VILNIAUS UNIVERSITETAS

MATEMATIKOS IR INFORMATIKOS FAKULTETAS

PROGRAMŲ SISTEMŲ KATEDRA

Elektroninės komercijos saugumas

eCommerce Security

Magistro baigiamasis darbas

Atliko: Andrius Budrionis (parašas)

Darbo vadovas: Doc. dr. Saulius Minkevičius (parašas)

Recenzentas: Doc. dr. Valdas Undzėnas (parašas)

Vilnius – 2010

SANTRAUKA

Darbe nagrinėjami šiuo metu rinkoje naudojami elektroninių atsiskaitymų modeliai ir jų saugumo problemos. Kadangi elektroninių transakcijų metu operuojama svarbiais ir konfidencialiais duomenimis, aukštesnio saugumo lygio užtikrinimo problema visada išlieka itin aktuali. Darbe išnagrinėtos dažniausiai sutinkamos elektroninių atsiskaitymų schemos (tiesioginis atsiskaitymas ir atsiskaitymas per *Paypal* sistemą), jų saugumo užtikrinimo principai, technikos ir spragos. Atsižvelgiant į dabartinius rinkos poreikius ir informacijos saugumo spragas šiuo metu naudojamuose modeliuose, suprojektuotas aukštesnio saugumo lygio elektroninių atsiskaitymų modelis ir realizuotas šio sprendimo prototipas. Šio prototipo projektas ir realizacija gali būti naudojamos kaip rekomendacijos kūrėjams, tobulinantiems elektroninių atsiskaitymų modelių saugumą.

SUMMARY

The work deals with electronic payment models used in the market and their security problems. As electronic transactions operate with important and confidential data, ensuring higher level of security is always an actual issue. The study generally concerns the main electronic payment schemes (direct payment and payment through Paypal), their safety principles, technical decisions and security ensuring gaps. Considering the current market needs and information security gaps in current eCommerce models, a new, ensuring higher level of security in electronic payments, model was designed and a prototype of this decision was implemented. The prototype design and implementation may be used as recommendations for developers, improving electronic payment security models.

Turinys

ĮVADAS

Šių dienų pasaulyje elektroninė komercija (toliau – el. komercija) ir elektroninių atsiskaitymų moduliai vis dažniau tampa viena iš verslo informacinių sistemų sudedamųjų dalių, kurių saugumas yra ypač svarbus tiek sistemos savininkui, tiek vartotojui. Nesaugūs el. komercijos moduliai veda prie konfidencialių asmens duomenų atskleidimo tretiesiems asmenims, o taip pat jų panaudojimo pasipelnymo tikslais. Tokie faktai skatina skeptišką dalies vartotojų požiūrį į elektroninius atsiskaitymus ir lėtina jų vystymąsi. Tačiau sėkminga atsiskaitymų internetu integracija į įmonės verslo procesus sąlygoja našesnį ir efektyvesnį darbą, greitesnį klientų aptarnavimą, mažesnes personalo išlaikymo išlaidas, mažina buhalterinių klaidų kiekį bei popierinių dokumentų srautus. O kur dar galimybė atlikti atsiskaitymus bet kuriuo paros metu iš bet kurio prie interneto prijungto kompiuterio. Dėl plačių galimybių ir teikiamos naudos el. komercija plinta vis labiau. Kiekvienai konkurencingumo siekiančiai įmonei ji darosi ne prabangos, o būtinu dalyku jų informacinėse sistemose. Tuo pačiu elektroninių atsiskaitymų modulių saugumas ir tobulinimas tampa vienu svarbiausių uždaviniu jų kūrėjams.

Darbo tikslas ir uždaviniai

Magistro darbo tikslas – aukštesnio, nei naudojami dabar, saugumo lygio elektroninių atsiskaitymų modelio sukūrimas, vertinant jį saugumo, greitaveikos ir reikalingų sąnaudų kriterijais, taip pat programinės įrangos prototipo pasiūlymas. Šiam tikslui įgyvendinti reikia:

- įvardinti galimus saugių elektroninių atsiskaitymų projektų rengimo būdus;
- įsigilinti į elektroninių sandorių saugumo aspektus bei būdus saugumui pasiekti;
- išanalizuoti dažniausiai sutinkamus elektroninių atsiskaitymų modelius ir nustatyti jų saugumo lygį, įvardijant saugumo „spragas“;
- nustatyti priemones ir technikas, kurių pagalba įmanoma pašalinti anksčiau paminėtas saugumo problemas;
- suprojektuoti aukštesnio saugumo lygio elektroninių atsiskaitymų modelį;
- realizuoti modelio prototipą;
- įvertinti modelį saugumo, greitaveikos ir reikalingų sąnaudų kriterijais;
- parengti rekomendacijas elektroninių atsiskaitymų modeliui kurti ir diegti.

Temos aktualumas ir naujumas

Saugumo užtikrinimas yra vienas svarbiausių reikalavimų elektroninių atsiskaitymų modeliams. Darbe kuriamas atsiskaitymų modelis, turintis aukštesnį saugumo lygį nei dabar naudojami analogiško funkcionalumo modeliai.

1. LITERATŪROS APŽVALGA

1.1. Pagrindinės saugumo užtikrinimo technikos

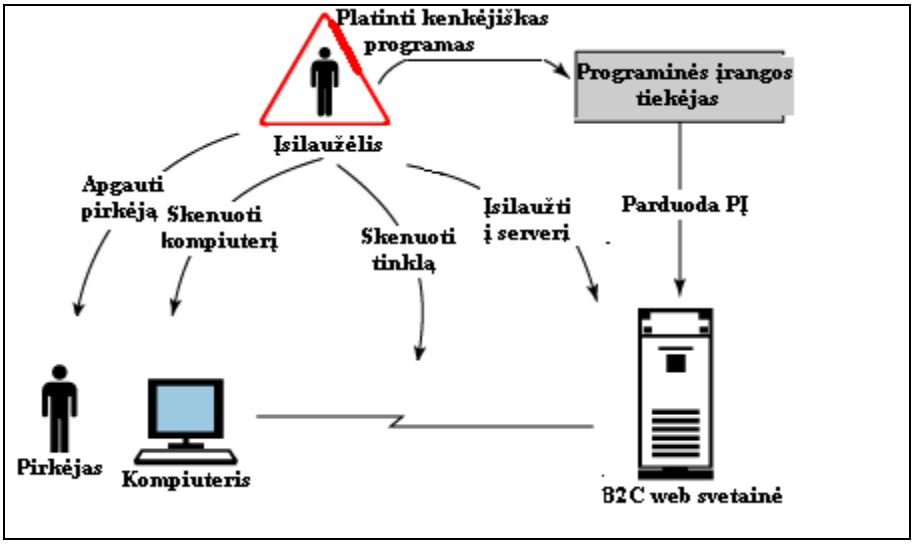
Kad būtų užtikrintas el. komercijos sistemos saugumas, koncentruojamasi į keletą sričių. Atitinkamas dėmesys joms leidžia sukurti saugias sistemas, tačiau minėtosios sritys sistemos saugumo negarantuoja, jos tik rekomenduoja, kaip pasiekti saugumą. Norimą saugumo lygį turime nustatyti patys arba remtis tai reglamentuojančiais dokumentais. Kaip gaires galime naudoti pagrindines saugumo užtikrinimo technikas:

- autentifikacija – tikrinimas, ar vartotojas yra tikrai tas, kuo jis dedasi. Užtikrinama, kad su atitinkamais prisijungimo duomenimis su sistema dirbs tik tam tikras žmogus;
- autorizacija – leidimas manipuliuoti tik būtinais resursais nustatytais būdais. Užtikrinama, kad vartotojas netyčia neištrins ar kitaip nepakeis svarbių duomenų;
- šifravimas – informacijos slėpimas ir užtikrinimas, kad elektroninių transakcijų duomenų šnipinėjimas taptų neįmanomas;
- auditas – atliktų veiksmų informacijos kaupimas registre, kad būtų galima patikrinti ir įsitikinti, koki veiksmai buvo atlikti.

Kuriant el. komercijos sistemas būtina atsižvelgti į šias saugumo užtikrinimo technikas, kurių pagalba įmanoma pasiekti reikiamą saugumą [OL05].

1.2. Pagrindiniai įsilaužėlių atakų taikiniai

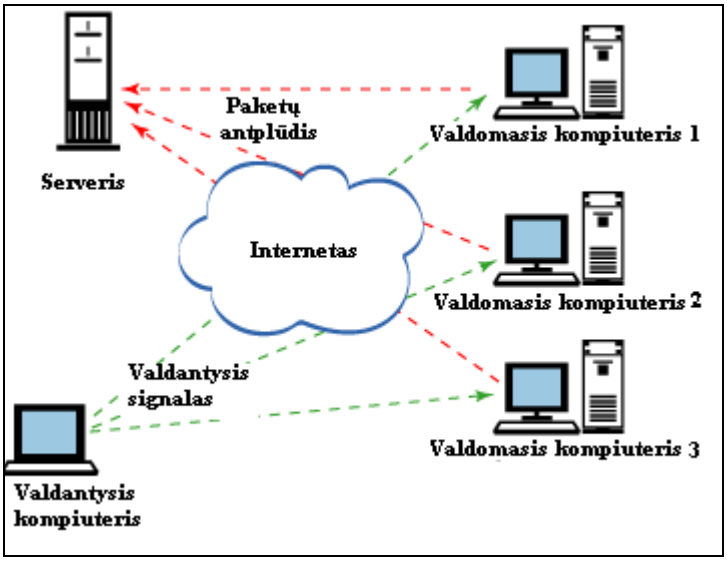
Pagrindiniai įsilaužimo į el. komercijos sistemas būdai ir taikiniai vaizduojami 1 pav.



1 pav. Pagrindiniai įsilaužėlių atakų taikiniai [Sch00]

Dažniausiai pasirenkami atakų taikiniai (žiūr. 1 pav.) ir būdai:

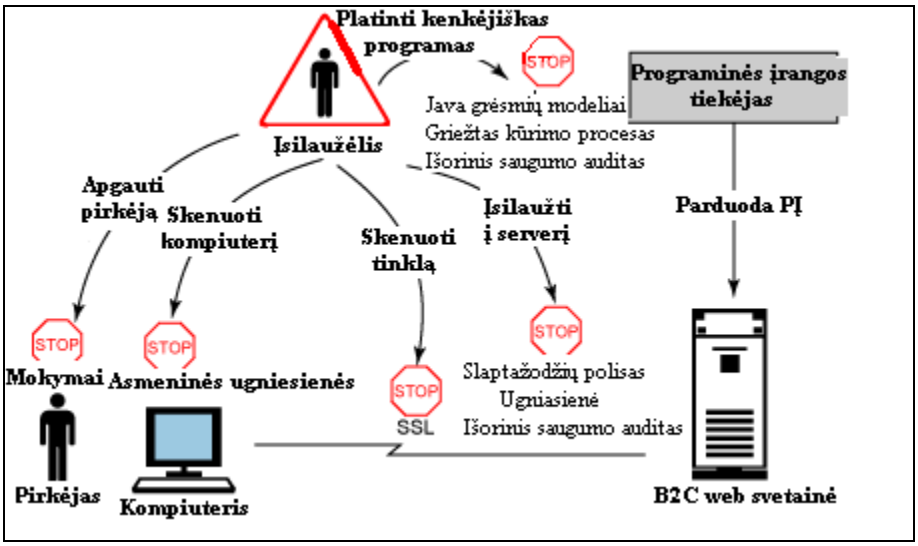
- vartotojo apgaulė – viena iš lengviausių atakų pagrįsta žmonių žinių trūkumu ir pasitikėjimu. Dažnas variantas, kai įsibrovėlis paprasčiausiai atspėja prisijungimo slaptažodžius (vienas dažniausiai naudojamų – mamos mergautinė pavardė) ir taip prisijungia prie sistemos. Kitas būdas – melagingas skambutis, kurio metu iš kliento išgaunami reikalingi duomenys. Taip pat dažnai sutinkama forma – gerai žinomų svetainių adresų kopijavimas ir tikėjimasis kad vartotojas suklys vesdamas adresą ir nepastebės, kad pateko ne į norimą svetainę (pvz. http://www.ibm.com/shop ir www.ibn.com/shop) [Sch00];
- kompiuterių šnipinėjimas – kompiuterius per atvirus prievadus skenuojančios programos suteikia priėjimą prie kliento kompiuteryje saugomų slaptažodžių ir kitos konfidencialios informacijos [Sch00];
- tinklo šnipinėjimas – skenuojami tinklu keliaujantys duomenų paketai ir juose ieškoma slaptos informacijos [Sch00];
- Denial of Service atakos – kenkėjiška veikla užsiimantis kompiuterio vartotojas išplatina virusus, kuriais užkrėsti kompiuteriai norimu laiku atakuoja pasirinktą serverį užklausomis. Kai užklausų kiekis išauga, serveris nebespėja su jomis tvarkytis ir tampa pažeidžiamas. Ataką iliustruoja 2 pav. [Rns00; OL05] .



2 pav. Denial of services atakos iliustracija [OL05]

1.3. Kovos su atakomis būdai

Pagrindiniai kovos su atakomis prieš el. komercijos sistemas ir saugumo užtikrinimo priemonės vaizduojamos 3 pav.

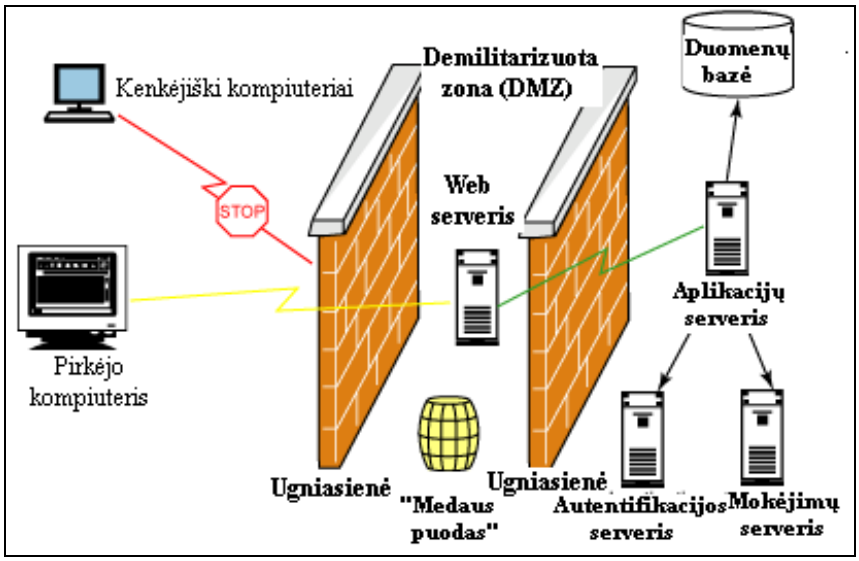


3 pav. Kovos su atakomis būdai [HL03]

Pagrindinės saugumo užtikrinimo technikos:

- mokymas - vartotojai turi būti supažindinti su galimomis grėsmėmis ir tinkamu asmeninių duomenų saugojimu, taip būtų sumažintas konfidencialios informacijos apgaunant vartotojus išgavimas;
- asmeninės ugniasienės – duomenų srautų ribojimas ir kontrolė;

- SSL – informacijos tarp vartotojo ir serverio srautų šifravimas, kad tinkle gauta informacija taptų neiššifruojama norint ją panaudoti be vartotojo sutikimo;
- serverių ugniasienės – demilitarizuotos zonos sukūrimas ir prisijungimų ribojimas, leidžiantis naudotis sistema tik jos vartotojams [HL03];



4 pav. Informacijos saugumo schema [HL03]

- ribojimai prisijungimo duomenims – nustatytas maksimalus bandymų prisijungti skaičius, maksimalus slaptažodžių galiojimo laikas, minimalus slaptažodžio ilgis ir t.t.

1.4. Gerosios saugių el. komercijos sistemų kūrimo praktikos

1.4.1. Saugumo nuostatos ir standartai

Galima išskirti šiuos pagrindinius saugumo užtikrinimo proceso principus:

- niekada nelaikyti vartotojų slaptažodžių tekstiniuose arba šifruotuose tekstiniuose failuose, vietoj to naudoti maišos (hash) algoritmus;
- įsitikinti, kad visi konfidencialių duomenų srautai yra šifruojami;
- testuoti, pasitelkiant konkrečias atakų technikas ir su tuo dirbančius asmenis.

1.4.2. Sausainiukų (*cookies*) naudojimas

Cookies yra dažnai naudojamas mechanizmas vartotojo sesijos duomenims saugoti. Kadangi HTTP protokolas neturi „būsenos“ saugojimo mechanizmo, tai yra vienintelis būdas apjungti vieno vartotojo užklausas. Reikiami duomenys išsaugomi cookie ir nuskaitomi kiekvieną kartą jų prireikus. Tai supaprastina svetainių kūrimą, nes nebereikia kaskart perduoti papildomų duomenų apie naudotoją. Taigi pagrindinis cookies panaudojimas yra autentifikacijos ir sesijos duomenims

saugoti. Cokies gali būti laikini (sunaikinami pasibaigus sesijai) arba riboto galiojimo (galiojimo laikas nustatomas serveryje).

1.4.3. Grėsmių modelio sudarymas

Grėsmių modelis padeda identifikuoti galimas grėsmes kuriamai sistemai. Reikia ypač atsižvelgti ir išryškinti galimus neteisėto priėjimo prie sistemos kelius ir scenarijus, numatyti pasekmes ir galimus sprendimo būdus. Žinomas grėsmių modelis palengvina sistemos projektavimą ir kūrimą, stiprinant „silpnus“ sistemos taškus pirmosiose kūrimo fazėse, taip užkertant kelią įvykdyti modelyje numatytus scenarijus, galinčius padaryti daug žalos. Išsamus ir platus grėsmių modelis - viena svarbiausių gerųjų praktikų padedančių sukurti saugią sistemą.

1.5. Rinkoje naudojamos elektroninių atsiskaitymų sistemos

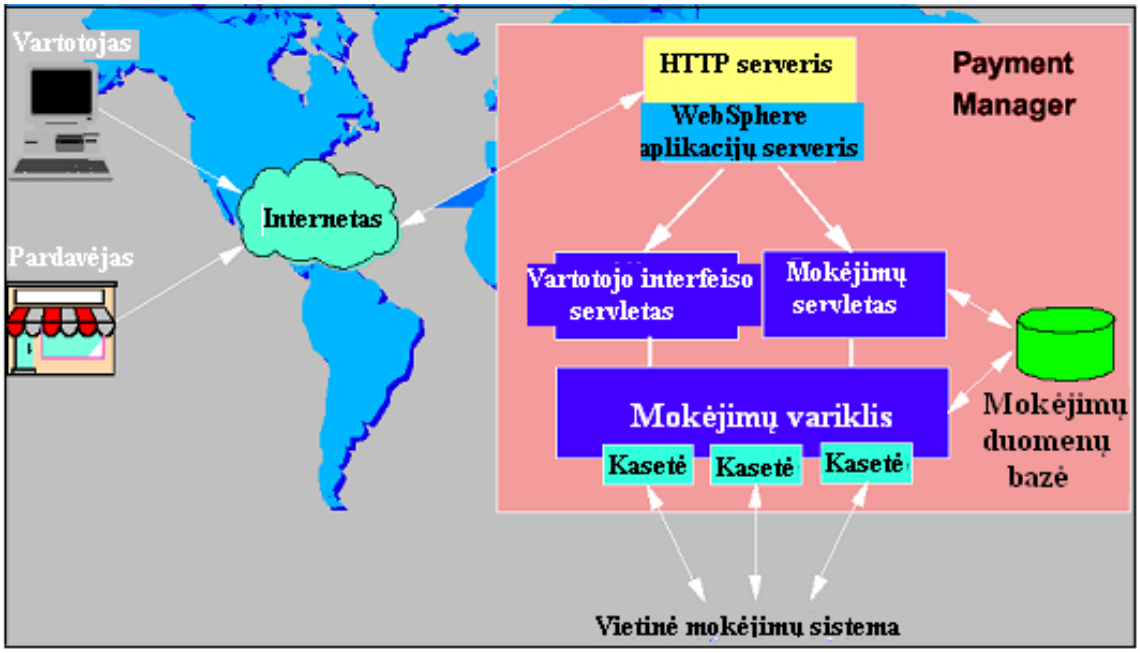
1.5.1. IBM sprendimas saugiems elektroniniams atsiskaitymams

Internetinė prekyba dažnai tampa ne papildomu, o pagrindiniu būdu parduoti prekes vartotojui. Kadangi tai naudinga tiek pirkėjui (nereikia gaišti laiko parduotuvėse, laukti eilėse), tiek ir pardavėjui, kuriam nereikia nuomoti patalpų, išlaikyti didžiulio personalo, tai išplito itin greit. Tiek pirkėjui, tiek pardavėjui svarbiausia šio proceso dalis yra apmokėjimas, o pagrindinis kriterijus tam vertinti yra saugumas. Kadangi žmonės nelinkę pasitikėti internetu, piniginės transakcijos turi būti kiek įmanoma saugios. Dažniausiai neaišku kokie žmonės slepiasi už internetinės parduotuvės interfeiso, todėl būna sunku patikėti vienintelius banko sąskaitai valdyti reikalingus duomenis. Vienas iš rinkoje siūlomų programinių produktų, realizuojantis elektroninių atsiskaitymų mechanizmą yra IBM WebSphere Payment Manager.

IBM WebSphere Payment Manager gali būti naudojamas kaip:

- pilnas internetinės parduotuvės sprendimas integruotas WebSphere Commerce Suite;
- Stand – Alone versija, kuri gali būti integruojama į egzistuojančią mokėjimų aplinką su web serveriais, internetinėmis parduotuvėmis ir duomenų bazių serveriais
- servisų tiekėjas suprogramuotai sistemai.

Kadangi IBM WebSphere Payment Manager gali būti taip plačiai panaudojamas, jis tiekiamas kartu su IBM HTTP serveriu, WebSphere application serveriu, IBM duomenų bazių serveriu ir kasečių, skirtų saugių elektroninių transakcijų (SET) protokolui, palaikymu.



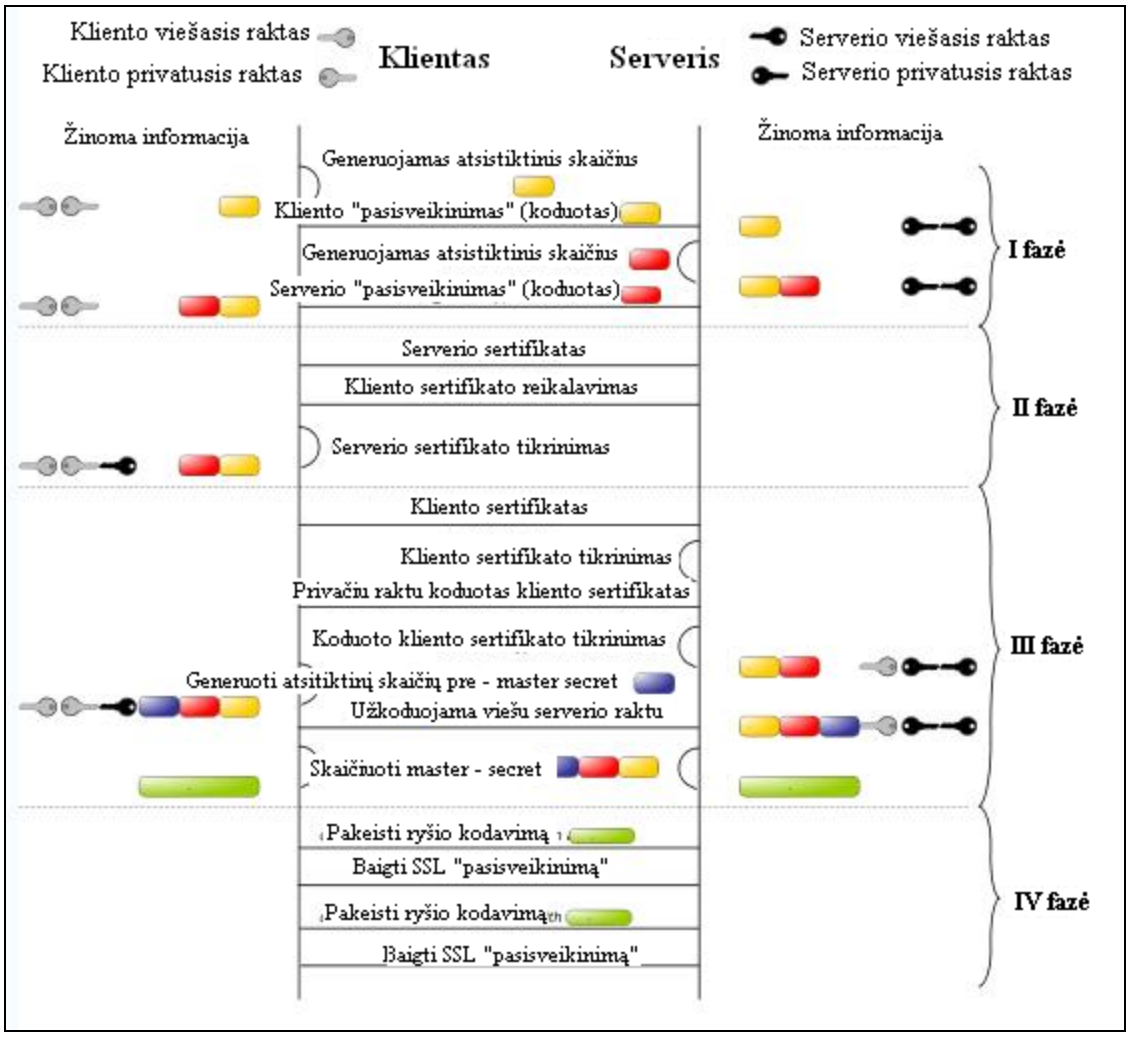
5 pav. IBM Payment Manager veikimo schema [Its01]

5 pav. grafiškai vaizduoja IBM elektroninių atsiskaitymų sprendimo dalis ir pagrindinę veikimo schemą, kurią toliau ir nagrinėsime.

Transakcijos pradžia laikysiu momentą, kai sistemos vartotojo duomenys pasiekia application serverį, jau atlikti pirminiai duomenų patikrinimai. Kad įsitikintume, ar vartotojas naudoja teisingus kreditinės kortelės duomenis, atliekamas vidinis tikrinimas, kurio metu pagal kortelės tipą ir numerį nustatoma, ar naudojama kortelė galioja. Šio tikrinimo privalumas yra tas, kad algoritmo dėka nereikalingas prisijungimas prie kortelę išdavusios bankinės institucijos duomenų bazės. Duomenų surinkimui ir tikrinimui privalomas HTTPS protokolas ir jo palaikomas saugumo lygis. Surinkus ir patikrinus visus reikalingus duomenis apie klientą vykdomas kreipinys į bankinės institucijos duomenų bazę, atliekamas galutinis patikrinimas – ar vartotojo sąskaitoje yra pakankamas kiekis pinigų. Įveikus visus patikrinimus, atliekamas atitinkamos sumos pinigų pervedimas iš pirkėjo sąskaitos į pardavėjo. [Its01]

1.5.2. TLS/SSL standartas

TLS (Transport Layer Security) ir jos pirmtakas SSL (Secure Sockets Layer) yra kriptografiniai protokolai užtikrinantys duomenų saugumą ir vientisumą perduodant juos nesaugiais tinklais koduodamas duomenis transporto lygmenyje. 6 pav. iliustruoja šio protokolo veikimą.



6 pav. TLS/SSL protokolo veikimo schema [Mog07]

TLS serveris ir klientas susijungimo ypatybes nustato „rankų paspaudimo“ būdu, kurio metu pasirenkamos saugumui užtikrinti reikalingos ryšio savybės. Procedūra inicijuojama klientui prisijungus prie serverio, paprašius saugios prieigos ir pateikus jo palaikomų kriptografinių funkcijų sąrašą. Serveris iš funkcijų sąrašo išrenką „stipriausią“ ir apie tai informuoja klientą. Abiejų tinklo esybių identifikacijai jos pasikeičia juos identifikuojančiais elektroniniais sertifikatais ir juos patikrina. Serverio sertifikatas turi ne tik jo vardą, duomenis apie sertifikato išdavėją, bet ir viešąjį

šifravimo raktą. Norėdamas sugeneruoti sesijos raktus, skirtus saugiam prisijungimui, klientas naudodamasis serverio viešuoju raktu užkoduoja pasirinktą skaičių ir siunčia jį serveriui, kuris jį dekoduoja naudodamas savo privatųjį raktą. Taip užtikrinamas saugus duomenų perdavimas, nes klientas žino tik pasirinktą skaičių ir viešąjį raktą, o serveris – privatųjį raktą ir skaičių (kai jį dekoduoja). Tretiesiems asmenims gali būti prieinamas tik viešasis raktas ir užkoduotas pranešimas. [Mog07, Rei06]

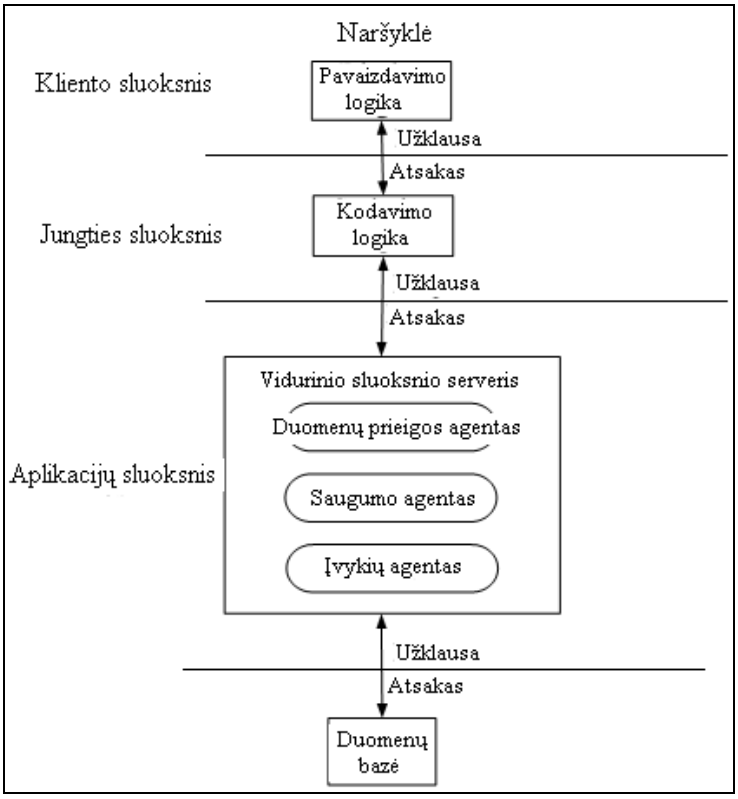
1.5.3. Agentinėmis technologijomis paremtas el. komercijos saugumo modelis

1.5.3.1. Įvadas

Agentinės technologijos el. komercijos saugumo kontekste naudojamos siekiant realizuoti išskirstytas dirbtinio intelekto sistemas, pasitarnaujančias saugumo užtikrinimui. Pagrindiniai tokios sistemos privalumai yra tobulesnis slaptažodžių sekimas, dinaminis apkrovos balansavimas, prisitaikymas prie vartotojo poreikių, galimybė aiškiai skirstyti logikos sritis į sluoksnius ir už tam tikrą sritį atsakingus agentus.

1.5.3.2. Multiagentinės 4 sluoksnių el. komercijos saugumo modelis

7 pav. vaizduoja multiagentinės 4 sluoksnių el. komercijos saugumo modelį.

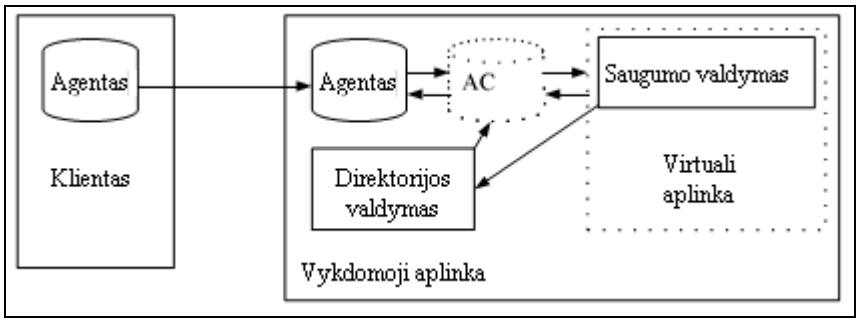


7 pav. Multiagentinės 4 sluoksnių elektroninės komercijos saugumo modelis [ZL05]

Kaip matome iš 7 pav. modelis padalintas į sluoksnius, kurių kiekvienas atsakingas už tam tikrą funkcionalumą. Programų (*application*) sluoksnyje realizuojami trys agentai, kurie veikia nepriklausomai ir netgi gali būti perkeliami į jungties (link) sluoksnį. Dėl šių ypatumų sistema tampa lengvai palaikoma ir atnaujinama. Dėl netiesioginio priėjimo prie duomenų bazės didėja jos saugumas. [ZL05]

1.5.3.3. Modelio veikimas

8 pav. iliustruoja modelio veikimą:



8 pav. Multiagentinio modelio veikimas [ZL05]

Modelio elementų ir funkcijų paaiškinimas:

- direktorijos valdymas yra atsakingas už vardų paslaugoms suteikimą, taip pat valdo ir registruoja visus agentus, tam kad agentas bet kuriuo metu galėtų rasti norimus resursus;
- saugumo valdymas (*security manager*) atsakingas už agentų saugumo peržiūras;

Darbas vyksta tokia tvarka:

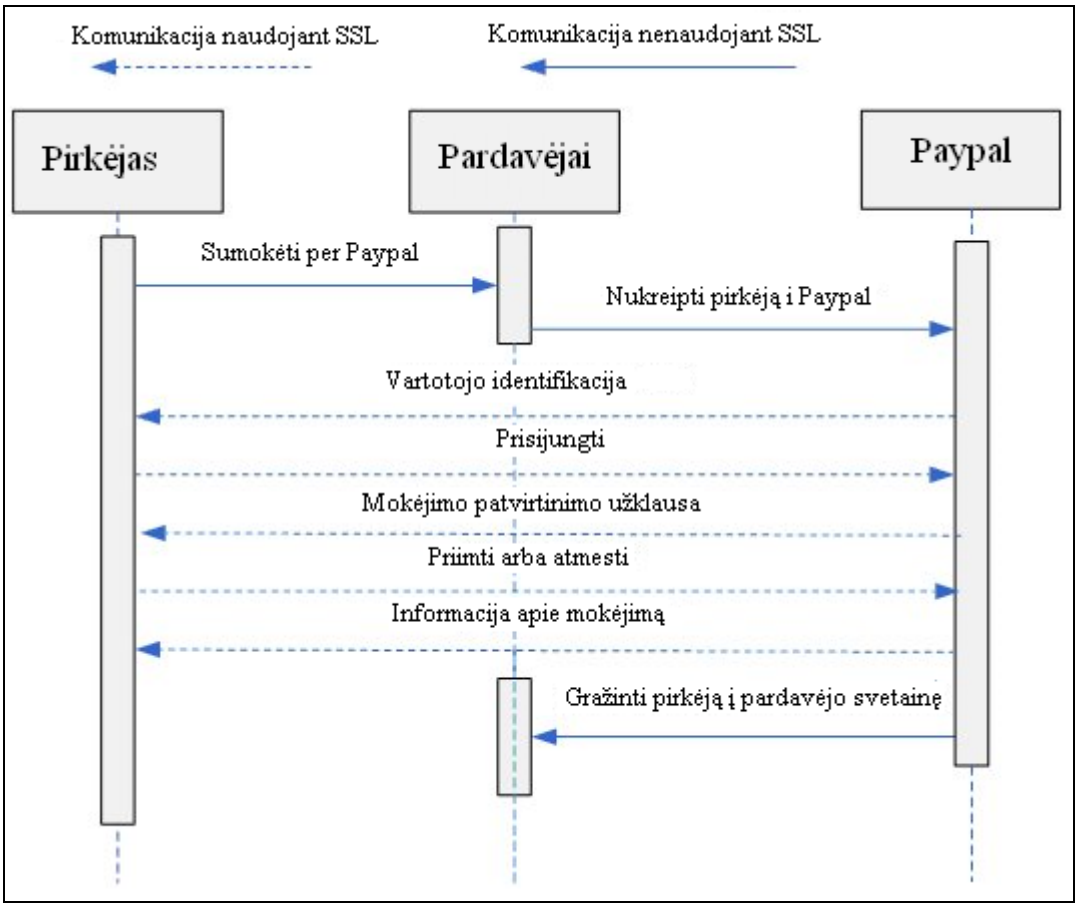
1. Agentas, turintis sertifikavimo centro patvirtintą skaitmeninį sertifikatą, sugeneruojamas kliento pusėje. Jis kreipiasi į serverio vykdomąją aplinką (*running environment*).
2. Vykdomas saugumo patikrinimas, kurio metu padaroma kiekvieno agento kopija (neturinti konfidencialių kliento duomenų, tik skaitmeninį identifikatorių ir savo veiklai reikalingas funkcijas).
3. Patikrinus skaitmeninio parašo teisingumą, agentui leidžiama veikti serverio aplinkoje, tačiau jo veiksmai įrašinėjami, o įrašai nagrinėjami stengiantis atrasti kenkėjiškų bruožų. Jei tokių nerandama, vartotojo kompiuteryje veikiančiam agentui siunčiamas patvirtinimas, kad jis gali naudotis serverio paslaugomis.

Agentai gali dinamiškai judėti tinklu pagal vartotojų norus, atlikti nepriklausomus besikeičiančios situacijos matavimus ir grąžinti rezultatus. Agentų technologija turi pašalinti tradicinio būdo principus ir prisitaikyti prie vartotojų ir rinkos poreikių. [ZL05]

1.5.4. *Paypal* el. komercijos saugumo modelis

Paypal yra vienas sėkmingiausių projektų elektroninių atsiskaitymų istorijoje, kurio pradžia laikomi 2000 metai. Jo sėkmę įrodo šie skaičiai: pelnas 2006 metais siekė 1,441 milijardo dolerių, 37% didesnis nei 2005 metais. Per 2006 metus *Paypal* transakcijomis buvo pervesti 37,75 milijardo dolerių, tai apie 1384 doleriai pervedami kiekvieną sekundę. Prie šios sėkmės prisidėjo ypač paprasta ir nieko nekainuojanti šios sistemos integracija į bet kokius el. komercijos objektus, o taip pat aukšto transakcijų saugumo ir patikimumo lygio užtikrinamas, kurio modelį aptarsime. [Eba07]

Saugumui užtikrinti *Paypal* naudoja SSL, modelio veikimo schema pavaizduota 9 pav.



9 pav. Paypal elektroninės komercijos modelis

Dėl naudojamo SSL 3.0 128 bitų ryšio su vartotoju šifravimo *Paypal* tenkina visus saugumo reikalavimus, o vartotojams, norintiems aukštesnio saugumo lygio siūlo nuolat generuojamus ir tikrinamus saugumo kodus, kuriems generuoti naudojamas tam skirtas kodų generatorius arba

sugeneruoti kodai iš sistemos atsiunčiami nurodytu telefonu numeriu SMS žinute. Norint atlikti transakcijas reikalingas ir sugeneruotas kodas. [Hoa09, Rei06]

Nors sistema yra pakankamai apsaugota, tačiau pasitaiko atvejų, kai įsilaužiama į vartotojų duomenų bazę ar vartotojai apgaunami siunčiant netikrus elektroninius laiškus, liepiančius prisijungti prie identišką grafinį interfeisą turinčio interneto puslapio taip siekiant išgauti prisijungimo duomenis. Tačiau šios problemos pažįstamos visiems el. komercijos paslaugų tiekėjams. [CH04]

1.6. Standartų reikalavimai

1.6.1. Informacijos saugumo valdymo brandos modelis ISM3

Vienas iš dokumentų padedančių apibrėžti reikalavimus el. komercijos moduliams yra informacijos saugumo valdymo brandos modelis. Kadangi šis modelis yra universalus, jame nėra konkrečių reikalavimų konkrečioms sistemų grupėms, tačiau galima rasti daug rekomendacijų, kaip sustiprinti informacijos saugumą ir jo valdymą. Viena didžiausių grėsmių laikomas ne prastas sistemos saugumas, o žmogiškasis faktorius – darbuotojai, kurie tampa silpniausiais informacijos saugumo taškais. Saugumo incidentai dažniausiai kyla ne dėl sistemos saugumo kaltės, o dėl prasto saugumo proceso valdymo. Todėl kuriant ir diegiant elektroninių atsiskaitymų modulius, įmonėse turi būti imtasi atitinkamų veiklų, kad informacijos saugumo procesas būtų sustiprintas, nes šių sistemų saugumas priklauso ne vien nuo naudojamų technologinių sprendimų, programavimo kokybės ar techninės įrangos. [Can06]

1.6.2. ISO/IEC 15408 standartas

Šis standartas, kaip ir daugelis kitų, yra universalus ir skirtas ne vien el. komercijos modulių saugumo reikalavimams formuluoti ir tikrinti. Jame apibrėžtos tikrinimo procedūros, tinkamos bet kokiai programinei įrangai, kuri reikalauja atitinkamo informacijos saugumo lygio. Standartas apibrėžia 7 programinės įrangos saugumo vertinimo lygius, pagal kuriuos gali būti formuluojami ir reikalavimai tokio tipo programiniams produktams.

I lygis – ištestuotas funkcionalumas – pagrindinis dėmesys skiriamas teisingam veikimui, į grėsmes saugumui nežiūrima rimtai. Sistema turi būti atspari tik dokumentacijoje nurodytoms saugumo grėsmėms.

II lygis – struktūriškai ištestuotas – analizuojamos saugumo užtikrinimo funkcijos, naudojantis specifikacijomis ir dokumentacijomis, kad jų veikimas taptų pilnai aiškus ir suprantamas.

III lygis - metodiškai ištestuotas – vykdomas saugumo užtikrinimo funkcijų testavimas pagal iš anksto sudarytą metodinį planą, funkcijos testuojamos tiek atskirai, tiek ir integruotos į bendrą produktą.

IV lygis – metodiškai suprojektuotas, ištestuotas ir peržiūrėtas – testavimas vykdomas pagal neformalų modelį, kuriame apibrėžti saugumo objektų reikalavimai ir sąryšiai su saugumą užtikrinančiomis funkcijomis.

V lygis – pusiau formaliai suprojektuotas ir ištestuotas – testavimui naudojamas formalus saugumo objektų modelis ir pusiau formali funkcinės specifikacijos prezentacija, vertinamas sąveikos tarp jų modelis.

VI lygis – pusiau formaliai verifikuotas ir ištestuotas projektas – skirtumas tarp V lygio yra tik tas, kad būtinas modulinis ir sluoksninis sistemos ir saugumo objektų vaizdas.

VII lygis – formaliai verifikuotas ir ištestuotas dizainas – ypač aukšto saugumo lygio užtikrinimas, nekreipiant dėmesio į kaštus. Testavimas vykdomas pasitelkiant plačiausią grėsmių modelį, todėl galutinis produktas pasiekia maksimalų saugumo lygį.

Tikslesnis lygių ir saugumo objektų apibrėžimas pateiktas ISO/IEC 15408 standarte. Pagal standarto rekomendacijas, kiekviena įmonė, norinti turėti informacinę sistemą su atitinkamu kiekiu saugumo objektų turi pati apsibrėžti konkrečius reikalavimus jų saugumui, standartas pateikia tik rekomendacijas kaip tai padaryti. [ISO05]

1.7. El. komercijos modelio vertinimas

1.7.1. Vertinimo kriterijai

Prieš pradedant el. komercijos modulio kūrimą, būtina nuspręsti, kokiu modeliu remsimės, t.y. kaip veiks kuriamoji sistema. Kad būtų galima objektyviai įvertinti skirtingus modelius, reikalingi tiksliai apibrėžti vertinimo kriterijai ir metrikos. Vertindami modelius naudosimės tokiu vertinamų savybių ir įverčių rinkiniu [Sah08]:

- identifikacija – pagrindinis tikslas – atskirti transakcijoje dalyvaujančias šalis (pirkėją, mokantį už prekes ir pardavėją, tiekiantį prekes ar paslaugas). Šis kriterijus stiprina pasitikėjimą tarp šalių, kurio ypač reikia aplinkoje, kurioje beveik nėra tiesioginio kontakto;

- konfidencialumas – kiekvienai šaliai atskleidžiama tik transakcijai vykdyti reikalinga kitos šalies informacija. Kriterijaus tikslas – užtikrinti anonimiškumą ir konfidencialių duomenų kontrolę. Pvz. Pardavėjas neturi žinoti kliento banko kortelių duomenų, nes jie reikalingi tik bankui įvykti transakciją, o bankas neturi žinoti kokios prekės ar paslaugos perkamos ir pan.

- integralumas (tikslumas) – siekiama užkirsti kelią klaidoms galinčioms įvykti transakcijos metu, tokioms kaip klaidingos informacijos pateikimas ar transakcijos įvykdymas du kartus;

- atskaitomumas – tikslas yra užkirsti kelią pirkėjui ar pardavėjui paneigti anksčiau priimtus įsipareigojimus, įsipareigojimų duomenys turi būti saugomi ir, esant reikalui, naudojami;

- atsisakymas mokėti – turi egzistuot efektyvus transakcijų atšaukimo mechanizmas, jei iškyla problemų su duomenų tikslumu;

- trukmė – greitas sistemos veikimas ir atsakas į užklausas, paprastos mokėjimo procedūros yra ypač svarbios tiek pirkėjams, tiek ir pardavėjams;

- likvidumas / gebėjimas kisti – galimybė bet kada vykdyti bet kokių valiutų konvertavimo veiksmus be papildomų procedūrų;

- anonimiškumas – užtikrinama, kad neįmanoma stebėti ir sekti konkretaus vartotojo pinigų srautų ir jų gavėjų;

- kaina pirkėjui – nuo verslo modelio priklausantys kaštai, tokie kaip programinės įrangos licencijų ir naudojimosi kainos;
- kaina pardavėjui – fiksuoti ir procentiniai transakcijų mokesčiai (kuriuos dažnai sumoka pirkėjas), programinės įrangos kaina;
- patogumas – elektroninių atsiskaitymų sistema turi būti lengvai suvokiama ir paprastai naudojama, nereikalaujanti sudėtingų procedūrų mokymosi. Taip pat sistemos veikimo greitis turi tenkinti visų šalių poreikius, pirkėjas turėtų apsieiti be papildomos programinės įrangos diegimo;
- sąveika su kitomis sistemomis – mokėjimų sistema turi būti pilnai suderinama su standartinėmis įvairių finansinių institucijų sistemomis, atvira plėtimui ir bet kokių naujų šalių prisijungimui [Hoa09].

1 lentelė vaizduoja elektroninė komercijos modelių vertinimo kriterijus.

1 lentelė. Elektroninės komercijos modelių vertinimo kriterijai [Sah08]

Savybė	Maksimalus įvertis
Saugumas: • identifikacija; • konfidencialumas; • autentifikacija; • integralumas (tikslumas); • atskaitomumas; • atsisakymas mokėti; • trukmė; • likvidumas / gebėjimas kisti; • anonimiškumas. Iš viso:	 2 2 2 2 2 3 2 2 3 20
Kaina: • pirkėjui; • pardavėjui. Iš viso:	 5 5 10
Patogumas: • diegimas / licencijos; • proceso sudėtingumas / greitis. Iš viso:	 5 5 10

Universalumas: • mokėjimo tipas; • sąveika su kitomis sistemomis. Iš viso:	 5 5 10

1.7.2. Dažniausiai sutinkamų el. komercijos modelių vertinimas

2 lentelė vaizduoja dažniausiai rinkoje sutinkamų elektroninės komercijos modelių vertinimus.

2 lentelė. Elektroninės komercijos modulių vertinimas [Sah08]

Savybė	SET	SSLI[1]	SSLWI[2]	Cyber Comm	E-certe bleue	Odysseo	e.Check.net	Paypal
Saugumas:								
• identifikacija;	1,5	1	1	2	1,5	1,5	1	1,5
• konfidencialumas;	2	2	2	2	2	2	2	2
• autentifikacija;	1,5	1	1	2	1,5	1	1	2
• integralumas;	2	2	2	2	2	2	2	2
• atskaitomumas;	2	1	0	2	0	2	0	2
• atsisakymas mokėti;	3	0	0	3	1	3	3	1,5
• trukmė;	2	2	2	2	2	1	2	1
• likvidumas / gebėjimas kisti;	2	2	2	2	2	0	2	1
• anonimiškumas.	2	2	0	2	2	3	2	2
Iš viso:	**18**	**13**	**10**	**19**	**14**	**15,5**	**15**	**15**
Kaina:								
• pirkėjui;	3	5	5	1	1	3	4	5
• pardavėjui.	0	2	5	0	4	2	2	4
Iš viso:	**3**	**7**	**10**	**1**	**5**	**5**	**6**	**9**
Patogumas:								
• diegimas / licencijos;	2,5	5	5	0,5	3	2	2,5	3,5
• proceso sudėtingumas / greitis.	0,5	3	5	0,5	4	2	2,5	4,5
Iš viso:	**3**	**8**	**10**	**1**	**7**	**4**	**5**	**8**

[1] SSLI – elektroniniai kreditinių ir debetinių kortelių atsiskaitymai, veikiantys SSL 3.0 protokolu, tarpininkaujant bankui ar kitai elektroninių atsiskaitymų paslaugas teikiančiai institucijai, kuri užtikrina mokėjimo apdorojimą ir tikslumą.

[2] SSLWI – elektroniniai kreditinių ir debetinių kortelių atsiskaitymai, veikiantys SSL 3.0 protokolu, netarpininkaujant atsiskaitymus kontroliuojančiai institucijai.

Universalumas:								
• mokėjimo tipas;	3	3	3	3	3	4,5	3	4
• sąveika su kitomis sistemomis.	2	5	5	2	5	1	3	3
Iš viso:	**5**	**8**	**8**	**5**	**8**	**5,5**	**6**	**7**
Iš viso (iš 50 galimų):	**29**	**36**	**38**	**26**	**34**	**30**	**31**	**39**

Gauti įverčiai modelius dalina į tris dalis:

- Bendra suma <= 30 – sistemos, kurioms buvo lemta išnykti (SET, CyberComm). Nors jos ir buvo ypač saugios, tačiau jas sužlugdė kiti faktoriai, pvz. SET buvo labai lėtas.

- 30 < bendra suma <= 35 – sistemos, dėl kurių kūrimo vis dar abejojama. Jos yra mažiau saugios nei pirmoji grupė, tačiau jų kainos ir patogumo įverčiai tai kompensuoja.

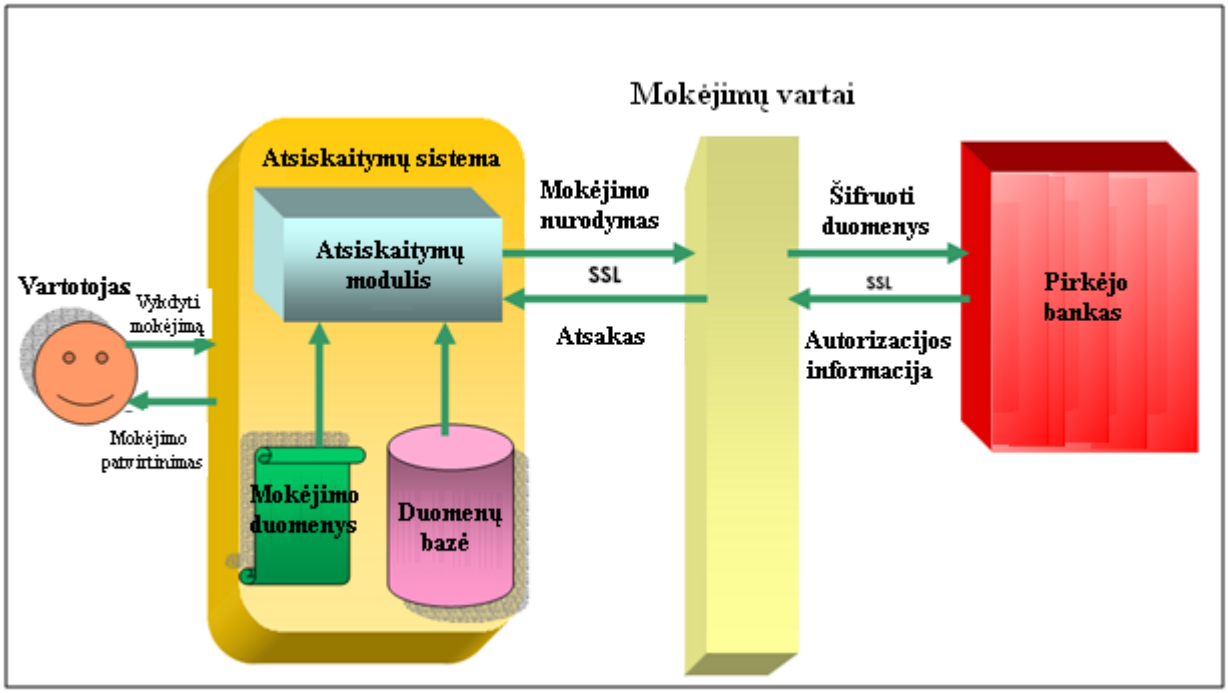
- Bendra suma > 35 – elektroninių atsiskaitymų sistemos, kurios sėkmingai naudojamos ir tobulinamos. Nors jų saugumas ir nėra itin aukštas, tačiau dėl ypač gerų kitų kriterijų įverčių jos sėkmingai naudojamos.

Kaip galime matyti iš el. komercijos modelių vertinimų, ankstesniais bandymais buvo siekiama maksimalaus saugumo, tačiau dėl to ypač išaugdavo kaina ir nukentėdavo naudojimosi patogumas. Supratus, kad rinka atmeta tokius sprendimus, buvo pereita prie žemesnio saugumo lygio ir reikalavimų. Nors SSL ir dažnai kritikuojamas dėl pakankamai žemo saugumo lygio, tačiau išlaiko lyderio pozicijas dėl paprastumo, mažos kainos, lengvo taikymo ir lankstumo. Vienintelis rimtas varžovas šiam modeliui yra Paypal sistema, kuri pasižymi panašiomis savybėmis, tačiau turi aukštesnį bendrą vertinimo balą. Šis vertinimas parodo, kad norint sukurti elektroninių atsiskaitymų modelį, svarbiausia atsižvelgti į naudotojų poreikius ir reikalavimus, nes tik nuo jų priklauso modelio sėkmė. [Sah08]

2. DAŽNIAUSIAI SUTINKAMI ELEKTRONINIŲ ATSISKAITYMŲ MODELIAI

2.1. Tiesioginis atsiskaitymas

Vienas populiariausių elektroninių atsiskaitymų būdų – tiesioginis atsiskaitymas, kurio schema pateikta 10 pav.

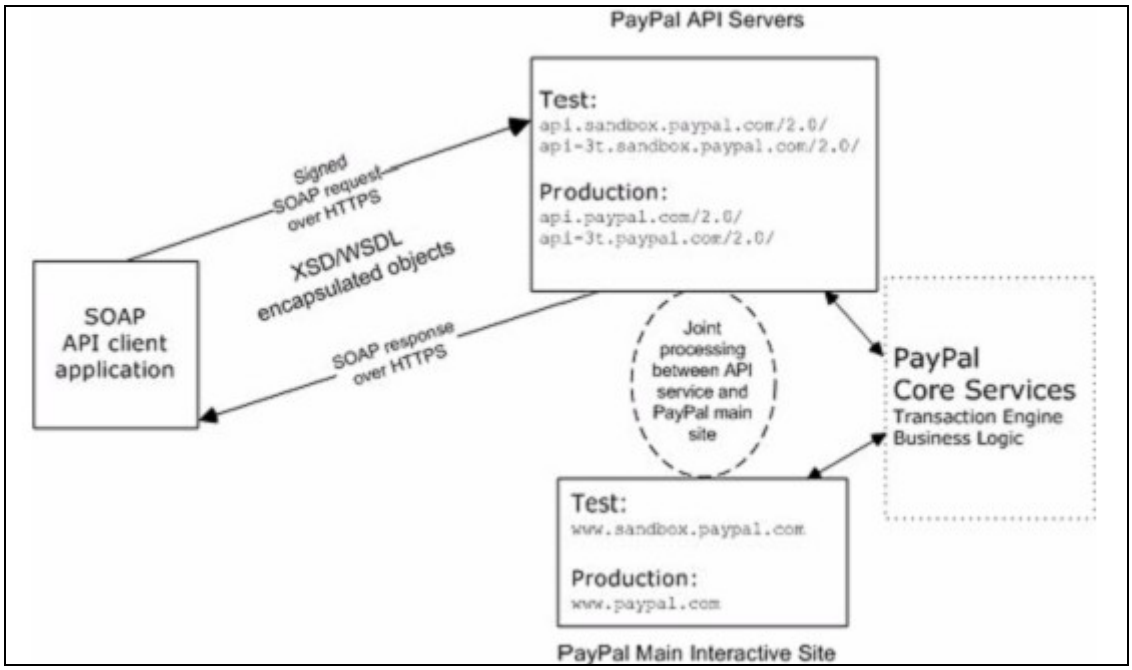


10 pav. Tiesioginio atsiskaitymo schema [CL08]

Tiesioginiai elektroniniai atsiskaitymai – tai atsiskaitymai, kuriems reikalingos bankinės institucijos išduotos kreditinės (arba debetinės) kortelės. Nesvarbu ar atsiskaitymas atliekamas internetu, ar kortele sumokant už prekes parduotuvėje, jis vykdomas remiantis tokia pačia schema: vartotojas, norintis sumokėti pardavėjui, naudojasi pardavėjo informacinėje sistemoje esančiu atsiskaitymų moduliu, kuris pagal mokėtojo įvestus duomenis ir įrašus duomenų bazėje sugeneruoja mokėjimo nurodymo pranešimą, kurį šifruotu SSL ryšiu perduoda į „mokėjimų vartus“. „Mokėjimų vartai“ yra tarptautinių organizacijų (VISA, MASTERCARD) el. komercijai teikiama paslauga, kuri atsakinga už mokėjimo nurodymo duomenų šifravimą ir perdavimą būtent tam bankui, kurio išduota kortele atsiskaitė pirkėjas. Bankas gavęs tokį mokėjimo nurodymą ir patikrinęs duomenis atlieka pinigų pervedimą, o vartotojui ir pardavėjui grąžiną tai patvirtinantį pranešimą. [CL08]

2.2. Atsiskaitymai per *Paypal* sistemą

Paypal elektroninių atsiskaitymų sistema pagrįsta laisvai prieinamais standartais, kuriuose apibrėžiami Web servisai, SOAP protokolas, WSDL web servisų aprašymo kalba, XML schemos apibrėžimo kalba XSD. Šių paslaugų (servisų) integraciją į konkrečią svetainę prieinama visiems, Paypal suteikia galimybę naudotis savo web servisais ir naudojantis jais atlikti elektroninius atsiskaitymus. Kaip ir daugelis web servisų, Paypal SOAP yra daug sudedamųjų dalių turinti sistema, kurios struktūra pavaizduota 11 pav.:



11 pav. Paypal SOAP pranešimų schema [PSA09]

Objektiškai orientuotame modelyje SOAP užklausų ir atsakymų interfeisui galima pateikti bet kokios programavimo kalbos objektus, nes jie generuojami pagal Paypal pateiktas WSDL ir XSD schemas, kurios apibrėžia pranešimų struktūrą. Žemiau pateiktas pavyzdinis Paypal SOAP užklausos pranešimas.

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:xsi= "  http://www.w3.org/2001/XMLSchema-instance"
     xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
     xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
><SOAP-ENV:Header>
     <RequesterCredentials xmlns="urn:ebay:api:PayPalAPI">
        <Credentials xmlns="urn:ebay:apis:eBLBaseComponents">
           <Username>api_username</Username>
           <Password>api_password</Password>
         <Signature/>
         <Subject/>
       </Credentials>
    </RequesterCredentials>
</SOAP-ENV:Header>
<SOAP-ENV:Body>
    <specific_api_name_Req xmlns="urn:ebay:api:PayPalAPI">
       <specific_api_name_Request>
          <Version xmlns=urn:ebay:apis:eBLBaseComponents">service_version
          </Version>
          <required_or_optional_fields xsi:type="some_type_here">data
          </required_or_optional_fields>
       </specific_api_name_Request>
    </specific_api_name_Req>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Pranešimas sudarytas iš dviejų pagrindinių dalių: pirmoji skirta identifikuoti vartotojui, o antrojoje formuojama užklausa.

Atsako struktūros pavyzdys:

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope
     xmlns:SOAP-ENV= "http://schemas.xmlsoap.org/soap/envelope/"
     xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:xsd="http://www.w3.org/2001/XMLSchema"
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xmlns:cc="urn:ebay:apis:CoreComponentTypes"
     xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
     xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/12/secext"
     xmlns:ebl="urn:ebay:apis:eBLBaseComponents"
     xmlns:ns="urn:ebay:api:PayPalAPI">
     <SOAP-ENV:Header>
        <Security
           xmlns="http://schemas.xmlsoap.org/ws/2002/12/secext"
           xsi:type="wsse:SecurityType"
        />
        <RequesterCredentials xmlns="urn:ebay:api:PayPalAPI"
           xsi:type="ebl:CustomSecurityHeaderType">
           <Credentials
              xmlns="urn:ebay:apis:eBLBaseComponents"
              xsi:type="ebl:UserIdPasswordType"
   />
  </RequesterCredentials>
</SOAP-ENV:Header>
<SOAP-ENV:Body id="_0">
  <specific_api_name_Response xmlns="urn:ebay:api:PayPalAPI">
     <Timestamp xmlns="urn:ebay:api:PayPalAPI"> dateTime_in_UTC/GMT
     </TIMESTAMP>
     <Ack xmlns="urn:ebay:apis:eBLBaseComponents">Success</Ack>
     <Version xmlns="urn:ebay:apis:eBLBaseComponents">
        serviceVersion
     </Version>
     <CorrelationId xmlns="urn:ebay:apis:eBLBaseComponents">
        applicationCorrelation
     </CorrelationID>
              <Build xmlns="urn:ebay:apis:eBLBaseComponents">
                 api_build_number
              </Build>
              <elements_for_specific_api_response> data
              </elements_for_specific_api_response>
           </specific_api_name_Response>
        </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

Tikslius kiekvieno pranešimo lauko aprašymus galima rasti programuotojo dokumentacijoje. [PSA09]. Dėl vartotojams pateiktų XSD ir WSDL schemų nekyla problemų dėl kiekvienos unikalios sistemos XML pranešimų standartizacijos.

2.3. Modelių saugumo problemos

2.3.1. Transakcijai atlikti reikalingų mokėtojo duomenų aspektas

Vienas iš svarbiausių elektroninės transakcijos saugumo užtikrinimo klausimų yra kokie mokėtoją identifikuojantys duomenys yra privalomi, norint sėkmingai įvykdyti pervedimą, ir ar tie duomenys yra tikrai nepasiekiami tretiesiems (neįgaliotiems) asmenims. Šiuo metu didžioji dalis interneto prekiautojų finansinius pavedimus iš VISA ir MASTERCARD kreditinių kortelių turėtojų sąskaitų vykdo internetinės parduotuvės duomenų įvedimo formoje užpildę šiuos duomenis:

1. Kortelės savininko vardą, pavardę ir gyvenamosios vietos adresą.
2. Kortelės numerį ir galiojimo datą.
3. Kortelės saugumo kodą (užrašytą antrojoje atsiskaitymo kortelės pusėje).

Tačiau šie duomenys nėra tokie slapti, kaip galėtų atrodyti iš pirmo žvilgsnio: asmens gyvenamosios vietos adresą ir kortelės galiojimo datą galima nesunkiai surasti iš banko gaunamoje korespondencijoje, o saugos kodą galima sėkmingai pastebėti žmogui naudojantis atsikaitymo kortele (pvz., mokant kortele parduotuvėje). Turint tokį duomenų rinkinį, galima be kortelės savininko žinios atsiskaityti už prekes ar paslaugas internetu. Žalą patiriantis asmuo nėra specialiai informuojamas apie pinigų nuskaitymus, nes niekas nežino, kad tai daro ne pats kortelės turėtojas. Mokėjimo kortelę jis turi su savimi ir toliau ja sėkmingai naudojasi, o apie pavogtus pinigus jis gali sužinoti praėjus pakankamai ilgam laiko tarpui (pvz., gavęs mėnesinę banko ataskaitą arba dar vėliau). Norint ištaisyti šią saugumo spragą reikalingi papildomi asmenį identifikuojantys duomenys (pvz., elektroninio parašo sertifikatas).

2.3.2. SSL/TLS saugumo problemos

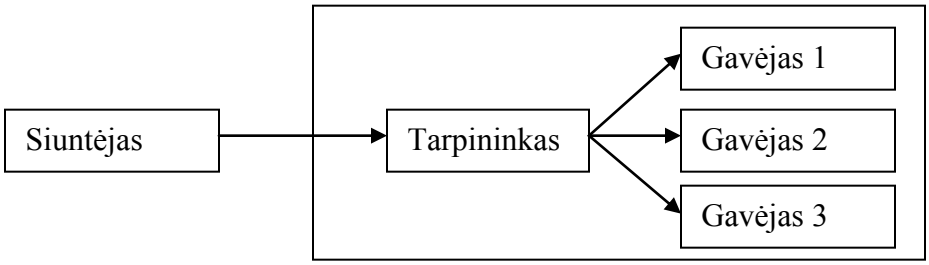
Duomenų šifravimas yra geras sprendimas norint užtikrinti siunčiamos informacijos saugumą, tačiau tai tik saugumo užtikrinimo proceso dalis. SSL/TLS yra transporto lygmens duomenų šifravimo protokolas, t.y. jo pagalba duomenys tampa neprieinami pakankamai žemame informacijos perdavimo kompiuterių tinklais OSI modelio sluoksnyje. Tačiau būtina atsižvelgti ir į aukštesnius šio modelio sluoksnius, kuriuose apdorojama iš transporto sluoksnio gauta informacija, kuri jau nebėra (arba vis dar nėra) šifruota, todėl atsiranda galimybė šią informaciją perimti. O jei tarp informacijos siuntėjo ir gavėjo yra vienas ar daugiau tarpinių taškų, kuriuose informacija dalinai

apdorojama ir siunčiama toliau, ji tampa pažeidžiama kiekviename iš jų. SSL/TLS užtikrina informacijos saugumą tik duomenų paketų siuntimo metu, tačiau tarpiniuose duomenų perdavimo taškuose paketus apdorojanti programinė įranga veikia ir aukštesniuose OSI modelio sluoksniuose, kuriuose SSL/TLS duomenų saugumo neužtikrina. Taip pat, šis duomenų šifravimo protokolas negali apsaugoti duomenų, jei buvo įsilaužta į serverį – jei duomenys nebuvo papildomai šifruoti, jie buvo pilnai prieinami įsilaužėliui. Dėl šių priežasčių yra būtina stipresnė duomenų apsauga, ypač aukštesniuose nei transporto OSI modelio sluoksniuose. [GKF06]

3. SIŪLOMAS ELEKTRONINIŲ ATSISKAITYMŲ MODELIS

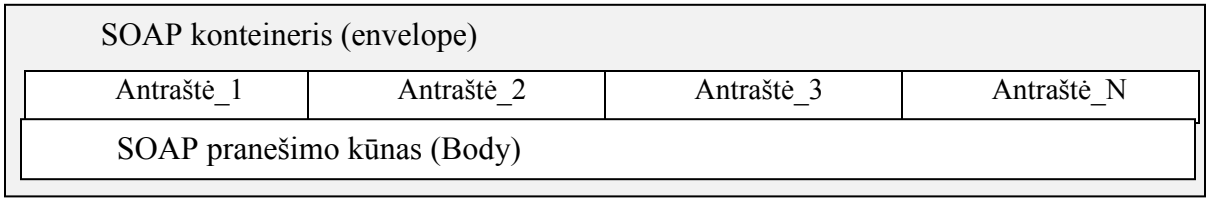
3.1. SOAP protokolas

SOAP (*Simple Object Access Protocol*) yra tinklinių paslaugų (*Web Services*) struktūrizuotų duomenų apsikeitimo protokolas, kurio pagrindas yra XML kalba. Jis skirtas perduoti duomenis tarp pradinio ir galutinio taškų. SOAP pranešimas yra XML pavidalo dokumentas, kurio struktūrą nustato duomenimis besikeičiančios šalys. SOAP pranešimų pavyzdžiai pateikti 4.2. skyrelyje. SAOP yra aukšto lygmens (aukštesnio nei OSI modelio aplikacijų sluoksnio) duomenų perdavimo protokolas, todėl SOAP pranešimai gali būti perduodami bet kuriuo aplikacijų lygmens protokolu (HTTP, net ir FTP). Dažnai SOAP yra naudojamas kartu su SSL/TLS. Pagrindinis to privalumas yra tas, kad SSL/TLS užtikrina informacijos perdavimo tinklu saugumą, o SOAP – informacijos saugumą, apdorojant iššifruotus iš tinklo gautus pranešimus tarpine programine įranga (12 pav.). Toks derinys užtikrina ne tik duomenų transporto, bet ir jų tarpinio apdorojimo saugumą.



12 pav. SOAP pranešimo apdorojimas

SOAP pranešimas susideda iš konteinerio (SOAP *envelope)*, antraščių (*Header*) ir kūno (*Body*). (13 pav.). *Envelope* yra šaknine pranešimo žymė, antraštės yra naudojamos protokolo išplėtimams, kuriuose nurodomi papildomi patikimumo, saugumo ir kt. nustatymai.



13 pav. SOAP pranešimo sandara

Pagrindiniai SOAP privalumai yra lengvesnė komunikacija per *proxy* serverius ir ugniasienes, galimybė naudoti įvairius duomenų perdavimo protokolus, pranešimai yra nepriklausomi nuo naudojamos platformos ar programavimo kalbos. [W3C07]

3.2. SOAP saugumo priemonės

SOAP protokolu bendraujančios esybės keičiasi XML kalbos pranešimais, kuriems yra taikomos šios informacijos saugumo priemonės:

1. Pranešimo šifravimas – dalis XML pranešimo gali būti užšifruota naudojant XML šifravimą, aprašytą kalbos šifravimo standarte. Šifruotų duomenų pradžią žymi <xenc:EncryptedData> žymė, pranešimas taip pat visada turi <xenc:DecryptionInfo> žymę, kurioje saugoma informacija reikalinga pranešimo iššifravimui.
2. Skaitmeninis parašas. Į SOAP pranešimą galima įdėti ir skaitmeniniais duomenimis besikeičiančių esybių parašus, kuriais patvirtinama kiekvienos jų tapatybė.

Kadangi perduodamas pranešimas šifruojamas/dešifruojamas OSI modelio aplikacijų sluoksnyje, kad ir kiek tarpinių taškų būtų perdavimo kelyje, informacija bus prieinama tik galutiniam jos gavėjui. Taip SOAP protokolas išsprendžia vieną iš pagrindinių SSL/TLS saugumo problemų – perduodamų duomenų saugumą aukštesniuose nei transporto OSI modelio sluoksniuose. [W3C07]

3.3. Elektroninio parašo infrastruktūra

Kad būtų užtikrintas pirkėjo ir pardavėjo transakcijai pateiktų duomenų tikslumas, jie gali būti pasirašyti abiejų pusių elektroniniais parašais. Šiais parašais šalys patvirtina, kad tai, kas parašyta mokėjimo nurodyme, yra teisinga ir įsipareigoja vykdyti savo pareigas.

Vykdomas standartinis duomenų pasirašymo elektroniniu parašu procesas: generuojama pasirašomo dokumento duomenų santrauka, ji užšifruojama pasirašančiojo privačiuoju šifravimo raktu ir pridedama prie pradinio dokumento. Į parašą įdedamas ir pasirašiusiojo skaitmeninis sertifikatas – liudijimas, kad šifravimo raktų pora (viešasis ir privatusis) priklauso konkrečiam asmeniui. Gavėjas, gavęs tokį duomenų paketą, atšifruoja duomenų santrauką naudodamas pasirašiusiojo sertifikate rastą viešąjį šifravimo raktą. Norėdamas įsitikinti, ar pasirašiusio asmens sertifikatas galioja, gavėjas kreipiasi į sertifikatų centrą, išdavusį sertifikatą pasirašiusiajam, ir gauna atsakymą apie sertifikato statusą. Jei sertifikatas galioja, gavėjas pats sukuria gauto dokumento santrauką ir palygina ją su atsiųsta ir iššifruota santrauka. Jei santraukos sutampa - gautas dokumentas yra toks, koks buvo pasirašytas. Priešingu atveju – dokumentas buvo pakeistas po pasirašymo.

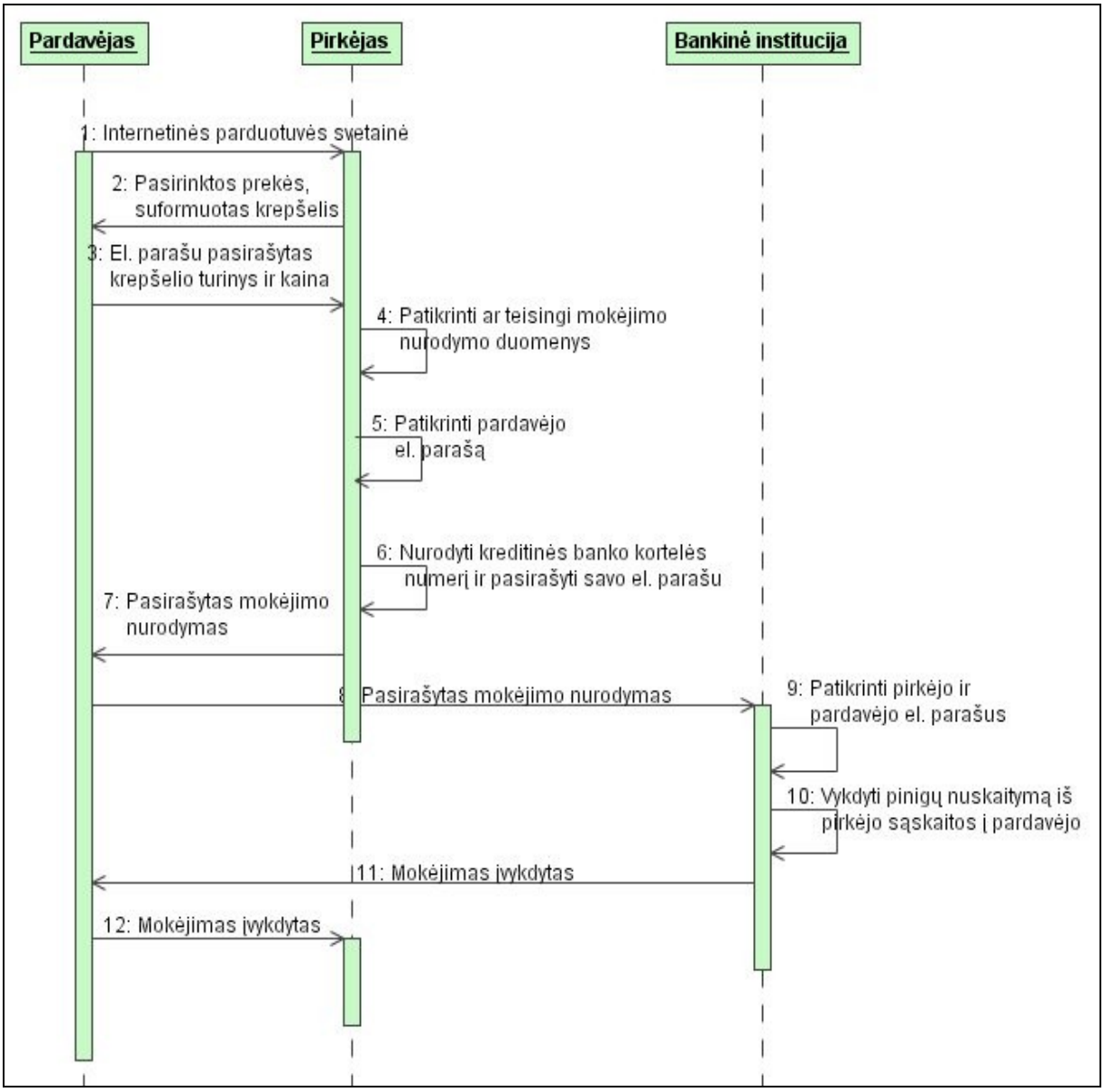
Elektroninio parašo sukūrimui reikalingas ne tik skaitmeninis sertifikatas, bet ir saugi parašo kūrimo įranga. Šią įrangą vartotojams suteikia pasirinktas sertifikatų centras, kuris sudarytą asmens sertifikatą ir privatųjį raktą įrašo į laikmeną – saugią elektroninio parašo kūrimo įrangą. Ši įranga ir yra atsakinga už elektroninio parašo sukūrimą konkrečiam dokumentui, naudojant privatųjį raktą ir įterpiant į kiekvieną parašą asmens skaitmeninio sertifikato duomenis. [Und08]

3.4. Siūlomo sprendimo aprašymas

Siūlomo sprendimo idėja iš dalies remiasi dabar naudojamais duomenų perdavimo ir šifravimo protokolais (SSL/TLS ir SOAP), kurių suteikiamam saugumui pagerinti dar pasitelkiama elektroninio parašo infrastruktūra. Trumpai tai galima pavadinti elektroniniais atsiskaitymais, kuriuose šalių tapatybei patvirtinti naudojamas elektroninio parašo sertifikatas.

Procese dalyvauja 4 šalys: pirkėjas, pardavėjas, bankinė institucija ir skaitmeninio sertifikavimo centras. Pirkėjas išsirenka norimas pardavėjo platinamas prekes ir paslaugas, suformuoja užsakymo krepšelį. Jo turinį ir kainą pardavėjas pasirašo savo el. parašu, taip patvirtindamas, kad pirkėjas gaus būtent tokias prekes, kurias jis užsisakė ir už jas mokės būtent

tiek, kiek nurodyta sąskaitoje. Pirkėjas, gavęs pardavėjo pasirašytą sąskaitą, visų pirma turi galimybę patikrinti, pardavėjo el. parašą ir sertifikato galiojimą. Tam jis kreipiasi į skaitmeninio sertifikavimo centrą, iš kurio gauna atsaką apie pardavėjo skaitmeninį sertifikatą. Jei sertifikato galiojimas nepasibaigęs ir pardavėjo pateiktos sąskaitos duomenys yra teisingi, pirkėjas į formą įrašo savo banko sąskaitos numerį ir visą dokumentą pasirašo savo el. parašu, taip patvirtindamas, kad pateiktoje sąskaitoje įrašyta pinigų suma bus pervesta iš pirkėjo banko sąskaitos į pardavėjo. Abiejų šalių pasirašytą dokumentą pardavėjas pateikia bankinei institucijai, kuri patikrinusi šalių el. parašus ir sertifikatų galiojimą perveda pinigus. Tokio atsiskaitymų modulio veiksmų sekų diagrama pateikta 14 pav.



14 pav. Elektroninių atsiskaitymų modulio veiksmų sekų diagrama

Elektroninių atsiskaitymų modelio saugumas susideda iš keleto dalių: atsiskaitymui įvykdyti reikalingos informacijos ir duomenų perdavimo slaptumo. Visų pirma – transakcijai įvykdyti reikalinga informacija. Remiantis modelio aprašymu, pardavėjui suformavus ir el. parašu pasirašius sąskaitą, pirkėjas į gautą formą įrašo tik savo kreditinės kortelės numerį ir dokumentą pasirašo savo el. parašu. Kreditinės kortelės numeris nėra slapta informacija, netgi jį atskleidus, žalos bet kuriai transakcijoje dalyvaujančiai pusei pavyktų išvengti. Žinant tik kortelės numerį jokie pinigų nuskaitymai neįmanomi. Kortelės turėtojas šiame procese identifikuojamas pagal jo elektroninį parašą, o jį sukurti gali tik pats asmuo turėdamas parašo kūrimo įrangą ir žinodamas atitinkamus slaptažodžius. El. parašo kūrimo įrangos vagystės atveju vartotojas pasiges šios įrangos. Todėl,

lyginant su dabar naudojamais atsiskaitymais, kai transakcijai įvykdyti užtenka žinoti keletą skaičių, parašytų ant kortelės (pati kortelė nereikalinga), pasiekiamas žymiai didesnis saugumas. Taip pat iš abiejų pusių pasirašyto dokumento išsiaiškinus tiek vartotoją, tiek jo sąskaitą identifikuojančius duomenis, jie yra beverčiai norint suklastoti mokėjimo nurodymą.

Duomenų perdavimo saugumui užtikrinti naudojamas SOAP protokolas, kurio pranešimo fragmentai, talpinantys transakcijai reikalingus duomenis, yra šifruojami 3.2 skyrelyje aprašytomis priemonėmis. Todėl duomenys tampa prieinami tik mokėtojui ir bankinei institucijai, nors perdavimo procese dalyvauja ir pardavėjas (galimas atvejis, kad ir daugiau tarpininkų).

Tai du pagrindiniai saugumo aspektai, kuriuos užtikrina siūlomas modelis. Tai nėra visa saugumo koncepcija, tačiau kiti saugumo užtikrinimo principai lieka nepakitę, t.y. anksčiau naudotos saugumo užtikrinimo procedūros (aprašytos magistrinio darbo literatūros apraše) papildomos šiais dviem aspektais ir bus naudojamos naujame elektroninių atsiskaitymų modelyje.

3.6. Teisiniai aspektai

Kad modelis būtų visiškai korektiškas, jis turi neprieštarauti šiuo metu galiojantiems įstatymams. Toliau aprašomi teisiniai aspektai yra daugiausiai susiję su elektroninio parašo naudojimu.

Pagal Lietuvos Respublikos elektroninio parašo įstatymą (Žin., 2000, Nr. 61-1827) saugus el. parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu sertifikatu, el. duomenims turi tokią pat teisinę galią kaip parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme. Tokie parašai turi būti techniškai korektiški, t.y. turi būti korektiškas skaitmeninis parašas, korektiška sertifikatų seka, nė vienas šios sekos sertifikatas neturi būti atšauktas, t.t. [Und08]

Visų pirma, sąskaitą apmokėjimui (su nurodytomis pirkėjo išsirinktomis prekėmis ir jų kainomis) savo el. parašu pasirašo pardavėjas, taip įsipareigodamas, gavęs užmokestį, pirkėją aprūpinti anksčiau minėtomis prekėmis. Jei pirkėją pasiekia ne tokios prekės, kokias jis užsisakė, pardavėjo el. parašu pasirašyta sąskaita gali būti panaudota kaip įrodymas teisme.

Pirkėjas, gavęs pardavėjo pasirašytą sąskaitą, atlikęs norimas patikrinimo procedūras, ją taip pat pasirašo savo el. parašu, taip patvirtindamas, kad jis sutinka, kad bankinė institucija sąskaitoje nurodytą pinigų sumą pervestų iš pirkėjo banko sąskaitos į pardavėjo. Kilus ginčams pasirašyta sąskaita gali būti panaudota kaip įrodymas teisme.

Į bankinę instituciją patenka abiejų šalių pasirašytas mokėjimo nurodymas, t.y. pirkėjas sutinka sumokėti, o pardavėjas – pateikti pirkėjui jo išsirinktas prekes. Atsiradus ginčytinoms

situacijoms visada turi būti atsižvelgiama į abiejų šalių pasirašytą mokėjimo nurodymą ir nustatoma, kuri šalis jį pažeidžia.

4. ELEKTRONINIŲ ATSISKAITYMŲ MODULIO REIKALAVIMAI

4.1. Funkciniai modulio reikalavimai

4.1.1. Pirkinių krepšelio duomenų pasirašymas ir perdavimas klientui

3 lentelėje pateikiami užduoties „pirkinių krepšelio duomenų pasirašymo ir perdavimo klientui“ reikalavimai.

3 lentelė. „Pirkinių krepšelio duomenų pasirašymo ir perdavimo klientui“ reikalavimai

Užduotis	Pradiniai duomenys	Rezultatai
Pirkinių krepšelio duomenų pasirašymas ir perdavimas klientui	1. Unikalūs pirkėjo pasirinktų prekių identifikatoriai. 2. Unikalus pirkėjo identifikatorius. 3. Pardavėjo el. parašo sertifikatas ir saugi parašo kūrimo įranga.	Mokėjimo nurodymas (XML pranešimas), kuriame yra: 1. Pirkėjo pasirinktų prekių pavadinimai, kodai ir kaina. 2. Pirkėjo vardas, pavardė, unikalus identifikatorius, gyvenamosios vietos adresas. 3. Pardavėją identifikuojantys duomenys, banko sąskaitos numeris. 4. Pardavėjo el. parašas.

4.1.2. Pirkinių krepšelio duomenų pasirašymas ir perdavimas pardavėjui

4 lentelėje pateikiami užduoties „pirkinių krepšelio duomenų pasirašymo ir perdavimo pardavėjui“ reikalavimai.

4 lentelė. „Pirkinių krepšelio duomenų pasirašymo ir perdavimo klientui“ reikalavimai

Užduotis	Pradiniai duomenys	Rezultatai
Pirkinių krepšelio duomenų pasirašymas ir perdavimas pardavėjui	1. Iš pardavėjo gautas mokėjimo nurodymas; 2. El. parašo tikrinimui ir	Mokėjimo nurodymas, kuris buvo papildytas: 1. Pirkėjo kreditinės kortelės

	pasirašymui skirtas vartotojo interfeisas; 3. Pirkėjo kreditinės kortelės nr.	numeriu; 2. Pirkėjo el. parašu.

4.1.3. Mokėjimo nurodymo perdavimas bankui

5 lentelėje pateikiami užduoties „mokėjimo nurodymo perdavimas bankui“ reikalavimai.

5 lentelė. „Mokėjimo nurodymo perdavimo bankui“ reikalavimai

Užduotis	Pradiniai duomenys	Rezultatai
Mokėjimo nurodymo perdavimas bankui	1. Mokėjimo nurodymas patirtintas pirkėjo ir pardavėjo el. parašais.	1. Mokėjimo nurodymas patirtintas pirkėjo ir pardavėjo el. parašais perduotas į reikiamą banką.

4.1.4. Bankinės transakcijos vykdymas

6 lentelėje pateikiami užduoties „mokėjimo nurodymo perdavimas bankui“ reikalavimai.

6 lentelė. „Bankinės transakcijos įvykdymo“ reikalavimai

Užduotis	Pradiniai duomenys	Rezultatai
Bankinės transakcijos vykdymas	1. Mokėjimo nurodymas patirtintas pirkėjo ir pardavėjo el. parašais.	1. Patikrinti abiejų transakcijoje dalyvaujančių šalių el. parašai. 2. Įvykdyta pinigų transakcija. 3. Išsiųstas transakcijos įvykdymo patvirtinimas.

4.2. Nefunkciniai modulio reikalavimai

4.2.1. Operacinės sistemos naudojimo reikalavimai

Modulio tarnybinėje stotyje naudojama Microsoft WINDOWS 2003 SERVER arba naujesnis analogiškas produktas operacinė sistema.

4.2.2. Sąveikos su duomenų bazėmis reikalavimai

Duomenys saugomi Microsoft SQL Server 2003 (arba naujesnėje analogiško veikimo) duomenų bazėje. Duomenų mainai vykdomi LINQ TO SQL technologijų pagalba.

4.2.3. Dokumentų mainų reikalavimai

Dokumentų mainai vykdomi žiniatinklio paslaugų (*web services*) pagalba, duomenims siųsti naudojamas SOAP protokolas. Konfidenciali informaciją, kuri gali būti panaudota trečiųjų šalių, koduojama.

4.2.4. Patikimumo reikalavimai

Modulis bus laikomas patikimu, jei gebės atlikti jam keliamas užduotis, trikį suprasime kaip modulio gebėjimo praradimą atlikti užduotį. Kuriamo modulio patikimumas suprantamas kaip trikių skaičius per laiko vienetą. Kadangi modulis dirba su ypač svarbiais duomenimis ir vykdo pinigines transakcijas, jis turi būti pilnai ištestuotas, kol bus pasiektas nulinis kritinių trikių (kurių metu įvyksta nepataisomos finansinės klaidos) skaičius per metus.

4.2.5. Robastiškumo reikalavimai

Trikių valdymui turi būti naudojamas transakcijų mechanizmas, kuris, įvykus trikiui, atšauks prieš tai padarytus veiksmus ir grąžins pakeistus duomenis į pradinę būseną. Taip pat privalomas ypač tikslus ir patikimas žurnalizavimo mechanizmas ir ilgalaikis žurnalizuotų įvykių saugojimas duomenų bazėje.

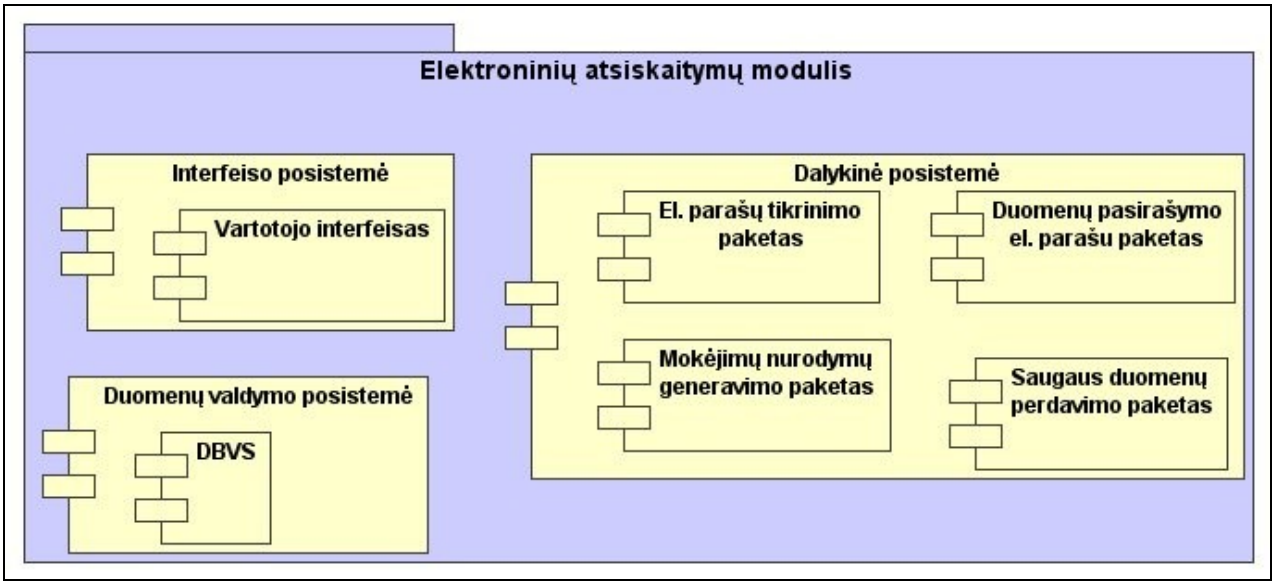
4.2.6. Našumo reikalavimai

Modulis, vienu metu atlikdamas 1000 užduočių, neturi naudoti daugiau kaip 5% tarnybinės stoties resursų. Mokėjimo nurodymas turi būti generuojamas ir pasirašomas ne ilgiau nei per 5 sekundes, o pirkėjo pasirašytas mokėjimo nurodymas turi būti apdorojamas ir išsiunčiamas į banką ne ilgiau nei per 7 sekundes.

5. SAUGIŲ ELEKTRONINIŲ ATSISKAITYMŲ MODULIO PROJEKTAS

5.1. Modulio dekompozicija

Elektroninių atsiskaitymų modulio dekompozicija paketais pateikta 15 pav.



15 pav. Elektroninių atsiskaitymų modulio dekompozicija

5.1.1. Elektroninių atsiskaitymų modulis::Interfeiso posistemė

Šioje posistemėje yra tik vienas paketas: vartotojo interfeisas

Reikalavimai šiam paketui:

1. Populiariausių kalbų palaikymas, galimybė lengvai pridėti naują kalbą į vartotojo interfeisą, dialogų tekstų saugojimas duomenų bazėje.
2. Informatyvus mokėjimo nurodymo peržiūros ir el. parašų tikrinimo rezultatų peržiūros interfeisas.
3. Užduočių vykdymo progreso rodymas vartotojui.
4. Informatyvūs klaidų pranešimai, padedantys išvengti panašaus tipo klaidų ir pateikiantys instrukcijas, kaip elgtis įvykus klaidai.

5.1.2. Elektroninių atsiskaitymų modulis::Dalykinė posistemė

Posistemėje yra keturi paketai:

- el. parašų tikrinimo paketas;
- mokėjimo nurodymo generavimo paketas;
- duomenų pasirašymo el. parašu paketas;
- saugaus duomenų perdavimo paketas.

5.1.2.1. Elektroninių atsiskaitymų modulis::Dalykinė posistemė::El. parašų tikrinimo paketas

Reikalavimai šiam paketui:

1. Populiariausių el. parašo santraukų algoritmų palaikymas (SHA1, RIPEMD160, SHA224, SHA256, SHA384, SHA512, WHIRLPOOL).
2. Galimybė tikrinti sertifikatų galiojimą OCSP protokolu ir naudojant atšauktų sertifikatų sąrašus (CRL).
3. Skirtingų parašo taisyklių palaikymas.

5.1.2.2. Elektroninių atsiskaitymų modulis::Dalykinė posistemė::Mokėjimo nurodymo generavimo paketas

Reikalavimai šiam paketui:

1. Galimybė keisti mokėjimo nurodymo formą ir atributus;
2. Galimybė pridėti papildomą informaciją prie pasirašyto mokėjimo nurodymo.

5.1.2.3. Elektroninių atsiskaitymų modulis::Dalykinė posistemė::Duomenų pasirašymo el. parašu paketas

Reikalavimai šiam paketui:

1. Galimybė pasirašymui naudoti tiek stacionarią, tiek ir mobilią elektroninio parašo infrastruktūrą;
2. Dviejų tipų pasirašymo procedūros: pardavėjo – sugeneravus mokėjimo nurodymą, naudojant pardavėjo saugaus parašo kūrimo įrangą (SSCD) ir sertifikatą; pirkėjo – pirkėjui panorus pasirašyti mokėjimo nurodymą ir pasirinkus parašo infrastruktūrą.

5.1.2.4. Elektroninių atsiskaitymų modulis::Dalykinė posistemė::Saugaus duomenų perdavimo paketas

Reikalavimai šiam paketui:

1. Duomenų perdavimas koduotu ryšiu naudojant SSL duomenų perdavimo protokolą.

5.1.3. Elektroninių atsiskaitymų modulis::Duomenų valdymo posistemė

Paketas dekomponuojamas į vieną paketą:

- DBVS

Reikalavimai šiam paketui:

1. Efektyvūs ir patikimi duomenų šifravimo algoritmai, užtikrinantys duomenų saugumą, pvz. Cipher Block Chaining (CBC);
2. Galioja visi standartiniai reliacinėms DBVS keliami reikalavimai.

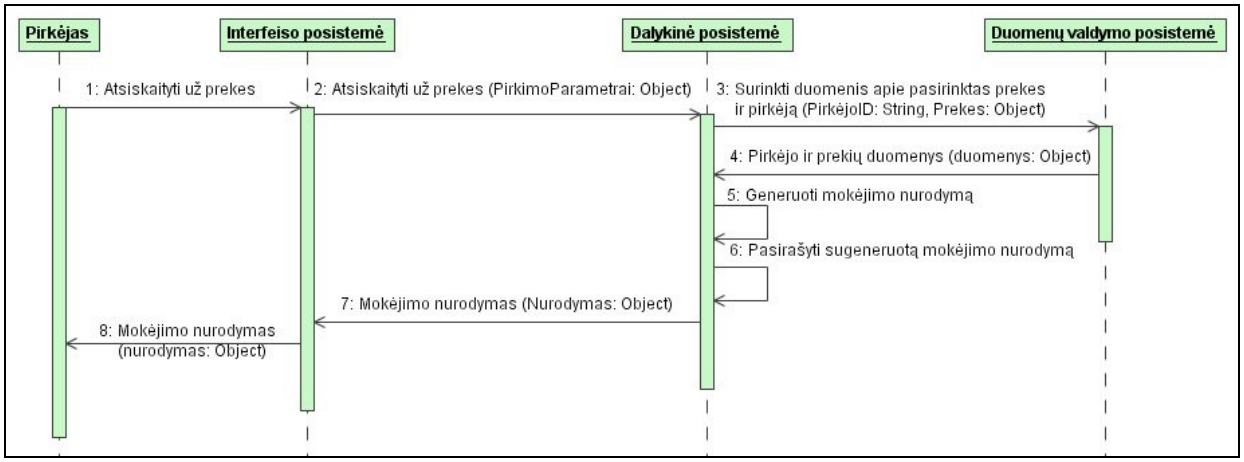
5.2. Modulio architektūra

Nors atsiskaitymo procesas gana vientisas, tačiau jį galima suskaidyti į keturias viena paskui kitą sekančias užduotis, kurios sujungtos į visumą ir sudaro visą elektroninio atsiskaitymo procesą. Atsiskaitymo proceso inicijavimu laikysiu pareikštą pirkėjo norą susimokėti už išsirinktas paslaugas (paspaustą mygtuką „atsiskaityti“).

5.2.1. Užduotys ir jų vykdymo scenarijai

5.2.1.1. Pirkinių krepšelio duomenų pasirašymas ir perdavimas klientui

Pirkinių krepšelio duomenų pasirašymo ir perdavimo klientui užduoties sekų diagrama pateikiama 16 pav.



16 pav. Pirkinių krepšelio duomenų pasirašymo ir perdavimo klientui užduoties sekų diagrama

Tikslas: pateikti pirkėjui tinkamai suformuotą ir pardavėjo el. parašu pasirašytą mokėjimo nurodymą.

„Prieš sąlygos“: klientas jau yra registruotas sistemoje, duomenų bazėje saugomi jo asmeniniai duomenys, tokie kaip vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, taip pat duomenų bazėje yra reikiami siūlomų prekių ar paslaugų duomenys (kaina, dydis, aprašymas)

„Po sąlygos“: klientas gavo mokėjimo nurodymą, kuriame nurodyta visos jo pasirinktos prekės ir jų kainos, o dokumentas pasirašytas pardavėjo el. parašu.

Pirminis agentas: pirkėjas.

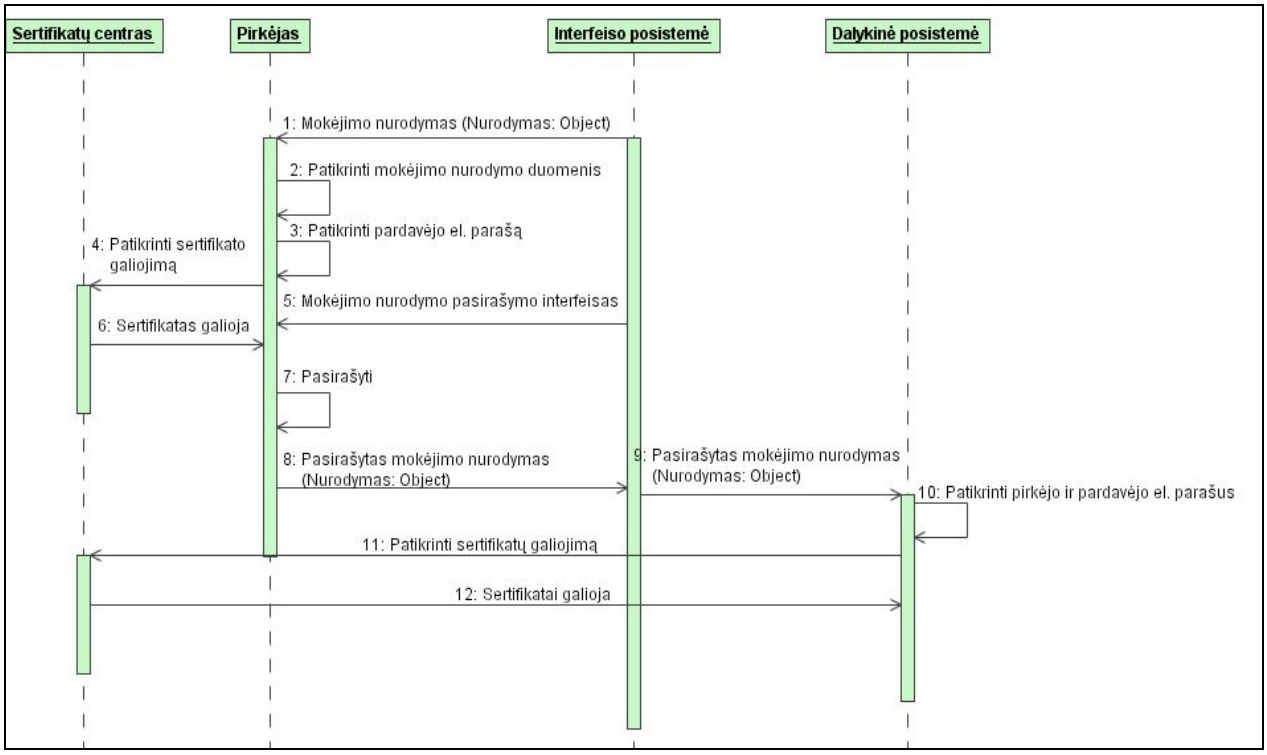
Antriniai agentai: elektroninių atsiskaitymų modulis.

Scenarijus: užduoties vykdymą inicijuoja pirkėjas, panoręs atsiskaityti už prekes ar paslaugas. Tai iššaukia tokius sistemos veiksmus:

1. Surinkti visus turimus duomenis apie pirkėją (vardą, pavardę, gyvenamosios vietos adresą) pagal unikalų pirkėjo identifikatorių.
2. Surinkti duomenis apie konkretaus pirkėjo pasirinktas prekes (kainą, matmenis, pristatymo laiką) pagal unikalius prekių identifikatorius.
3. Pagal surinktus duomenis sugeneruoti mokėjimo nurodymą.
4. Pasirašyti mokėjimo nurodymą pardavėjo el. parašu.
5. Persiųsti mokėjimo nurodymą pirkėjo peržiurai.

5.2.1.2. Pirkinių krepšelio duomenų pasirašymas ir perdavimas pardavėjui

Pirkinių krepšelio duomenų pasirašymo ir perdavimo pardavėjui užduoties sekų diagrama pateikiama 17 pav.



17 pav. Pirkinių krepšelio duomenų pasirašymo ir perdavimo pardavėjui sekų diagrama

Tikslas: gauti pirkėjo sutikimą, leidžiantį bankui pervesti mokėjimo nurodyme įrašytą sumą iš pirkėjo sąskaitos į pardavėjo. Šį sutikimą atspindi pirkėjo elektroniniu parašu pasirašytas mokėjimo nurodymas.

„Prieš sąlygos“: pardavėjo el. parašu pasirašytas mokėjimo nurodymas pasiekė pirkėją.

„Po sąlygos“: pirkėjo el. parašu pasirašytas mokėjimo nurodymas perduotas pardavėjo elektroninių atsiskaitymų sistemai.

Pirminis agentas: elektroninių atsiskaitymų modulis.

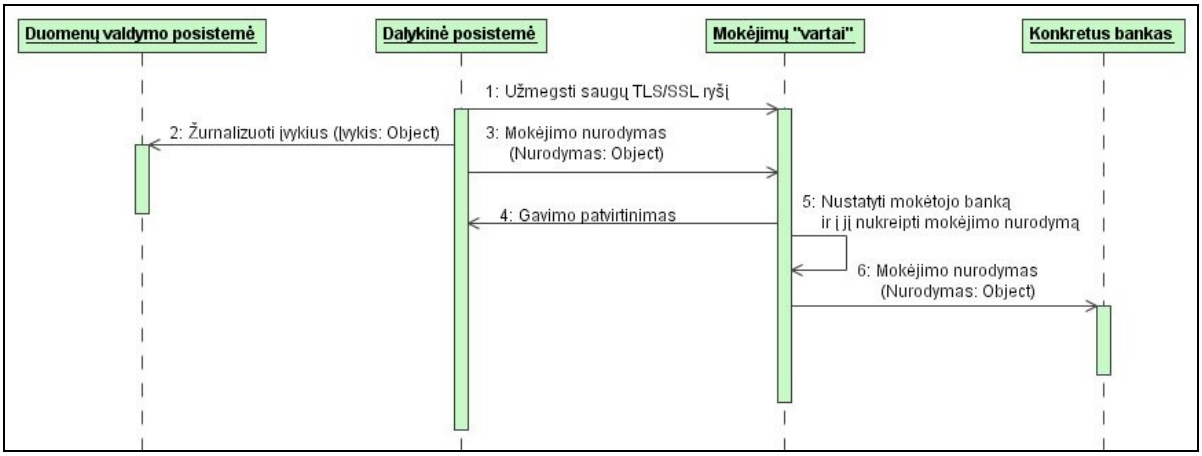
Antriniai agentai: pirkėjas.

Scenarijus:

1. Patikrinti mokėjimo nurodymo duomenis (prekių pavadinimus ir kainas, pirkėjo duomenis).
2. Patikrinti pardavėjo el. parašą, sertifikato galiojimą.
3. Nurodyti kreditinės banko kortelės numerį ir pasirašyti mokėjimo nurodymą el. parašu.
4. Perduoti mokėjimo nurodymą pardavėjo elektroninių atsiskaitymų sistemai.

5.2.1.3. Mokėjimo nurodymo perdavimas bankui

Mokėjimo nurodymo perdavimo bankui užduoties sekų diagrama pateikiama 18 pav.



18 pav. Mokėjimo nurodymo perdavimo bankui užduoties sekų diagrama

Tikslas: saugiu ryšio kanalu perduoti mokėjimo nurodymą mokėtojo bankui.

„Prieš sąlygos“: mokėjimo nurodymas pasirašytas pardavėjo ir pirkėjo el. parašais.

„Po sąlygos“: pirkėjo bankas gavo mokėjimo nurodymą.

Pirminis agentas: elektroninių atsiskaitymų modulis.

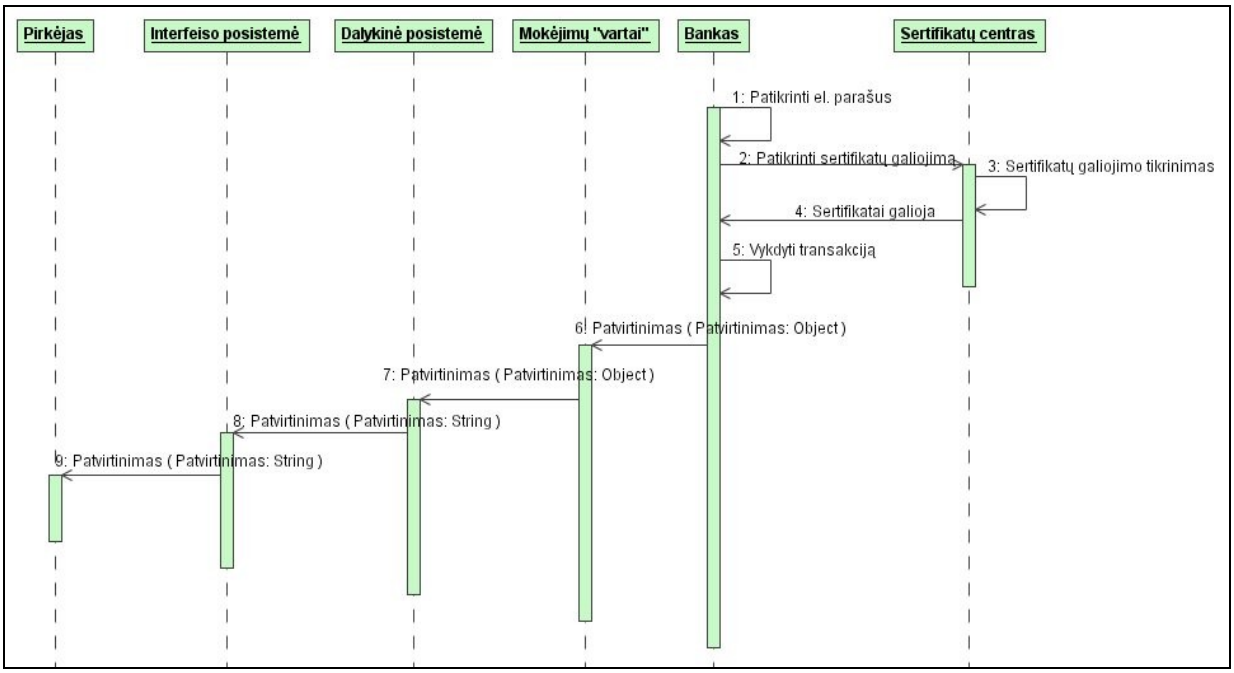
Antriniai agentai: „mokėjimų vartai“, konkretaus banko transakcijų sistema.

Scenarijus:

1. Užmezgamas saugus duomenų perdavimo ryšys su „mokėjimų vartais“.
2. Perduodamas užšifruotas mokėjimo nurodymas.
3. Nustatomas mokėtojo bankas ir užmezgamas saugus duomenų perdavimo ryšys su jo sistema.
4. Perduodamas užšifruotas mokėjimo nurodymas.

5.2.1.4. Bankinės transakcijos vykdymas

Bankinės transakcijos vykdymo užduoties sekų diagrama pateikiama 19 pav.



19 pav. Bankinės transakcijos vykdymo užduoties sekų diagrama

Tikslas: įvykdyti mokėjimo nurodyme įrašytos pinigų sumos pervedimą iš mokėtojo sąskaitos į pardavėjo.

„Prieš sąlygos“: banko transakcijų sistema gavo mokėjimo nurodymą.

„Po sąlygos“: pardavėjas ir mokėtojas informuotas apie įvykdytą transakciją.

Pirminis agentas: banko transakcijų sistema.

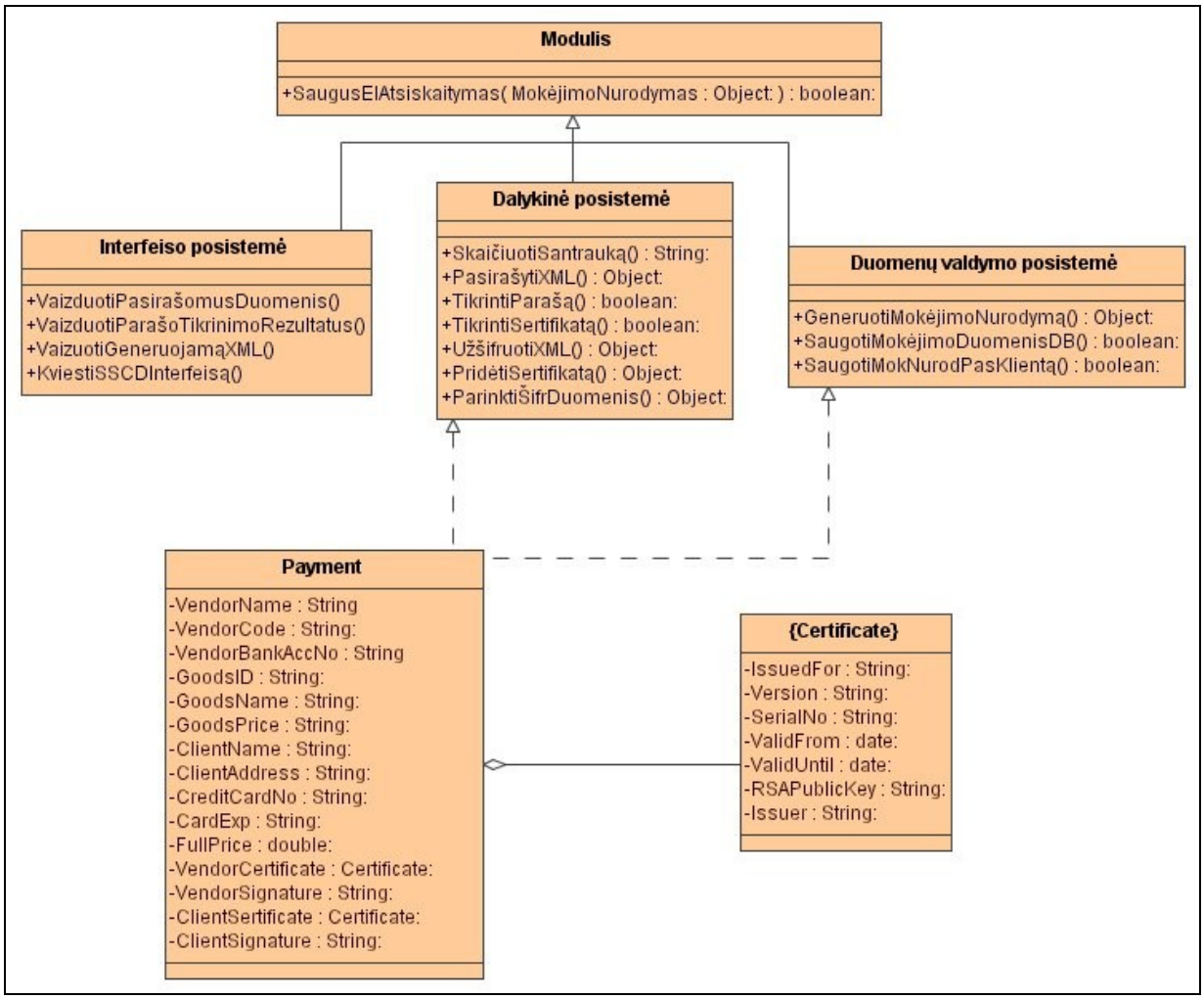
Antriniai agentai: elektroninių atsiskaitymų modulis, pirkėjas

Scenarijus:

1. Patikrinami pirkėjo ir pardavėjo el. parašai ir jų eiliškumas.
2. Patikrinamas pirkėjo ir pardavėjo sertifikatų galiojimas.
3. Vykdomas pinigų pervedimas iš pirkėjo banko sąskaitos į pardavėjo.
4. Išsiunčiamas transakcijos įvykdymo patvirtinimas, kuris per „mokėjimo vartus“ ir pardavėjo elektroninių atsiskaitymų sistemą pasiekia pirkėją.

5.3. Modulio klasių diagrama

20 pav. pateikiama saugių el. atsiskaitymų modulio klasių diagrama.



20 pav. Saugių el. atsiskaitymų modulio klasių diagrama

5.4. Duomenų apsikeitimo su banku pranešimo struktūra

Elektroninių atsiskaitymų modulis informacijos mainams su bankine institucija generuoja XML pranešimą, kurio struktūra pateikta žemiau. XML pranešimo pavyzdys pateiktas 1 priede.

```
<mokej>
    <VendorName> </VendorName>
    <VendorCode></VendorCode>
    <VendorBankAccNo> </VendorBankAccNo>
    <GoodsID></GoodsID>
    <GoodsName> </GoodsName>
    <GoodsPrice></GoodsPrice>
    <ClientName> </ClientName>
    <ClientAddress> </ClientAddress>
    <CreditCardNo></ CreditCardNo >
    <CardExp></ CardExp >
    <FullPrice></FullPrice>
    <VendorCertificate>
        <IssuedFor> </IssuedFor>
        <Version> </Version>
        <SerialNo></SerialNo>
        <ValidFrom></ValidFrom>
        <ValidUntil></ValidUntil>
        <RSAPublicKey>  </RSAPublicKey>
        <Issuer> </Issuer>
    </VendorCertificate>
    <VendorSignature>  </VendorSignature>
    <ClientCertificate>
        <IssuedFor> </IssuedFor>
        <Version> </Version>
        <SerialNo></SerialNo>
        <ValidFrom></ValidFrom>
        <ValidUntil></ValidUntil>
        <RSAPublicKey>  </RSAPublicKey>
```

```
            <Issuer> </Issuer>
        </ClientCertificate>
        <ClientSignature></ClientSignature>
</mokej>
```

Siekiant užtikrinti konfidencialios pirkėjo informacijos saugumą, XML pranešimo žymos <CreditCardNo> ir <CardExp> šifruojamos konkretaus pirkėjo banko viešuoju šifravimo raktu ir tampa prieinamos tik pačiam transakciją vykdančiam bankui. Apie šiose žymose saugomos informacijos svarbą plačiau kalbama 2.3.1 skyrelyje. [Miy04]

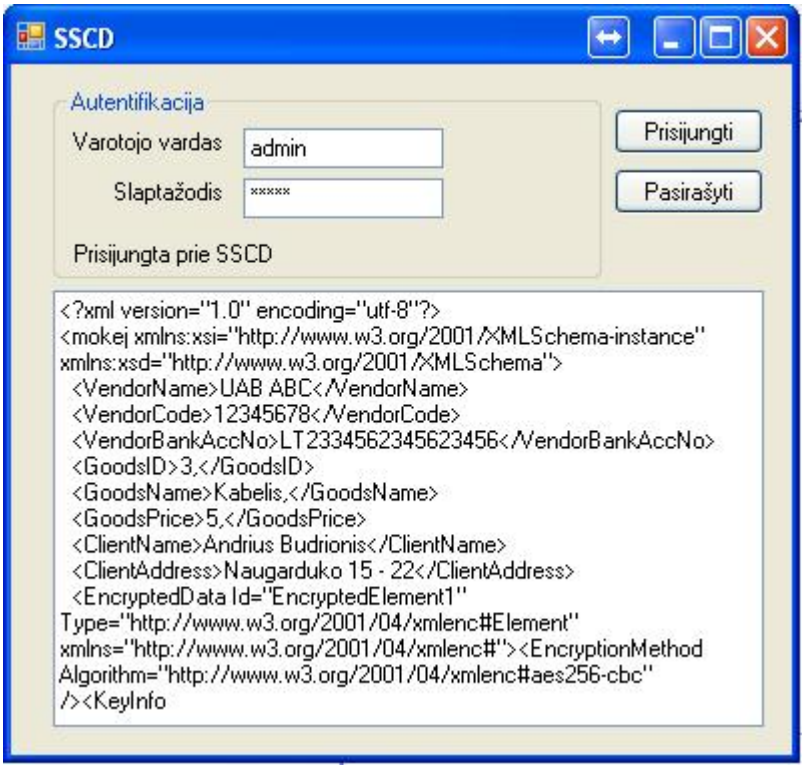
6. SAUGIŲ ATSISKAITYMŲ MODULIO PROTOTIPAS

Elektroninių atsiskaitymų modulio prototipo realizacijai buvo pasirinkta Microsoft .Net platforma ir jos teikiamas funkcionalumas. Pranešimų pasirašymui ir žymų šifravimui buvo pasirinktos XML standarte aprašytos pranešimų pasirašymo el. parašu ir šifravimo priemonės.

6.1. Saugaus elektroninio parašo kūrimo įranga (SSCD)

Siekiant kuo tiksliau imituoti visą elektroninio atsiskaitymo procesą, saugaus el. parašo kūrimo įranga buvo būtina. Šiuo metu Lietuvoje paplitusi parašo kūrimo įranga netiko, dėl viešai neplatinamų programavimui ir darbui su SSCD reikalingų bibliotekų. Dėl šios priežasties šią įrangą nuspręsta imituoti, realizuojant modulį, kuris būtų atsakingas už parašo kūrimo procesą. Pagrindinė modulio funkcija – pasirašyti XML pranešimą naudojant privatųjį vartotojo šifravimo raktą ir prie pranešimo pridėti naudotojo sertifikatą. Prisijungimas prie SSCD apsaugotas vartotojo slaptažodžiu. Grafinė SSCD vartotojo sąsaja pateikta 20 pav.

Kuriant šią programinę įrangą buvo remiamasi šaltinyje [Und08] pateiktais reikalavimais šios paskirties įrangai.



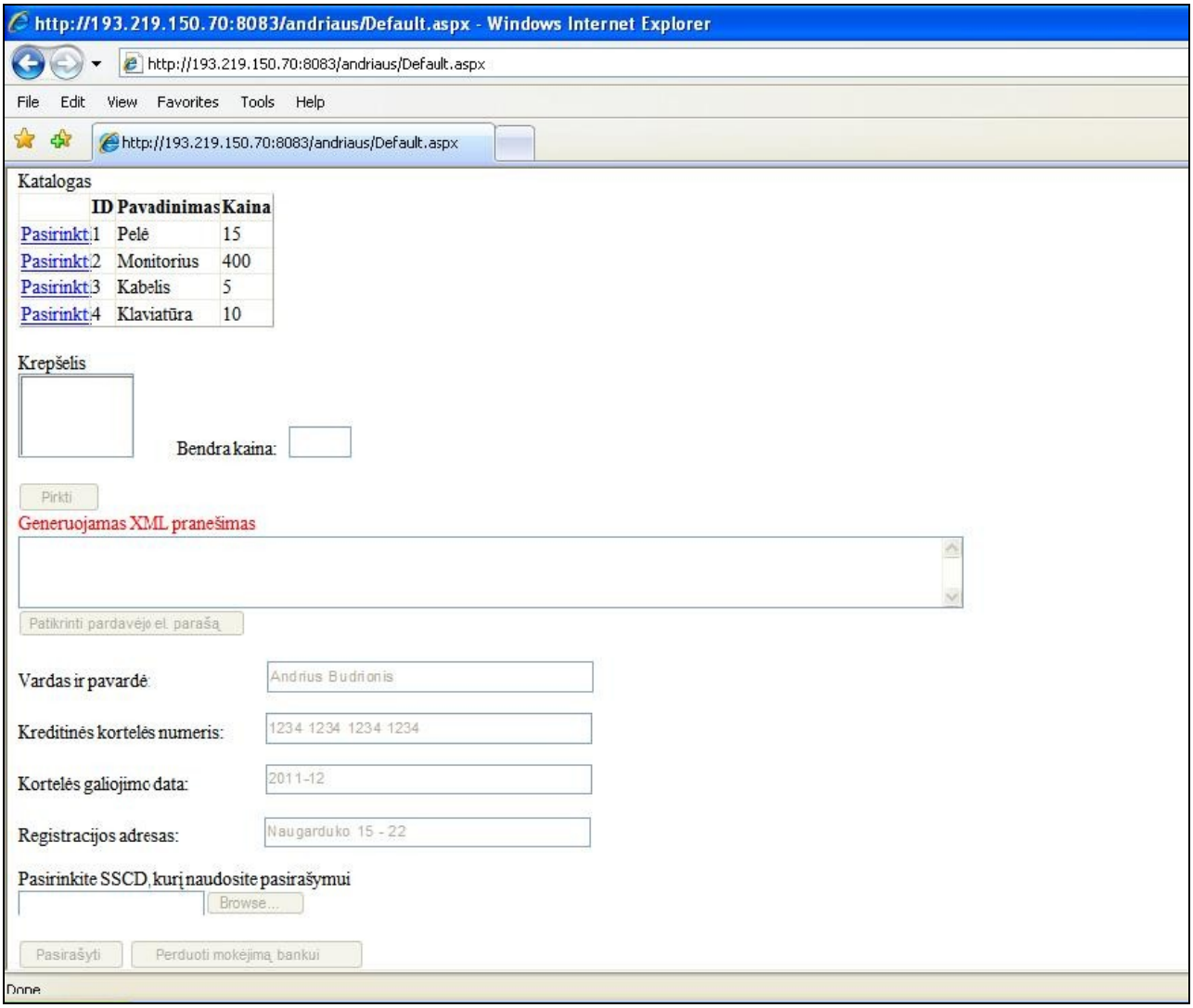
21 pav. Saugaus el. parašo kūrimo įrangos (SSCD) grafinė vartotojo sąsaja

6.2. Elektroninių atsiskaitymų modulio prototipas

Remiantis el. komercijos modulio projektu, pateiktu 5 darbo skyriuje, buvo realizuotas projektą atitinkantis programinės įrangos prototipas. Kadangi pilna prototipo realizacija nebuvo įmanoma (dėl bankinių sistemų uždarumo), buvo apsiribota daliniu sprendimo prototipu iliustruojančiu pagrindinį funkcionalumą. Galutinis prototipo kuriamas produktas yra ne įvykdyta transakcija, o XML pranešimas, kuris pateikiamas bankui ir pagal kurį turėtų būti įvykdytas pinigų pervedimas. Banko sistema, gavusi tokio tipo pranešimą, visų pirma turi patikrinti abiejų transakcijoje dalyvaujančių šalių el. parašus, jei jie yra galiojantys, atšifruoti reikalingus kliento duomenis ir vykdyti transakciją.

Siekiant ištestuoti realizuotą prototipą jis integruotas į testavimo tikslais sukurtą el. parduotuvės vartotojo sąsają, kurios pagalba programinis produktas veikia artimomis realybei sąlygomis. Kadangi tai yra testavimui skirtas prototipas, vartotojui nuolat pateikiamas kiekviename žingsnyje kintantis sistemos generuojamas XML pranešimas, kuriama atsispindi mokėjimo nurodymo forma. Prototipo grafinė vartotojo sąsaja pateikta 21 pav.

Prototipas yra viešai prieinamas adresu http://193.219.150.70:8083/andriaus/Default.aspx, parašo kūrimui reikalinga įranga (SSCD) prieinama http://193.219.150.70:8083/andriaus/SSCD.rar adresu.



22 pav. Saugių el. atsiskaitymų modulio prototipo grafinė vartotojo sąsaja

REZULTATAI IR IŠVADOS

Didėjantys elektroninių atsiskaitymų kiekiai ir mąstai verčia verslą keltis į elektroninę erdvę ir pinigines operacijas atlikti internetu. Ši pažanga naudinga ir pirkėjams ir pardavėjams, tačiau dažnai interneto vartotojai dar nepasitiki šiuo apmokėjimo būdu dėl galimų saugumo spragų. Kadangi technologijos yra sąlyginai naujos, baimė ir nepasitikėjimas jomis yra pakankamai pagrįstas dalykas. Kiekvienas išbandęs šio tipo atsiskaitymus galėtų sugalvoti būdų saugumo užtikrinimo procesui pažeisti, nes šiandieniniai mokėjimų modeliai ypač aplaidžiai žiūri į kai kuriuos saugumo pažeidimus, pvz. galimybę atsiskaityti ne banko kortelės savininko vardu. Nors šios spragos yra akivaizdžios, dėl nusistovėjusios tvarkos nesiimama priemonių saugumo lygiui padidinti. Šio magistro darbo tikslas buvo įvardinti informacijos, susijusios su el. atsiskaitymais, saugumo užtikrinimo trūkumais, kurių nepašalina naudojamos technologijos ir sprendimai, ir pasiūlyti aukštesnio saugumo lygio el. komercijos modelį bei realizuoti programinį jo prototipą.

Darbo metu išsiaiškintos naudojamų technologijų saugumo spragos, lyginti įvairūs rinkoje esantys elektroninių atsiskaitymų modeliai ir naudojamos informacijos saugumo užtikrinimo technologijos. Šių produktų ir technikų analizė leido suprasti pagrindines saugumo problemas, kurių sprendimai ir tapo reikalavimų, projektuojamam elektroninių atsiskaitymų modeliui, dalimi.

Pagrindinė darbe pasiūlyto elektroninių atsiskaitymų modelio idėja remiasi el. parašo infrastruktūros panaudojimu atliekant elektroninius atsiskaitymus. Ši technologija užtikrina, kad mokėjimas atliekamas remiantis juridinę galią turinčiais dokumentais – mokėjimo nurodymais. Kadangi šie dokumentai yra pasirašyti abiejų transakcijoje dalyvaujančių šalių (pirkėjo ir pardavėjo) el. parašais, jie tampa puikia ginčų sprendimo priemone, įgalinančia įrodyti šalies įsipareigojimų nevykdymą ar kitus pažeidimus. Tiek pirkėjas, tiek bankinė institucija, vykdanti piniginę transakciją, turi įsitikinti, kad mokėjimo nurodyme esantys šalių parašai yra teisingi. Šis faktas garantuoja, kad dokumentas, pagal kurį vykdomas mokėjimas, nebuvo niekieno pakeistas po pasirašymo ir kad abi šalys sutinka su jame nurodytos pinigų sumos pervedimu. Taip pat naudojant el. parašo infrastruktūrą gerokai sumažėja atsiskaitymo ne banko sąskaitos savininko vardu galimybė, nes el. parašų kūrėjų tapatybę kontroliuoja trečioji šalis – sertifikatų centras, kuris garantuoja kad konkreti šifravimo raktų pora ir parašo kūrimo įranga priklauso konkrečiam asmeniui.

Kita siūlomo sprendimo dalis susijusi su elektroninių atsiskaitymų sistemose naudojamu šifruotu duomenų perdavimu TLS/SSL protokolu. Tobulėjant tinklo ir duomenų perdavimo bei apdorojimo technologijoms šio protokolo užtikrinamas informacijos šifravimas tampa per mažai

patikimas, nes informacija šifruojama per žemame OSI informacijos perdavimo kompiuterių tinklais sluoksnyje. Duomenys gali būti nutekinti dar nepasiekus OSI transporto sluoksnio (kur jie bus užšifruoti) arba duomenis apdorojant aukštesnio nei transporto sluoksnis tinklo įrenginiuose (pvz. *gateway*). Kad taip nenutiktų, duomenims perduoti siūloma naudoti SOAP protokolą ir XML pranešimų šifravimą vykdomą aukštesniame OSI modelio sluoksnyje.

Atsižvelgiant į visus informacijos saugumo užtikrinimo reikalavimus buvo suprojektuotas elektroninių atsiskaitymų modelis, o siekiant iliustruoti jo veikimą realizuotas programinis prototipas. Kadangi pilna prototipo realizacija (įtraukiant ir transakcijas vykdančias bankines institucijas) buvo neįmanoma, apsiribota daliniu prototipu, kurio realizacija baigiama bankinei institucijai perduodamo pranešimo generavimu ir imituojamu jo perdavimu. Šie darbo rezultatai įrodo galimybę realizuoti ir naudoti saugesnes elektroninių atsiskaitymų schemas, kurios garantuoja ne tik didesnę konfidencialių duomenų apsaugą, bet ir supaprastina ginčų, kylančių tarp pirkėjų ir pardavėjų internetinėje erdvėje, sprendimą, trukdo plisti „netikriems“ prekeiviams.

Modelio užtikrinamas aukštesnis saugumo lygis, realizacijos ir naudojimo paprastumas yra pagrindinės schemos tobulinimo ir diegimo priežastys. Šiame darbe siūlomo sprendimo aprašymai, atlikta analizė, projektavimo bei realizacijos darbai gali būti pagrindas tolimesniam šios atsiskaitymų schemos vystymui ir tobulinimui.

ŠALTINIAI

[Can06] VICENTE ACEITUNO CANAL, CREATIVE COMMONS ATTRIB-NODERIVS LICENSE, Information Security Management Maturity Model ISM3, 2006, 82 psl.

[CH04] Siv Fern Chang, Farah Hayat, An Analysis of Online Payment Systems using PayPal as a Test Case, 2004

[CL08] Crimson Logic – Integration Guidelines for PCS e-payment gateway, 2008.

[Čap07] Albertas Čaplinskas. „Reikalavimų inžinerija“. 2007

[Čap96] Albertas Čaplinskas. „Programų sistemų inžinerijos pagrindai“ I dalis 1996.

[Čap98] Albertas Čaplinskas. „Programų sistemų inžinerijos pagrindai“ II dalis 1998

[Eba07] eBAY INC. SECOND QUARTER 2007 FINANCIAL RESULTS, [žiūrėta 2009-06-10], prieiga per internetą: <http://files.shareholder.com/downloads/EBAY/0x0x119929/e860561d-950b-4415-8dc1-7bfe06dfa972/eBay_EarningsReleaseQ22007_FINAL.pdf>

[GKF06] Zbigniew Gołębiewski, Mirosław Kutyłowski and Filip Zagórski, Institute of Mathematics and Computer Science, Wrocław University of Technology, Stealing Secrets with SSL/TLS and SSH – Kleptographic Attacks, 2006

[GLMS08] Sebastian Gajek, Lijun Liao, Bodo Möller, Jörg Schwenk, Horst Görtz Institute for IT Security, Ruhr-Universität, 44780 Bochum, Germany, SSL-over-SOAP: Towards a Token-based Key Establishment framework for Web services, 2008

[HL03] Michael Howard, David LeBland. Writing Secure Code, Second Edition, Microsoft Press, 2003, 768 psl.

[Hoa09] Thuan Nguyen Hoang “Types of electronic payment system: The requirements from different actors’ perspective” 2009, [žiūrėta 2009-11-10], prieiga per internetą: <http://knol.google.com/k/thuan-nguyen-hoang/types-of-electronic-payment-system-the/25lgke3rt3f2g/5#>

[ISO05] ISO/IEC 15408 “Information technology – Security Techniques – Evaluation Criteria for IT security”, 2005

[Its01] International Technical Support Organisation „e-commerce Payment Solutions Implementation and Integration Using IBM WebSphere Payment Manager“, 2001[žiūrėta 2009-04-17]. Prieiga per internetą

<http://www.redbooks.ibm.com/redbooks/pdfs/sg246177.pdf>

[Yan00] Jianxin Jeff Yan, Computer Laboratory, Cambridge University. Denial of Service: Another Example, 2000, 9 psl. [žiūrėta 2009-05-05]. Prieiga per internetą <http://homepages.cs.ncl.ac.uk/jeff.yan/sec2002.pdf>

[Miy04] Koji Miyauchi „XML Signature/Encryption – the Basis of Web Services Security“, NEC Journal of Advanced Technology, Vol. 2., No 1. 2004, [žiūrėta 2010-02-15], prieiga per internetą: <www.nec.co.jp/techrep/en/r_and_d/a05/a05-no1/a035.pdf>

[Mog07] Manuel Mogollon. Cryptography and Security Services– Mechanisms and Applications, Idea Group Inc (IGI), 2007, 471 psl.

[MPS08] Monetra Payment Software, Secure Implementation Guide, 2008, [žiūrėta 2009-12-10], prieiga per internetą: <http://www.monetra.com/docs/support/Monetra_SIG-v2.0.pdf >

[OL05] George S. Oreku, Jianzhong Li. Rethinking e-commerce security, IEEE, 0-7695-2504-0/05, 2005, 6 psl.

[PSA09] PayPal SOAP API Developer Reference, 2009, žiūrėta 2009-11-20], prieiga per internetą: <https://cms.paypal.com/cms_content/US/en_US/files/developer/PP_API_Reference.pdf>

[Rei06] Paul Michael Reinheimer. PROFESSIONAL WEB APIs WITH PHP: EBAY, GOOGLE, PAYPAL, AMAZON, FEDEX, PLUS WEB FEEDS, Wiley-India, 2006, 356 psl.

[Rns00] Jianxin Jeff Yan, Computer Laboratory, Cambridge University. Denial of Service: Another Example, 2000, 9 psl. [žiūrėta 2009-05-05]. Prieiga per internetą <http://homepages.cs.ncl.ac.uk/jeff.yan/sec2002.pdf>

[Sah08] Jean – Michel Sahut, Amiens school of Management. Security and Adoption of Internet Payment, IEEE, 978-0-7695-3329-2/08, 2008, 6 psl.

[Sch00] Bruce Schneier. Secrets and Lies: Digital Security In A Networked World, John Wiley and Sons, Inc., 2000, 412 psl.

[Und08] Valdas Undzėnas. Elektronio parašo infrastruktūra ir el. komercija. Mokymo medžiaga, 2008

[W3C07] W3C, Simple Object Access Protocol (SOAP) 1.2, 2007, [žiūrėta 2009-11-17], prieiga per internetą: <http://www.w3.org/TR/2007/REC-soap12-part0-20070427/>

[ZL05] Gengming Zhu, Junguo Liao „Design and Realization of Security Model of E-Commerce System“, IEEE, 978-0-7695-3497-8/08978-0-7695-3497-8/08978-0-7695-3497-8/08, 2008, 5 psl.

SĄVOKŲ APIBRĖŽIMAI

Šios darbe panaudotos sąvokos reiškia:

mokėjimų vartai (angl. *payment gateway*) – tarptautinių organizacijų (VISA, MASTERCARD) el. komercijai teikiama paslauga, kurios paskirtis yra mokėjimo nurodymo duomenų šifravimas ir perdavimas būtent tam bankui, kurio išduota kortele atsiskaitė pirkėjas;

LINQ TO SQL (angl. *Language Integrated Query to SQL*) – Microsoft .NET platformos komponentas, supaprastinantis darbą su duomenų bazėmis;

žiniatinklio paslauga (angl. *web service*) – programinės įrangos funkcija, įgalinanti tarpmašininį bendravimą kompiuterių tinkluose, kurio pranešimai yra suformatuoti ir apibrėžti mašinoms suprantama kalba (WSDL).

SANTRUMPOS

SOAP - angl. *Simple Object Access Protocol,* paprastas kreipimosi į objektus protokolas;

SHA – angl. *Secure Hash Algorithm,* saugus santraukos algoritmas;

SSL/TLS – angl. *Secure Socket Layer / Transport Layer Security,* saugus jungties sluoksnis / transporto sluoksnio saugumas;

WSDL – angl. *Web Service Definition Language,* žiniatinklio paslaugų apibrėžimo kalba;

XML – angl. *Extensible Markup Language,* išplėstinė aprašų žymių kalba;

XSD – angl. *XML Schema Definition,* išplėstinės aprašų žymių kalbos schemos apibrėžimas;

SSCD – angl. *Secure Signature - Creation Device*, saugaus el. parašo kūrimo įranga;

DBVS – Duomenų bazių valdymo sistema;

OCSP – angl. *Online Certificate Status Protocol,* sertifikatų tikrinimo realiu laiku protokolas;

UML – angl. *Unified Modelling Language,* unifikuota modeliavimo kalba.

PRIEDAI

1 priedas. XML pranešimo pavyzdys

```
<?xml version="1.0" encoding="utf-8" ?>
<mokej xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <VendorName>UAB ABC</VendorName>
  <VendorCode>12345678</VendorCode>
  <VendorBankAccNo>LT2334562345623456</VendorBankAccNo>
  <GoodsID>2,</GoodsID>
  <GoodsName>Monitorius,</GoodsName>
  <GoodsPrice>400,</GoodsPrice>
  <ClientName>Andrius Budrionis</ClientName>
  <ClientAddress>Naugarduko 15 - 22</ClientAddress>
   <EncryptedData Id="EncryptedElement1"
Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
 <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
 <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <KeyName>rsaKey</KeyName>
  </KeyInfo>
 <CipherData>
<CipherValue>LcRMya8yUKEC/d9/RdEf8OHU8ohlMguFs6Shg0SjqC1CCkGTP4koBwnSJ
NKbwHMGZ2eUtK/0ec1k022N4EC0gWbYJsFiiIjWmlg5j/huR84OtDkDvc4j37vyB316GY
Ai8J9IJnO6nv5HT9Eype4mX+6Mp8G2MCjcwIqvZXkWN9s=</CipherValue>
  </CipherData>
 <ReferenceList>
  <DataReference URI="#EncryptedElement1" />
  </ReferenceList>
  </EncryptedKey>
  </KeyInfo>
 <CipherData>

<CipherValue>cBD1ZJZ4I6F/y5HCVvjn/6hk3fVoSTDvY8QAaeNZC9mU8nfsSI7l2t1GbpQ
pALFQ6i3GLawnzXcdDR+vysoOrm6RJVIJHP5OKQlIIzqd2Ks=</CipherValue>
  </CipherData>
  </EncryptedData>
 <EncryptedData Id="EncryptedElement2"
Type="http://www.w3.org/2001/04/xmlenc#Element"
xmlns="http://www.w3.org/2001/04/xmlenc#">
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc" />
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
 <EncryptedKey xmlns="http://www.w3.org/2001/04/xmlenc#">
  <EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
 <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
  <KeyName>rsaKey</KeyName>
  </KeyInfo>
```

<CipherData>
<CipherValue>**i0JDCcMyB+CUtaY7+QL5Gy5tXsXBPiNRx8nQ1KeWwXnrVphL97h9lisVvBz+mVyl4teHp3Xp02bZanSuoFKz0aNfRoESeZPlagvyJscb4Nm4rwe0GO3HBihntbmz6dYVopybcZaIqVULz6daeMD/0l+HzMmkZtEisdo8oKYpsBM=**</CipherValue>
</CipherData>
<ReferenceList>
<DataReference URI="**#EncryptedElement2**" />
</ReferenceList>
</EncryptedKey>
</KeyInfo>
<CipherData>
<CipherValue>**jESJn2LA6IAl7GKuaE8tq2BqO33l9DFeBDnEr9+xGUv3fLjPdrkxTB+5g+c5S9te**</CipherValue>
</CipherData>
</EncryptedData>
<FullPrice>**400**</FullPrice>
<VendorCertificate>
<IssuedFor>**UAB ABC**</IssuedFor>
<Version>**v1**</Version>
<SerialNo>**123456**</SerialNo>
<ValidFrom>**2010-01-01**</ValidFrom>
<ValidUntil>**2012-01-01**</ValidUntil>
<RSAPublicKey>
<RSAKeyValue>
<Modulus>**nzKbDkcbsr9qOMukAdjCytuAICMXyNetQ4GNL05+v/i7ccISirqwD0yFrFni1w9NnhjQPUh0WKNn2mY/pmcmSprOUNAIRa8CyaHfQHb1ibPtxq6KsdJvToenSlYUPoRHLd1fh3zRmw3cQ01cwJBsEZ6AthQxbWN67dgFIQSP7AM=**</Modulus>
<Exponent>**AQAB**</Exponent>
</RSAKeyValue>
</RSAPublicKey>
<Issuer>**UAB Certification Authority**</Issuer>
</VendorCertificate>
<Signature xmlns="**http://www.w3.org/2000/09/xmldsig#**">
<SignedInfo>
<CanonicalizationMethod Algorithm="**http://www.w3.org/TR/2001/REC-xml-c14n-20010315**" />
<SignatureMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#rsa-sha1**" />
<Reference URI="">
<Transforms>
<Transform Algorithm="**http://www.w3.org/2000/09/xmldsig#enveloped-signature**" />
</Transforms>
<DigestMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#sha1**" />
<DigestValue>**yzMxdF7KiMRYcpM0XfAY6lVCeXg=**</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>**LTRXU+f0Bx7wrOCCb07vroLWgpiwcrY7W6urISM5Ai+b3znbJtH33lCYQRhKovTLXdGqBAhEP/cxcCfck6F5+UeKrgHuHVdRl7oiZgRBq4HKkqPps/PlBnfdkR82NzkxqBaQh47mghTmt8u3s7hevjZJjDNh6L117VebTvCLyVM=**</SignatureValue>
</Signature>
<VendorCertificate>
<IssuedFor>**Andrius Budrionis**</IssuedFor>
<Version>**v1**</Version>

<SerialNo>**345678**</SerialNo>
<ValidFrom>**2010-01-01**</ValidFrom>
<ValidUntil>**2012-01-01**</ValidUntil>
<RSAPublicKey>
<RSAKeyValue>
<Modulus>**yIW96x4ia5H/UsB9meFH1FsaFzW4B5YQHLVM+dyAmr5BpSYxkojTx9Tc/44ZaQtGpgr40kh9/2jo1Zf61wC8L4n7AKg9fCzgt1rtliI304a+KmswXHD/nMaMwG1fCRESrJC22QID2o6ppJ7Hr2f+djr2pXitVvN3CXP2dcozZCk=**</Modulus>
<Exponent>**AQAB**</Exponent>
</RSAKeyValue>
</RSAPublicKey>
<Issuer>**UAB Certification Authority**</Issuer>
</VendorCertificate>
<Signature xmlns="**http://www.w3.org/2000/09/xmldsig#**">
<SignedInfo>
<CanonicalizationMethod Algorithm="**http://www.w3.org/TR/2001/REC-xml-c14n-20010315**" />
<SignatureMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#rsa-sha1**" />
<Reference URI="">
<Transforms>
<Transform Algorithm="**http://www.w3.org/2000/09/xmldsig#enveloped-signature**" />
</Transforms>
<DigestMethod Algorithm="**http://www.w3.org/2000/09/xmldsig#sha1**" />
<DigestValue>**WZeEVlTsBAoaclTPIisWThXJt5w=**</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>**DpxWOPpIF0nxRJCEbyRwo5GPeK6W6G8fUiJwqfmG5J/ZSvJokDTdwZCdzlKhnvsSw5BxCnClykZDA4uDtnIIUfWetrN6kDRAZ9dVVDRvBWs39l/85Sgx9l+km684OGXFa3fwEN9QnfPryTYeBKutDs3C7yGxaESyDa78NToTkJo=**</SignatureValue>
</Signature>
</mokej>