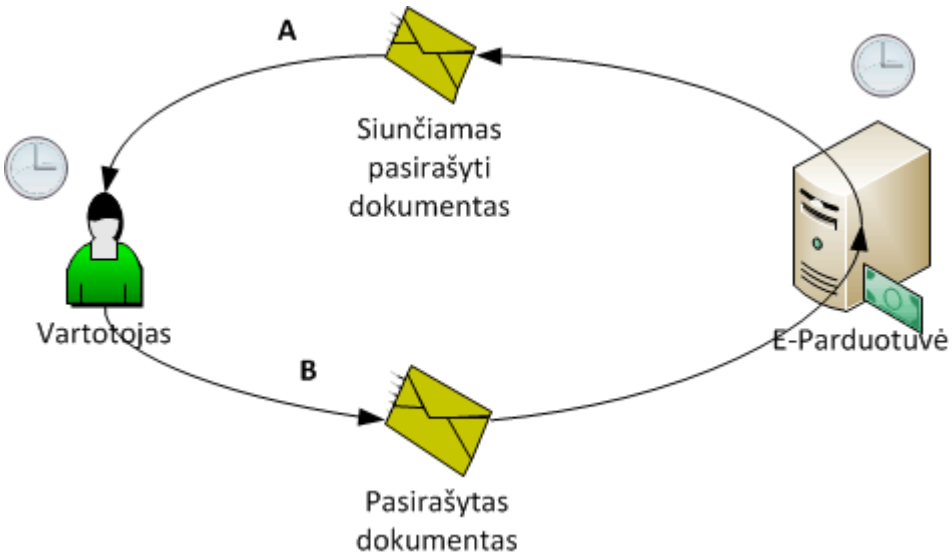


27. pav. E-parduotuvės registracijos forma.

3.4.2 Kriptografinis identifikacijos ir autentifikacijos 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. 27 A dalis). Vartotojas turi 12 minučių suformuota failą pasirašyti ir vėl grąžinti sistemai (pav. 27

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 pranešimo informaciją ir vartotojui suteikiamas priėjimas prie sistemos. Vienas iš pagrindinių tokio identifikavimo ir autentifikavimo metodo privalumų yra tai, kad vartotojui nereikia žinoti jokio papildomo prisijungimo vardo ir atsiminti dar vieno slaptažodžio.



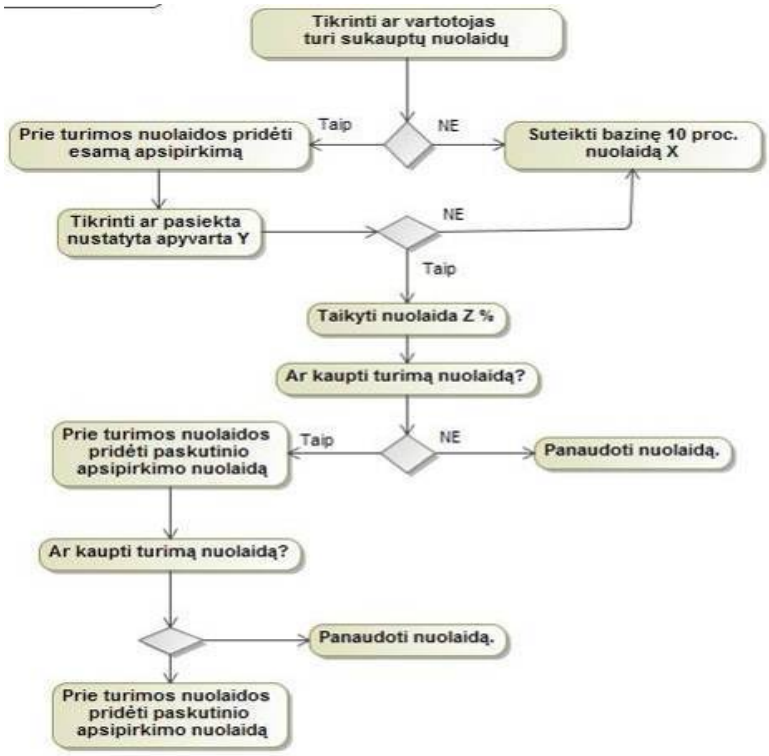
28. pav. Identifikacijos ir autentifikacijos schema.

Siūlomame indentifikacijos modelyje nėra siunčiami prisijungimo duomenys atviru tekstu į el.paštą. Taip pat nereikalingas slaptažodžio priminimas jį pamiršus, tai kas yra dažniausiai darom šiuo metu esamose sistemose. Vartotojas šiame modelyje turi pilną anonimiškumą, nes sertifikatu centras pasirašo aklai jo sugeneruota pranešima kuriame jis turi galimybę nenurodyti savo tapatybės, o pasirinkti savo susikurta slapyvardį. Lojalumo sistema vartotoją identifikuos pagal slapyvardį ir jam teiks visus lojalumo pasiūlymus ir akcijas.

29. Pav., e-parduotuvės prisijungimo forma

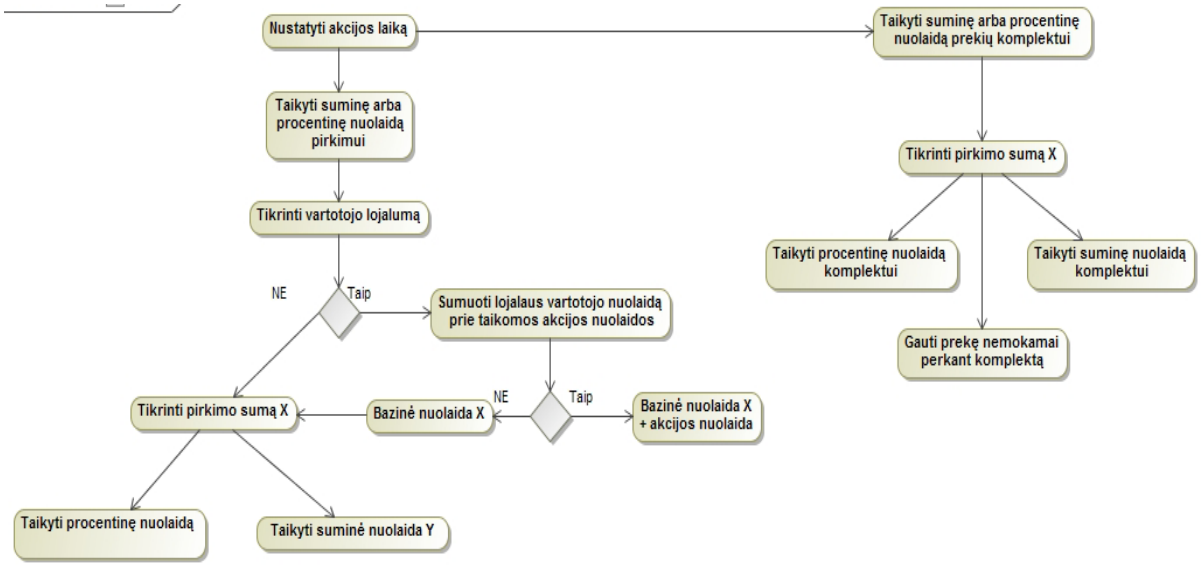
3.4.2.3 E-parduotuvės lojalumo sistemos veikimo algoritmas.

Lojalumo sistema skirta pritraukti vartotojus. Apžvelgsime siūlomos lojalumo sistemos algoritmą. Lojalumo sistemos paskirtis skatinti vartotojo pirkimus. Siūloma lojalumo sistema suteikia vartotojui pasirinkimo galimybę. Vartotojas gali rinkti, ar už įsigytas prekes e-parduotuvėje gautus lojalumo taškus toliau kaupti ar juos išleisti esamo pirkimo metu. Taip pat lojalumo sistema leidžia keisti siūlomų nuolaidų dydį vartotojui.



30. pav. Lojalumo sistemos veikimo algoritmas.

Akcijų modulis skirtas didinti vartotojų krepšelio turinį, siūlant įsigyti papildomai įvairias prekes, bei prekių rinkinius už patrauklią kainą vartotojui.



31. Pav., Akcijų modulio veikimo algoritmas.

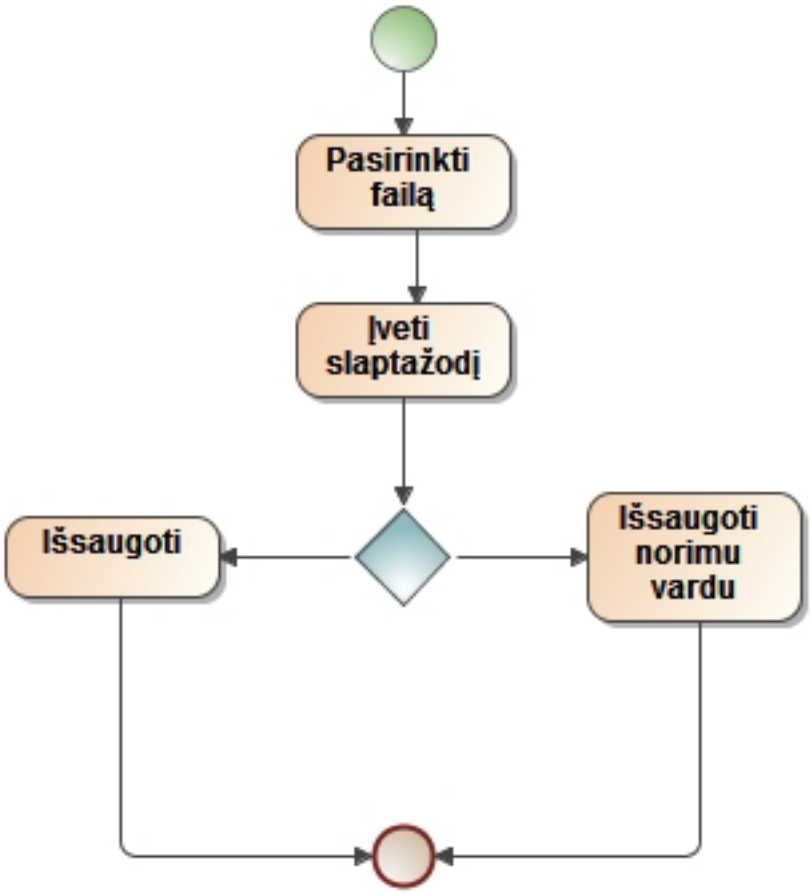
3.4.3 Veiklos diagramos panaudojimo atvejam

3.4.3.1 Prisijungimo prie sistemos

32. 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.

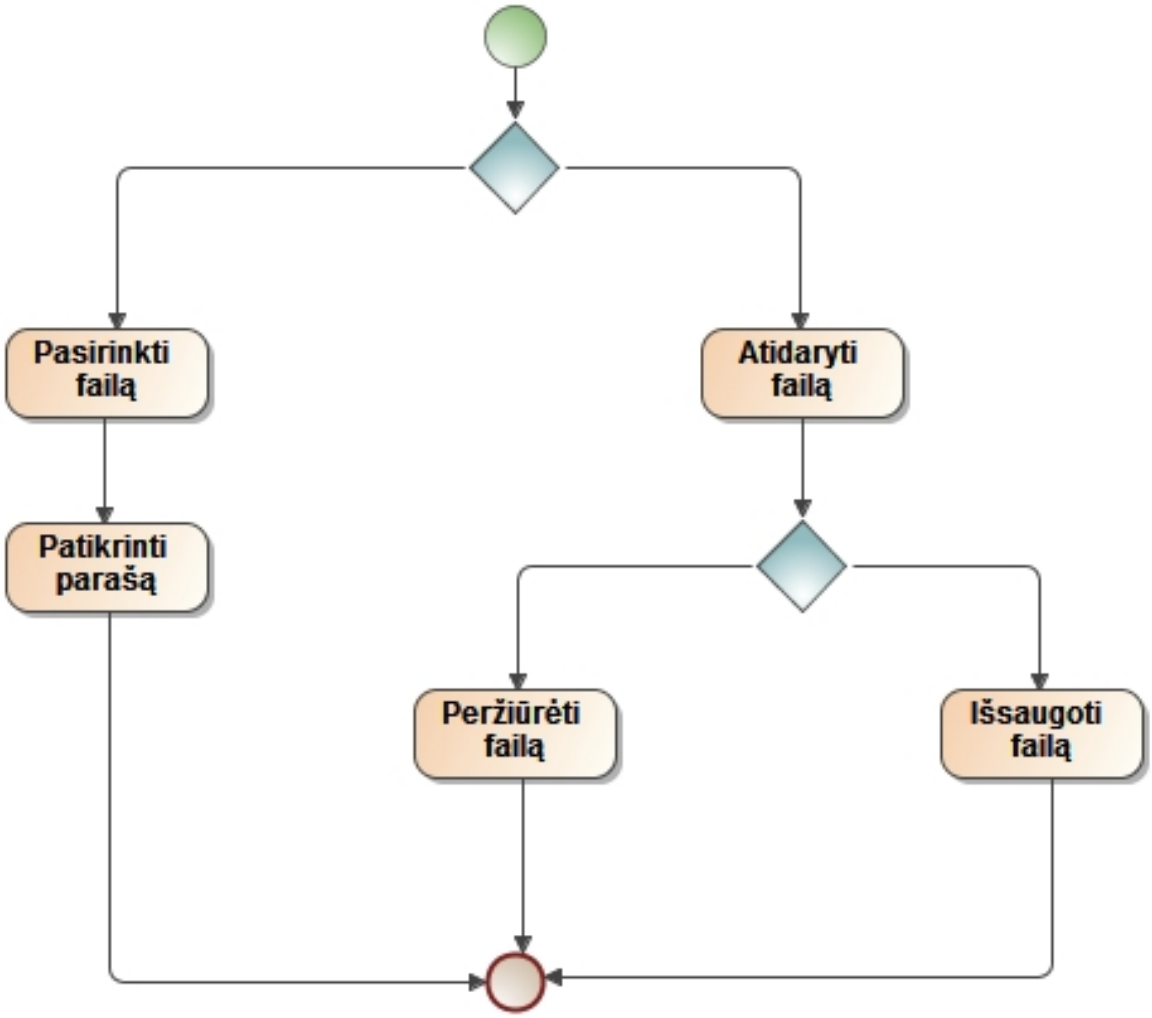
3.4.3.2 Registracijos pranešimo pasirašymas e-parašu.



33. pav. Dokumento pasirašymo veiklos diagrama.

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

3.4.3.3 Pasirašyto registracijos pranešimo peržiūra ir e-parašo tikrinimas.



34. 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.

3.7 Projektinės dalies išvados

1. Suprojektuoti e-parduotuvės Indentifikacijos ir autentifikacijos modeliai.
2. Darbe suprojektuota sistema leidžianti apmokėjimus, neatskleidžiant pirkėjo tapatybės, tačiau leidžianti taikyti lojalumo sistemą peikėjui.
3. Vartotojo registracijai, indentifikavimui ir autentifikavimui naudojame patvirtintus sertifikatų centro specializuotus pranešimus .

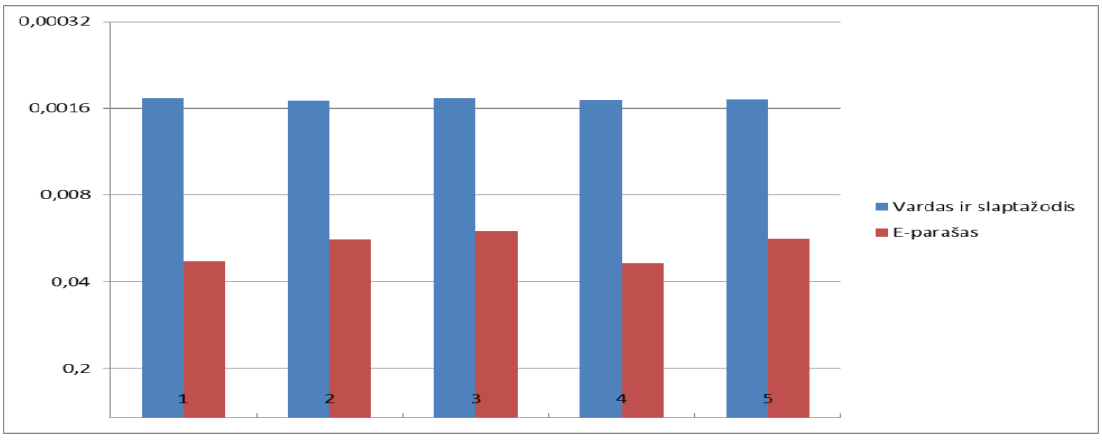
4. E-parduotuvės testavimo rezultatai

E. parašo taikymo e-parduotuvės sistemos autentifikavime ir šifravime eksperimentinis tyrimas Sukurtoje e-parduotuvės sistemoje realizavus autentifikavimui skirtą e-Parašo mechanizmą, svarbu nustatyti jo įtaką, prisijungimo prie sistemos laikui, lyginant su standartiniu vartotojo vardo ir slaptažodžio autentifikavimo mechanizmu. Minėtos charakteristikos tyrimas aptariamas pirmojoje eksperimentinio tyrimo dalyje.

4.1 Autentifikavimo e. parašu palyginimas su standartiniu prisijungimu. Siekiant nustatyti, kuris prisijungimo prie sistemos būdas yra greitesnis, buvo atliktas eksperimentinis tyrimas. Jo metu gauti prisijungimo prie sistemos laiko rezultatai, autentifikavimui naudojant e. parašą (36 pav.) ir naudojant vartotojo vardą, bei slaptažodį (37 pav.). Lentelėje Nr. 7 pateikiami 5 bandomųjų prisijungimų rezultatai.

7. Lentelė. Autentifikavimas e. parašu

Bandymu sk.	1	2	3	4	5
Laikas	Sekundėmis				
Autentifikavimas vardas ir slaptažodis	0,00134	0,00138	0,00133	0,00137	0,00135
Autentifikavimas e-parašu	0,02762	0,01837	0,01573	0,02863	0,01807



35. pav. Autentifikavimo e. parašu palyginimas su standartiniu prisijungimu.

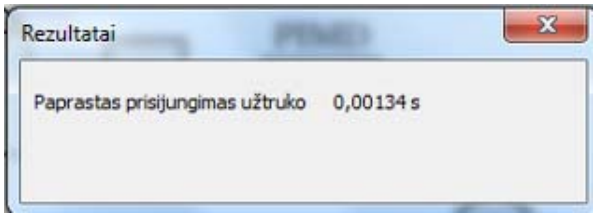
Iš lentelėje pateiktų duomenų matosi, jog vartotojo prijungimo prie sistemos laikai skiriasi. Toks skirtumas susidaro dėl skirtingo atliekamų veiksmų skaičiaus norint autentifikuoti vartotoją.

Autentifikuojant vartotojo vardu ir slaptažodžiu atliekami tokie veiksmai:

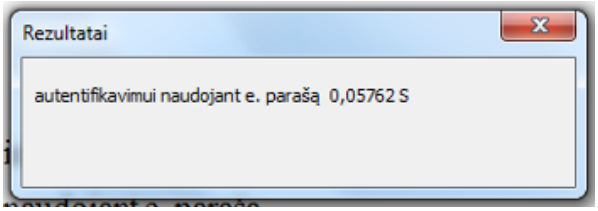
- Vartotojas nurodo savo vartotojo vardą bei slaptažodį ir spaudžia mygtuką prisijungti
- Sistema atlieka paiešką pagal pateiktą vartotojo vardą, jeigu netinkamas vartotojo prijungimas nutraukiamas
- Patikrinamas pateiktas slaptažodis su saugomu sistemos duomenų bazėje, jeigu netinkamas vartotojo prijungimas nutraukiamas

Vartotojas prijungiamas prie sistemos. Autentifikuojant e. parašu atliekami tokie veiksmai:

- Sistema sugeneruoja frazę
- Vartotojas pasirašo pateiktą sistemos sugeneruotą frazę, prideda savo sertifikatą ir spaudžia prisijungimo mygtuką
- Sistema patikrina sertifikate esančią informaciją, pagal kurią vartotojas identifikuojamas
- Sistema kreipiasi į sertifikavimo centrą patikrinti ar vartotojo pateiktas sertifikatas nepanaikintas
- Sistema patikrina pasirašytą frazę
- Vartotojas prijungiamas prie sistemos, jei atlikti visi tikrinimo etapai. Gauti rezultatai parodė, jog autentifikavimas e. parašu yra žymiai lėtesnis nei autentifikavimas vartotojo vardu ir slaptažodžiu.



36. pav. Prisijungimo prie sistemos laiko rezultatai.



37. pav. Prisijungimo prie sistemos laiko rezultatai, autentifikavimui naudojant e-parašą

Elektroninės parduotuvės kūrime buvo panaudoti šie įrankiai:

1) MySQL - reliacinė duomenų bazių valdymo sistema.

2) PHP - dinaminė interpretuojama programavimo kalba, kuri yra gana lanksti - veikia daugumoje operacinių sistemų, palaiko nemažai reliacinių duomenų bazių bei veikia su dauguma Interneto „serverių“.

3) Operacinė sistema Windows 7.

4) Internetinės naršyklės Internet Explorer 9, Mozilla Firefox ir Opera.

4.1 išvados

Realizavus siūlomą autentifikavimo metodą paremtą e. parašu buvo atliekamas tyrimas, kuriame lyginamas e. parašo autentifikavimo greitis su vartotojo vardo ir slaptažodžio autentifikavimo greičiu. Tyrimo metu nustatyta:

1. Kad atliekant vartotojo vardo ir slaptažodžio autentifikavimą sistema turi surasti vartotoja duomenų bazėje ir sulyginti duomenų bazėje laikomą slaptažodį.

2. Atliekant vartotojo autentifikavimą e-parašu, sistema turi sugeneruoti pranešimą pateikti jį vartotojui pasirašyti, patikrina pranešimo autentiškumą ir vartotojas prijungiamas prie sistemos tik tuomet kuomet atlikti visi tikrinimo etapai.

3. Vartotojo vardo ir slaptažodžio autentifikavimas saugumo prasme negali būti sulyginamas su autentifikavimu naudojant e. parašą.

5. Išvados

1. Suprojektuota e. parduotuvės lojalumo sistema, remiantis kompromisu tarp pirkėjų anonimiškumo (anonimity) ir atsekamumo (traceability) reikalavimų. Darbe suprojektuota sistema leidžianti apmokėjimus, neatskleidžiant pirkėjo tapatybės, tačiau leidžianti taikyti lojalumo sistemą peikėjui.

2. Panaudojant aklą e. parašą pirkėjas išlaiko anonimiškumą pardavėjo atžvilgiu, tačiau pardavėjas turi galimybę fiksuoti pirkėjo pirkimus ir taikyti jam lojalumo programą. Šios sistemos saugumas paremtas skaičių faktorizacijos uždavinio sudėtingumu.

3. Saugumo ir realizacijos paprastumo įgyvendinimui taikoma prijugties (on-line) mokėjimo sistema SET (Secure Electronic Transaction).

4. Pateikta lojalumo sistema turi tą savybę, kad ją gali naudotis tiktai registruoti vartotojai, kurie turi sertifikatų centro patvirtintus specializuotus sertifikatus. Tai leidžia išvengti įgyto lojalumo perdavimą kitiems vartotojams ir tokiu būdu išlaisvina pardavėjus nuo nepagrįstų išlaidų.

6. Literatūros sąrašas

1. SAKALAUSKAS, E. et al. Kriptografinės sistemos. Kaunas, 2008
2. Jo Ann S. Barefoot. Privacy under scrutiny. In *Banking Strategies*, Nov/Dec 2006.
3. Muhammad Saad Ahsan, Travis Creason. SET vs. SSL. ECE 578, 2007
4. William Stallings, Cryptography and Network Security Principles and Practices. Prentice Hall, 2008.
5. Yang Li & Yun Wang. Secure Electronic Transaction (SET protocol). 2005
6. mondex.com [interaktyvus] [žiūrėta 2012-02-11]. Prieiga per internetą <http://www.mondex.com>
7. paypal.com [interaktyvus] [žiūrėta 2011-12-09]. Prieiga per internetą <http://www.paypal.com>
8. Ruth N. Bolton, P. K. Kannan and Matthew D. Bramlett. Implications of loyalty program membership and service experiences for customer retention and value. In Journal of Academy of Marketing Science. Greenvale, Winter 2000.
9. Stefan Brands. An efficient off-line electronic cash system based on the representation problem. Report CS-R9323, Centrum voor Wiskunde en Informatica, March 1993.
10. David Chaum, Amos Fiat and Moni Naor. Untraceable electronic cash. In *Advances* in Cryptology – proceedings of CRYPTO 88, Lecture Notes in Computer Science 403, Springer-Verlag, 1990.
11. Simson Garfinkel, Gene Spafford, Web Security, Privacy & Commerce. O'Reilly Media.
12. MAO, W Modern Cryptography: Theory and Practice. New Jersey, 2003 ISBN: 0-13-066943-1
13. OPPLIGER, R Contemporary Cryptography. Norwood, 2007. ISBN 1-58053-642
14. SARR, Augustin P., et al. A Secure and Efficient Authenticated Diffie–Hellman Protocol. [interaktyvus] [žiūrėta 2012-04-25] Prieiga per internetą http://eprint.iacr.org/2009/408.pdf

15. Memon J. M., Khan A., Baig A., Shah A. A Study of Software Protection Techniques. Innovations and Advanced Techniques in Computer and Information Sciences and Engineering. 2007, 249-253, DOI: 10.1007/978-1-4020-6268-1_45.

16. Codework [interaktyvus]. [žiūrėta 2012-04-28] <http://codework.com/wibu>.

17. Codework [interaktyvus]. [žiūrėta 2011-10-29]. Prieiga per internetą http://www.codework.com/wibu/hardware.html

18. Akademinis e. parašas programa [interaktyvus]. [žiūrėta 2012-05-22]. Prieiga per internetą http://crypto.fmf.ktu.lt/print/a-sign/5_e-pp_portable/index.php

TERMINŲ IR SANTRUMPŲ ŽODYNAS

Identifikacija - tai asmens tapatybės nustatymas ir pripažinimas, sutapatinimas.

ISO - tarptautinė standartizacijos organizacija (angl. *International Organization for Standardization*)

PHP - programavimo kalba

kbps - kilobitai per sekundę

FIPS – Federalinis Informacijos Apdorojimo Standartas (angl. *Federal Information Processing Standards*)

SET – Saugūs elektroniniai atsiskaitymai (Secure Electronic Transaction).