KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Giedrius Mickevičius

Internetinio atsiskaitymo sistemos vartotojo autentifikavimo, paremto elektroniniu parašu, sukūrimas ir tyrimas

Magistro darbas

Darbo vadovas
prof. dr. E. Sakalauskas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Giedrius Mickevičius

Internetinio atsiskaitymo sistemos vartotojo autentifikavimo, paremto elektroniniu parašu, sukūrimas ir tyrimas

Magistro darbas

Recenzentas
doc. dr. G. Ziberkas
2010-05-26

Vadovas
prof. dr. E. Sakalauskas
2010-05-26

Atliko
IFN-8/3 gr. stud.
Giedrius Mickevičius
2010-05-26

Kaunas, 2010

TURINYS

USER AUTHENTICATION BASED ON ELECTRONIC SIGNATURE – CREATION AND INVESTIGATION FOR USE IN ONLINE PAYMENT SYSTEM.

SUMMARY

There is a lot of internet shopping done nowadays. People are buying goods from electronic shops and paying for them in online payment systems. These systems need to provide secure user authentication method for user to log in and to pay for the goods.

The main purpose of this work is to create and investigate new online payment system with better user authentication method. This method is based on user's electronic signature.

In this work there were investigated the most popular online payment systems to find out which authentication method they are using to authenticate user. All of those systems provide password based user authentication which we found to be not secure enough because there are some ways for third party to find out users passwords. There were also investigated most popular user authentication methods to find out their advantages and disadvantages.

After implementation of new online payment system's user authentication method there was done investigation of this method. There were done some researches to find out this authentication method advantages and disadvantages. It was found that this method is more secure because it uses PKI (Public Key Infrastructure) which ensures integrity and authenticity. New authentication method was compared with existing authentication method used in real online payment systems and found that it takes twice longer time for user to be authenticated than it is done in existing online payment systems. But it takes only about 100 ms to be authenticated which user won't feel. Also new authentication method may be difficult for user to use so before using it in real life he needs to be trained. There were also investigated possible solutions of using different types of order file formats and electronic signature methods.

ĮVADAS

Šiuo metu labai daug įvairiausios informacijos yra apsikeičiama interneto pagalba. Ši informacija gali būti slapta, skirta tik tam tikram asmeniui ar tam tikrai organizacijai, arba ji gali būti visiškai neslapta, skirta apsikeisti paprastomis užklausomis internetu. Slapta informacija gali būti įvairūs organizacijos finansiniai duomenys, informacija susijusi su organizacijos veikla, fizinio asmens asmeniniai bei finansiniai duomenys. Tokius duomenis sužinojęs trečias asmuo, juos gali panaudoti saviem tikslam. Internetu keliaujančią informaciją, pasinaudojus tam tikromis priemonėmis, galima peržiūrėti, ją analizuoti, todėl svarbią, slaptą informaciją reikią apsaugoti nuo trečiųjų asmenų, kuriem ta informacija nėra skirta ir kurie ja negalėtų pasinaudoti saviem, nebūtinai piktiem tikslam įgyvendinti. Taigi tokią informaciją būtina apsaugoti, kad jos negalėtų perskaityti, negalėtų jos pakeisti ir kad būtų užtikrinta, jog toji informacija yra tikrai nuo to asmens ar organizacijos, iš kurios ir tikimasi ją gauti - turi būti užtikrintas informacijos autentiškumas, konfidencialumas, vientisumas.

Internetinė prekyba – vienas iš sparčiausiai plintančių paslaugų internete. Vis daugiau parduotuvių persikelia į virtualią erdvę. To priežastis – mažesnis darbo jėgos poreikis (įmonė sutaupo samdydama mažesnį darbuotojų skaičių), patogumas vartotojui (vartotojas, būdamas bet kuriame pasaulio taške ir turėdamas interneto prieiga, gali įsigyti prekes net neišeidamas iš namų). Šios parduotuvės pirkėjui pateikia visą asortimentą prekių ar paslaugų su jų aprašymais, iliustracijomis, todėl sudaromos labai panašios sąlygos lyg vartotojas apžiūrinėtų prekes būdamas įprastoje parduotuvėje. Visi pirkimai, atsiskaitymai už prekes vyksta interneto pagalba. Vartotojas pirkdamas prekes pateikia savo kreditinės kortelės informaciją internetinei parduotuvei arba internetinio atsiskaitymo sistemai. Pastaroji yra tarpininkas, atliekantis finansines operacijas - iš pirkėjo sąskaitos nuskaito reikiamą pinigų sumą ir ją perveda į parduotuvės sąskaitą.

Siekiant, kad vartotojas galėtų finansines operacijas padaryti saugiai, internetinio atsiskaitymo sistemos turi pasirūpinti vartotojo duomenų saugumu. Visų pirma turi būti sukurtas patikimas vartotojo autentifikavimo būdas, kadangi tai yra pirmasis žingsnis atsiskaitymo procese. Nuo jo priklauso ar teisingai bus autentifikuotas vartotojas. Egzistuoja rizika, jog piktavalis gali bandyti prisijungti vartotojo vardu ir atlikti finansines operacijas savo naudai, todėl autentifikavimo metodas turi užtikrinti, kad to piktavaliui nepavyktų padaryti.

Vartotojams autentifikuoti egzistuoja keletas autentifikavimo metodų. Keletas jų yra plačiai naudojami vartotojams autentifikuoti ne tik internetinio atsiskaitymo sistemose, tačiau

ir kitose sistemose (įmonės vidinėje sistemoje, socialiniuose tinklapiuose ir panašiai). Dalis autentifikavimo metodų yra netinkami naudoti internetinio atsiskaitymo sistemose, kadangi jie yra nepritaikyti panaudojimui tokio tipo sistemose, yra per brangūs arba turi tam tikrų trūkumų. Šiuo metu egzistuoja keletas internetinių atsiskaitymo sistemų, kurios teikia atsiskaitymų už prekes paslaugą. Viena iš populiariausių - PayPal. Šioje ir kitose internetinių atsiskaitymų sistemose naudojamas tas pats, elektroniniu pašto adresu ir slaptažodžiu paremtas, vartotojo autentifikavimo metodas. Šis autentifikavimo metodas nėra pakankamai saugus, kadangi yra tikimybė jog pirkėjo slaptažodį gali sužinoti piktavalis spėjimo būdu, apsimetimo būdu arba perimant slaptažodžių failą ar slaptažodį keliaujantį internetu, bei šį slaptažodį pirkėjas gali užmiršti, kadangi jis turi tenkinti tam tikrus saugumo reikalavimus, nuo kurio jis pasidaro sudėtingas ir sunku jį prisiminti.

Šio darbo tikslas yra sukurti internetinio atsiskaitymo sistemos vartotojo autentifikavimo metodą, kuris užtikrintų patikimą vartotojo autentifikavimą. Darbe pasiūlytas naujas metodas, kurio idėja – vartotojo autentifikavimas paremtas jo elektroniniu parašu. Tai yra viešojo rakto infrastruktūra paremtas autentifikavimo metodas, kuris kartu užtikrina ir autentiškumą ir konfidencialumą ir integralumą – tris pagrindinius saugumo kriterijus.

1. INTERNETINIO ATSISKAITYMO SISTEMOS VARTOTOJO AUTENTIFIKAVIMO ANALIZĖ

Šios analizės tikslas yra išanalizuoti internetinės prekybos veikimo principus, išsiaiškinti atsiskaitymo sistemų veikimą. Analizė susideda iš analizės būdų, kaip atliekamas vartotojo autentifikavimas jam jungiantis prie atsiskaitymo sistemos, bei kokia apsisaugojimo nuo galimų informacijos praradimų ar klastojimų sauga yra naudojama. Analizuojamos atsiskaitymo sistemos, jų veikimo principai ir jos tarpusavyje palyginamos, siekiant išsiaiškinti vienų ar kitų sistemų pranašumus ir trūkumus, į kuriuos būtų galima atsižvelgti kuriant naują tokių sistemų autentifikavimo būdą.

Ši analizė padės apsispręsti ir priimti sprendimus, kaip sukurti naują autentifikavimo būdą, kokias technologijas panaudoti.

1.1. Autentiškumas ir jo būtinybė

Autentiškumas – tai yra autentifikacijos procesu įrodyta asmens ar asmenų grupės tapatybė.

Autentifikacija yra procesas, kurio metu nustatoma, ar vartotojas yra tas asmuo kuriuo jis dedasi esąs. Vartotojas yra autentifikuojamas pagal tai ką jis žino (pvz. slaptažodis), pagal tai ką jis turi (kažkoks saugos prietaisas) ar pagal kažkokią jo dalį (pvz. biometriniai požymiai).

Autentifikacijos būna kelių rūšių, priklausomai nuo vietos, kurioje reikalinga vartotoją autentifikuoti. Skirtingose sistemose, programose gali būti naudojami skirtingi autentifikacijos būdai, arba jų iš vis gali ir nebūti. Sistemose, kuriose informacija yra labai griežtai saugoma turi būti panaudota aukšto lygio autentifikacija, užtikrinanti, kad niekas kitas, išskyrus kažkokius, tam teise turinčius, asmenis galėtų prieiti prie šių duomenų. Tačiau jei informacija nėra labai svarbi, tuomet gali būti panaudoti patys primityviausi autentifikacijos būdai arba jų gali iš vis nebūti.

Autentifikacija priklauso nuo asmens tapatybės nustatymo ir registracijos procesų. Tarkime pilietis Jonas, kurį įmonė nori pasamdyti, pateikia visus duomenis apie save kas jis toks yra. Tai gali būti: vardas, pavardė, vairuotojo pažymėjimo numeris, asmens kodas ir pan. Įmonė gali iš karto priimti asmenį į darbą, arba gali jį patikrinti ar tai tikrai tas asmuo, ar jis neturi kažkokios tamsios praeities, kažkokios kriminalinės istorijos. Tai yra daroma tam, kad firma, kurios veikla gali būti susijusi su slapta informacija, būtų tikra, kad tas asmuo nėra

kažkoks nusikaltėlis ir nepakenks įmonės veiklai. Kai įmonė patikrins asmens tapatybę, tik tuomet įtrauks šį asmenį į savo darbuotojų sąrašą. Tuomet įmonė įregistruos šį asmenį į savo sistemą, suteiks jam kažkokius prisijungimo prie sistemos duomenis, tokius kaip slaptažodį, ar įtrauks į sistemą kažkokia naujojo darbuotojo biometrinę informaciją. Po šių veiksmų asmuo, kiekvieną kartą jungiantis prie įmonės sistemos, turės būti autentifikuojamas, panaudojus vieną iš minėtų autentifikacijos būdų. Priklausomai nuo to, kaip buvo užregistruotas asmuo sistemoje, kaip jo tapatybė buvo patikrinta, priklauso ir autentifikacija. Jei informacija surinkta apie naują žmogų buvo nepakankama, ateityje gali atsirasti kažkokių nišų sistemoje, kuriom gali pasinaudoti kiti, tam teisės neturintys asmenys, apsimetę kitais, teisėtais asmenimis.

1.2. Objektas - internetinio atsiskaitymo sistemos vartotojo autentifikavimas

PayPal yra viena iš populiariausių atsiskaitymo sistemų naudojamų internete. Daugelis žmonių pasitiki šia sistema ir patiki jei saugoti savo svarbius duomenis, tokius kaip kortelės numerį, asmens informaciją. Ši sistema naudojama atsiskaitymui už įvairiausias prekes ar paslaugas, perkamas internetu. PayPal pati neprekiauja kažkokiomis prekėmis ar paslaugomis, ji tik suteikia atsiskaitymo už jas paslaugą internetinėms parduotuvėms. Sistema naudoja įvairias apsaugos priemones, kad apsaugotų klientų slaptą informaciją. Kadangi didelis kiekis žmonių pasitiki šia sistema, todėl ir internetinių parduotuvių naudojančių šią atsiskaitymo sistemą yra daug. Kad sistema galėtų pasinaudoti vartotojas, jis turi joje užsiregistruoti, pateikdamas įvairią asmeninę informaciją apie save: vardas, pavardė, gyvenamoji vieta, telefono numeris, elektroninio pašto adresas, bankinės kortelės informacija, kortelės išdavimo vieta, jos galiojimo laikas ir t.t. Šia sistema vartotojas naudojasi interneto pagalba, užeidamas arba internetinės parduotuvės nukreipiamas į PayPal internetinę svetainę, kurioje ir atliekamos atsikaitymo operacijos [9].

1.3. PayPal sistemos vartotojo autentifikavimo problema

Viena iš stambesnių internetinių parduotuvių, kuri naudojasi PayPal paslaugomis yra Ebay. Tai yra internetinė parduotuvė, kurioje prekes galima nusipirkti iš karto, arba dalyvauti internetiniame aukcione. Šioje parduotuvėje vartotojas turi užsiregistruoti. Tai yra reikalinga tam, kad būtų saugojami jo duomenys apie kokias prekes jis yra domėjęsis anksčiau, kokias prekes pirko, kokios prekės iki šiol yra aktyvios ir dalyvauja aukcione, tačiau jokios svarbios informacijos, susijusios su mokėjimo kortelės informacija, ši parduotuvė nesaugo. Tai yra

todėl, kad pati ši parduotuvė nedalyvauja mokėjimo procese, ji tik padeda vartotojui išsirinkti prekę ar dalyvauti aukcione. Kai jau vartotojas pasirenka prekę ir žino jos kainą, tuomet jis turi už ją susimokėti. Tai jis daro pasinaudodamas PayPal sistemos paslauga. Jis turi būti susikūręs šios sistemos vartotoją ir tik tada galės atlikti mokėjimus už pasirinktas prekes. Šioje stadijoje Ebay parduotuvė nedalyvauja, ji savo darbą laikinai baigė ir toliau operacijos vyksta jau PayPal svetainėje. Pereinant iš Ebay svetainės į PayPal, duomenys susiję su prekės kainą, bei prekės pardavėju (jo bankinės sąskaitos informacija ir pan.) yra automatiškai perkeliami į PayPal svetainę ir vartotojas jau gali atlikti mokėjimus [6].

Taigi norint atlikti kažkokius pirkimus internete pasinaudojant PayPal sistemos paslaugomis, reikia būti prisiregistravusiam prie šios sistemos. Registruojantis vartotojas pasirenka slaptažodį. Šis slaptažodis turi tenkinti tam tikrus reikalavimus, kad būtų užtikrinama, kad jis yra pakankamai saugus ir, kad trečias asmuo (piktavalis) jo neatspės. PayPal sistema savo klientų pasirenkamam slaptažodžiui kelia tokius reikalavimus, kad slaptažodžio ilgis turėtų būti bent 8 simbolių, bei turi būti panaudotas bent vienas skaičius arba ne abėcėlinis simbolis. Tokiu būdu slaptažodį yra sunkiau atspėti, kadangi vartotojui pasirinkus slaptažodį kokį nors jam gerai žinomą žodį, kitas asmuo gali jį tiesiog atspėt. Tačiau jei jis prie to žodžio dar pridės kažkokį ne abėcėlinį simbolį arba skaičių, tuomet piktavaliui bus žymiai sunkiau atspėti šį slaptažodį spėliojimo būdu.

Jungiantis prie PayPal sistemos vartotojas autentifikuojamas pagal jo elektroninio pašto adresą bei slaptažodį. Toks autentifikavimas yra reikalingas tam, kad kiti asmenys negalėtų prieiti prie vartotojo duomenų šioje sistemoje ir neatliktų kažkokių finansinių operacijų arba nesužinotų vartotojo bankinės kortelės informacijos. Vartotojo internetu siunčiami duomenys yra apsaugoti SSL protokolu, kuris yra paremtas viešojo rakto infrastruktūra, kuomet komunikuojančios šalys (šiuo atveju vartotojas ir PayPal) apsikeičia slaptais raktais ir internetu keliaujantys duomenys yra šifruojami. Vartotojas šioje sistemoje yra autentifikuojamas tokia tvarka:

- suvedama į atitinkamus PayPal internetinėje svetainėje esančius laukus autentifikavimosi informacija - elektroninio pašto adresas, bei slaptažodis,
- vartotojui patvirtinus suvestus duomenis, ši informacija yra siunčiama į svetainės serverį,
- į serverį atkeliavusi informacija yra ieškoma sistemos serverio duomenų bazėje:
    - jei tokie įrašai yra surandami, tuomet vartotojas yra autentifikuojamas ir jam suteikiama prieiga prie jo duomenų.
    - jei vartotojo įvesti duomenys nerandami duomenų bazėje, tuomet jam apie tai yra pranešama ir vartotojas gali toliau mėginti suvesti prisijungimo duomenis.

Vartotojas gali mėginti prisijungti tol, kol suves teisingus ir jo asmeninius duomenis (jo elektroninio pašto adresą bei jo susikurtą slaptažodį) arba tokių mėginimų prisijungti skaičius neviršys nustatyto skaičiaus. Ši sistema suteikia 3 bandymus vartotojui prisijungti. Viršijus leistiną neteisingo prisijungimo skaičių, vartotojo PayPal sąskaita yra blokuojama saugumo sumetimais, kad kiti vartotojai (piktavaliai) negalėtų prisijungti prie šios sąskaitos ir atlikti mokėjimus.

Vartotojo elektroninio pašto adresą piktavalis gali lengvai sužinoti, o slaptažodį gali pamatyti kai vartotojas neatsargiai suvedinėja klaviatūra arba panaudojant tam tikras programines priemones. Tokios priemonės yra paremtos vartotojo paspaustų mygtukų stebėjimu. Taip pat vartotojo slaptažodžiui gauti galima apsimetimo būdu, kuomet piktavalis gali apsimesti kitu, vartotojui patikimu asmeniu ir paprašyti slaptažodžio.

Kitas vartotojų autentifikavimo būdas, kurį naudoja PayPal sistema, tai saugos raktas (Security Key). Šis raktas - tai yra nedidelis įrenginys, kuris kartu yra ir raktų pakabukas. Rakto viduje yra įdiegta sistema, kuri generuoja pagal tam tikrą, unikalų tam raktui priskirtą numerį, šešių skaitmenų skaičių, kurį parodo ekranėlyje. Šis unikalus skaičius yra žinomas PayPal ir vartotojui. Įsigijus šį raktą ir jį užregistravus, PayPal sistema tą raktą aktyvuoja. Aktyvacija pagrįsta tuo, kad nuo to momento, kada vartotojas praneša sistemai, kad jis tą raktą gavo, ji padidina vartotojo saugumą, labiau apsaugodama jo autentifikaciją dar vienu punktu – slaptos skaičių sekos įvedimu. Taigi, kai vartotojas suves savo elektroninio pašto adresą ir slaptažodį, jo dar bus paprašyta suvesti šešių skaitmenų kodą, kurį rodo saugos raktas. Šis skaitmuo yra generuojamas kas 30 sekundžių naudojant tam tikrą algoritmą, kuriame, kaip parametras yra naudojamas to rakto unikalus skaitmuo. Tokį pati šešių skaitmenų skaičių generuoja ir PayPal sistema savo internetiniame serveryje. Tuomet, kai vartotojas jungiasi prie sistemos ir suvedęs visus reikiamus prisijungimo duomenis ir šį skaitmenį, duomenų bazėje bus tikrinama ar tas skaičius sutampa su tuo, kurį pateikė vartotojas ir atitinkamai vartotojas bus autentifikuotas arba ne. Šis autentifikavimo būdas padidina saugumą autentifikavimui užtikrinti [6,7].

1.4. Egzistuojančių internetinių atsiskaitymo sistemų palyginimas

Norint sukurti naują sistemos vartotojo autentifikavimo būdą, reikia išsiaiškinti kokios kitos internetinės atsiskaitymo sistemos egzistuoja ir kokias priemones jos naudoja vartotojams autentifikuoti. Tuomet pamačius kaip vienos ar kitos sistemos realizavo vartotojų

autentifikavimą, būtų galima atrinkti patį optimaliausią variantą ir panašų būdą galima panaudoti kuriant naują vartotojo autentifikavimo būdą.

PayPal yra viena iš populiariausių internetinių atsiskaitymo sistemų, tačiau egzistuoja ir kitų panašių sistemų. Jos kaip ir PayPal, yra naudojamos internetinėse parduotuvėse mokėjimams už prekes ar paslaugas atlikti. Galima paminėt vienas iš labiausiai aptinkamų atsiskaitymo sistemų, tai: Google CheckOut bei Amazon. Išanalizavus kaip šios sistemos autentifikuoja vartotojus, pastebėta, kad jos kaip ir PayPal sistema, naudoja elektroninio pašto adresu ir slaptažodžiu paremtu autentifikaciją.

1.5. Egzistuojantys vartotojo autentifikavimo metodai

1.5.1. Slaptažodžiu paremta autentifikacija

Slaptažodžiu paremta autentifikacija yra vienas iš populiariausių autentifikacijos būdų. Tačiau jis yra mažiausiai saugus būdas autentifikuoti. Asmuo yra autentifikuojamas kai jis įveda į tam tikras vietas savo prisijungimo vardą ir slaptažodį, kurį jis vienas težino. Tuomet jo įvesti duomenys yra tikrinami sistemos duomenų bazėje, ir jei ten tokie yra, vartotojas yra autentifikuojamas. Yra labai svarbu kokio ilgio, kokius simbolius ir kiek jų panaudos savo slaptažodyje vartotojas, nes nėra sunku atspėti slaptažodį. Jam atspėti yra sukurta programinių priemonių, kuriomis gali pasinaudoti piktavalis. Taigi sistemos, asmeniui autentifikuoti naudoja tokio tipo autentifikavimo metodą, kai prisijungęs prie sistemos vartotojas turi mažai teisių ar galimybių atlikti kažkokius svarbius veiksmus, kurie galėtų pakenkti įmonės veiklai. Tai gali būto tik vienas iš etapų asmeniui autentifikuoti. Tokių etapų gali būti keli, priklausomai nuo sistemos paskirties ar saugomos informacijos slaptumo.

Siekiant, kad slaptažodį nebūtų galima atspėti arba kitais būdais išgauti, yra sukurta įvairių saugumo priemonių šioms rizikoms sumažinti. Dažniausiai sutinkama saugumo priemonė, tai vartotojui vedant slaptažodį į slaptažodžiui skirtą vietą, ekrane nėra matomas įvedamas tekstas, o vietoj jo rodomos žvaigždutės. Taip yra apsisaugojama, kad kitas asmuo, esantis šalia, negalėtų pamatyt kokį slaptažodį jis įvedė. Kitas būdas tai saugoti slaptažodžius kaip maišos funkcijos reikšmę. Šiuo atveju slaptažodžiai duomenų bazėje arba slaptažodžių byloje yra saugojami ne tokiu pavidalu, kokį žino vartotojas, o saugojamos suskaičiuotos šių slaptažodžių maišos funkcijos reikšmės. Tokiu būdu piktavaliui perėmus šiuos slaptažodžius atkurti normalius slaptažodžius būtų praktiškai neįmanoma. Dar vienas būdas, naudojamas apsisaugoti nuo galimo slaptažodžio atspėjimo daugybės bandymų metu - riboti galimų bandymų prisijungti prie sistemos kiekį arba stebėti ir įrašyti įvykių žurnale vartotojų

bandymus prisijungti prie sistemos. Tokiu atveju aptikus, jog vartotojo vardu buvo bandoma kelis kartus tačiau nesėkmingai prisijungti, tolimesnis vartotojo prisijungimas būtų blokuojamas [3].

1.5.2. Biometriniais duomenimis paremta autentifikacija

Biometriniais duomenimis paremta autentifikacija yra procesas, kurio metu yra nuskaitoma kažkokia asmens kūno dalis. Tai gali būti akies rainelė, pirštų ar plaštakos antspaudai, taip pat skaitmeninis parašo nuskaitymas. Toliau šie nuskaityti duomenys yra paverčiami į skaitmeninę formą. Šie duomenys yra sulyginami su tais, kurie jau anksčiau yra išsaugoti ir susieti su šiuo vartotoju. Jai atitikimai rasti, tuomet vartotojas yra autentifikuojamas. Kiekvienas asmuo turi unikalias tam tikrų kūno dalių charakteristikas, dėl to tikimybė, kad asmuo bus autentifikuotas kaip kitas asmuo yra mažai tikėtina. Šio autentifikavimo būdo privalumas yra tas, vartotojui nereikia nieko žinoti ir nieko turėti. Jis tiesiog prideda tam tikrą savo kūno vietą prie skaitytuvo ir yra autentifikuojamas.

1.5.3. Viešojo rakto infrastruktūros autentifikacija (PKI – public key infrastructure)

Viešojo rakto infrastruktūros autentifikacija yra kitas būdas autentifikuoti asmenį. Asmeniui sertifikatų centras suteikia skaitmeninį sertifikatą, kuris vėliau yra panaudojamas autentifikacijai. Šiuo būdu užtikrinama, kad tas asmuo yra tikrai tas kuom jis dedasi esąs. Kiekvienas sertifikatas gali skirtis atsižvelgiant į tai, kokios rizikos, kokio slaptumo yra informaciją, kurią galima pasiekti panaudojus šį sertifikatą. Kiekvienas toks sertifikatas sudaromas priklausomai nuo to, kokia informaciją pateikė asmuo, registruojantis įmonėje ir kokia informacija yra pateikiama pačiame sertifikate. Vis labiau ir labiau yra naudojama skaitmeniniu sertifikatu paremta autentifikacija vienintelės registracijos sistemose, dokumentų valdymo sistemose ir internetiniuose serveriuose. Remiantis šia viešojo rakto infrastruktūra buvo sukurti keli autentifikavimo būdai: protingosios kortelės (Smart card) ir saugos raktas (Security token).

Protingoji kortelė – tai plastikinė kortelė, kurioje yra integruotas mikroprocesorius, kuris gali taip saugoti kažkokią informaciją ir ją apdoroti. Tokios kortelė yra plačiai naudojamos telefonijoje (sim kortelės), elektroniniuose mokėjimuose (kreditinės kortelės) ir kitose srityse. Šios kortelės yra naudojamos vartotojui autentifikuoti, remiantis viešojo rakto infrastruktūra. Kortelėje yra saugojamas užšifruotas sertifikatas bei visa kita informacija apie

vartotojo asmenybę. Dauguma organizacijų tokias korteles naudoja tam, kad būtų atpažinti jos darbuotojai. Jie tiesiog perbraukia, įkišą arba tik priliečia prie skaitytuvo kortelę ir jei asmuo yra autentifikuojamas tai organizacijos duomenų bazėje pažymima, kad jis jau darbe ir pan. Kuomet kortelė yra apjungiama su biometriniu vartotojų autentifikavimu, tuomet kortelė suteikia dviejų arba trijų lygių autentifikaciją. Tai žymiai sustiprina vartotojo autentifikacija, nes kiti asmenys negalės ja pasinaudot [12].

Autentifikavimo procesas vyksta sekančia tvarka:

1. Vartotojas įkiša kortelę į tam kortelių skaitytuvą
2. Tuomet kai kurie skaitytuvai reikalauja įvesti kortelės PIN numerį
3. Jei įvestas PIN numeris sutampa su tikruoju kortelės numeriu, tuomet vartotojo kortelė yra atpažįstama
4. Tuomet kortelės skaitytuvas perskaito informaciją iš kortelės arba siunčia į kortelę duomenis tam, kad būtų atlikta kažkokia operacija, tokia kaip pasirašymas su skaitmeniniu parašu (priklausomai nuo konkrečios situacijos kur ta kortelė yra naudojama).
5. Pasirašyti duomenys kartu su skaitmeniniu parašu ir sertifikatu, kurį jis pateikė kartu su siunčiamais duomenimis, keliauja į organizacijos informacijos apdorojimo įrenginius. Autentifikacija vyksta organizacijai kreipiantis į trečiąją šalį, sertifikavimo centrą, kuris ir išdavė vartotojui sertifikatą. Tuomet sertifikavimo centras patvirtina arba paneigia asmens tapatybę.
6. Kai organizacija gauna informaciją apie asmens tapatybę, kuri yra nepaneigiama, kadangi sertifikatas buvo išduotas konkrečiam asmeniui ir jis yra unikalus, tuomet organizacija gali atlikti kažkokias operacijas susijusias su to asmens duomenimis.

Lygiai toks pats autentifikavimo principas yra įgyvendintas saugumo rakte. Saugumo raktai yra dviejų tipų. Tai gali būti kažkoks prietaisas, savyje saugojantis informaciją, tokią kaip privatųjį raktą ar sertifikatą ir atliekantis duomenų pasirašymą. Kitas tipas tai programa, kuri yra įrašoma į vartotojo kompiuterį ir kuri taip pat savyje saugo vartotojo privatųjį raktą ar sertifikatą, bei atlieka pasirašymo funkciją. Visa informacija saugoma viename ar kitame saugumo rakte yra užšifruota panaudojant tik vartotojui žinomą PIN numerį arba slaptažodį. Taigi pametus tokį raktą ar pavogus, tokiu raktu būtų sunku pasinaudoti, kadangi būtų reikalingas slaptas PIN numeris arba slaptažodis tam raktui aktyvuoti. Šiuo atveju vartotojas turi atsiminti tik šį aktyvavimo numerį arba slaptažodį, o toliau, pasinaudodamas šiuo raktu, jis bus autentifikuotas taip, kaip autentifikuojama protingosios kortelės atveju [13].

1.5.4. Saugumo įranga paremta autentifikacija

Saugumo įranga paremta autentifikacija – tai yra kažkoks elektroninis prietaisas, skirtas autentifikuoti asmenį, kuris tą prietaisą turi. Egzistuoja RSA secureID prietaisas, kuris, jungiantis prie kažkokios sistemos, kuri yra susieta su tuo įrenginiu, sugeneruoja kažkokią atsitiktinę reikšmę, kurią reikia įvesti į atitinkamas vietas. Kadangi reikšmės nuolat kinta ir atsitiktine tvarka, todėl tokio tipo autentifikacija yra naudojama ten, kur reikalaujamas didesnis saugumas. Taip pat ši technologija yra brangesnė nei naudoti paprastą slaptažodžiu paremtą autentifikaciją, kadangi reikia kiekvienam iš vartotojų išduoti jo asmeninį prietaisą, tas prietaisas po kažkurio laiko yra keičiamas nauju ar atnaujinamas, o tai atitinkamai yra papildomos išlaidos [11].

1.5.5. Vienintelės registracijos autentifikacija

Vienintelė registracija (SSO – single sign on), sumažinta registracija (RSO – reduced sign on) arba įmonės vienintelė registracija (ESSO – enterprise single sign on) yra būdas sumažinti prisijungimo duomenų skaičių, kurį kiekvienas vartotojas turi atsiminti. Tokiu būdu vartotojas užsiregistruoja vienintelį kartą, kurio metu yra surenkama visa reikalinga ir svarbi informacija apie jį. Kai asmuo jungiasi prie sistemos, kurioje informacija nėra labai slapta, jis naudoja paprasčiausia autorizacijos būdą, tai slaptažodį. Jei tas pats asmuo nori prieiti prie slaptesnės informacijos, tai dėka šios SSO technologijos, jis turės įvesti kažkokia kitokią, svarbesnę informaciją, kad jis būtų autentifikuotas (tai gali būti biometriniai duomenys, sertifikatai, ar kažkokie įrenginiai autentifikacijai, kuriuos turi tik tas asmuo). Taigi yra išvengiama kelių registracijų toje pačioje sistemoje tam, kad pasiekti skirtingo saugumo lygio resursus. Vienintelės registracijos atvejo pavyzdys: atėjus į darbą, į kompiuterio kortelių skaitytuvą įkišama protingoji kortelė (angl. Smart Card), suvedamas PIN kodas, kad ji būtų aktyvuojama ir likusią dienos dalį nereikia atlikti kažkokių kitų prisijungimo veiksmų, nes viską atlieka protingoji kortelė [14].

1.5.6. Stipri autentifikacija

Stipri autentifikacija reiškia didesnis pasitikėjimas pačia autentifikacija. Pavyzdžiui, sėkmingai prisijungus prie sistemos panaudojant prisijungimo vardą bei slaptažodį, bus galima naudotis tik mažos rizikos informacija, kuri neturėtų padaryti didelės žalos, jei ji būtų pakeista ar sunaikinta. Tai yra todėl, kad slaptažodžiai nėra saugiausias būdas asmeniui

autentifikuoti, kadangi egzistuoja technologijos, kurių pagalba galima nesunkiai atspėti slaptažodžius. Taigi stipri autentifikacija – tai biometriniais duomenimis paremtos autentifikacijos, sertifikatų, kažkokios saugumo įrangos, panaudojimas. Daugelis įmonių naudoją šių autentifikacijų kombinacijas kartu su slaptažodžiu, tam, kad būtų apsaugoti skirtingos rizikos duomenys.

1.6. Autentifikavimo metodų rizikų ir trūkumų analizė

Kiekvienas iš prieš tai paminėtų autentifikavimo metodai turi ne tik gerų, bet ir blogų savybių ar trūkumų. Žemiau yra išvardinti kiekvienas iš minėtų autentifikavimo metodų ir jų trūkumai ir galimos rizikos, dėl kurių galimas klaidingas vartotojo autentifikavimas.

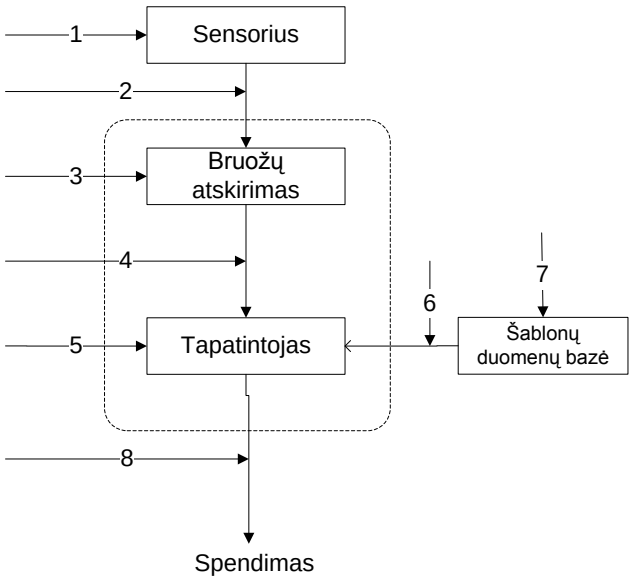
1.6.1. Slaptažodžiu paremtos autentifikacijos trūkumai ir galimos rizikos

Šis autentifikavimo būdas yra dažniausiai naudojamas įvairiose sistemose ar internetinėse svetainėse. Tai yra dėl to, kad šį autentifikavimo mechanizmą nesudėtinga realizuoti ir nedideli realizavimo kaštai. Tačiau jis nėra pakankamai saugus:

- Ryšio linijos stebėjimas. Įsilaužėlis stebi duomenų srautus tinkle ir mėgina perimti autentifikavimo metu siunčiamus atvirus arba užšifruotus slaptažodžius. Net ir užšifravus slaptažodį, galima mėginti vykdyti atkartojimo ataką, kurios metu mėginama atkartoti perimtus šifruotus pranešimus, juos įterpiant į ryšio liniją.
- Slaptažodžių failo perėmimas ir slaptažodžių iššifravimas. Šie failai operacinėse sistemose yra žinomi, o slaptažodžiai juose užšifruoti, tačiau gavus šį failą, daug paprasčiau vykdyti perrinkimo atakas.
- Grubios jėgos (angl. Brutus force), žodyno ir kitokios atakos, kurių esmė yra bandymas atspėti slaptažodį perrenkant įvairias kombinacijas (grubios jėgos atakos atveju), arba bandant įvairius žodžius (žodyno atakos atveju).
- Socialinė inžinerija. Tai mėginimas išgauti slaptažodžius iš žmonių, naudojančių atakuojamas sistemas. Ši ataka apima įbauginimo, apsimetimo metodus, taip pat netechninius slaptažodžių išgavimo būdus.
- Įvairios programinės įrangos, kurių pagalba yra išgaunami slaptažodžiai iš vartotojo kompiuterio (pvz. Trojos Arkliai) [3, 7].

1.6.2. Biometriniais duomenimis paremtos autentifikacijos galimos rizikos

Šis autentifikavimo būdas yra naudojamas svarbiuose įmonės ar įstaigos padaliniuose siekiant didesnio saugumo. Šiai technologijai realizuoti naudojama pakankamai brangi įranga. Tačiau ir šis autentifikavimo būdas turi savų trūkumų. Žemiau pateiktame paveikslėlyje (1 pav.) yra pavaizduota primityvi biometrinio autentifikavimo prietaiso schema ir sužymėtos vietos, kuriose galimos piktavalio atakos.



1 pav. Biometrinio autentifikatoriaus principinė schema

1. Piktavalis gali pateikti padirbtus biometrinius duomenis (pvz. dirbtinius piršto antspaudus, dirbtinį veidą, rainelę) juos nuskaitančiam sensoriui.
2. Pakartojant prieš tai nuskaitytus duomenis.
3. Piktavalis gali apgauti biometrinius duomenis apdorojantį modulį pateikdamas jam klaidingus duomenis.
4. Biometrinių duomenų tapatintojui pateikiami piktavalio duomenys, kuriuos jis sukeitė su tikraisiais vartotojo duomenimis.
5. Tapatintojas gali būti modifikuotas taip, kad piktavalio pateikti biometriniai duomenys būtų sutapatinami taip, kad gražintų teigiamą atsakymą, tai yra piktavalis būtų autentifikuotas.
6. Piktavalis gali sukeisti biometrinių duomenų šabloną kuris pateikiamas tapatintojui iš duomenų bazės.
7. Duomenų bazėje gali būti įterpti piktavalio biometriniai duomenys ir taip piktavalis galėtų būti laisvai autentifikuojamas .

8. Galiausiai gali būti pakeistas biometrinių duomenų skaitytuvo modulio rezultatas/sprendimas [4].

Šie atakų būdai yra itin sudėtingi ir reikalauja didelių pastangų.

Be šių atakų dar egzistuoja neigiama šio autentifikavimo metodo savybė, jog atsitikus kokiai nors tos kūno vietos, pagal kuria vartotojas autentifikuojamas, nelaimei (įsipjovus pirštą ar ranką ir panašiai), yra tikimybė jog vartotojas jau niekada nebebus autentifikuotas. Taip pat yra tikimybė jog vartotojas gali būti autentifikuotas ne iš pirmo karto arba piktavaliui bandantis autentifikuotis, sistema klaidingai nustatys jo tapatybę ir jis bus autentifikuotas [3].

1.6.3. Autentifikacijos paremtos viešojo rakto infrastruktūra trūkumai ir rizikos

Nors šia infrastruktūra paremtas autentifikavimo būdas naudoja įvairius matematinius algoritmus, kurių pagalba užtikrinamas duomenų saugumas, tačiau egzistuoja keli, šia infrastruktūra paremto autentifikavimo trukumai:

- Kad vartotojas galėtų pasinaudoti savo sertifikatu pasirašant dokumentus, jis turi suvesti PIN numerį arba slaptažodį, kurio pagalba bus aktyvuojamas sertifikato privatusis rakta. Taigi, kaip ir slaptažodžiu paremtoje autentifikacijoje, vartotojo PIN numeris arba slaptažodis gali būti išgaunamas įbauginimo, apsimetimo ar jėgos panaudojimo metu.
- Pamiršus sertifikato PIN numerį arba slaptažodį nėra galimybės jį kaip nors sužinoti, todėl reikėtų vėl kreiptis į sertifikavimo centrą, kad šis išduotų naują sertifikatą.
- Vartotojas per klaidą gali įtraukti nepatikimą sertifikatą į patikimų sertifikatų sąrašą [10].

1.6.4. Saugumo įranga paremtos autentifikacijos trūkumai

Ši technologija naudoja „autentifikatorių“ – tai yra prietaisą, kuris generuoja atsitiktinių skaičių seką, kurią reikia suvesti po to, kai vartotojas suveda savo PIN kodą ir gali tęsti tolimesnius veiksmus. Šis kodas kaip ir slaptažodis gali būti sužinomas jau aptartais būdais. Taigi vartotojas su savimi visą laiką turi nešiotis įrenginį, kuris reikalingas tik skaičių generavimui ir be kurio autentifikavimas neįmanomas. Taip pat gali sutrikti šios įrangos funkcionavimas jai sušlapus ar nukritus [2].

1.6.5. Vienintelės registracijos autentifikacijos trūkumai

Šis autentifikavimo būdas taip pat nėra pakankamai saugus, nes įkišus protingąją kortelę į kortelių skaitytuvą ir nuėjus nuo darbo kompiuterio kažkas kitas gali pasinaudoti ja ir prisijungti prie kažkokių įmonės resursų ar kitos sistemos [14].

1.6.6. Stiprios autentifikacijos trūkumai.

Tai yra gan saugus vartotojo autentifikavimo būdas, tačiau naudojama ne viena iš prieš tai išvardintų autentifikavimo technologijų, todėl realizuoti keletą iš jų yra brangu. Taip pat naudojant prieš tai išvardintus autentifikavimo būdus šioje autentifikacijoje, galioja tie patys trūkumai kaip ir kiekvieno iš jų. Šis autentifikavimo būdas yra naudojamas apsaugoti itin svarbius duomenis.

1.7. Analizės išvados

Šioje darbo dalyje buvo analizuojamos esamos atsiskaitymo sistemos ir egzistuojantys vartotojo autentifikavimo metodai ir pastebėta, jog:

- visos internetinio atsiskaitymo sistemos naudoja tą patį vartotojo autentifikavimo metodą – elektroniniu paštu bei slaptažodžiu paremtą vartotojo autentifikaciją;
- pastebėti keli šio vartotojų autentifikavimo metodo trūkumai:
  - Šis autentifikavimo būdas vartotojui gali būti nepatogus, kadangi reikia atsiminti sudėtingą slaptažodį, kuris turi tenkinti tam tikrus reikalavimus, o jį pamiršus, reikia užpildyti keletą internetinių apklausų, kad sistema būtų tikra, jog vartotojas yra tikrai tas asmuo, kuris bando jungtis prie atsiskaitymo sistemos.
  - Piktavaliui bandant prisijungti prie sistemos vartotojo sąskaitos (angl. account), po keleto nesėkmingų bandymų jis neturės galimybės toliau bandyti prisijungti. Tokiu atveju vartotojas, po kiekvieno tokio piktavalio bandymo, turės pildyti autentiškumui įrodyti reikalingas internetines apklausas, kadangi sistema bus užblokavus vartotojo sąskaitą. Tai yra apsisaugojimo priemonė, kad piktavalis spėliojimo ar žodyno atakos pagalba negalėtų prisijungti prie sistemos, tačiau vartotojui tai sukeltų nepatogumų.

- Taip pat, išanalizavus egzistuojančius vartotojo autentifikavimo būdus, galima teigti, jog šis autentifikavimo metodas nėra saugus, kadangi vartotojo slaptažodį piktavalis gali sužinoti apsimetimo ar įbauginimo būdu.

- kiekvienas iš analizuotų vartotojo autentifikavimo metodų turi savų privalumų, kurie vienu ar kitu atveju užtikrina saugų vartotojo autentifikavimą, tačiau taip pat egzistuoja ir trūkumai, dėl kurių piktavalis gali būti autentifikuotas vietoje tikrojo vartotojo.

2. INTERNETINIO ATSISKAITYMO SISTEMOS AUTENTIFIKAVIMO METODO SUKŪRIMO TIKSLAS IR REIKALAVIMAI

Atlikus egzistuojančių internetinių atsiskaitymo sistemų vartotojų autentifikavimo analizę, pastebėta, jog egzistuojantis autentifikavimo būdas visose analizuotose sistemose nėra pakankamai saugus. Norint padidinti vartotojų autentifikavimo šiose sistemose saugumą, reikia ieškoti kitų, geresnių, saugesnių, patikimesnių autentifikavimo metodų. Vienas iš būdų - autentifikuoti vartotoją pagal jo elektroninį parašą. Šis būdas remiasi analizės dalyje aptarta viešojo rakto infrastruktūra, kuri naudoja technologijas bei priemones, kurios užtikrina ne tik vartotojų autentifikavimą bei identifikavimą, bet ir duomenų konfidencialumą bei vientisumą, t.y. pagrindines saugumo savybes.

2.1. Nefunkciniai reikalavimai

Siekiant sukurti sistemą, kuri būtų paremta viešojo rakto infrastruktūra, reikia sudaryti reikalavimų sąrašą, kokias priemones naudoti ir kaip turėtų būti autentifikuojamas vartotojas sukurtoje sistemoje.

2.1.1. Užsakymo dokumentas

Internetinėje prekyboje perkant prekes ar paslaugas internetu yra sudaromas užsakymo dokumentas, kuris dažniausiai yra tik atvaizduojamas internetinės naršyklės ekrane. Tačiau kai kurios internetinės prekių ar paslaugų parduotuvės užsakymo dokumentą sukuria parsisiuntimui. Tai dažniausiai būna PDF (angl. Portable Document Format) formato dokumentas, kuriame yra pagrindinė informacija apie pirkėją, parduotuvę, užsakymo datą, prekių sąrašas su kiekiais ir prekių pavadinimais bei kainomis.

Kuriamoje sistemoje užsakymo dokumentas turėtų būti sukuriamas XML (angl. Extensible Markup Language) formato. XML – išplečiama ženklinimo kalba (angl. Extensible Markup Language), kuri yra universalus struktūrizuotų duomenų ir dokumentų formatas pasauliniame žiniatinklyje. XML vadinama išplečiama dėl to, kad ją galima išplėsti taikant verslo, valdžios, mokslo, akademinės veiklos ir kt. reikmėms, t.y. visur kur keičiamasi informacija. Pagrindinis XML sistemos komponentas yra duomenys. Šiuose dokumentuose yra duomenys ir žymos, kuriuos apibudina ką šie duomenys reiškia. Tai vienas iš pagrindinių dokumento formatų naudojamas keičiantis duomenimis tarp komunikuojančių šalių. Šis formatas yra nepriklausomas nuo platformos kurioje jis naudojamas, t.y. bet kuri programa,

pritaikyta šiam duomenų formatui, gali skaityti, rašyti ir apdoroti bet kokius duomenis esančius šiame dokumente, neatsižvelgiant į operacinę sistemą ar techninę įrangą.

Šiame dokumente, kaip ir prieš tai minėtame PDF formato dokumente, turėtų būti saugomi tokie patys duomenys, tačiau struktūrizuotai, t.y. sudėlioti į tam tikrus laukelius, vadinamus žymomis.

Kad XML dokumentas būtų sukurtas tvarkingai, t.y. kad duomenys atitiktų tam tikrus formatus, jų ilgis neviršytų tam tikro dydžio ir kad būtų saugomi visi reikalingi duomenys, reikia nustatyti tam tikras, šiam dokumentui skirtas taisykles. Šias taisykles saugo XML schemos. Tai taip pat XML dokumentas, kuriame saugojama informacija, kaip XML dokumentai turėtų būti kuriami, t.y. XML schema yra taisyklių rinkinys, rodantis, kas gali ir ko negali būti atskirose XML dokumento vietose. Šiame dokumente yra saugojami aprašai, kurie nusako duomenų tipus, galinčius būti kiekvienoje XML failo žymoje, taip pat saugojami papildomi sekų aprašai, rodantys žymių eilės tvarką duomenų faile, bei saugojami duomenų tipai, kontroliuojantys, kokie duomenų tipai gali būti kiekvienoje duomenų failo žymoje: tekstas, skaičius, taip ir ne pasirinkimas ir pan. Šios schemos užtikrina saugumą nuo nepageidaujamų duomenų, kurie galėjo būti įterpti piktavalio kuriuo nors XML dokumento kūrimo ar siuntimo metu. Taigi turėtų būti sukurta XML schema užsakymo dokumentui teisingai suformuoti.

2.1.2. Dokumento elektroninis parašas

Kuriamas autentifikavimo būdas, kuris vartotoją autentifikuos pagal jo elektroninį parašą. Šis parašas kaip ir įprastas žmogaus parašas dokumento pabaigoje, taip ir čia yra papildoma informacija pridedama prie dokumento, pagal kurią galima nustatyti (autentifikuoti) dokumento autorių.

Kadangi duomenims apsikeisti bus naudojamas XML formato dokumentas, tuomet atitinkamai e. parašas turės būti įterptas į šį dokumentą.

2.1.3. Duomenų konfidencialumas

Užsakymo dokumentas kuriamoje sistemoje turės informaciją apie perkamas prekes, jų kainas, visą įsigyjamų prekių sumą. Tai yra privatūs duomenys, t.y. niekas šių duomenų neturėtų matyti, nes tai galėtų atskleisti vartotojo finansinę būklę, jo įsigyjamą turtą ir panašiai. Nors tarpusavyje bendrauja tik prekyboje dalyvaujančios šalys, galimas ir piktavalių įsikišimas (žmogus viduryje ataka). Piktavalis galėtų perimti duomenis siunčiamus ar iš parduotuvės pirkėjui, ar iš pirkėjo atgal į parduotuvę, ar iš parduotuvės apmokėjimo sistemai.

Perėmęs duomenis jis galėtų juos pakeisti, sunaikinti arba tiesiog perskaityti ir siųsti tikrajam gavėjui. Pakeistus duomenis gavėjas iš kart tai aptiktų, kadangi naudojamas e. parašas, kuris užtikrina duomenų vientisumą. Tačiau piktavaliui tik perskaičius ir siuntus toliau duomenis, apie tai nesužinotų gavėjas. Taigi tam, kad piktavalis perėmęs duomenis, keliaujančius internetu tarp internetinėje prekyboje dalyvaujančių šalių, negalėtų perskaityti siunčiamos informacijos, XML dokumento duomenys turėtų būti šifruojami, tokiu būdu užtikrinant duomenų konfidencialumą. Tokiu atveju turėtų būti naudojamas SSL protokolas, kuris internetu keliaujančius duomenis užšifruoja panaudojant vieną iš simetrinių šifravimo algoritmų. Naudojamas simetrinis šifravimo algoritmas, kadangi užšifruoti duomenys yra greičiau iššifruojami, o tai yra svarbu, kuomet reikalingas greitas atsakymas iš kliento serveriui ar atvirkščiai.

2.2. Funkciniai reikalavimai

2.2.1. Reikalavimai vartotojui ir jo programinei įrangai

Vartotojas (pirkėjas) – fizinis arba juridinis asmuo, kuris perka prekes internetinėje parduotuvėje. Tai yra pagrindinis prekybos dalyvis. Kad vartotojas galėtu atsiskaityti už prekes kuriamoje atsiskaitymo sistemoje, jis turi turėti savo asmeninį sertifikatą, kurį jam turėtų išduoti sertifikavimo centras. Turint sertifikatą vartotojas turi gauti programinę įrangą, skirtą pasirašinėti dokumentus. Su internetinio atsiskaitymo sistema vartotojas turėtų sudaryti sutartį ir susikurti savo vartotojo sąskaitą, kurioje galės patalpinti norimą kiekį pinigų. Šia institucija vartotojas turi visiškai pasitikėti.

Vartotojas, norėdamas pirkti prekes internetu, turi turėti įrankį, kurio pagalba tai galėtų atlikti. Tai gali būti personalinis kompiuteris ar kita įranga, kuri gali prisijungti prie interneto ir naršyti internetines svetaines. Ši įranga turi turėti įdiegtą internetinę naršyklę, per kurią pirkėjas galėtų pasiekti internetinės parduotuvės svetainę. Taip pat turi būti užtikrinamas bent minimalus internetinis ryšys, kad būtų įmanoma atlikti pirkimus. Jeigu vartotojas sertifikatą, bei programinę įrangą, skirtą pasirašinėti dokumentams, turi USB atmintinėje, tuomet įrenginys, per kurį bus atliekamas pirkimas, taip pat turi turėti USB jungtį. Nesvarbu ar tai yra draugo, ar kaimyno, ar viešosios įstaigos kompiuteris, turėdamas šią atmintinę, jis galės atlikti pirkimus ir mokėjimus už prekes ar paslaugas.

Kai vartotojas gauna užsakymo dokumentą, kurią jam atsiuntė internetinė parduotuvė, jis turi turėti galimybę tą dokumentą peržiūrėti. Tai yra būtina funkcija, kurią turi atlikti programinė įranga vartotojo kompiuteryje, kadangi vartotojas turi žinoti ką jis pasirašinėja.

Taip pat turi būti galimybė vartotojui patikrinti internetinės parduotuvės parašą, kad įsitikinti, jog gautas užsakymo dokumentas yra nepakeistas ir tikrai iš tos parduotuvės, kurioje jis užsisakė prekes. Kita svarbi funkcija, kurią turi atlikti vartotojas savo kompiuteryje, tai pasirašyti užsakymo dokumentą. Turėdamas sertifikatą, bei pasirašymo programinę įrangą, vartotojas savo kompiuteryje peržiūrėjęs gautą dokumentą ir įsitikinęs, jog tai yra ta parduotuvė, tą patį dokumentą pasirašo pats. Tai yra pagrindinis kuriamos sistemos kriterijus. Pagal vartotojo parašą jis bus vėliau autentifikuotas atsiskaitymo sistemoje, su kuria, kaip prieš tai minėta, yra sudaryta sutartis ir bus atlikti mokėjimai. Gautą užsakymo dokumentą vartotojas turi išsisaugoti kompiuteryje, todėl, jeigu pirkimai ir mokėjimai yra atliekami ne su savo personaliniu kompiuteriu ar ne savo vartotoju sistemoje, tuomet būtina pasirūpinti, kad gautas ir vėliau pirkėjo pasirašytas užsakymo dokumentas (byla) būtų pilnai pašalintas iš kompiuterio, arba jis turi būti saugomas vartotojo USB atmintinėje. Toliau šį užsakymo dokumentą vartotojo programinė įranga turėtų nusiųsti atgal internetinei parduotuvei iš kurios jis gautas. Iš šios parduotuvės iškart turėtų gauti atsakymą apie pavykusį ar nepavykusį apmokėjimą.

2.2.2. Reikalavimai internetinei parduotuvei

Internetinė parduotuvė – tai parduotuvė, kuri prekes ar paslaugas pardavinėja internetu. Ji pateikia prekių ar paslaugų sąrašą su jų aprašymais, iliustracijomis bei kaina. Pirkėjui turi būti suteikta galimybė sudaryti prekių krepšelį, t.y. pirkėjui pasirinkus norimas prekes iš pateikto sąrašo, jos turi būti kaupiamos krepšelyje ir vėliau krepšelį būtų galima modifikuoti (pašalinti prekes, padidinti esamų prekių kiekį ir pan.). Pasirinkus prekes vartotojas turi gauti užsakymo dokumentą su prekių sąrašu bei prekių kainomis. Tuo pačiu parduotuvė rezervuoja prekes, kurias pasirinko vartotojas. Ši parduotuvė, taip pat kaip ir kiekvienas pirkėjas, turi būti sudarius kažkokia sutartį su atsiskaitymo sistema, kadangi per ją bus atliekami visi mokėjimai už įsigytas prekes ar paslaugas. Taip pat parduotuvė turi turėti jai išduotą sertifikatą. Jai sertifikatas reikalingas tam, kad galėtų su juo pasirašinėti pirkėjams siunčiamus užsakymo dokumentus. Tokius dokumentus pirkėjas gali patikrinti ir įsitikinti kad tai yra ta parduotuvė, kurioje jis perka prekes ar paslaugas. Internetinė parduotuvė turi, pagal tam tikras taisykles sudaryti užsakymo dokumentą. Šis dokumentas remiasi XML struktūra, kuriame turi būti patys būtiniausi duomenys apie įsigyjamas prekes, jų kainas, bei kiekius. Šį dokumentą parduotuvė turi pasirašyti savo elektroniniu parašu, kad būtų užtikrintas dokumento vientisumas, kai jis bus nusiųsta pirkėjui, o vėliau ir bus autentifikuota parduotuvė. Pirkėjui patvirtinus perkamu prekių sąrašą, pasirašytas užsakymo dokumentas

turi būti siunčiamas pirkėjui. Vėliau, gavus patvirtinimą iš atsiskaitymo sistemos, kad mokėjimas atliktas, parduotuvė turi nusiųsti prekes pirkėjui.

2.2.3. Reikalavimai internetinio atsiskaitymo sistemai

Internetinio apmokėjimo sistema – tai sistema, kuri atlieka saugius apmokėjimus už internetinėje parduotuvėje pasirinktas prekes ar paslaugas, kurios paslaugomis gali naudotis internetinės parduotuvės, sudariusios sutartis su šia sistema. Sistema taip pat naudosis ir patys pirkėjai, kurie taip pat sudarę sutartis su ja. Pirkėjai šioje sistemoje susikurs savo vartotoją, pateikę visą būtiną informaciją, kartu ir savo viešojo rakto sertifikatą, kad ši sistema vėliau galėtų pilnai autentifikuoti pirkėją sistemoje. Turėdamas sertifikatą pirkėjas iš šios sistemos turi gauti pasirašymo programinę įrangą. Ši įranga vartotojui gali būti įteikta USB atmintinėje, kuri vėliau bus naudojama pasirašant užsakymo dokumentus. Taip pat pirkėjas gali turėti kreditą, kuris reikalingas užmokėti už prekes ar paslaugas. Sertifikatą taip pat turi turėti ir internetinės parduotuvės, nes jos taip pat dalyvauja internetinio atsiskaitymo procese. Visos vartotojų šalys turi pasitikėti šia sistema.

Pirkėjui užsisakius prekes internetinėje parduotuvėje, ši atsiunčia abiejų, ir parduotuvės ir pirkėjo pasirašytą užsakymo dokumentą. Šiuos parašus sistema turi patikrinti, kad įsitikinti, jog tai yra tie veikėjai kurie ir turi būti ir, kad atkeliavę duomenys nebuvo pakeisti keliaujant internetu. Patikrinus parašus, vartotojas šioje sistemoje turi būti autentifikuojamas remiantis jo e. parašu. Šiame paraše esanti sertifikato informacija yra panaudojama surandant pirkėjo ar parduotuvės sąskaitų duomenis apmokėjimo sistemoje. Kadangi vartotojas ir internetinė parduotuvė registruodamiesi apmokėjimo sistemoje pateikė savo sertifikatą kaip asmens duomenis, todėl pagal tai jie bus atsekami sistemoje ir surandami jų sąskaitų duomenys. Tuomet sistema turi nuskaityti duomenis iš užsakymo dokumento, kad sužinoti kokią sumą pirkėjas turi sumokėti. Taip pat turi patikrinti ar yra pakankamas kredito limitas, kad susimokėti už prekes ar paslaugas. Jei kredito neužtenka apmokėti, tuomet sistema turi siųsti pranešimą internetinei parduotuvei, kad mokėjimas nepavyko. Savo ruožtu internetinė parduotuvė turi informuoti pirkėją apie nepavykusį mokėjimą. Jei kredito limitas yra pakankamas, tuomet sistema turi nuskaičiuoti reikiamą sumą iš vartotojo kredito sąskaitos, o apie pavykusį mokėjimą turi pranešti internetinei parduotuvei, kuri toliau galėtų atlikti tolimesnius veiksmus, tokius kaip prekių siuntimą pirkėjui.

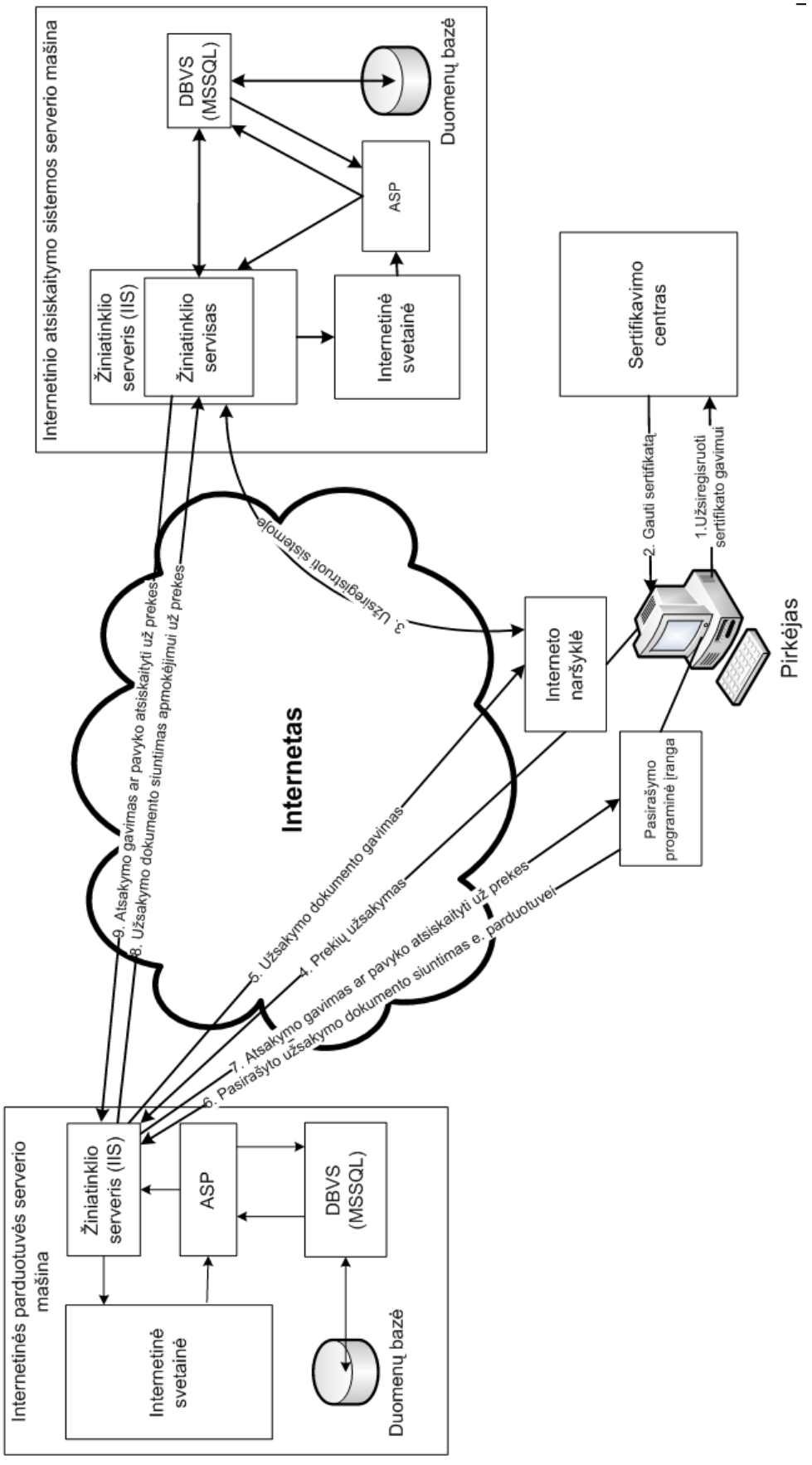
3. INTERNETINIO ATSISKAITYMO SISTEMOS MODELIS

3.1. Kuriamo vartotojo autentifikavimo apibrėžimas

Siekiant sukurti naują internetinio atsiskaitymo sistemų vartotojo autentifikavimo būdą, bus sukurtos trys internetinėje prekyboje komunikuojančios šalys: pirkėjas (programinė įranga užsakymo dokumentų pasirašymui), e. parduotuvė ir atsiskaitymo sistema. Šioje sistemoje vartotojas bus autentifikuojamas pagal jo parašą, kuris bus užsakymo dokumente. Kad tai atlikti bus sukurta programinė įranga – saugos raktas, kuris atliks duomenų pasirašymo funkciją. Šis saugos raktas bus įdiegtas vartotojo kompiuteryje. Kiekvienas internetinės prekybos vartotojas turės turėti asmeninį sertifikatą, bei gauti saugos raktą, su kuriuo bus atliekamas užsakymo dokumentų pasirašymas. Kuriamos sistemos tikslas nėra parodyti kokias operacijas atlieka atsiskaitymo sistema apmokant už prekes, bet kaip galėtų būti autentifikuojamas vartotojas internetinio atsiskaitymo sistemoje panaudojant e. parašą.

Sistema bus realizuota panaudojant ASP.NET technologiją, C# programavimo kalbą ir MS SQL duomenų bazės valdymo sistemą.

3.2. Internetinio atsiskaitymo sistemos konteksto schema



2. pav. Internetinio atsiskaitymo sistemos konteksto schema

Pateiktoje konteksto schemoje (2 pav.) yra pavaizduota visa seka veiksmų tarp internetinėje prekyboje dalyvaujančių šalių. Kaip matome jų yra trys: pirkėjas, internetinė parduotuvė, apmokėjimo sistema. Visos dalyvaujančios šalys tarpusavyje bendrauja per viešąjį tinklą – internetą.

Kuriamoje sistemoje tik apmokėjimo sistema autentifikuoja kitas šalis tam, kad jos galėtų sėkmingai vykdyti prekių pardavimus, užsakymus ir atsiskaitymus už jas. Kadangi apmokėjimo sistema kartu yra ir trečioji patikimoji šalis, todėl vartotojas pasitiki ja ir jam autentifikuoti parduotuvės nereikia, nes ji ir taip bus autentifikuota trečios patikimos šalies, t.y. apmokėjimo sistemos. Vartotojas turi tik patikrinti ar parduotuvės atsiųstas dokumentas nebuvo modifikuotas. Nors tą pati vėliau atliks ir apmokėjimo sistema, tačiau vartotojas gali patikrinti ar duomenys nebuvo pakeisti. Kaip ir vartotojas taip ir parduotuvė turi patikrinti dokumento vientisumą ar vartotojas nepakeitė dokumento prieš atsiunčiant jį parduotuvei. Ši parduotuvė taip pat pasitiki apmokėjimo sistema kaip trečiąja patikima šalimi ir jai vartotojo autentifikuoti nėra būtinybės.

Kad apmokėjimo sistema galėtų autentifikuoti prekyboje dalyvaujančius pirkėjus ir e. parduotuves, jie turi turėti patikimus sertifikatus, tai yra sertifikatus, kuriuos išdavė patikimas sertifikavimo centras, kuriuo pasitiki visos prekyboje dalyvaujančios šalys. Šių sertifikavimo centrų sertifikatus atsiskaitymo sistema turėtų įtraukti į patikimų sertifikatų sąrašą ir vėliau galima būtų autentifikuoti kiekvieną vartotoją, jai jų sertifikatai buvo išduoti iš vienos iš šių sertifikavimo centrų.

3.3. Dokumento elektroninio parašo formavimas

3.3.1. XML dokumentas

Kuriamoje sistemoje XML vyrauja perduodant informaciją iš internetinės parduotuvės pirkėjui, pirkėjui atgal siunčiant parduotuvei ir pastarajai siunčiant atsiskaitymo sistemai. Šio tipo dokumente yra saugojama visa reikalinga informacija, susijusi su prekėmis, kurias pirkėjas užsisakinėja, t.y.: prekės pavadinimas, kaina, kiekis, užsakymo data ir pan. Taip pat siunčiama kita, viena svarbiausių dokumento dalių tai elektroninis parašas, kuris yra tame pačiame XML dokumente.

XML dokumentus kuria internetinė parduotuvė tuomet, kai pirkėjas pareikalauja užsakymo dokumento. Tuomet yra sugeneruojamas XML dokumentas ir atsiunčiamas pirkėjui. Kad pirkėjas galėtų tinkamai perskaityti šiame dokumente saugomą informaciją, jis turi žinoti kaip tas dokumentas yra sudarytas. Atsiskaitymo sistema, gaudama šį dokumentą,

taip pat turi žinoti kaip šis dokumentas yra sudarytas. Taigi visos šalys turi žinoti kuriamo dokumento sandara, kitaip tariant, dokumentas turi būti sudarytas pagal tam tikrus kriterijus ir taisykles, kurias žino visos šalys. Taigi užsakymo XML dokumentas turi būti sukuriamas remiantis XML schema. Pagal šią schemą, visos trys šalys (internetinė parduotuvė, pirkėjas ir atsiskaitymo sistema) žino kokie ir kiek duomenų, gautų XML duomenų failo pavidale, gali ir turi būti. Taip pat įsitikinama, jog dokumentas yra taisyklingas, kad jo niekas nemodifikavo ir kad įvesti duomenys atitinka keliamus reikalavimus.

Šią schemą turi sukurti atsiskaitymo sistema, kadangi ji yra atsakinga už kliento duomenų patikimumą ir saugumą. Taigi, pagal atsiskaitymo sistemos sukurtą schemą, internetinė parduotuvė turės sukurti XML failą su tokiais duomenimis ir tokia tvarka, ir taisyklingumu, kokie yra aprašyti toje schemoje. Šią schema atsiskaitymo sistema paskelbia visoms šalims, kadangi ir vartotojas turi patikrinti, ar gauta iš parduotuvės užsakymo forma yra teisinga. Vartotojas tikrina dėl to, kadangi turės pasirašyti šią formą, todėl jam reikės ją peržiūrėt prieš pasirašant, kad jis žinotų ką pasirašinėja: kad visi duomenys yra taisyklingi, kad prekių pavadinimai, kainos ir kiekiai yra tokie, kokius jis pats pasirinko, rinkdamasis prekes toje internetinėje parduotuvėje, kad nėra jokių kitų papildomų duomenų, kurie nėra įtraukti į XML schemos aprašus. Tai gali atsitikti tuomet, kai piktavalis, perėmęs siunčiamą failą, įterpia savo duomenis. Pastarąjį atvejį tikrina ir atsiskaitymo sistema, kadangi, jeigu bus įvesti papildomi duomenys, tai nuskaitant duomenis gali būti nuskaityti šie, piktavalio įvesti duomenys, ir tuomet bus atlikti veiksmai, naudingi piktavaliui (pvz. pinigai už prekes pervesti ne internetinei parduotuvei, o pervesti į piktavalio sąskaitą).

3.3.2. Elektroninis parašas.

Elektroninis parašas – tai technologija, leidžianti naudoti elektroninius dokumentus užtikrinant jų autentiškumą ir vientisumą. Tai bet kokio pavidalo koduota informacija, pagal kurią vienas kompiuterių sistemos vartotojas gali patvirtinti savo tapatybę bet kuriam kitam sistemos vartotojui ir pagal kurią parašo gavėjas nešališkai trečiajai šaliai gali įrodyti, kad parašas yra autentiškas. E. parašas atitinka tradicinį, ranka rašytą parašą, tačiau viskas vyksta elektroninėje erdvėje. E. parašas – tai prie duomenų bloko pridėti duomenys arba jų kriptografinė transformacija, leidžianti duomenų bloko gavėjui įrodyti duomenų bloko kilmę bei vientisumą ir apsisaugoti nuo klastojimo [8]. Taigi elektroninis parašas užtikrina duomenų vientisumą, autentiškumą bei neišsiginamumą.

Kuriamoje atsiskaitymo sistemoje bus naudojama RSA parašo sistema. Šioje sistemoje raktų pora generuojama analogiškai kaip ir asimetrinio šifravimo sistemose. Raktų

generavimo algoritmui pateikiamas saugumo parametras, kurį atitinka RSA modulio ilgis bitais. Algoritmo rezultatas yra raktų pora.

Kuriamoje sistemoje vartotojas raktų porą gaus kartu su jo asmeniniu sertifikatu. Tai yra elektroninis liudijimas, susiejantis parašo tikrinimo duomenis su pasirašančiuoju asmeniu ir patvirtinantis (arba leidžiantis nustatyti) pasirašančiojo asmens tapatybę. Dažniausiai naudojami X.509 standarto sertifikatai, o parašo tikrinimo duomenys su pasirašančiojo asmens duomenimis paprastai susiejami sertifikavimo centro e. parašu.

Viešojo rakto sertifikate būtinai turi būti šie duomenys:

- vartotojo vardas (arba slapyvardis) (subject);
- vartotojo viešasis raktas, atitinkantis jo turimą privatų raktą (subjectPublicKey);
- sertifikato galiojimo pradžios ir pabaigos terminai (notBefore ir notAfter);
- sertifikatą sudariusiojo SC ir jo buveinės bei šalies identifikatoriai (issuer);
- sertifikato, kurį suteikia SC, identifikatorius (serialNumber);
- sertifikato naudojimo paskirtis;
- SC e. parašas [7].

Skaitmeninius sertifikatus galima saugoti visuose įrenginiuose, kuriais perduodama informacija į kompiuterį, nes bet kurį sertifikatą galima išsaugoti įprastame apibrėžtos struktūros faile. Kuriamoje sistemoje sertifikatai bus saugojami tiek vartotojo kompiuteryje, tiek internetinės svetainės serveryje.

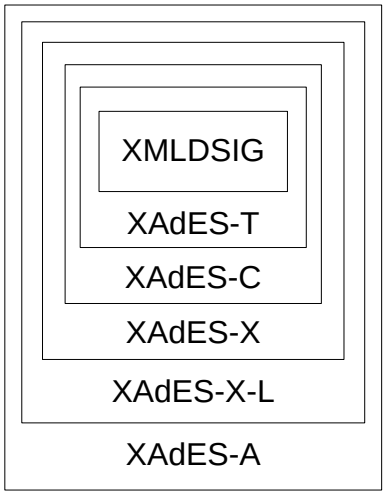
3.3.3. XML dokumento e. parašas

E. parašas bus formuojamas remiantis XAdES specifikacija, kuri aprašo XML parašų apdorojimo taisykles ir sintaksę. Pagal šią specifikaciją, galima pasirašyti atskirus XML dokumento objektus arba visą dokumentą. Kuriamoje sistemoje bus pasirašomas visas XML dokumento turinys, kadangi visa informacija yra svarbi ir pakeitimai pasirašytame dokumente yra netoleruojami.

Kuriamoje sistemoje bus pasirašinėjamas tas pats XML dokumentas, kurį sugeneruoja internetinė parduotuvė. Šį dokumentą turės pasirašyti ir internetinė parduotuvė ir pirkėjas. Tai yra daroma todėl, kad pirkėjas galėtų įsitikinti, kad gautas XML dokumentas nebuvo pakeistas pakeliui pas jį, bei pirkėjui pasirašius, atsiskaitymo sistema galės jį autentifikuoti pagal parašą, kas ir yra šio kuriamo autentifikavimo būdo pagrindinis akcentas. Atsiskaitymo sistema taip pat turės patikrinti ir internetinės parduotuvės parašą, kad žinotų kokiai parduotuvei pervesti pinigus, kuriuos sumoka pirkėjas pirkdamas prekes.

XAdES specifikacija aiškiai nurodo kaip turi būti pasirašyti dokumentai, kur elektroninio parašo informacija turi būti saugoma (apvilktas parašas ar atskiras parašas), taip pat joje yra nurodoma kokius algoritmus naudoti skaičiuojant santraukas (*SHA-1*), pasirašant (privalomas *DSA*, rekomenduojamas *RSA*), autentifikuojant pranešimą (*HMAC*), suvedant i kanoninį pavidalą, transformavimui (*Enveloped Signature, XPath*). Kiti svarbūs duomenys, kurie turi būti patalpinti į pasirašomą XML dokumentą - pasirašiusiojo viešojo rakto sertifikatas. Jis bus reikalingas patikrinant gautų duomenų vientisumą, bei autentifikuojant vartotojus.

XAdES parašų realizavimas yra pagrįstas *Object* elementu, kuriame saugojamos patikslinamosios parašų savybės. Pagal funkcionalumą skirstomos pasirašomos ir nepasirašomos savybės. Pasirašomos savybės yra apsaugotos tuo pačių pasirašančiojo parašu kaip ir dokumentas, o nepasirašomos savybės tai duomenys, kuriems tokia apsauga nebereikalinga arba apskritai tokių duomenų nėra (pasirašymo metu tokie duomenys neegzistuoja). Pagal funkcionalumą skiriamos kelios tolygiai didėjančio sudėtingumo XAdES sintaksės formos. Visos šios formos yra glaudžiai susijusios su XMLDSIG. Šios formos pateiktos paveiksliuke (3 pav.).



3 pav. XAdES sintaksės formos [7]

Pirmoji bazinė forma yra XAdES (angl. *XML Advanced Electronic Signature*). Šis standartas yra tokios pačios struktūros kaip ir XMLDSIG standartas, tačiau turi papildomas, pasirašomas savybes (*SigningTime*, *SigningCertificate*, *SignaturePolicyIndentifies*, *SignatureProductionPlace*, *SignerRole*, *AllDataObjectsTimeStamp*, *IdividualDataObjectTimeStamp*, *DataObjectFormat* ir *CommitmentTypeIndication*) ir nepasirašomas savybes (*CounterSignature*). Ši parašo forma užtikrina, jog pakeitus sertifikatą, kurio vienodi raktai, bet skirtinga pasirašiusiojo (sertifikavimo centro) informacija

ar skirtinga panaudojimo paskirtis, parašas būtų laikomas negeru, kadangi pasirašomosiose savybėse būtų saugojama pasirašiusiojo sertifikavimo centro informacija ir pasirašiusiojo vartotojo sertifikato duomenys (pvz. sertifikato serijos numeris). Kita standarto forma yra XAdES-T (angl. *XML Advanced Electronic Signature with Time-Stamp*), kurioje papildomai įdedama laiko žyma (angl. *time-stamp*) į XAdES formą tam, kad užtikrintų, jog parašas egzistavo prieš joje nurodytą laiko momentą. Jei tuo laiko momentu signataro sertifikatas galiojo ir nebuvo atšauktas, parašą galima laikyti galiojančiu net tuomet, kai šios dvi sąlygos netenkinamos. Ši žyma turėtų būti pridedama netrukus, kai dokumentas buvo pasirašytas. Šios formos standarte lyginant su XAdES forma *UnsignedSignatureProperties* elemente papildomai atsiranda vaikinis elementas *SignatureTimeStamp*. XAdES-C (angl. *XML Advanced Electronic Signature with Complete validation data*) yra kita XAdES standarto forma, kuri prideda parašo nuorodas į duomenis, lengvinančius parašo tikrinimą – sertifikatų grandinėlės hierarchiją, bei atitinkamą atšaukimo informaciją. Šios formos standarte lyginant su XAdES forma *UnsignedSignatureProperties* elemente papildomai atsiranda vaikiniai elementai *CompleteCertificateRefs* ir *CompleteRevocationRefs*. Sekanti forma XAdES-X (angl. *XML Advanced Electronic Signature with eXtended validation data*) laiko žyma apsaugo nuorodas į parašo tikrinimo duomenis, o jai reikia ir *ds:Signature* elementą. Papildomai *UnsignedSignatureProperties* elemente dar atsiranda *RefsOnlyTimeStamp* ir *SigAndRefsTimeStamp*. XAdES-X-L (angl. *XML Advanced Electronic Signature with eXtended validation data incorporated for the Long term*) prideda parašo tikrinimo duomenis. Kitaip nei XAdES-C, saugomi patys duomeys: forma skirta tiems atvejams, kai negalima pasinaudoti PKI paslaugų tiekėjo archyvais. Papildomai *UnsignedSignatureProperties* elemente atsiranda *CertificateValues* ir *RevocationValues*. Paskutinė standarto forma XAdES-A (angl. *XML Advanced Electronic Signature with Archiving data*) prideda papildomas laiko žymas, apsaugančias parašus nuo kriptografinių duomenų susilpnėjimo. *UnsignedSignatureProperties* elemente papildomai atsiranda *ArchiveTimeStamp* [7, 15].

Kuriamoje sistemoje naudosime pirmąją XAdES parašų formą. XML parašas generuojamas dviem žingsniais:

- Generuojamos nuorodos;
- Generuojamas parašas.

Nuorodų generavimo etapai:

- Duomenų objekto transformacija;
- Gauto rezultato santraukos apskaičiavimas;
- Nuorodos elemento (*reference*) sukūrimas su įvardytu santraukos algoritmu ir santraukos reikšme.

Parašo generavimas:

- Sukuriamas pasirašytos informacijos elementas (*SignedInfo*), nurodžius parašo metodą (*SignatureMethod*), kanoninio pavidalo sudarymo metodą (*CanonicalizationMethod*) ir nuorodą;
- Pasirašyta informacija verčiama kanoniniu pavidalu ir apskaičiuojama parašo reikšmė (*SignatureValue*) pasirašytoje informacijoje nurodytais algoritmais.
- Sukuriamas parašo elementas (*Signature*), kuriame yra pasirašyta informacija, rakto informacija (jei reikia) ir parašo reikšmė.

Atitinkamai XMLDSIG parašo tikrinimas specifikacijoje yra vadinamas *core validation*. Jį sudaro du etapai: nuorodos tikrinimas (dokumentų santraukų tikrinimas) ir parašo tikrinimas (*SignatureValue* reikšmės tikrinimas).

Nuorodos tikrinimas:

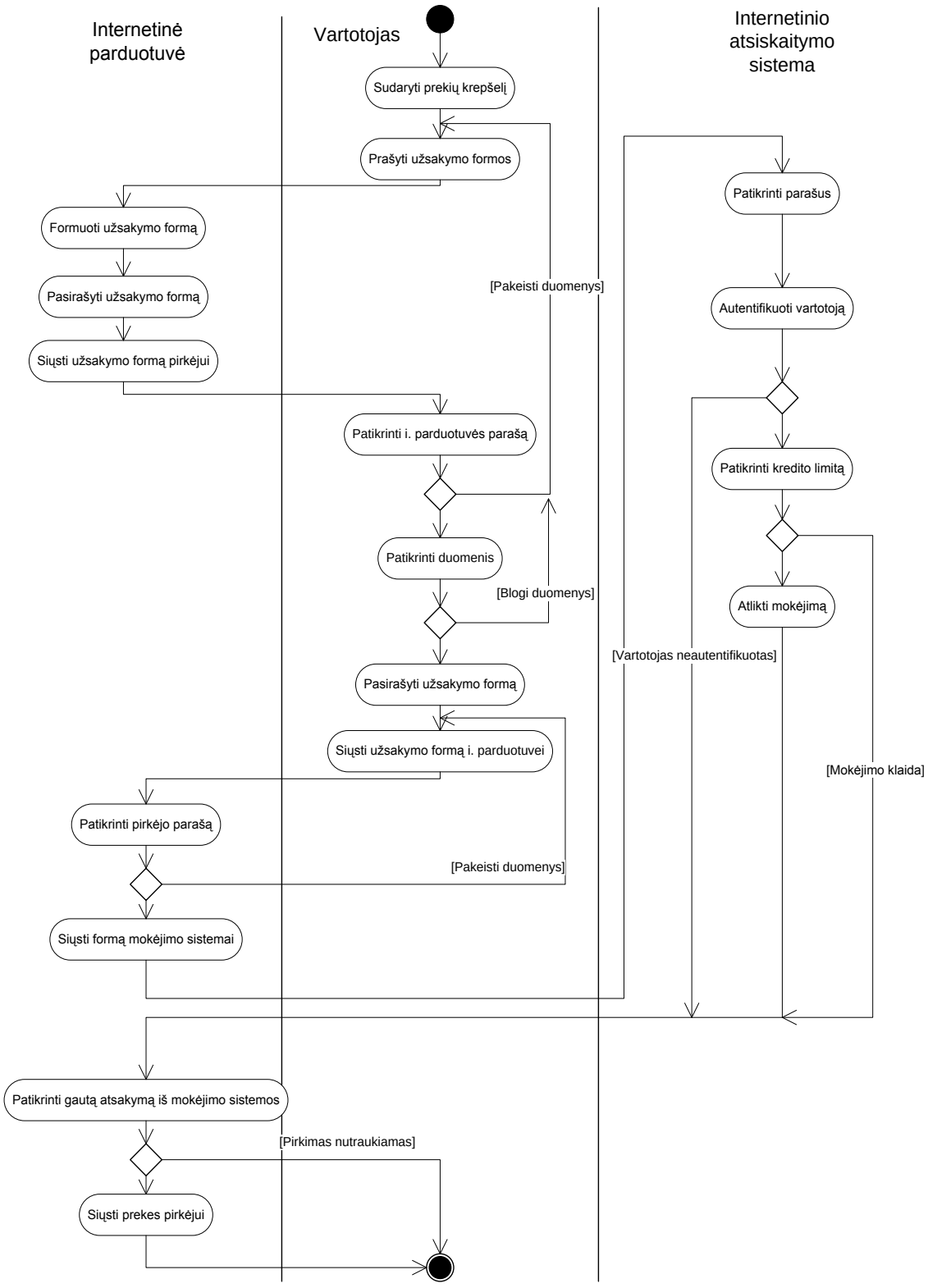
- Pasirašytų duomenų išgavimas;
- Santraukos apskaičiavimas nurodytais metodais
- Gautos santraukos palyginimas su pasirašytos informacijos nuorodoje esančia santrauka.

Parašo tikrinimo etapai:

- Išgaunamas rakto informacija iš ranto informacijos elemento arba išorinio šaltinio.
- Pagal nurodytą metodą apskaičiuojamas pasirašytos informacijos elemento kanoninis pavidalas, kuris kartu su rakto informacija naudojamas parašo reikšmei patikrinti.

KeyInfo elementas nurodo parašui tikrinti reikalingus raktus [7].

3.4. Internetinės prekybos veiklos diagrama.



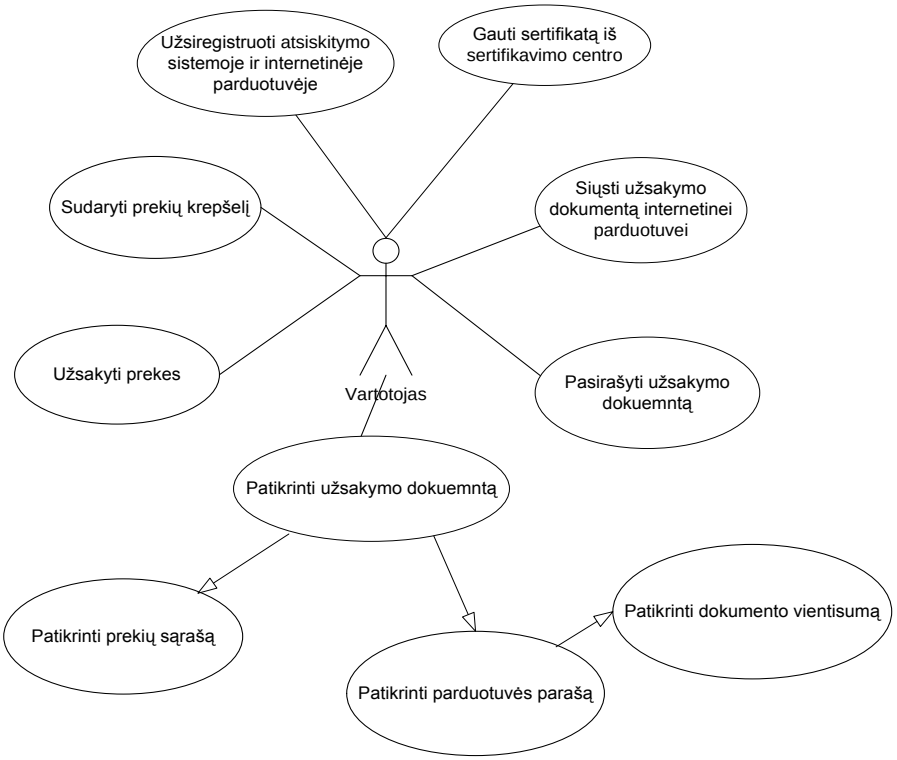
4 pav. Internetinės prekybos veiklos diagrama

Diagramoje matome kokie pagrindiniai veiksmai yra vykdomi internetinėje prekyboje tarp joje dalyvaujančių šalių. Kaip matome apmokėjimo procese pirkėjas tiesiogiai su

atsiskaitymo sistema nekomunikuoja, tai už jį daro internetinė parduotuvė, taip pirkėjui sumažinamas papildomų veiksmų ir žinių kiekis.

3.4.1. Vartotojo (pirkėjo) funkcijos

Žemiau yra pateikta pirkėjo panaudos atvejų diagrama (5 pav.), bei lentelėse išsamiai paaiškintas kiekvienas panaudos atvejis, nurodant pirminius reikalavimus, proceso eiga bei gaunamus rezultatus.



5 pav. Vartotojo panaudos atvejų diagrama.

1 lentelė. Skaitmeninio sertifikato gavimas

Panaudojimo atvejo pavadinimas	Gauti sertifikatą iš sertifikavimo centro
Santrauka	Pirkėjas, norėdamas pirkti prekes internetu ir atsiskaitinėti už jas kuriamoje sistemoje, turi turėti skaitmeninį sertifikatą.
Pirminiai reikalavimai	Sertifikatas turi būti išduodamas patikimo sertifikavimo centro, turi būti galiojantis, neatšauktas.

Bendroji proceso eiga	• Pirkėjas pateikia savo asmeninę informaciją sertifikavimo centro registracijos tarnybai. • Registracijos tarnyba patikrina asmens tapatybę ir ją arba patvirtina arba paneigia. • Jai asmens tapatybe patvirtinama, sertifikavimo centras išduoda sertifikatą.
Rezultatai	Pirkėjas gauna patikimą skaitmeninį sertifikatą, kuris yra galiojantis, ir neatšauktas.

2 lentelė. Užsiregistravimas internetinio atsiskaitymo sistemoje ir internetinėje parduotuvėje

Panaudojimo atvejo pavadinimas	Užsiregistruoti atsiskaitymo sistemoje ir internetinėje parduotuvėje
Santrauka	Pirkėjas, norėdamas pirkti prekes internetu ir atsiskaitinėti už jas per kuriamą atsiskaitymo sistemą, tuomet jis joje užsiregistruoti. Taip pat jis turi užsiregistruoti ir internetinėje parduotuvėje, kurioje pirks prekes.
Pirminiai reikalavimai	Kad užsiregistruoti apmokėjimo sistemoje, pirkėjas turi turėti patikimo sertifikavimo centro išduotą skaitmeninį sertifikatą. Norėdamas pirkti prekes ir už jas atsiskaitinėti per kuriamą atsiskaitymo sistemą, turi pasirinkti tą internetinę parduotuvę, kuri vykdo atsiskaitymą už jas per kuriamą apmokėjimo sistemą.
Bendroji proceso eiga	• Pirkėjas užsiregistruoja internetinio atsiskaitymo sistemoje, pateikdamas savo viešojo rakto sertifikatą kaip asmens tapatybės dokumentą, bei nurodo kitą papildomą asmeninę informaciją, tokią kaip banko sąskaitos numeris ir pan. • Pirkėjas registruojasi internetinėje parduotuvėje, pateikdamas joje tik minimalią informaciją apie save.
Rezultatai	Pirkėjas užsiregistravęs internetinio atsiskaitymo sistemoje ir internetinėje parduotuvėje gali pirkti prekes ir už jas atsiskaitinėti.

3 lentelė. Prekių krepšelio sudarymas

Panaudojimo atvejo pavadinimas	Sudaryti prekių krepšelį
Santrauka	Pirkėjas renkasi prekes iš sąrašo, kurį pateikia internetinė parduotuvė. Pasirinktas prekes jis talpina į tam skirtą „prekių krepšelį“.
Pirminiai reikalavimai	Pasirinktas prekes pirkėjas turi talpinti į prekių krepšelį, kad galėtų jas įsigyti. Turi būti suteikta galimybė pirkėjui prekių krepšelį koreguoti, t.y. pridėti prekes arba sumažinti prekių kiekį.
Bendroji proceso eiga	• Pirkėjas pasirenka prekę iš prekių sąrašo ir talpina į prekių krepšelį. • Redaguoja prekių krepšelį: prideda arba šalina prekes.
Rezultatai	Sukaupiamas vartotojo pasirinktų prekių sąrašas su visa informacija apie prekes: kaina, kiekis, pavadinimas ir pan.

4 lentelė. Prekių užsakymas

Panaudojimo atvejo pavadinimas	Užsakyti prekes
Santrauka	Pirkėjas patvirtina, jog jis perka pasirinktas prekes, kurios randasi jo sukauptame prekių krepšelyje.
Bendroji proceso eiga	• Vartotojas praneša internetinei parduotuvei, kad jis perka pasirinktas prekes.
Rezultatai	Internetinė parduotuvė gauna patvirtinimą, kad pirkėjas perka jo pasirinktas prekes ir rezervuoja šias prekes.

5 lentelė. Užsakymo formos patikrinimas

Panaudojimo atvejo pavadinimas	Patikrinti užsakymo dokumentą
Santrauka	Pirkėjas gavęs iš internetinės parduotuvės užsakymo formą ją patikrina ar ji nebuvo pakeista ir ar užsakymo formą atsiuntė toji internetinė parduotuvė, kurioje jis perka prekes.

Pirminiai reikalavimai	Kad patikrintų užsakymo formos vientisumą, jis turi patikrinti internetinės parduotuvės elektroninį parašą. Pagal šį parašą jis gali patikrinti tiek internetinės parduotuvės autentiškumą, tiek gautų duomenų vientisumą.
Bendroji proceso eiga	• Patikrinama XML dokumento struktūra ar ji tenkina reikalavimus kurie aprašyti sukurtoje XML schemoje. • Pirkėjo programinė įranga apskaičiuoja užsakymo duomenų santraukos reikšmę. • Gautą elektroninį parašą kartu su atsiųstu dokumentu iššifruoja ir gauna santrauką. • Patikrina abiejų santraukų panašumus. • Patikrina internetinės parduotuvės autentiškumą pagal gautą jos viešojo rakto sertifikatą.
Rezultatai	Jeigu gautos santraukos reikšmės sutapo, tuomet pirkėjas gali būti garantuotas, jog atsiųsti duomenys nebuvo pakeisti pakeliui pas jį. Taip pat, jei patikrinus internetinės parduotuvės tapatybę, vartotojas įsitikina, jog bendrauja su ta parduotuve su kuria ir turi, tuomet gali toliau tęsti pirkimo procesą. Jeigu kažkuris iš išvardintų atvejų nepasisekė, arba gautų reikšmių palyginimas turi neigiamą atsakymą, tuomet vartotojas arba pakartotinai paprašo internetinės parduotuvės atsiųsti užsakymo formą, arba nutraukia prekybą (priklausomai nuo gauto atsakymo tipo).
Pastabos	Būtina sąlyga, kad vartotojas patikrintų gautą dokumentą kartu su e. parašu.

6 lentelė. Užsakymo formos pasirašymas

Panaudojimo atvejo pavadinimas	Pasirašyti užsakymo dokumentą
Santrauka	Patikrintą užsakymo dokumentą pirkėjas pasirašo savo elektroniniu parašu. Tai jis daro tam, kad nusiuntus užsakymo dokumentą internetinei parduotuvei, o ši atsiskaitymo sistemai, galėtų autentifikuoti pirkėją ir tuo pačiu patikrinti gautų duomenų vientisumą.

Pirminiai reikalavimai	Kad pasirašytų užsakymo dokumentą, pirkėjas turi turėti sertifikatą bei pasirašymo įrangą. Ši sertifikatą turi išduoti patikimas sertifikavimo centras. Sertifikatas turi būti galiojantis, kitaip vartotojas nebus autentifikuotas. Į suformuotą XML dokumentą turi būti įtraukta informacija apie naudotą sertifikatą, kurio pagalba vėliau bus galima patikrinti pasirašiusiojo tapatybę, bei dokumento vientisumą.
Bendroji proceso eiga	• Apskaičiuojama užsakymo dokumento santraukos reikšmė. • Ši reikšmė užšifruojama pirkėjo privačiuoju raktu, kuris yra jam išduotame sertifikate. • Gauta eilutė, su kita papildoma informacija apie naudotus algoritmus santraukai apskaičiuoti ir užšifruoti, įterpiama į užsakymo dokumentą.
Rezultatai	Užsakymo dokumentas yra pasirašytas internetinės parduotuvės bei pirkėjo, kas reiškia, kad atsiskaitymo sistema, gavusi šį užsakymo dokumentą, galės autentifikuoti visas prekyboje dalyvaujančias šalis. Taip pat, šį dokumentą galės patikrinti ar jis nebuvo pakeistas, kad jis yra toks, kokią internetinė parduotuvė suformavo ir kokį pasirašė pirkėjas. Tai yra labai svarbu, nes piktavalis galėtų įterpti savo informacijos į šį dokumentą, ir atsiskaitymo sistemai nepastebėjus to ir nepatikrinus dokumento vientisumo, galėtų iš to pasipelnyti.
Pastabos	Būtina sąlyga, kad internetinės parduotuvės bei pirkėjo sertifikatas galiotų ir kad užsakymo dokumentas būtų pasirašytas.

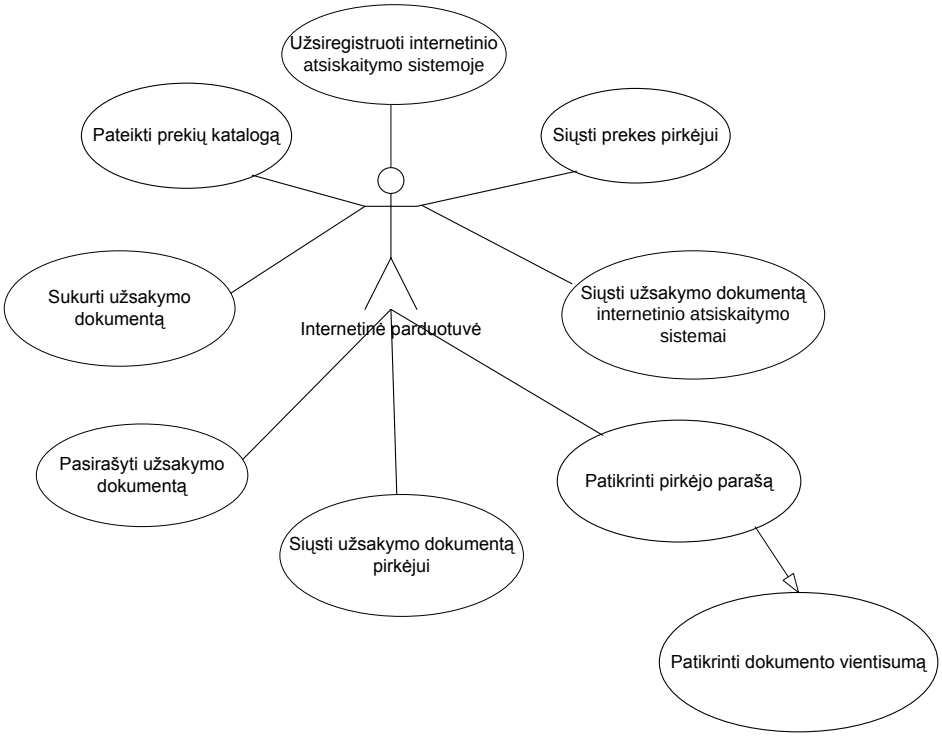
7 lentelė. Užsakymo formos siuntimas internetinei parduotuvei

Panaudojimo atvejo pavadinimas	Siųsti užsakymo dokumentą internetinei parduotuvei
Santrauka	Kai pirkėjas pasirašo užsakymo formą, jis ją persiunčia internetinei parduotuvei, kad ši galėtų persiųsti ją atsiskaitymo sistemai.

Pirminiai reikalavimai	Tarp internetinės parduotuvės ir pirkėjo galėtų būti užmegztas saugus internetinis ryšys (SSL), kad duomenys siunčiami internetu būtų šifruojami.
Bendroji proceso eiga	• Siunčiama užsakymo forma internetinei parduotuvei.
Rezultatai	Internetinė parduotuvė gauna pirkėjo pasirašytą užsakymo formą.

3.4.2. Internetinės parduotuvė funkcijos

Žemiau yra pateikta internetinės parduotuvės panaudos atvejų diagrama (6 pav.), bei lentelėse išsamiai paaiškintas kiekvienas panaudos atvejis, nurodant pirminius reikalavimus, proceso eiga bei gaunamus rezultatus.



6 pav. Internetinės parduotuvės panaudos atvejų diagrama.

8 lentelė. Prekių katalogo pateikimas

Panaudojimo atvejo pavadinimas	Užsiregistruoti internetinio atsiskaitymo sistemoje
Santrauka	Internetinė parduotuvė, norėdama, kad pirkėjai galėtų atsiskaitinėti per kuriamą atsiskaitymo sistemą turi joje užsiregistruoti.

Pirminiai reikalavimai	Internetinė parduotuvė turi turėti galiojantį ir neatšauktą, patikimo sertifikavimo centro išduotą sertifikatą.
Bendroji proceso eiga	• Internetinė parduotuvė užsiregistruoja internetinio atsiskaitymo sistemoje, pateikdamas savo viešojo rakto sertifikatą kaip įmonės tapatybės dokumentą, bei nurodo kitą papildomą įmonės informaciją, tokią kaip banko sąskaitos numeris ir pan.
Rezultatai	Užsiregistravusi internetinio atsiskaitymo sistemoje, pirkėjai pirkti šioje parduotuvėje prekes, o atsiskaitinėti kuriamoje internetinio atsiskaitymo sistemoje.

9 lentelė. Prekių katalogo pateikimas

Panaudojimo atvejo pavadinimas	Pateikti prekių katalogą
Santrauka	Internetinė parduotuvė suformuoja prekių katalogą su prekių pavadinimais, trumpais aprašymais, iliustracijomis, kainomis bei galimų įsigyti prekių kiekis.
Pirminiai reikalavimai	Prekių katalogas visuomet turi būti atnaujinamas, kad pirkėjui būtų pateikta naujausia informacija apie prekių kiekius bei kainas. Pateikta informacija turi būti teisinga ir informatyvi. Katalogas turi būti patogiai suformuotas, kad pirkėjui nesudaryti papildomų rūpesčių renkantis prekes.

10 lentelė. Užsakymo formos suformavimas

Panaudojimo atvejo pavadinimas	Sudaryti užsakymo dokumentą
Santrauka	Pirkėjui pasirinkus visas jam norimas prekes, internetinė parduotuvė turi suformuoti užsakymo dokumentą XML formatu. Šiame dokumente turi būti pateikta visa svarbiausia informacija susijusi su perkamomis prekėmis: prekių pavadinimas, kodas, kaina bei kiekis.

Pirminiai reikalavimai	Užsakymo dokumentas turi būti sudarytas pagal tam tikrus reikalavimus, kuriuos aprašo internetinei parduotuvei įteikta XML schema. Duomenys turi atitikti visus reikalavimus, jų turi būti ne daugiau nei reikalaujama. Užsakymo dokumente turi būti šie duomenys: prekės pavadinimas, jos kodas, kaina, užsakytų prekių kiekis bei visa suma, kurią turės sumokėti pirkėjas ir t.t.
Bendroji proceso eiga	• Pasirenkami duomenys iš duomenų bazės apie prekes, kurias užsisakė pirkėjas. • Iš šių duomenų formuojamas užsakymo dokumentas pagal pateiktą XML schemą. • Apskaičiuojama mokėjimo suma ir taip pat įterpiama į užsakymo formą.
Rezultatai	Sudarytas užsakymo dokumentas tenkina visus reikalavimus aprašytus XML schemoje ir visos visame šiame procese dalyvaujančios šalys galės taisyklingai perskaityti visus duomenis esančius jame.
Pastabos	Būtina sąlyga, kad užsakymo dokumentas būtų sudarytas pagal sutartą XML schemą, kurią internetinei parduotuvei nurodė atsiskaitymo sistema.

11 lentelė. Užsakymo formos pasirašymas

Panaudojimo atvejo pavadinimas	Pasirašyti užsakymo dokumentą
Santrauka	Suformuotą užsakymo dokumentą internetinė parduotuvė pasirašo savo elektroniniu parašu. Tai ji daro tam, kad nusiuntus užsakymo dokumentą pirkėjui internetu, pirkėjas galėtų patikrinti ar duomenys nebuvo pakeisti ir patikrinti parduotuvės autentiškumą, t.y. įsitikinti, jog bendrauja su ta internetine parduotuve su kuria ir turi.

Pirminiai reikalavimai	Kad pasirašytų užsakymo dokumentą, internetinė parduotuvė turi turėti sertifikatą. Šį sertifikatą jai turi išduoti patikimas sertifikavimo centras. Sertifikatas turi būti galiojantis, kitaip atsiskaitymo sistema nepasitikės šia internetine parduotuve. Į suformuotą XML dokumentą turi būti įtraukta informacija apie naudotą sertifikatą, kurio pagalba vėliau bus galima patikrinti pasirašiusiojo tapatybę, bei dokumento vientisumą.
Bendroji proceso eiga	• Apskaičiuojama užsakymo dokumento santraukos reikšmė. • Ši reikšmė užšifruojama internetinės parduotuvės privačiuoju raktu, kuris randasi jai išduotame sertifikate. • Gauta eilutė, su kita papildoma informacija apie naudotus algoritmus santraukai apskaičiuoti ir užšifruoti, įterpiama į užsakymo dokumentą.
Rezultatai	Užsakymo dokumentas yra pasirašytas internetinės parduotuvės elektroniniu parašu, kas reiškia, kad atsiskaitymo sistema, gavus šį užsakymo dokumentą, galėtų įsitikinti, jog tai yra tikrai tos parduotuvės sudarytas užsakymo dokumentas. Taip pat, šį dokumentą galėtų patikrinti ar jis nebuvo pakeista, kad jis yra toks, kokį internetinė parduotuvė suformavo. Tai yra labai svarbu, kadangi piktavalis galėjo įterpti savo informaciją į šį dokumentą, ir vartotojui nepastebėjus to ir nepatikrinus dokumento vientisumo, piktavalis galėtų iš to pasipelnyti.
Pastabos	Būtina sąlyga, kad internetinės parduotuvės sertifikatas galiotų ir kad užsakymo dokumentas būtų pasirašytas parduotuvės elektroniniu parašu.

12 lentelė. Užsakymo formos siuntimas pirkėjui

Panaudojimo atvejo pavadinimas	Siųsti užsakymo dokumentą pirkėjui
Santrauka	Suformuotas ir pasirašytas užsakymo dokumentas siunčiamas pirkėjui, kad šis galėtų jį patikrinti ir pasirašyti, taip patvirtindamas, kad jis tikrai perka tas prekes.

Pirminiai reikalavimai	Tarp internetinės parduotuvės ir pirkėjo galėtų būti užmegztas saugus internetinis ryšys (SSL), kad duomenys siunčiami internetu būtų šifruojami.
Bendroji proceso eiga	• Suformuotas užsakymo dokumentas XML formatu siunčiama pirkėjui.
Rezultatai	Pirkėjas gauna internetinės parduotuvės suformuotą bei pasirašytą užsakymo dokumentą.

13 lentelė. Parašo patikrinimas

Panaudojimo atvejo pavadinimas	Patikrinti pirkėjo parašą. Patikrinti dokumento vientisumą.
Santrauka	Gavus pirkėjo pasirašytą užsakymo dokumentą, internetinė parduotuvė patikrina pirkėjo parašą, kad įsitikinti, jog dokumentą pasirašė tas pirkėjas kuris ir turėjo ir kad internetu atkeliavęs dokumentas nebuvo pakeistas.
Pirminiai reikalavimai	Kad patikrinti pasirašyto dokumento autentiškumą, internetinė parduotuvė turi pasiimti pirkėjo viešąjį raktą ir patikrinti jo parašą.
Bendroji proceso eiga	• Pasiimamas viešasis pirkėjo raktas. • Iššifruojamas dokumento parašas ir gaunama santrauka. • Apskaičiuojama atsiustų duomenų santrauka. • Abi santraukos sulyginamos ar vienodos. • Galima paklausti trečiosios šalies (sertifikavimo centro) ar tai tikrai yra to pirkėjo viešasis raktas ar ne.
Rezultatai	Jeigu sulyginus gautas santraukas jos yra vienodos, tuomet vadinasi, kad duomenys nebuvo pakeisti ir parašas galioja. Patikrinus pasirašiusiojo elektroninį parašą, įsitikinama, kad tai yra tikrai tas pirkėjas su kuriuo ir bendraujama. Tačiau jei abu šie patikrinimai buvo nesėkmingi, tuomet parduotuvė arba nutraukia prekybą su tuo pirkėju, arba dar kartą paprašo jo atsiusti pasirašytą užsakymo dokumentą (priklausomai nuo situacijos dėl ko parduotuvė negalėjo priimti atsiųsto užsakymo dokumento).

Pastabos	Parduotuvė turi būtinai patikrinti vartotojo pasirašytą ir atsiųstą užsakymo dokumentą, nes keliaujant internetu, šis dokumentas galėjo būti pakeistas piktavalio.

14 lentelė. Užsakymo formos siuntimas atsiskaitymo sistemai

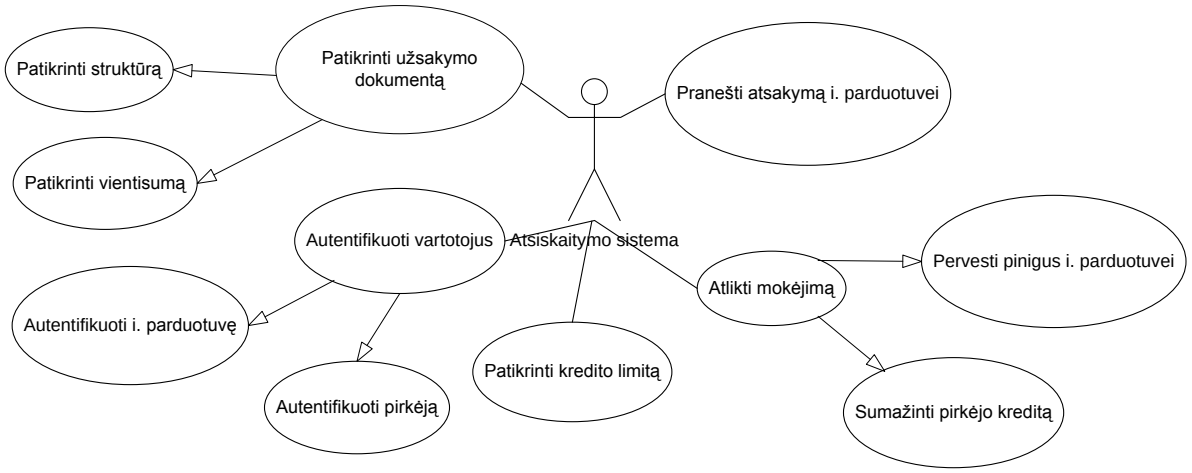
Panaudojimo atvejo pavadinimas	Siųsti užsakymo dokumentą atsiskaitymo sistemai.
Santrauka	Kai internetinė parduotuvė patikrina pirkėjo atsiųstą pasirašytą užsakymo dokumentą, ji ją persiunčia atsiskaitymo sistemai, kad ši galėtų atlikti mokėjimus.
Pirminiai reikalavimai	Tarp internetinės parduotuvės ir atsiskaitymo sistemos galėtų būti užmegztas saugus internetinis ryšys (SSL), kad duomenys siunčiami internetu būtų šifruojami.
Bendroji proceso eiga	• Siunčiamas užsakymo dokumentas atsiskaitymo sistemai.
Rezultatai	Atsiskaitymo sistema gauna internetinės parduotuvės ir pirkėjo pasirašytą užsakymo dokumentą.

15 lentelė. Prekių siuntimas pirkėjui

Panaudojimo atvejo pavadinimas	Siųsti prekes pirkėjui.
Santrauka	Kai internetinė parduotuvė gauną teigiamą atsakymą iš atsiskaitymo sistemos, jog mokėjimas yra sėkmingai atliktas, ji siunčia prekes pirkėjui.
Pirminiai reikalavimai	Internetinė parduotuvė turi gauti teigiamą atsakymą, kad galėtų išsiųsti prekes pirkėjui.
Bendroji proceso eiga	• Internetinė parduotuvė išsiunčia pirkėjo pasirinktas ir apmokėtas prekes.
Rezultatai	Pirkėjas gauną prekes, kurias pasirinko ir už kurias sumokėjo.

3.4.3. Internetinio atsiskaitymo sistemos funkcijos

Žemiau yra pateikta internetinio atsiskaitymo sistemos panaudos atvejų diagrama (7 pav.), bei lentelėse išsamiai paaiškintas kiekvienas panaudos atvejis, nurodant pirminius reikalavimus, proceso eiga bei gaunamus rezultatus.



7 pav. Internetinio atsiskaitymo sistemos panaudos atvejų diagrama

16 lentelė. Užsakymo formos patikrinimas

Panaudojimo atvejo pavadinimas	Patikrinti užsakymo dokumentą
Santrauka	Atsiskaitymo sistema gavusi iš internetinės parduotuvės užsakymo dokumentą jį patikrina ar jis nebuvo pakeistas. Taip pat patikrinama gauto dokumento struktūra, t.y. patikrinama ar teisingai suformuotas užsakymo dokumentas ir ar jis tenkina reikalavimus, aprašytus XML schemoje.
Pirminiai reikalavimai	Kad patikrintų užsakymo dokumento vientisumą, ji turi pasiimti internetinės parduotuvės arba pirkėjo elektroninį parašą. Turėdama parašą ji gali patikrinti tiek internetinės parduotuvės ir pirkėjo autentiškumą, tiek gautų duomenų vientisumą.
Bendroji proceso eiga	• Patikrinama XML dokumento struktūra ar ji tenkina reikalavimus kurie aprašyti sukurtoje XML schemoje. • Atsiskaitymo sistema apskaičiuoja užsakymo dokumento santraukos reikšmę. • Gautus elektroninius parašus kartu su atsiųstu dokumentu iššifruoja ir gauna santraukas. • Patikrina santraukų panašumus.

Rezultatai	Jeigu gautos santraukos reikšmės sutapo, tuomet atsiskaitymo sistema gali būti garantuota, jog atsiųsti duomenys nebuvo pakeisti pakeliui pas ją. Jeigu santraukos nesutapo, tuomet atsiskaitymo sistema arba pakartotinai paprašo internetinės parduotuvės atsiųsti užsakymo dokumentą, arba nutraukia atsiskaitymo procesą (priklausomai nuo gauto atsakymo tipo).
Pastabos	Būtina sąlyga, kad atsiskaitymo sistema patikrintų gautą dokumentą kartu su e. parašu.

17 lentelė. Vartotojų autentifikavimas

Panaudojimo atvejo pavadinimas	Autentifikuoti vartotojus.
Santrauka	Kad atsiskaitymo sistema galėtų atlikti mokėjimus už prekes, ji turi žinoti kas jas perka, bei kam pervesti pinigus už perkamas prekes. Taigi ji turi autentifikuoti vartotojus. Autentifikavimas vykdomas pagal gautus duomenis, kurie buvo gauti kartu su užsakymo informacija.
Pirminiai reikalavimai	Kad autentifikuoti internetinės prekybos dalyvius, atsiskaitymo sistema turi paimti duomenis apie parašus, kurie yra kartu su užsakymo dokumentu. Kadangi atsiskaitymo sistema pasitiki visos prekyboje dalyvaujančios šalys, todėl patiki jai autentifikuoti vartotojus ir atlikti mokėjimus.
Bendroji proceso eiga	• Patikrinamas internetinės parduotuvės autentiškumas • Patikrinamas pirkėjo autentiškumas.
Rezultatai	Autentifikuojami prekyboje dalyvaujantys dalyviai pagal jų parašus. Jeigu nepavyko nors vieno dalyvio autentifikuoti, tuomet atsiskaitymo sistema praneša apie nesėkmę internetinei parduotuvei, o ši, jei reikia, pirkėjui (priklausomai nuo atvejo).
Pastabos	Būtina sąlyga, kad būtų autentifikuoti abu prekybos dalyviai, kadangi atsiskaitymo sistema turi žinoti kas perka prekes ir kam pervesti pinigus už prekes.

18 lentelė. Kredito limito patikrinimas

Panaudojimo atvejo pavadinimas	Patikrinti kredito limitą

Santrauka	Autentifikavus pirkėją, atsiskaitymo sistema patikrina ar pakankamas kredito limitas pirkėjo sąskaitoje už prekes sumokėti.
Bendroji proceso eiga	• Patikrinamas kredito limitas
Rezultatai	Jeigu kreditas yra pakankamas, tuomet atsiskaitymo sistema gali pereiti prie sekančio žingsnio, o jei nepakankamas, tuomet internetinei parduotuvei pranešama apie nesėkmingą mokėjimą, o ši apie tai praneša pirkėjui.

19 lentelė. Mokėjimas

Panaudojimo atvejo pavadinimas	Atlikti mokėjimą
Santrauka	Patikrinus kredito limitą ir jam esant pakankamu, internetinė parduotuvė nuskaičiuoja reikiamą sumą nuo pirkėjo sąskaitos ir juos perveda į internetinės parduotuvės sąskaitą (šioje vietoje galimas papildomų šalių panaudojimas mokėjimams atlikti).
Pirminiai reikalavimai	Kredito limitas turi būti pakankamas prekėm įsigyti.
Bendroji proceso eiga	• Nuskaičiuojamas reikiamas kiekis pinigų iš pirkėjo sąskaitos • Ta pati suma pinigų yra pervedama į internetinės parduotuvės sąskaitą. • Galimas papildomas mokestis už atsiskaitymo sistemos atliekamas paslaugas.
Rezultatai	Nuskaičiavus reikiamą sumą nuo pirkėjo sąskaitos ir ją pervedus į internetinės parduotuvės sąskaitą, atsiskaitymo sistema gali tęsti tolimesnius darbus.
Pastabos	Būtina sąlyga, kad kredito limitas būtų pakankamas prekėms įsigyti.

20 lentelė. Pranešimo siuntimas internetinei parduotuvei

Panaudojimo atvejo pavadinimas	Pranešti atsakymą internetinei parduotuvei.

Santrauka	Jeigu atlikti veiksmai pavyko arba nepavyko, bet kuriuo atveju atsiskaitymo sistema informuoja internetinę parduotuvę. Pranešimas gali reikšti jog mokėjimas nepavyko dėl pirkėjo kaltės (pvz. mažas kredito limitas), dėl internetinės parduotuvės kaltės (pvz. blogai suformuota užsakymo forma) ir gali reikšti, jog mokėjimas sėkmingai atliktas ir internetinė parduotuvė gali siųsti prekes pirkėjui.
Pirminiai reikalavimai	Bet kuriuo atveju atsiskaitymo sistema turi nusiųsti atsakymą internetinei parduotuvei apie pavykusį arba nepavykusį mokėjimą. Atsakymas turi būti informatyvus ir suprantamas.
Bendroji proceso eiga	Esant bet kokiai operacijai ir jei pavykus arba nepavykus, siunčiamas pranešimas apie kažkokią klaidą arba sėkmę, neatskleidžiant smulkmenų.
Rezultatai	Gavusi atsakymą iš atsiskaitymo sistemos, internetinė parduotuvė arba nutraukia prekybą, arba ją tęsia, priklausomai nuo gauto atsakymo.
Pastabos	Bet kokiu atveju atsiskaitymo sistema turi siųsti pranešimą internetinei parduotuvei.

4. INTERNETINĖS ATSISKAITYMO SISTEMOS REALIZAVIMAS IR TYRIMAS

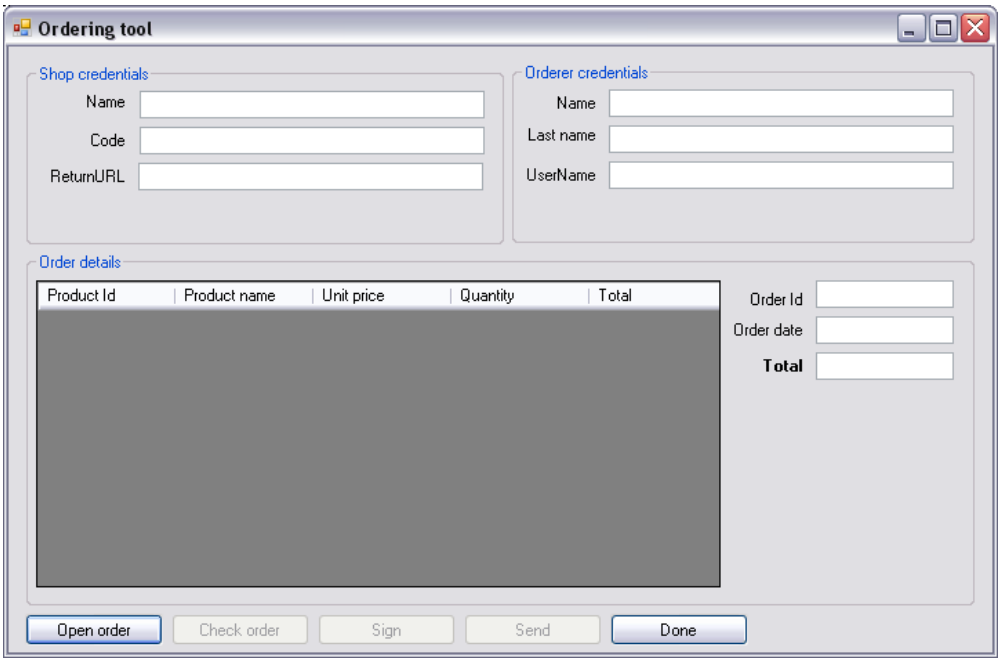
Atlikus analizę, nustačius reikalavimus ir suprojektavus naują internetinio atsiskaitymo sistemos vartotojo autentifikavimą, buvo realizuota pavyzdinė sistema, kurioje yra atliekamos pagrindinės, projektinėje dalyje aprašytos funkcijos. Sukurta sistema atlieka tik tas funkcijas, kurios reikalingos vartotojams autentifikuoti. Buvo realizuotos pagrindinės trys komunikuojančios šalys: vartotojo programinė įranga, su kuria vartotojas pasirašinėja užsakymo dokumentą, internetinės parduotuvės svetainė su prekių katalogu, bei atsiskaitymo sistema, kuri ir autentifikuoja vartotojus. Internetinei parduotuvei ir pirkėjui buvo sukurti sertifikatai, kurie nėra išduoti patikimo sertifikavimo centro, tačiau to pakanka, kad būtų galima ištirti kaip internetinės prekybos vartotojai gali būti autentifikuojami pagal jų elektroninį parašą. Šioje sistemoje galima panaudoti ir kitų sertifikavimo centrų išduotus sertifikatus.

4.1. Realizuotos internetinėje prekyboje dalyvaujančios šalys

4.1.1. Pirkėjo pasirašymo programinė įranga

Pirkėjas, norėdamas pirkti prekes internetu tose parduotuvėse, kuriose taikomas kuriamas autentifikavimo metodas, turi turėti sertifikatą ir programinę įrangą, kurios pagalba galėtų pasirašinėti užsakymo dokumentus. Pirkėjui buvo sukurtas sertifikatas, kuris nėra išduotas patikimo sertifikavimo centro, tačiau kuriamos sistemos veikimui parodyti, toks sertifikatas visiškai tinka.

Internetinio apmokėjimo sistema vartotojui registruojantis išduoda pasirašymo programinę įrangą. Programa ne tik pasirašinėja dokumentus, tačiau ir atvaizduoja jų turinį, t.y. prekių sąrašą, kurį užsisakė internetinėj parduotuvėje, dokumento sudarymo data, vartotojo informacija, internetinės parduotuvės informacija. Ši programa taip pat naudoją ir nefunkciniuose reikalavimuose aptartą XML schemą, pagal kurią tikrina ar gautas iš internetinės parduotuvės XML užsakymo dokumentas yra tvarkingas, atitinka apsibrėžtus parametrus ir pan.



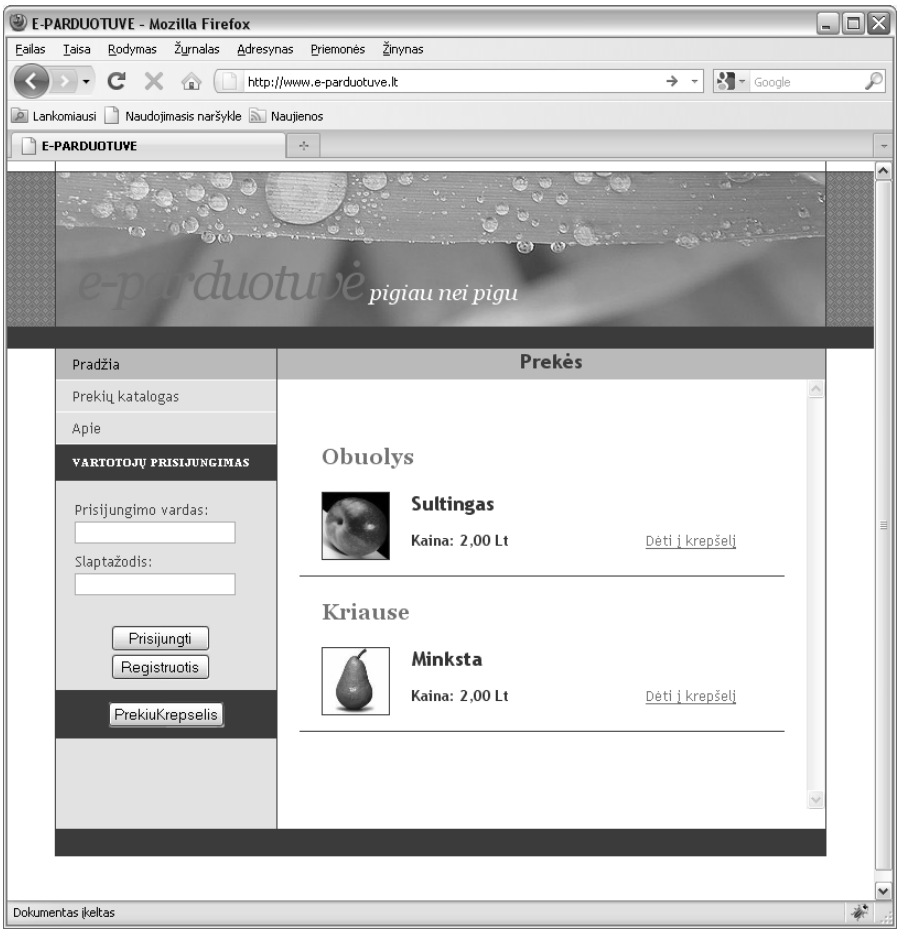
8 pav. Pirkėjo programinės įrangos grafinė sąsaja

Šiame paveiksliuke yra parodyta pirkėjo programos grafinė sąsaja. Kaip matome šiame programos lange yra laukai, kuriuose atvaizduojami duomenys apie parduotuvę, kurioje perka pirkėjas (parduotuvės pavadinimas, parduotuvės arba įmonės kodas, bei nuoroda kur bus siunčiami pasirašytas dokumentas), laukeliai skirti pirkėjo informacijai atvaizduoti (vardas, pavardė, vartotojo vardas internetinės parduotuvės sistemoje). Pagrindinis laukas šiame programos lange yra skirtas atvaizduoti prekes, kurias pirkėjas užsisakė, jų pavadinimus, kainas, kiekius ir bendrą sumą. Taip pat atvaizduojamas ir užsakymo numeris, užsakymo data bei visa mokėjimo suma, kurią turės sumokėti pirkėjas. Visi šie duomenys yra gaunami iš XML užsakymo dokumento. Žemiau yra išdėstyti mygtukai, kurių dalis gali būti aktyvuoti arba ne. Tai priklauso nuo to, ar dokumentas yra taisyklingai suformuotas ir ar pavyko pasirašyti dokumentą. Paspaudus pirmąjį mygtuką „Open order“, vartotojas turės pasirinkti užsakymo XML dokumentą, kurį gavo iš internetinės parduotuvės. Jeigu pirkėjo pasirinktas dokumentas buvo suformuotas teisingai, tuomet jis galės atlikti tolimesnius veiksmus. Paspaudus sekantį mygtuką „Check order“ tikrinama ar užsakymo XML dokumentas nebuvo pakeistas, tai yra tikrinamas dokumento vientisumas pagal parduotuvės elektroninį parašą. Jai dokumentas yra nekeistas ir parašas yra teisingas, tuomet yra aktyvuojamas sekanti mygtukas „Sign“, kurį paspaudus atliekamas dokumento pasirašymas vartotojo e. parašu. Kad vartotojas galėtų pasirašyti šį užsakymo dokumentą, jis turi atsivėrusiame dialoge įvesti sertifikato aktyvavimo slaptažodį. Jai buvo įvestas teisingas slaptažodis, tuomet dokumentas yra pasirašomas. Pavykus pasirašymui, aktyvuojamas sekantis mygtukas „Send“, kurį paspaudus dokumento duomenys POST metodu siunčiami

nurodytu adresu „ReturnURL“ ir iš kurio vėliau gauna atsakymą apie pavykusį ar nepavykusį apmokėjimą už prekes. Paskutinis mygtukas „Done“ užbaigia darbą bet kuriuo metu.

4.1.2. Internetinė parduotuvė

Sukurta pavyzdinė internetinė parduotuvė. Kad pirkėjas galėtų apsipirkti šioje parduotuvėje, jis turi turėti prieš tai aptartą pirkėjo programinę įrangą, nes šioje parduotuvėje internetiniai apmokėjimai vyksta per kuriamą atsiskaitymo sistemą. Kartu su šia įranga jis taip pat turi turėti sertifikatą. Šiai parduotuvei buvo sukurtas sertifikatas, tam kad galėtų pasirašyti užsakymo dokumentus savo elektroniniu parašu. Ši internetinė parduotuvė turi savo duomenų bazę, kurioje buvo suvestos kelios prekės ir informacija apie jas (kainos, aprašymas, paveiksliukai), taip pat saugojami vartotojų prisijungimo duomenys. Prisijungimas šioje svetainėje reikalingas tam, kad tik registruoti vartotojai galėtų naudotis jos paslaugomis. Skaitmeninis sertifikatas yra saugojamas internetinės parduotuvės serveryje. Vartotojams prisijungti yra skirti du įvesties laukai, į kuriuos reikia įvesti vartotojo prisijungimo vardą bei slaptažodį. Jai vartotojas nėra užsiregistravęs šioje parduotuvėje, tuomet jis negalės pirkti prekių, tačiau galės peržiūrėti parduotuvės pardavinėjamas prekes. Norint užsiregistruoti parduotuvėje reikia užpildyti registravimosi formą, kurią pateikia parduotuvė. Joje reikia nurodyti informaciją apie savo gyvenamą vietą, vardą pavardę. Jokios finansinės informacijos pirkėjas registruodamasis šioje parduotuvėje nepateikia, nes parduotuvė pati apmokėjimo nevykdo, už ją tai padaro atsiskaitymo sistema. Ji reikalauja, kad vartotojai užsiregistruotu, siekiant išvengti nepageidaujamų, klaidingų užklausų iš piktavalių vartotojų, kuomet bandoma dideliais kiekiais užklausų apkrauti internetinės parduotuvės serverį.



9 pav. Internetinės parduotuvės svetainė

Paveikslėlyje matome internetinės parduotuvės internetinę svetainę. Joje yra pateikiamas sąrašas prekių, kurias gali pasirinkti pirkėjas. Pasirinkęs prekę, pirkėjas ją deda į prekių krepšelį. Šiame krepšelyje jis gali padidinti arba sumažinti prekių kieki, pašalinti prekes iš krepšelio. Vėliau, kuomet vartotojas jau apsisprendžia pirkti prekes, jis paspaudžia mygtuką „Užsakyti“. Tuomet internetinė parduotuvė suformuoja XML užsakymo dokumentą pagal sukurtą XML schemą, jį pasirašo savo elektroniniu parašu, kuris yra apskaičiuojamas panaudojant internetinės parduotuvės skaitmeninį sertifikatą. Apskaičiavus šį parašą, jis yra įterpiamas į sukurtą užsakymo XML dokumentą ir siunčiamas pirkėjui, kuris savo ruožtu jį turi išsisaugoti savo kompiuteryje. Vėliau, kuomet pirkėjas pasirašo šį dokumentą savo elektroniniu parašu, jis atkeliauja atgal į šią parduotuvę. Jį internetinė parduotuvė patikrina ar nebuvo pakeitimų (patikrina dokumento vientisumą pagal elektroninį parašą) ir persiunčia internetinio atsiskaitymo sistemai. Jai apmokėjimas pavyko, tuomet iš atsiskaitymo sistemos gaunamas teigiamas atsakymas ir internetinė parduotuvė apie tai informuoja pirkėją.

4.1.3. Apmokėjimo sistema

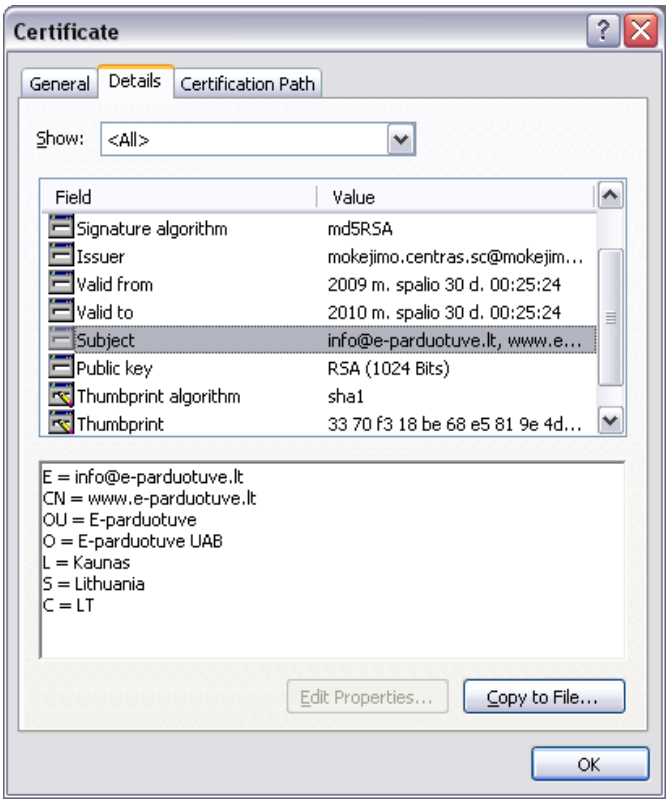
Sukurta atsiskaitymo sistema, kurios serveryje veikia žiniatinklio servisas. Šiuo servisu naudojasi internetinės parduotuvės, kuomet perduodami duomenys apie mokėjimo sumą ir gaunamas atsakymas apie pavykusį ar nepavykusį apmokėjimą. Ši technologija yra sukurta remiantis XML ir HTTP technologijomis. Duomenys keliaujantys internetu keliauja SOAP žinutėmis kurios yra XML pavidalo, o užklausos duomenims gauti ar siųsti yra gaunamos HTTP užklausomis. Atsiskaitymo sistema turi savo duomenų bazę, kurioje yra saugojama informacija apie vartotojus bei internetines parduotuves. Informaciją apie juos sistema gauna kuomet jie registruojasi ir siunčia savo viešojo rakto sertifikatą, kaip asmens tapatybės dokumentą, bei pateikia savo kreditinės kortelės informaciją, kad ši sistema galėtų atlikti kažkokius finansinius pervedimus. Taigi parduotuvei siunčiant duomenis šiai apmokėjimo sistemai, ji patikrina abiejų prekyboje dalyvaujančių šalių elektroninius parašus. Jeigu e. parašai yra tikri, nesuklastoti ir jeigu sertifikatai, kurie yra tuose e. parašuose yra galiojantys ir išduoti patikimo sertifikavimo centro, tuomet laikoma, jog dokumentas yra tinkamas tolesniems veiksmam atlikti. Taigi yra autentifikuojami internetinės prekybos vartotojai, nes sertifikatuose yra saugojama informacija apie asmenį ar internetinę parduotuvę, kuriai jis yra išduotas. Tuo pačiu šioje sistemoje yra saugojami sertifikavimo centrų viešųjų raktų sertifikatai, todėl kartu yra patikrinama ar tai tikrai tie prekybos dalyviai, kuriais jie dedasi esą. Kadangi registruojantis vartotojai pateikė savo viešojo rakto sertifikatus, todėl jie yra nesunkiai atsekami ir surandama jų informacija šioje apmokėjimo sistemoje. Sukurtoje sistemoje nėra realizuotas atsiskaitymas už prekes, kadangi tikslas yra parodyti kaip vartotojai yra autentifikuojami pagal jų elektroninį parašą. Taigi, jeigu laikysime, jog atsiskaitymai pavyko, tuomet ši atsiskaitymo sistema siunčia atsakymą apie pavykusį apmokėjimą internetinei parduotuvei, o ši pirkėjui. Kitu atveju siunčiamas neigiamas atsakymas, jog apmokėti nepavyko.

4.2. Realizacijoje naudotos technologijos ir standartai.

4.2.1. Sertifikatai

Sertifikatai buvo kuriami su OpenSSL atviro kodo programiniu paketu, kuris palaiko įvairius kriptografinius algoritmus, todėl galima susikurti sertifikatus pagal pasirinktą algoritmą, rakto ilgį bei kitus parametrus. Kad sukurti sertifikatą, skirtą pirkėjui ar internetinei parduotuvei, jis turi būti pasirašomas sertifikavimo centro elektroniniu parašu tam, kad jo

duomenys negalėtų būti pakeisti. Galima sukurti sertifikatus, kurie yra pasirašyti savo paties elektroniniu parašu, tačiau kuriamoje sistemoje tokie sertifikatai negaliotų, kadangi jie būtų laikomi išduoti nepatikimo sertifikavimo centro. Kiekvieną tokį vartotoją įtraukti į patikimų sertifikavimo centro sąrašą negalima, kadangi vėliau sistema negalės patikrinti sertifikato savininko tapatybės. Taigi buvo sukurtas ir sertifikavimo centro sertifikatas, kuris šiuo atveju yra pasirašytas savo paties elektroniniu parašu. Vėliau buvo sukurti skaitmeniniai sertifikatai ir internetinei parduotuvei ir pirkėjui. Juos pasirašėme su sukurto sertifikavimo centro elektroniniu parašu. Tokiu atveju reikėtų įtraukti tik sertifikavimo centro sertifikatą i patikimų sertifikavimo centrų sąrašą, o visi kiti sertifikatai, kurie būtų pasirašyti šiuo sertifikatu, būtų laikomi patikimais. Šie sukurti sertifikatai yra apsaugoti slaptažodžiu, kurį žino tik sertifikato gavėjas. Taip pat buvo sukurti viešojo rakto sertifikatai, kurie taip pat įterpiami į užsakymo dokumento elektroninį parašą, tam kad internetinėje prekyboje dalyvaujančios šalys, registruodamosi internetinio atsiskaitymo sistemoje, galėtų juos pateikti kaip tapatybės dokumentą. Kadangi šie sertifikatai buvo išduoti nepatikimo sertifikavimo centro, todėl bandant panaudoti juos kitose vietose, būtų pranešama apie nepatikimą sertifikatą, kad yra nepasitikima sertifikavimo centru, kuris šį sertifikatą išdavė. Tačiau kuriamoje sistemoje laikome, jog šie sertifikatai yra išduoti patikimo sertifikavimo centro ir šio sertifikavimo centro sertifikatą įtraukiame į internetinio atsiskaitymo sistemos patikimų sertifikavimo centrų sąrašą.



10 pav. Skaitmeninio sertifikato informacija

Šiame paveikslėlyje matome kaip atrodo internetinės parduotuvės viešojo rakto sertifikatas. Sertifikate yra saugojamas RSA viešasis raktas, kuris yra 1024 bitų ilgio. Kuriant elektroninius parašus turėtų būti naudojama md5 santraukos funkcijos algoritmas, bei RSA šifravimo algoritmas. *Subject* laukelyje matome, jog sertifikatas buvo išduotas internetinei parduotuvei, *Issuer* laukelyje matome, kas jį išdavė (šiuo atveju tai yra sukurtas sertifikavimo centras (sertifikatas pasirašytas jo privačiuoju raktu)), sertifikato galiojimo laikas. Pirkėjo viešojo rakto sertifikatas atrodo panašiai, tačiau skiriasi sertifikato serijos numeris, *Subject* laukelio duomenys, bei sertifikato „piršto antspaudo“ (angl. Thumbprint) laukelis, kuris yra unikalus kiekvienam sertifikatui.

4.2.2. Užsakymo dokumento sudarymo taisyklės (XML schema).

Užsakymo dokumentas - tai dokumentas, pagal kurį autentifikuojamas ne tik vartotojas, bet ir internetinė parduotuvė. Kad atsiskaitymų sistema galėtų autentifikuoti šias abi internetinėje prekyboje dalyvaujančias šalis, ji turi žinoti kaip šis dokumentas yra sudarytas. T.y. dokumentui turi būti taikomos tam tikros sudarymo taisyklės. Jeigu taisyklių nebus, tuomet atsiskaitymų sistema nežinos kaip autentifikuoti vartotoją. Pagal šias taisykles atsiskaitymų sistema žino kur kokie duomenys yra saugojami užsakymo dokumente, šiuo atveju tai yra XML formato dokumente. Šios taisyklės yra saugojamos XML schemoje, kurią sudarė atsiskaitymo sistema. Šis dokumentas yra pateikiamas visoms internetinėje prekyboje dalyvaujančioms šalims tam, kad jos sudarytų dokumentus remiantis šiomis taisyklėmis ir be vargo galėtų būti autentifikuojamos. Žemiau yra pateikti ir paaiškinti fragmentai iš šių taisyklių rinkinio:

21 lentelė. XML schemos tėvinis elementas

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
     targetNamespace="http://giedriaus.kompiuteris.magistras.xsd"
     elementFormDefault="qualified"
     attributeFormDefault="unqualified">
```

schema elementas yra tėvinis elementas, naudojamas visuose XML schemose. Jis turi keletą atributų. *xmlns:xs* atributas reiškia, kad elementai ir duomenų tipai naudojami šioje schemoje yra iš *http://www.w3.org/2001/XMLSchema* vardų srities. Taip pat pažymima, jog visi duomenys šioje schemoje turės prefiksą *xs*.

22 lentelė. Duomenų tipų aprašas

```
<xs:simpleType name="_String">
     <xs:restriction base="xs:string">
          <xs:minLength value="2"/>
```

```
          <xs:maxLength value="15"/>
     </xs:restriction>
</xs:simpleType>
<xs:simpleType name="_Decimal">
     <xs:restriction base="xs:decimal">
          <xs:fractionDigits value="2"/>
          <xs:totalDigits value="5"/>
     </xs:restriction>
</xs:simpleType>
```

Elementas *simpleType* saugo informaciją apie vieną iš elementų, kurio vardas nurodytas *name* atribute. Elemente *restriction* nurodomi kokie yra apribojimai tėviniam elementui (tėvinis elementas yra elementas apgaubiantis ši elementą). Šiame fragmente yra aprašomi keli duomenų tipai, kurie yra priskirti tam tikriems elementams, toliau esantiems taisyklių rinkinyje. Duomenų tipas *_String* saugo tokias savybes: duomenys yra eilutės tipo, turi būti ne ilgesni nei 15 ir ne trumpesni nei 2 simboliai. Duomenų tipas *_Decimal* saugo tokias savybes: duomenys yra dešimtainis skaičius, kuris po kablelio gali turėti tik 2 skaičius, o sveiko skaičiaus dydis turi būti sudarytas ne daugiau kaip iš 5 skaičių.

23 lentelė. Pagrindiniai būtini užsakymo dokumento elementai

```
<xs:complexType name="PurchaseOrder">
     <xs:sequence>
          <xs:element name="OrderDetails" type="OrderDetails"/>
          <xs:element name="OrdererCredentials" type="OrdererDetails"/>
          <xs:element name="ShopCredentials" type="ShopDetails"/>
          <xs:element name="ReturnURL" type="xs:string"/>
          <xs:element name="Signatures">
               <xs:complexType>
                    <xs:sequence>
                         <xs:element name="ShopSignature"/>
                         <xs:element name="UserSignature"/>
                    </xs:sequence>
               </xs:complexType>
          </xs:element>
     </xs:sequence>
</xs:complexType>
```

Elementas *complexType* saugo informaciją apie kelis elementus ar jų grupes. Šis fragmentas parodo, iš kokių duomenų grupių turi susidaryti visas užsakymo dokumentas. Taigi jis turi susidėti iš: *OrderDetails* (duomenys apie užsakymą), *OrdererCredentials*

(duomenys apie užsakovą), *ShopCredentials* (duomenys apie internetinę parduotuvę), *ReturnUrl* (duomenų gražinimo internetinei parduotuvei nuoroda). Kiekvienas iš jų atitinka tam tikrą tipą, kurie aprašo kokie duomenys turi būti pateikti kiekvienai šiai duomenų grupei. Elementas *Signatures* nurodo, kad jame bus saugojami elektroniniai parašai. Šis elementas savyje turi du elementus: *ShopSignature* ir *UserSignature*. Šie elementai turėtų saugoti internetinės parduotuvės bei pirkėjo elektroninius parašus.

24 lentelė. Reikalavimai pateikiamai informacijai apie užsakovą

```
<xs:complexType name="OrdererDetails">
     <xs:sequence>
          <xs:element name="Name" type="_String"/>
          <xs:element name="Surename" type="_String"/>
          <xs:element name="UserName">
               <xs:simpleType>
                    <xs:restriction base="xs:string">
                         <xs:maxLength value="25"/>
                         <xs:minLength value="3"/>
                    </xs:restriction>
               </xs:simpleType>
          </xs:element>
     </xs:sequence>
</xs:complexType>
```

Šioje taisyklių ištraukoje yra pateikta kokie elementai turi būti užsakymo dokumente apie užsakovą. Taigi turi būti visi 3 elementai: *Name* (vardas), *SureName* (pavardė), *UserName* (vartotojo vardas parduotuvės sistemoje). Visų šių elementų duomenys turi tenkinti tam tikras sąlygas, t.y. vardas ir pavardė turi būti *_String* tipo (anksčiau aprašytas), vartotojo vardas (parduotuvės sistemoje) užsakymo dokumente turi būti eilutės tipo ir mažiausiai 3 ir daugiausiai 25 simbolių.

25 lentelė. Reikalavimai pateikiamai informacijai apie parduotuvę

```
<xs:complexType name="ShopDetails">
     <xs:sequence>
          <xs:element name="Name" type="xs:string"/>
          <xs:element name="ShopCode">
             <xs:simpleType>
               <xs:restriction base="xs:string">
                 <xs:pattern value="[0-9]{5}|[0-9]{6}|[0-9]{7}|[0-9]{8}"/>
               </xs:restriction>
```

```
            </xs:simpleType>
         </xs:element>
     </xs:sequence>
</xs:complexType>
```

Ištraukoje yra pateikta kokie elementai turi būti pateikti apie internetinę parduotuvę: *Name* (parduotuvės pavadinimas), *ShopCode* (parduotuvės kodas (įmonės kodas)). Parduotuvės pavadinimas ir kodas turi būti eilutės tipo. Taip pat parduotuvės kodas turi būti sudarytas mažiausiai iš 5 ir daugiausiai iš 8 skaitmenų.

26 lentelė. Reikalavimai pateikiamai informacijai apie užsakomą

```
<xs:complexType name="OrderDetails">
     <xs:sequence>
          <xs:element name="Products">
               <xs:complexType>
                  <xs:sequence>
                     <xs:element name="Product" maxOccurs="unbounded">
                        <xs:complexType mixed="false">
                           <xs:complexContent mixed="false">
                              <xs:extension base="OrderedProducts">
                                 <xs:atribute name="ProductId" use="required">
                                     <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                           <xs:minLength value="1"/>
                                           <xs:maxLength value="10"/>
                                        </xs:restriction>
                                     </xs:simpleType>
                                  </xs:attribute>
                              </xs:extension>
                           </xs:complexContent>
                        </xs:complexType>
                     </xs:element>
                  </xs:sequence>
               </xs:complexType>
          </xs:element>
          <xs:element name="OrderId" type="xs:int"/>
          <xs:element name="OrderDate" type="xs:date"/>
          <xs:element name="Total" type="xs:float"/>
     </xs:sequence>
</xs:complexType>
```

Šiame fragmente (26 lentelė) yra aprašomi užsakymo elementai: *Products* (prekės), *OrderId* (užsakymo numeris), *Total* (galutinė suma). *Products* elementas yra sudarytas iš elemento *Product* (prekė) su atributu *ProductId*, kuris reiškia produkto numerį. Šis elementas yra sudarytas dar iš kitų elementų, kurie yra aprašyti *OrderedProducts* elementų grupėje. Reikalavimai prekės atributui yra tokie, kad reikšmė yra eilutės tipo ir turi būti sudaryta bent iš 1 elemento, bei neturi viršyti 10 elementų. Šis atributas yra privalomas.

27 lentelė. Reikalavimai pateikiamai informacijai apie užsakytas prekes

```
<xs:complexType name="OrderedProducts">
     <xs:sequence>
          <xs:element name="Name" type="_String"/>
          <xs:element name="UnitPrice">
               <xs:simpleType>
                    <xs:restriction base="_Decimal">
                         <xs:whiteSpace value="collapse"/>
                    </xs:restriction>
               </xs:simpleType>
          </xs:element>
          <xs:element name="Quantity">
               <xs:simpleType>
                    <xs:restriction base="xs:int">
                         <xs:totalDigits value="2"/>
                         <xs:whiteSpace value="collapse"/>
                    </xs:restriction>
               </xs:simpleType>
          </xs:element>
          <xs:element name="Total">
               <xs:simpleType>
                    <xs:restriction base="_Decimal">
                         <xs:whiteSpace value="collapse"/>
                    </xs:restriction>
               </xs:simpleType>
          </xs:element>
     </xs:sequence>
</xs:complexType>
```

Šis paskutinis elementas XML schemoje aprašo elementus, kurie yra *Product* elemento vaikiniai elementai. Taigi aprašomie šie elementai: *Name* (prekės pavadinimas), *UnitPrice* (prekės vieneto kaina), *Quantity* (užsakytas kiekis), *Total* (užsakytos prekės visa suma). Prekės pavadinimo elemente duomenys turi būti *_String* duomenų tipo. Vieneto kaina

ir visa kaina turi būti *_Decimal* duomenų tipo ir kad bus pašalinti tarpai, jai jų bus pateiktoje reikšmėje. Kiekio elemente turi būti duomenys sveiko skaičiaus pavidalu. Šis skaičius neturi viršyti 2 skaitmenų skaičiaus, tai yra prekių kiekis turi būti mažesnis nei 100. Taip pat panaikinami tarpai, jai jie yra tarp pateiktų duomenų [17].

Taigi, pateiktos XML schemos ištraukos sudaro visą XML schemą, pagal kurią formuojamas užsakymo dokumentas. Visi paminėti laukai yra būtini dokumente ir negali būti daugiau elementų nei nurodyta XML schemoje. Šią schemą turi internetinės parduotuvės ir pirkėjai tam, kad galėtų patikrinti užsakymo dokumentą ar jis tenkina visas taisykles, kadangi dokumentas gali būti sukurtas gerai, tačiau keliaudamas pas gavėją jis gali būti modifikuotas piktavalio, pridedant ar pakeičiant duomenis užsakymo dokumente. Tuomet atkeliavęs pas gavėją jis bus patikrintas ir bus pastebėti neatitikimai.

4.2.3. Užsakymo dokumentas.

Užsakymo dokumentą formuoja internetinė parduotuvė. Pirkėjas šį dokumentą tik papildo įdėdamas savo parašą. Taigi vartotojui užsisakant prekes internetinėje parduotuvėje yra sudaromas XML užsakymo dokumentas, kuriame elementai, kuriuos minėjome XML schemoje, bei internetinės parduotuvės e. parašas. Toliau pateikiami internetinės parduotuvės sukurto XML užsakymo dokumento fragmentai ir jų paaiškinimai:

28 lentelė. XML dokumento versija ir naudojama koduotė

```
<?xml version="1.0" encoding="UTF-8"?>
```

Šis fragmentas nurodo XML dokumento versiją, bei koks kodavimas naudojamas. Taigi šis XML dokumentas yra 1.0 versijos ir naudojama UTF-8 koduotė.

29 lentelė. XML užsakymo dokumentas

```
<Order>
    <OrderDetails xmlns="">
        <Products>
            <Product ProductId="1">
                <Name>Obuolys</Name>
                <UnitPrice>2.00</UnitPrice>
                <Quantity>1</Quantity>
                <Total>2.00</Total>
            </Product>
            <Product ProductId="2">
```

```
                    <Name>Kriause</Name>
                    <UnitPrice>2.00</UnitPrice>
                    <Quantity>1</Quantity>
                    <Total>2.00</Total>
               </Product>
          </Products>
          <OrderId>174</OrderId>
          <OrderDate>2010-04-18</OrderDate>
          <Total>4.00</Total>
     </OrderDetails>
     <OrdererCredentials xmlns="">
          <Name>Giedrius</Name>
          <Surename>Mickevicius</Surename>
          <UserName>giedrius</UserName>
     </OrdererCredentials>
     <ShopCredentials xmlns="">
          <Name>e-perduotuve</Name>
          <ShopCode>123456</ShopCode>
     </ShopCredentials>
     <ReturnURL>http://www.e-parduotuve.lt?OrderConfirmation.aspx
       </ReturnURL>
     <Signatures>
          <ShopSignature />
          <UserSignature />
     </Signatures>
</Order>
```

Kaip matome informacija apie užsakymą susideda iš elementų, kurie paminėti XML schemoje: *OrderDetails* (užsakymo duomenys, kuris savyje saugo *Products* (prekes), *OrderDate* (užsakymo datą), *OrderId* (užsakymo numerį), *Total* (galutinę sumą)), *OrdererCredentials* (duomenys apie užsakovą), *ShopCredentials* (duomenys apie parduotuvę) ir *ReturnUrl* (duomenų grąžinimo nuoroda). Šiame dokumente yra pateikta pavyzdinė informacija apie užsakymą. Visi duomenys ir visi elementai esantys šiame užsakymo dokumento elemente tenkina visas taisykles, kurios aprašytos XML schemoje.

30 lentelė. Elementai, kuriuose talpinami pirkėjo ir parduotuvės elektroniniai parašai

```
<Signatures>
     <ShopSignature>
          ...
     </ShopSignature>
```

```
    <UserSignature/>
</Signatures>
```

Signatures elemente yra saugojami elementai, kuriuose patalpinami internetinės parduotuvės bei pirkėjo elektroniniai parašai. Internetinei parduotuvei sukūrus užsakymo dokumentą, yra užpildoams tik *ShopSignature* elementas, į kurį įdedamas internetinės parduotuvės elektroninis parašas. *UserSignature* elementas yra pridedamas taip pat prie dokumento, tačiau tuščias, kadangi vartotojas pasirašys vėliau ir savo elektroninį parašą talpins būtent jame.

4.2.4. Užsakymo dokumento elektroninis parašas

Toliau pateikiami XML dokumento fragmentai yra elektroninio parašo sudedamosios dalys. E. parašas yra sudarytas pagal XAdES specifikaciją, t. y. turi visus reikalingus elementus kuriuose saugojami atskiri elementai su duomenimis, kurie visi sudaro dokumento e. parašą:

31 lentelė. XML elektroninio parašo tėvinis elementas

```
<Signature Id="Signature1" xmlns="http://www.w3.org/2000/09/xmldsig#">
          ...
</Signature>
```

Tai yra XML elektroninio parašo tėvinis elementas, kurio viduje yra saugojami kiti elementai, kurie visi kartu sudaro visą XML elektroninį parašą. Šis elementas turi atributą *Id* , kuris yra šio elemento identifikacinis pavadinimas. Kitas atributas *xmlns* nurodo, jog duomenų tipai, naudojami šiame elemente yra iš *http://www.w3.org/2000/09/xmldsig#* vardų srities.

32 lentelė. Elektroninio parašo pasirašoma informacija

```
<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="#SignedProps"       Type="http://uri.etsi.org/01903#
SignedProperties">
     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
     <DigestValue>3cTtz8akA20XxJGY/oUdzpGckd4=</DigestValue>
  </Reference>
  <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>T4EJerInd+orSe4iqlDWUQ1PZTo=</DigestValue>
  </Reference>
</SignedInfo>
```

SignedInfo – pasirašytos užsakymo dokumento informacijos elementas. Jis savyje saugo parašo metodą (*SignatureMethod*), kanoninio pavidalo sudarymo metodą (*Canonicalization Method*). Taip pat yra saugojami du nuorodų (*Reference*) elementai. Pirmasis nuorodos elementas turi atributą *URI* su reikšme *#SignedProps*, kas reiškia, jog bus pasirašytas ir elementas, kurio *Id* atributas yra lygus šiai reikšmei. Kitas nuorodos elementas nurodo pasirašytinos informacijos objektą. Kadangi elemento atributas turi tuščią reikšmę, todėl tai yra tolygu tėviniam elementui *Order*. Antrasis nuorodos elementai saugoja *Transforms* elementą, kuris nurodo jog parašas yra apvilktas (angl. enveloped signature). Elementuose *DigestMethod* yra nurodomas algoritmas, kuriuo apskaičiuota pasirašomų duomenų santrauka, o elemente *DigestValue* yra pati santraukos reikšmė.

33 lentelė. Elektroninio parašo reikšmės elementas

```
<SignatureValue>
aOE3hkBhXbWQxmcwn2RC+uLtoSGGS5eouoltgzuAZg+xa1lel5U3WaMMeFBkz7Hll5FgDxoshLv
pfrCUU8I63HzmLhT9g00YzEO1gTriwwh1uqFtv1weNe+9G59ZZ0Do37s7wYZUDmIkkcGZSVWQJn
lqeR638HKhETJvmr+wWD4=
</SignatureValue>
```

Šiame elemente yra saugojama e. parašo reikšmė, kuri buvo apskaičiuota užšifruojant dokumento santrauką vartotojo privačiuoju raktu, kuris yra saugojamas skaitmeniniame sertifikate. Parašas apskaičiuotas nurodytais algoritmais, kurie yra nurodyti *SignedInfo* elemente.

34 lentelė. Naudojamų raktų bei skaitmeninio sertifikato elementai

```
<KeyInfo>
     <KeyValue>
          <RSAKeyValue>
               <Modulus>
                    z42F7EXKAr7lIB2nXYKTOCtjx+o3froV2W5M2ao+1hYzafEm0kNXjio8
                    G1y0jh+1KuuU2G60d3UR5QV12Darlzof1thqQIBGkHE4CvjYUvaAiT9P
```

```
                    3v3/x20Pd8n4L0EPP9HQbr6BRaggPA0Xm6BKliPZKt3grgJo97L9Q9jR
                    wCc=
               </Modulus>
               <Exponent>AQAB</Exponent>
          </RSAKeyValue>
     </KeyValue>
     <X509Data>
          <X509Certificate>
               MIIC8DCCAlkCAQEwDQYJKoZIhvcNAQEEBQAwgdgxCzAJBgNVBAYTAkxUMRIwE
               AYDVQQIEwlMaXRodWFuaWExDzANBgNVBAcTBkthdW5hczEdMBsGA1UEChMUTW
               9rZWppbW8gY2VudHJhcyBVQUIxLzAtBgNVBAsTJk1va2VqaW1vIGNlbnRyYXM
               gU2VydGlmaWthdmltbyBjZW50cmFzMRwwGgYDVQQDExNNb2tlamltbyBjZW50
               cmFzIFNDMTYwNAYJKoZIhvcNAQkBFidtb2tlamltby5jZW50cmFzLnNjQG1va
               2VqaW1vLmNlbnRyYXMubHQwHhcNMDkxMDI5MjEyNTI0WhcNMTAxMDI5MjEyNT
               I0WjCBpzELMAkGA1UEBhMCTFQxEjAQBgNVBAgTCUxpdGh1YW5pYTEPMA0GA1U
               EBxMGS2F1bmFzMRkwFwYDVQQKExBFLXBhcmR1b3R1dmUgVUFCMRUwEwYDVQQL
               EwxFLXBhcmR1b3R1dmUxHDAaBgNVBAMTE3d3dy5lLXBhcmR1b3R1dmUubHQxI
               zAhBgkqhkiG9w0BCQEWFGluZm9AZS1wYXJkdW90dXZlLmx0MIGfMA0GCSqGSI
               b3DQEBAQUAA4GNADCBiQKBgQDPjYXsRcoCvuUgHaddgpM4K2PH6jd+uhXZbkz
               Zqj7WFjNp8SbSQ1eOKjwbXLSOH7Uq65TYbrR3dRHlBXXYNquXOh/W2GpAgEaQ
               cTgK+NhS9oCJP0/e/f/HbQ93yfgvQQ8/0dBuvoFFqCA8DRebоEqWI9kq3eCuA
               mj3sv1D2NHAJwIDAQABMA0GCSqGSIb3DQEBBAUAA4GBAGqUPGzkRahPTjziNr
               JXME6Jzk3OLz1RzV8VxR6ECWfkf5swNDmxdpkh5HdhDoAYygAy3d63hqvqHyF
               iASNLbuuFL6aVToJHPx0F2+Dr4/jAe9Z741spk+5ArZpKPL6yiwK7uRVJ1V+g
               DQAEXmGGahIvRjbAd473mAlAnkFND1GY
          </X509Certificate>
     </X509Data>
</KeyInfo>
```

KeyInfo elementas nurodo parašui tikrinti reikalingus raktus. Raktai saugojami išskaidyti kriptografiniais elementais. *RSAKeyValue* saugoja dvi reikšmes: *n* (*Modulus*) ir *e*(*Exponent*). Šios dvi reikšmės kartu sudaro viešąjį raktą. Elementas X*509Data* saugoja sertifikato informaciją. Sertifikato informacija yra užkoduojama *base64* koduote ir patalpinama *X509Certificate* elemente.

35 lentelė. XML elektroninio parašo savybių elementai

```
<Object>
     <QualifyingProperties Target="#Signature1"
xmlns="http://uri.etsi.org/01903/v1.1.1#">
          <SignedProperties Id="SignedProps">
               <SignedSignatureProperties>
                    <SigningTime>2010-05-16T11:39:04.271Z</SigningTime>
```

```
                    <SigningCertificate>
                         <Cert>
                              <CertDigest>
                                   <DigestMethod Algorithm="http://www.w3.org
/2000/09/xmldsig#sha1" />
                                   <DigestValue>
                                   3370F318BE68E5819E4DE5DA161B2FED52C008C9
                                   </DigestValue>
                              </CertDigest>
                              <IssuerSerial>
                                <X509IssuerName>
                                  E=mokejimo.centras.sc@ mokejimo.centras.lt,
                                  CN=Mokejimo centras SC,
                                  OU=Mokejimo centras Sertifikavimo centras,
                                  O=Mokejimo centras UAB,
                                  L=Kaunas,
                                  S=Lithuania,
                                  C=LT
                                </X509IssuerName>
                                <X509SerialNumber>01</X509SerialNumber>
                             </IssuerSerial>
                         </Cert>
                    </SigningCertificate>
               <SignaturePolicyIdentifier />
            </SignedSignatureProperties>
            <SignedDataObjectProperties />
          </SignedProperties>
          <UnsignedProperties>
              <UnsignedSignatureProperties />
          </UnsignedProperties>
     </QualifyingProperties>
</Object>
```

Object elemente yra saugojamos elektroninio parašo savybės, kurios aprašytos XAdES parašo specifikacijoje. *QualifyingProperties* elementas yra XML parašo parametrų tėvinis elementas. Jo atributas *Target* nurodo kurio iš XML dokumento elektroninių parašų parametrai yra saugomi šiame elemente, o atributas *xmlns* nurodo, jog duomenų tipai, naudojami šiame elemente yra naudojami iš *http://uri.etsi.org/01903/v1.1.1#*. *SignedProperties* elementas saugoja pasirašomas elektroninio parašo savybes. Jo atributas *Id* nurodo šio elemento identifikacinę reikšmę, pagal kurią šis elementas bus surastas, kuomet bus generuojamas elektroninis parašas. Tuomet bus apskaičiuota šio elemento santrauka ir

patalpinta *SignedInfo* elemento vaikinį elementą *DigestValue*. *SigningTime* elementas saugoja pasirašymo laiką, kuomet buvo sugeneruotas šio dokumento elektroninis parašas. *SigningCertificate* saugoja pasirašiusio sertifikato informaciją, tokią kaip sertifikato santrauką (*CertDigest*), sertifikavimo centro informacija (*X509IssueName*) ir sertifikato serijos numerį (*X509SerialNumber*). *UnisignedProperties* elemente galėtų būt saugojami elektroninio parašo parametrai, kuriuos būtų nebūtina pasirašyti [7][16].

4.3. Sukurto autentifikavimo metodo privalumų ir trūkumų analizė

Analizės dalyje buvo aptarti keli autentifikavimo būdai, paminėti keli jų trūkumai, dėl kurių galėtų būti nesaugu ar nepatogu juos naudoti. Sukurtas autentifikavimo būdas taip pat turi trūkumų ir privalumų:

Privalumai:

- Šiame autentifikavimo metode yra naudojamas elektroninis parašas, kuris yra sukuriamas panaudojant viešojo rakto infrastruktūrą. Parašo reikšmė yra apskaičiuojama panaudojant kriptografinius algoritmus ir tokią reikšmę iššifruoti praktiškai neįmanoma.
- Kadangi sertifikavimo centrų gali būti ne vienas, dėl to, norint patikrinti sertifikato autentiškumą, reikia turėti kiekvieno iš šių sertifikavimo centrų sertifikatus. Tačiau vartotojas turi būti tikras, jog sertifikavimo centras yra patikimas ir tik tada jį įtraukti į patikimų sertifikavimo centrų sertifikatų sąrašą. Šioje atsiskaitymo sistemoje vartotojui pas save kompiuteryje šių sertifikatų nesaugoja, nes jis pats netikrina sertifikatų autentiškumo. Už jį tai padaro atsiskaitymo sistema. Joje yra saugojami patikimų sertifikavimo centrų viešojo rakto sertifikatai. Taigi yra užtikrinama, jog bus autentifikuojami tik patikimų sertifikavimo centrų išduoti sertifikatai.
- Kaip ir saugumo įranga paremtoje autentifikacijoje vartotojas su savimi turi turėti prietaisą, atmintinę, kurioje būtų saugojama vartotojo pasirašymo programa. Pametus šią atmintinę, piktavalis negalėtų pasinaudoti šia programa, kadangi jam reikėtų žinoti sertifikato slaptažodį. Taip pat vartotojas turėtų pranešti apie tai sertifikatą išdavusiam sertifikavimo centrui, kad šis atšauktų sertifikato galiojimą.
- Pamiršus sertifikato slaptažodį, nėra galimybės jo kaip nors sužinoti.

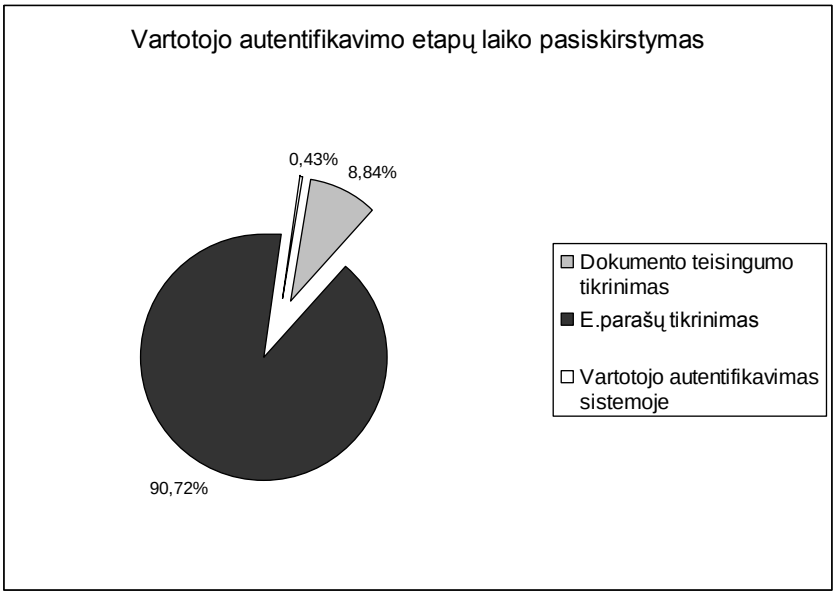
Trūkumai:

- Vartotojas yra autentifikuojamas pagal jo e. parašą. Kad vartotojas galėtų pasirašyti dokumentą, jis turi aktyvuoti savo sertifikatą, kuriame saugojamas jo privatusis raktas. Kad tai padaryt jis turi suvesti slaptažodį. Slaptažodis gali būti sužinomas piktavalio

analizės dalyje aptartais būdais, tačiau šiuo atveju slaptažodžiai nėra saugomi slaptažodžių faile, slaptažodžiai nekeliauja internetu. Slaptažodį piktavalis gali sužinoti įbauginimo metu, panaudojant smurtą. Taip pat piktavaliui kokiu nors būdu gavus vartotojo privataus rakto sertifikatą, jis galėtų neribotą kiekį kartų bandyti atspėti sertifikato slaptažodį, panaudojant analizės dalyje paminėtas technologijas (žodyno atakas, grubios jėgos (angl. Brutus force) atakas).

- Sukurtas autentifikavimo būdas gali būti sudėtingesnis vartotojui, kadangi jis turi žinoti kaip reikia elgtis vienu ar kitu atveju: turi žinoti kaip parsisiųsti užsakymo dokumentą iš internetinės parduotuvės, turi mokėti susirasti šį dokumentą pas save kompiuteryje, turi žinoti tolimesnius veiksmus kaip elgtis su vartotojui sukurta pasirašymo programine įranga. Todėl vartotoją, prieš jam atliekant pirkimus internetu, reikėtų apmokyti.
- Pamiršus sertifikato slaptažodį vartotojui nėra galimybės jo kažkaip atkurti ar sužinoti, dėl to reikėtų vėl kreiptis į sertifikavimo centrą, kad šis išduotų naują sertifikatą, o tai vartotojui sudarytų nepatogumų.

Atliktas tyrimas patikrinti kiek laiko užtrunka autentifikuoti vartotoją, kuomet naudojamas slaptažodžiu paremtas autentifikavimo metodas ir kuomet vartotojas autentifikuojamas pagal jo elektroninį parašą. Tyrimui atlikti buvo apskaičiuotas vidutinis laikas, kiek užtrunka vartotojui autentifikuoti. Buvo 100 kartų bandoma autentifikuoti vartotoją pagal jo prisijungimo vardą (elektroninio pašto adresą) bei slaptažodį, bei tiek pat kartų buvo bandoma autentifikuoti vartotoją pagal jo elektroninį parašą. Slaptažodžiu paremto autentifikavimo atveju apskaičiavome, jog vidutinis autentifikavimo laikas yra 52,34 milisekundes, tuo tarpu elektroniniu parašu paremto autentifikavimo atveju, vartotojas buvo autentifikuotas vidutiniškai per 106,25 milisekundės. Taigi sukurtoje atsiskaitymo sistemoje vartotojas autentifikuojamas beveik dvigubai lėčiau nei slaptažodžiu paremto autentifikavimo atveju. Tai yra todėl, jog vartotojui autentifikuojantis jo elektroniniu parašu, reikia patikrinti gauto XML dokumento teisingumą (remiantis XML schema), patikrinti elektroninius parašus (dokumento vientisumą) bei autentifikuoti vartotoją. Žemiau esančioje diagramoje (11 pav.) yra pateikta kokią laiko dalį užima kiekvienas iš autentifikavimo etapų:



11 pav. Vartotojų autentifikavimo etapų laiko pasiskirstymo diagrama

Kaip matome didžiąją dalį vartotojo autentifikavimo laiko užima elektroninių parašų tikrinimas. Šis trunka 96,39 milisekundės. Tai yra dėl to, jog užsakymo dokumente egzistuoja du elektroniniai parašai (pirkėjo ir internetinės parduotuvės) , kuriuos abu reikia patikrinti, siekiant įsitikinti, jog dokumentas nebuvo pakeistas kurios nors iš prekyboje dalyvaujančių šalių.

Šie skaičiavimai atlikti vietinėje darbo stotyje, kuri veikia kaip žiniatinklio serveris (buvo kreipiamasi į žiniatinklio serverį iš tos pačios darbo stoties), dėl to duomenys internetu nekeliavo, kas galėtų įtakot dar ilgesnį vartotojų autentifikavimo laiką. Darbo stoties procesoriaus taktinis dažnis – 2.0 GHz.

Taigi pastebėta, jog sukurtas autentifikavimo būdas turi ir trūkumų ir privalumų, lyginant su kitais būdais. Šis būdas yra saugesnis nei naudojant slaptažodžiu paremtą autentifikaciją, kadangi slaptažodžiai internetu nekeliauja, o naudojamas tik vietiniame kompiuteryje, tačiau kaip parodė tyrimas, sukurtas vartotojo autentifikavimo procesas užtruktų dvigubai lėčiau nei slaptažodžiu paremtoje autentifikacijoje. Tačiau autentifikavimo laikas yra labai trumpas ir siekia vos dešimtadalį sekundės, todėl vartotojas to net nepastebės. Lyginant su saugumo įranga paremta autentifikacija sukurta autentifikavimo sistema taip pat naudoja tam tikrą įrenginį (atmintinę su pasirašymo programine įranga). Abiem atvejais pametus šią autentifikavimui naudojamą įrangą ir tretiesiems asmenims radus, ja pasinaudoti negalės, nes nežinos aktyvavimo slaptažodžio ar kodo. Tačiau vartotojui pamiršus šį aktyvavimo kodą ar slaptažodį sukurtame autentifikavimo metode nėra galimybės kažkaip sužinoti ar atgauti slaptažodį, ne taip kaip aptartoje saugumo įrangoje paremtoje autentifikacijoje, kurioje vartotojas gali pasikeisti aktyvavimo kodą net internetu [11]. Taip

pat, piktavaliui kažkokiu būdu (vartotojui pametus, dėl neatsargumo palikus apsirašymo įrangą ir kartu sertifikatą viešo naudojimo kompiuteryje arba piktavaliui jėga gavus šią pasirašymo įrangą ir sertifikatą) gavus vartotojo privataus rakto sertifikatą, jis galėtų bandyti atspėti slaptažodį neribotą kiekį kartų. Dėl to vartotojui reikėtų nedelsiant pranešti apie prarastą sertifikatą sertifikatus išduodančiai įstaigai, kuri panaikintų šio sertifikato galiojimą.

4.4. Galimi alternatyvūs sprendimo būdai ir jų palyginimas

4.4.1. Alternatyvūs užsakymo dokumentai bei jų e. parašo formavimo būdai.

PDF

PDF (angl. Portable Document Format) – tai Adobe Systems kompanijos sukurtas duomenų failo formatas, kuriame gali būti saugoma bet kokia dvimatė informacija. Tokio tipo dokumentai yra skirti duomenų apsikeitimui ir peržiūrai ir nepriklauso nuo programinės įrangos ar operacinės sistemos kurioje šis dokumentas buvo sukurtas. Šis dokumentas susideda iš objektų, kurie visi kartu sudaro visumą to, ką vartotojas mato. Tie objektai gali būti paveiksliukai, tekstas, interaktyvūs elementai. Tokio tipo dokumentas taip pat gali būti naudojamas internetiniuose atsiskaitymuose kaip užsakymo dokumentas. Kuriamoje sistemoje vartotojas yra autentifikuojamas pagal jo e. parašą, kurį jis padeda užsakymo dokumente. PDF dokumentas taip pat gali būti pasirašomas vartotojo ir vėliau pagal šį parašą autentifikuojamas. Parašas gali būti grynai matematiškas, t.y. panaudojant viešojo/privataus rakto užkoduotą dokumento santrauką, taip pat gali būti biometrinio tipo parašas, toks kaip ranka rašytas parašas, piršto antspaudas arba tinklainės skanavimas. Šios autentifikavimui naudojamos priemonės yra tvarkomos ir vartotojas yra autentifikuojamas panaudojant parašo tvarkykle, kuri gali būti integruota į reikiamą sistemą. Norint autentifikuoti pasinaudojant savo ar trečiųjų asmenų autentifikavimo įrankiu, tai jis turi būti užregistruotas Adobe kompanijoje. E. parašas yra laikomas parašo elemente. Parašas yra suformuojamas apskaičiuojant dokumento ar dokumento dalies santrauką, ir ją užšifruojant pasirašančiojo privačiuoju raktu. Šis parašas yra saugojamas PDF dokumente. Parašo elementas susideda iš šių laukų: *Filter* – rodo pageidautino manipuliatoriaus pavadinimą, kuriuo parašas buvo sudarytas arba kuri panaudojus būtų tikrinamas e. parašas, *Content* – e. parašo reikšmė, *ByteRange* – sveikųjų skaičių porų masyvas, tiksliai nusakantis baitų diapazoną, pagal kurį skaičiuojama santrauka. Tai pat yra ir daugiau parašo elemento laukų, tačiau juos naudoti nėra privaloma. Jai naudojamas *adbe.x509.rsa.sha1* pofiltris (angl. subfilter), tuomet parašo elemente turi būti laukas *SubFilter*. Pofiltris apibrėžia parašo reikšmės ir rakto informacijos

formatą (kodavimą), taip pat naudojamus kriptografinius algoritmus. Egzistuoja kelios pofiltrių reikšmės: *adbe.pkcs7.detached, adbe.pkcs7.sha1* ir *adbe.x509.rsa.sha1*. Žemiau esančioje lentelėje yra pateikiamos galimos pofiltrių reikšmės ir atitinkami kriptografiniai algoritmai:

36 lentelė. Pofiltrių reikšmės ir atitinkami algoritmai [1]

	SubFilter reikšmė		
	adbe.pkcs7.detached	*adbe.pkcs7.sha1*	*adbe.x509.rsa.sha1*
Santraukos reiškmės	SHA1 (PDF 1.3) SHA256 (PDF 1.6) SHA384 (PDF 1.7) SHA512 (PDF 1.7) RIPEMD160 (PDF 1.7)	SHA1 (PDF 1.3)	SHA1 (PDF 1.3) SHA256 (PDF 1.6) SHA384 (PDF 1.7) SHA512 (PDF 1.7) RIPEMD160 (PDF 1.7)
Suderinamumas su RSA algoritmu	Iki 1024-bit (PDF 1.3) Iki 2048-bit (PDF 1.5) Iki 4096-bit (PDF 1.5)		
Suderinamumas su DSA algoritmu	Iki 4096-bit (PDF 1.6)		nesuderinama

PDF dokumentuose sertifikato informacija yra saugoma atsižvelgiant į pasirinktą pofiltrį. Jai tai yra *adbe.x509.rsa.sha1,* tuomet parašas yra saugojamas atskirame parašo elemente *Cert* kaip baitų eilutė, atitinkanti X.509 sertifikatą. Kitų pofiltrių atveju sertifikatas yra saugojamas elemente *Contents.*

PDF dokumente gali būti tokių tipų e. parašai:

- Vieno ar kelių dokumento parašų. Parašo elementas turi turėti *ByteRange* lauką, kuriame būtų baitų diapazonas. Parašas tikrinamas perskaičiuojant dokumento santrauką ir palyginant su ta, kuri saugojama paraše. Jeigu dokumentas buvo modifikuotas ir išsaugotas, tuomet originalaus parašo baitų diapazonas yra nekeičiama ir jeigu parašas yra teisingas, tuomet galima atkurti dokumento būseną, kuri buvo kuomet dokumentas buvo pasirašomas.
- Ne daugiau kaip vienas MDP (angl. modification detection and prevention) parašas. MDP parašo elemente turi būti parašo, bei *ByteRange* reikšmės. Šis parašas leidžia dokumento autoriui nurodyti, kas gali būti pakeista(išsaugant originalų parašą), o kas ne (po pakeitimo parašas taptų nebegaliojantis). Šis parašas naudoja *DocMDP* transformacijos metodą.

- Ne daugiau kaip du teisės naudotis parašai (UR). Tai viena iš Adobe Acrobat sistemų galimybių suteikti vartotojams teises atlikti tam tikrus veiksmus, t.y. sukurti dokumentus, suteikiančius specialias teises, kurios būtų grindžiamos vartotojų teisių parašu. Programai įsitikinus, jog parašas geras, vartotojui suteikiamos nurodytos teisės [1].

Kuriamoje sistemoje tokio formato dokumentas taip pat galėtų būt panaudotas užsakymo dokumentui kurti, tačiau kiekviena internetinėje prekyboje dalyvaujanti šalis turi programiškai nuskaityti ir apdoroti užsakymo duomenis esančius tokiame dokumente. Šio dokumento nuskaitymas yra nepatogus tuo, kad duomenys yra nestruktūrizuotai sudėlioti pačiame dokumente. Tai yra tekstinis dokumentas, kuriame visi duomenys surašyti eilute ir surasti reikiamus duomenis yra sudėtinga. XML dokumentas yra patogesnis šiuo atžvilgiu, nes duomenys yra struktūrizuotai sudėti į tam tikrus elementus.

Microsoft Office dokumentų formatai: XLSX, DOCX, PPTX

Microsoft Office yra Microsoft kompanijos sukurtas programų paketas, skirtas dirbti su tekstiniais dokumentais (Word), prezentacijomis(PowerPoint), atliekant skaičiavimus (Excel), pašto programa (Outlook) ir pan. Šiuo metu yra išleistos 2010 metų programų bandomosios versijos. Tai šiuo metu yra naujausias programų paketas. Šios programos skirtos Microsoft Windows ir Apple Macintosh operacinėms sistemoms.

2010 ir 2007 metų versijų programų dokumentų formatai yra paremti XML technologija, kuri dar kitaip vadinama Office Open XML. Ši technologija palengvina duomenų apdorojimą, valdymą ir atstatymą. Taip pat, skirtingai nei senesnės versijos, jau naudoja skaitmeninius parašus dokumentams pasirašyti. Šiems parašams sudaryti yra naudojamas XMLDSIG. Sukūrus dokumentą su viena iš programų ir juos pasirašant, senesnės versijos programos neatpažins šio parašo ir jį ignoruos.

Galimi du būdai kaip pasirašyti Microsoft Office dokumentą:

- Pasirašyti nematomu parašu
- Pasirašyti įdedant viena ar kelias e. parašui skirtas vietas

Jeigu nėra būtinybės vartotojui matyti parašo, bet vis tiek reikia dokumentą pasirašyti tam, kad užtikrinti dokumento autentiškumą, integralumą ir originalumą, galima dokumentą pasirašyti nematomu parašu. Tokiu parašu galima pasirašyti Word, Excel ir PowerPoint programomis sukurtus dokumentus. Toks parašas nebus matomas pačiame dokumente, tačiau tai galima pastebėti peržiūrinėjant dokumento parašus ar pastebėjus ženkliuką programos lange, kuris informuoja apie tai, jog dokumentas buvo pasirašytas. Norint, kad vartotojas ar

dokumento gavėjas matytų, jog dokumente yra e. parašas, galima į dokumentą įterpti e. parašui skirtas vietas. Šios vietos - tai gali būti paveiksliukas vartotojo ranka rašyto parašo. Šis paveiksliukas bus tik įrodymas, jog dokumentas yra pasirašytas, o po šiuo paveiksliuku slėpsis vartotojo e. parašas. Šis parašas sudaromas pasirenkant sertifikatą, kuriame saugojamas vartotojo privatusis raktas, o programa pati suskaičiuoja pasirašomo dokumento santrauką ir ją pasirašo, o parašo duomenis sudeda į atitinkamą XMLDSIG struktūrą, kurios vartotojas dokumente nemato. Taip pat galima sukurti parašui skirtą vietą su instrukcijomis, skirtomis gavėjui, kad šis pasirašytų dokumentą [5].

Microsoft Office dokumentų elektroninį parašą sudaro:

- E. parašo šaltinio dalis: tai pradinis dokumento e. parašų analizės taškas. Dokumento vidiniuose ryšiuose pateikiama nuoroda į šią dalį ir jau nuo jos prasideda atskirų parašų analizė. Dokumente gali būti ne viena šaltinio dalis.
- E. parašo XML parašo dalis: tai dokumento vieno e. parašo informacija, pateikta ženklinimo kalba. Šioje vietoje gali būti ir viešųjų taktų X.5009 sertifikato informacija.
- E. parašo sertifikato dalis. Joje yra viešųjų raktų X.509 sertifikato, skirto parašui patikrinti informacija.

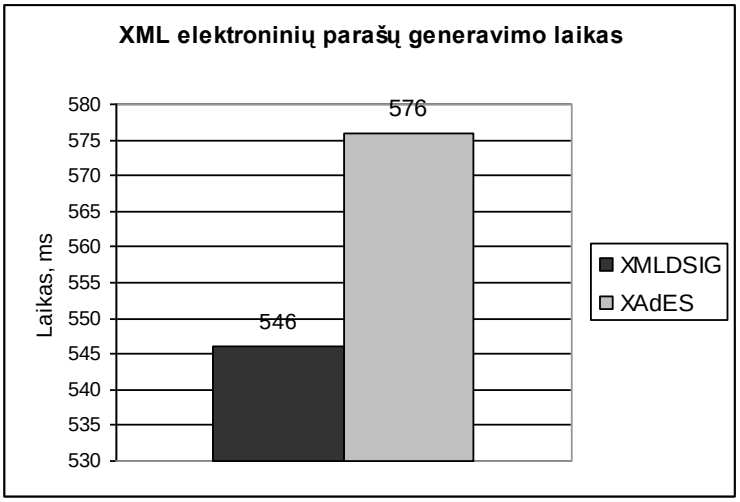
E. parašo XML parašo dalį sudaro XMLDSIG specifikacijoje aprašyti laukai. Tarp jų: *SignedInfo* (pasirašyta informacija, apimanti vertimo kanoniniu pavidalu algoritmą, parašo algoritmą ir sudarytą nuorodą), *SignatureValue* (e. parašo reikšmė), *KeyInfo* (viešojo rakto informacija), *Object* (papildoma informacija, detalizuojanti parašo sudarymą ir padedanti lengviau jį patikrinti). E. parašo generavimas ir tikrinimas vyksta remiantis XMLDSIG specifikacija: nuorodos generavimas ir tikrinimas, bei parašo generavimas ir tikrinimas pagal gautą nuorodą. Taip pat yra numatyti RSA ir DSA e. parašo algoritmai, bei SHA-1 santraukų algoritmai [7].

Šie dokumentų formatai taip pat galėtų būti panaudoti kuriamoje sistemoje, kadangi duomenys šiuose dokumentuose yra saugojami taip pat XML pavidalu. Tačiau, kad šiuos dokumentus galima būtų kurti ir peržiūrėti, kiekvienas pirkėjas ir e. parduotuvė turėtų turėti Microsoft programinę įrangą, kurią reikia pirkti ir kuri yra brangi. Taigi kurti tokius dokumentus būtų per brangu ir pirkėjams ir pardavėjams, juolab paprastus XML dokumentus galima kurti bet kuria teksto redagavimo programa.

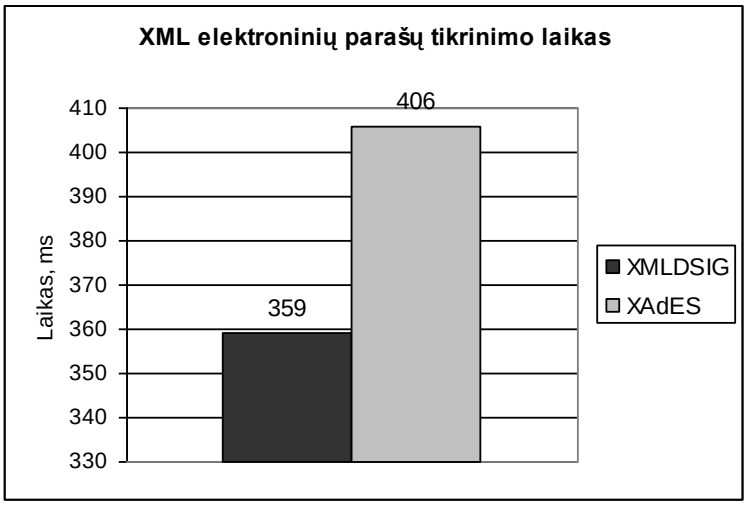
4.4.2. XMLDSIG – galimas alternatyvus XML dokumento elektroninio parašo formavimo metodas

XMLDSIG - XML elektroninio parašo standartas, kuris yra XAdES standarto viena iš sudedamųjų dalių. Pagal šią XML elektroninio parašo specifikaciją sukurtas parašas, kitaip nei pagal XAdES specifikaciją sukurtas parašas, nesaugoja šio parašo parametrų, naudojamų greitesniam ir patikimesniam vartotojo autentifikavimui. Taigi XAdES elektroninio parašo standartas yra pranašesnis už XMLDSIG parašo standartą, kadangi saugojama daugiau papildomos informacijos apie patį e. parašą. Tačiau dėl šių papildomų elementų e. paraše dokumentas užima daugiau vietos. To paties XML dokumento pagal XMLDSIG specifikaciją sugeneruotas elektroninis parašas, dydis užima 3331 baitus (3,25 KB) kompiuterio atminties, tuo tarpu pagal XAdES specifikaciją sugeneruotas elektroninis parašas užima 4964 baitus (4,84 KB). Didėjant dokumento dydžiui šio dokumento ir jo elektroninio parašo, sugeneruoto pagal abi specifikacijas, dydžių skirtumas nekinta, kadangi parašo turinys išlieka sudarytas iš tokių pačių elementų, skiriasi tik elementų reikšmės.

Žemiau esančiose diagramose yra pateikta pagal šiuos du aptartus XML elektroninių parašų standartus sugeneruotų ir patikrintų 100 elektroninių parašų laikinės charakteristikos.



12 pav. XML elektroninių parašų generavimo laiko diagrama

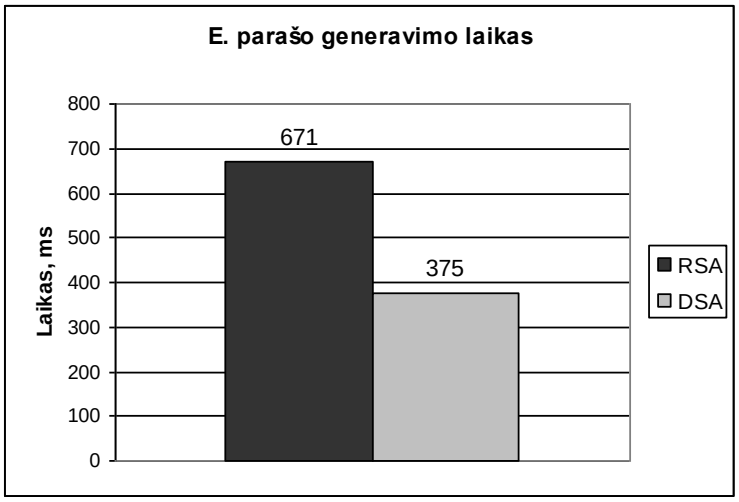


13 pav. XML elektroninių parašų tikrinimo laiko diagrama

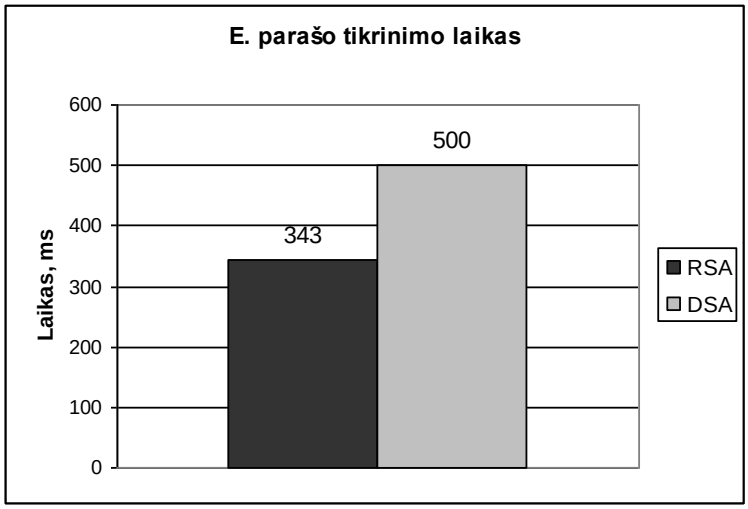
Iš diagramų matome, jog pagal XMLDSIG elektroninio parašo specifikaciją sugeneruotų e. parašų generavimo laikas yra mažesnis nei sugeneruotų pagal XAdES specifikaciją. Šis skirtumas yra nedidelis ir vartotojas to nepastebės, juolab, kad buvo sugeneruota 100 parašų, o generavimo laikas nesiekė vienos sekundės. Taip pat nedidelis laiko skirtumas yra ir kuomet tikrinami elektroniniai parašai. Čia pranašesnis yra vėlgi XMLDSIG standartas. Šiems skaičiavimams atlikti buvo pasirašomas nedidelės apimties (876 baitų) XML dokumentas.

4.4.3. DSA – galima alternatyvi elektroninio parašo sistema

DSA (angl. *Digital Signature Algorithm*) – viena iš populiariausių e. parašo sistemų, naudojamų raktų poros generavimui, pasirašymui ir e. parašo tikrinimui. Ši sistema yra mažiau populiari nei RSA (pagal autorių pavardes: R.L.Rivest, A.Shamir, L.Adelman). Nors e. parašo generavimas pagal DSA sistemą yra greitesnis nei generuojant pagal RSA, tačiau e. parašo tikrinimas užima žymiai daugiau laiko. Žemiau esančiuose diagramose yra pateiktos e. parašo generavimo ir tikrinimo laikinės charakteristikos.



14 pav. Elektroninio parašo, sugeneruoto pagal DSA e. parašo sistemą, generavimo laiko diagrama



15 pav. Elektroninio parašo, sugeneruoto pagal DSA e. parašo sistemą, tikrinimo laiko diagrama

Su kiekviena iš sistemų buvo sugeneruota ir patikrinta 100 parašų. Iš diagramų (14, 15 pav.) matosi, jog panaudojus RSA sistemą, e. parašų generavimas truko 671 ms. Tai yra vos ne dvigubai ilgiau nei panaudojus DSA sistemą (375 ms), tačiau atvirkščias rezultatas matosi kuomet parašai yra tikrinami. Šiuo atžvilgiu RSA sistema (343 ms) aplenkė DSA sistemą (500 ms). Šiems skaičiavimas atlikti buvo pasirašomas nedidelės apimties XML dokumentas. Kuo didesnis pasirašomas dokumentas, tuo ilgiau užtrunka jo pasirašymas - šie skaičiai gali žymiai padidėti. Kadangi e. parašas generuojamas tik vieną kartą, o tikrinamas kelis kartus, todėl aktualesnė yra sistema, pagal kurią sukurtas e. parašas yra greičiau patikrinamas. Taigi šioje kuriamoje sistemoje e. parašams kurti pasirinkome RSA sistemą.

Be šių dviejų elektroninio parašo sistemų egzistuoja ir kitos, mažiau populiarios e. parašo sistemos: Rabin, ECDSA, ElGamal, RSA-PSS [7].

4.5. Išvados

- Realizuotos prekyboje dalyvaujančios šalys:
  - Pirkėjo pasirašymo programinė įranga
  - Internetinės parduotuvės svetainė.
  - Dalinai realizuota atsiskaitymo sistema.
- Sukurtos papildomos priemonės, kurių dėka yra autentifikuojamos internetinėje prekyboje dalyvaujančios šalys:
  - Kiekvienai prekyboje dalyvaujančiai šaliai buvo sukurti skaitmeniniai sertifikatai.
  - Sukurtas XML dokumento taisyklių dokumentas – XML schema
  - Išsiaiškinome darbe panaudoto XML dokumento elektroninio parašo XAdES struktūrą.
- Išanalizavome sukurtą autentifikavimo metodą ir pastebėjome, jog jis yra pranašesnis už egzistuojančių atsiskaitymo sistemų autentifikavimo būdą. Šis autentifikavimo metodas remiasi viešojo rakto infrastruktūra, kuri užtikrina jog vartotojas bus autentifikuotas teisingai (užtikrinamas autentiškumas ir integralumas).
- Taip pat pastebėta jog ši sistema turi ir trūkumų. Vienas jų – autentifikavimo laikas, kuris yra dvigubai ilgesnis nei egzistuojančių sistemų autentifikavimo laikas. Tačiau šis trunka tik apie dešimtadalį sekundės, todėl vartotojas, jungdamasis prie sistemos, to nepastebės. Kitas trūkumas – vartotojui pernelyg sudėtingas prekybos ir atsiskaitymo procesas, dėl to reikėtų jį apmokyti.
- Pagrindinis sistemos trūkumas – vartotojo privataus rakto sertifikato ir jo aktyvavimo slaptažodžio atskleidimas. Todėl juos reikėtų itin saugoti nuo pašalinių asmenų.
- Ištyrėme alternatyvius sistemoje naudojamų technologijų sprendimo būdus:
  - Išsiaiškinome alternatyvius užsakymo dokumento, bei jų elektroninio parašo formavimo būdus ir pastebėjome, jog kiekvienas iš tirtų būdų nėra tinkamas pritaikyti kuriamoje sistemoje.
  - Ištyrėme galimą alternatyvų elektroninio parašo standartą – XMLDSIG, kuris galėtų būti pritaikytas kuriamoje sistemoje. Atliktame tyrime pastebėjome, jog patikimesnis yra XAdES standartas, dėl naudojamų papildomų saugumo užtikrinimo priemonių.
  - Ištyrėme DSA elektroninio parašo sistemą, kuri taip pat galėtų būti panaudota kuriamoje sistemoje vietoj RSA, ir pastebėjome, jog tinkamesnė naudojimui yra RSA, dėl trumpesnio elektroninio parašo tikrinimo laiko.

IŠVADOS

- Išanalizuotos internetinio atsiskaitymo sistemos, bei metodai kaip jose yra autentifikuojami vartotojai. Nustatyta, jog visos jos naudoja tą patį vartotojo autentifikavimo metodą – elektroniniu paštu bei slaptažodžiu paremtą vartotojo autentifikaciją, kuri nėra pakankamai saugi.
- Išanalizuota kokie vartotojo autentifikavimo metodai egzistuoja ir kokie yra jų privalumai bei trūkumai.
- Atlikus analizę ir išsiaiškinus egzistuojančių sistemų autentifikavimo trūkumus, buvo iškelti funkcinius ir nefunkcinius reikalavimus kuriamai sistemai.
- Sudarytas kuriamos internetinio atsiskaitymo sistemos modelis, nubraižytos UML diagramos, kurios apibudina kiekvienos iš sistemos sudedamųjų dalių veikimo principą.
- Realizuotos internetinėje prekyboje dalyvaujančių šalių programinės įrangos (vartotojo pasirašymo programinė įranga, internetinės parduotuvės svetainė, internetinio atsiskaitymo sistema). Realizavimui panaudota ASP.NET technologija, C# programavimo kalba ir MS SQL Server 2005 duomenų bazės valdymo sistema.
- Sukurtas taisyklių rinkinys (XML schema), pagal kurį sudaromas užsakymo dokumentas. Išsiaiškinta darbe panaudoto XML dokumento elektroninio parašo XAdES struktūra.
- Atlikus tyrimą nustatyta, jog sukurtas autentifikavimo būdas pranašesnis už egzistuojančių internetinių atsiskaitymo sistemų autentifikavimo metodą, kadangi šis autentifikavimo metodas remiasi viešojo rakto infrastruktūra, kuri užtikrina jog vartotojas bus autentifikuotas teisingai (užtikrinamas autentiškumas ir integralumas). Taip pat buvo nustatyti keli sukurtos sistemos trūkumai.
- Išnagrinėti alternatyvūs užsakymo dokumento formatai PDF ir Microsoft Office dokumentų formatai ir nustatyta, jog kiekvienas iš jų nėra tinkamas pritaikyti kuriamoje sistemoje.
- Ištirtas galimas alternatyvaus dokumento elektroninio parašo standarto XMLDSIG panaudojimas sukurtoje sistemoje. Iš gautų tyrimo rezultatų nustatyta, jog šis standartas yra greitesnis, tačiau mažiau saugesnis nei XAdES.
- Ištyrėme DSA elektroninio parašo sistemos panaudojimą kuriamoje sistemoje, ir pastebėjome, jog tinkamesnė yra RSA dėl greitesnio elektroninio parašo tikrinimo.

LITERATŪRA

1. Adobe PDF Reference, sixth edition: Adobe Portable Document Format Version 1.7. Adobe® Systems Incorporated. [interaktyvus]. 2006 m. Lapkritis. [žiūrėta 2010-04-13]. Prieiga per internetą: http://www.adobe.com/devnet/acrobat/pdfs/pdf_reference_1-7.pdf
2. Authentication and Authorization in Mobile Environment. Teppo Halonen. Helsinki University of Technology, Department of Computer Science, Tik-110.501 Seminar on Network Security. 2000
3. Authentication: From Passwords to Public Keys. Richard E. Smith. Addison Wesley 2002.
4. Attacks on Biometric Systems: A Case Study in Fingerprints. Umut Uludag, Anil K. Jain. Department of Computer Science and Engineering, Michigan State University.
5. Digital Signing of Microsoft® 2007 Office System Documents. Microsoft Corporation. 2007 Rugpjūtis.
6. eBay Inc.[interaktyvus]. [žiūrėta 2009-01-15]. Prieiga per internetą: http://www.ebay.com
7. Elektroninių dokumentų ir duomenų sauga. Eligijus Sakalauskas, Tomas Blažauskas, Kęstutis Lukšys. Kauno Technologijos Universitetas. 2008
8. Magistratūros studijų modulis „Kriptografinės sistemos“ 2 dalis. Praktinių darbų mokomoji medžiaga. Kauno technologijos universitetas. 2008.
9. Online Payment, Merchant Account – PayPal [interaktyvus]. [žiūrėta 2009-01-13]. Prieiga per internetą: http://www.paypal.com
10. RSA, The Security Division of EMC [interaktyvus]. [žiūrėta 2009-01-12]. Prieiga per internetą: http://www.rsa.com/rsalabs/node.asp?id=2124
11. RSA SecurID Ready Implementation Guide, Hitachi ID Systems Inc. [interaktyvus]. 2008 [žiūrėta 2010-01-23]. Prieiga per internetą: http://www.upek.com/pdf/Authenticator_UPEK_Protector_Suite_QL_58.pdf
12. SearchSecurity.com and Information Security magazine. Smart Card. [interaktyvus]. [žiūrėta 2009-01-15]. Prieiga per internetą: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213004,00.html
13. SearchSecurity.com and Information Security magazine. Security Token [interaktyvus].[žiūrėta 2009-01-09]. Prieiga per internetą: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci795971,00.html
14. Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure. Carl Ellison, Bruce Schneier, Computer Security Journal Volume XVI. 2000 Lapkričio 1
15. W3C XML Advanced Electronic Signatures (XAdES) [interaktyvus]. [žiūrėta 2010-04-23]. Prieiga per internetą: http://www.w3.org/TR/XAdES/

16. W3C XML Signature Syntax and Processing (Second Edition) [interaktyvus]. [žiūrėta 2010-04-28]. Prieiga per internetą: http://www.w3.org/TR/xmldsig-core/
17. W3C XML Shema [interaktyvus]. [žiūrėta 2010-03-25]. Prieiga per internetą: http://www.w3.org/XML/Schema