KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Ovidijus Petrulis

Pasirašytų XML dokumentų saugojimo ir judėjimo programinė įranga

Magistro darbas

Darbo vadovas
doc. dr. E. Karčiauskas

Kaunas, 2010

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

Ovidijus Petrulis

Pasirašytų XML dokumentų saugojimo ir judėjimo programinė įranga

Magistro darbas

Recenzentas
doc. dr. A. Barila
2010-05-27

Vadovas
doc. dr. E. Karčiauskas
2010-05-27

Atliko
IFN-8/3 gr. stud.
Ovidijus Petrulis
2010-05-25

Kaunas, 2010

SOFTWARE FOR SIGNED XML DOCUMENTS STORAGE AND MANAGEMENT

SUMMARY

Nowadays usual paper documents are being moved to electronic space. It became easier to manage, edit, store it and gave opportunity to access documents for more persons. In most of cases it‘s advantages but it also creates threat of unauthorized access of documents.

Problem examined by this work is ensuring consistency of data in databases. One of solutions could be use of database triggers to detect any change of data, but it can be turned off by sophisticated individual. Therefore, this solution does not meet the requirements.

The proposed solution to the problem: to create an additional database that contains the same data, but written in the form of signed XML documents. Whenever the data is entered into the original database, the copy of data is signed and stored into additional database: “Secure XML Archive” (“SXA”). Any changes of data stored in the original database can be found after comparison with data stored in SXA database. Likewise changes to data stored in SXA are observed after document signature verification.

The research goal was to find appropriate means to better meet the requirements for software. These means includes XML signature types and standards.

During the experiment, software was designed to support both XML digital signature standards: XMLDSig and XAdES. Calculations were performed with each of standards and turned out that XML signing is only about 10% slower with XAdES and it takes about 1.06KB more space compared with XMLDSig. After evaluation of XAdES functionality advantages was chosen XAdES-BES standard. It can be extended to XAdES-T on demand for long-term data storing.

Turinys

1. Įvadas

Dokumentus perkėlus į elektroninę erdvę, tapo lengviau juos valdyti, keisti, saugoti ir pasiekti didesniam skaičiui žmonių. Daugeliu atvejų tai privalumai, tačiau iškilo grėsmė, kad duomenys gali būti pakeisti neautorizuotų asmenų, kurie neturi teisės to daryti.

Duomenų saugojimas duomenų bazėse turi daug privalumų prieš tų pačių duomenų saugojimą failuose. Visų pirma atsiranda didesnės paieškos, duomenų filtravimo, duomenų agregavimo galimybės, paprastesnis duomenų kopijų darymas ir kt.

Duomenų bazės valdymo sistemos (DBVS) paprastai turi įrankių, vartotojų teisėms valdyti, tačiau tam tikra vartotojų dalis privalo turėti pilnas teises, norint sėkmingai administruoti ir daryti pakeitimus sistemoje, (pvz. IT skyrius). Taigi sistemoje yra bent viena vartotojų grupė, kurie gali daryti duomenų pakeitimus, niekam to nepastebėjus. O jeigu duomenys yra labai svarbūs ir privaloma užtikrinti, kad niekas negalėtų jų pakeisti po sukūrimo, o jei ir būtų pakeisti, tai tuos pakeitimus būtų galima pastebėti? Viena iš galimybių naudoti duomenų bazės trigerius (angl. trigger), tačiau jie lengvai gali būti išjungti prieš darant duomenų pakeitimus, todėl ši priemonė netenkina reikalavimų.

Siūlomas problemos sprendimo būdas: sukurti papildomą duomenų bazę, kurioje būtų saugomi tie patys duomenys, tačiau pasirašytų XML dokumentų pavidalu. Tokiu atveju esama sistema ir jos duomenų bazė nekeičiama, o šalia sukuriama papildoma DB, toliau vadinama SXA DB (Saugaus XML Archyvo DB) ir įdiegiama programinė įranga, skirta darbui su originalia sistemos DB ir naująja SXA DB.

Įdiegus pakeitimus esamoje sistemoje, viena duomenų kopija, kaip ir prieš pakeitimų įdiegimą, išsaugoma originalioje sistemos DB, o kita duomenų kopija pasirašoma vartotojo skaitmeniniu parašu ir išsaugoma SXA duomenų bazėje. Atlikus bet kokius pakeitimus originalioje duomenų bazėje, jie bus pastebėti sulyginus duomenis su saugomais SXA DB. Atlikus bet kokius pakeitimus SXA duomenų bazėje, jie taip pat bus pastebėti, kadangi patikrinus parašą bus pastebėta, kad jis neatitinka pasirašytų duomenų (parašas netikras).

Sukurta programinė įranga pritaikyta vienai sričiai: darbui su akademinės informacinės sistemos duomenimis.

Kadangi sukurta programinė įranga apima ne tik dokumentų pasirašymą ir išsaugojimą duomenų bazėse, tačiau ir dokumentų importą, eksportą, duomenų tarp duomenų bazių tapatumo kontrolę, duomenų sinchronizaciją, skirtingų dokumentų versijų saugojimą ir kt., todėl šiame darbe

nagrinėjamos dokumentų valdymo sistemos, jų teikiamos funkcijos, taip pat programinė įranga, skirta XML dokumentų pasirašymui ir parašų tikrinimui.

Iškeltam uždaviniui spręsti gali būti panaudotos skirtingos priemonės, t.y. skirtingi parašų tipai ir standartai. Tyrimo tikslas – išsiaiškinti kurios priemonės tinkamesnės ir geriau atitinka programinei įrangai keliamus reikalavimus.

2. Dokumentų valdymo sistemų ir XML duomenų tipo pasirašymo programinės įrangos analizė

2.1. Tyrimo sritis, objektas ir problema

Tyrimo sritis. Tyrimo sritį sudaro dokumentų valdymo sistemos, tokių sistemų teikiamos galimybės ir procesai, taip pat XML duomenų tipas ir XML pasirašymo skaitmeniniu parašu galimybės.

Tyrimo objektas. Tyrimo objektas – XML parašo standartai, struktūros tipai, jų pritaikymas pasirašytų XML dokumentų saugojimo ir judėjimo programinei įrangai realizuoti.

Problema. Duomenų nekintamumo užtikrinimas duomenų bazėse.

2.2. Dokumentų valdymo sistemos ir XML duomenų tipas

2.2.1. Dokumentų valdymo sistemos.

Verslo duomenų tvarkymui ir apskaitai vesti atsisakoma popierinių dokumentų, vietoj jų naudojami elektroniniai dokumentų variantai. Tai įtakoja tradicinį verslą, keičiasi įmonių struktūra, veiklos principai. Įmonėms būtina planuoti informacijos srautus, pertvarkyti informacijos technologijas, keisti gamybos ir paslaugų tiekimo būdus, taikyti naujus vadybos metodus ir rinkodaros priemones. Vystantis šiuolaikinėms technologijoms šalia tradicinio verslo, jau įsitvirtino elektroninis verslas, kuris darbuotojus, vartotojus, kompanijas apjungia ir įgalina tarpusavyje sąveikauti virtualioje erdvėje išlaikant pasitikėjimą ir konfidencialumą. Šiandien sėkmingai dirbančios kompanijos nuolat atlieka savo veiklos procesų analizę, siekdamos išsiaiškinti visas įmanomas veiklos racionalizavimo ir tobulinimo galimybes ir pasinaudoti jomis, įgyjant strateginį pranašumą prieš konkurentus. Tinkamas dokumentų valdymas – viena iš tokių galimybių. Iki šiol dokumentas buvo traktuojamas kaip duomenų struktūra ir visas dėmesys buvo nukreiptas duomenų saugojimui, ryšiams tarp jų, paieškai organizuoti. Nebuvo galima dokumento perduoti, koreguoti, keisti jo struktūros ir pan. Šiandien pasikeitė pats požiūris į dokumentų valdymą. Dokumentų valdyme kalbama jau ne apie dokumentų, bet apie informacijos valdymą. Tai labai svarbus akcentas, nes dokumento vertė ir yra jame esančioje informacijoje. Bet esmė yra tai, kad dėka dokumentų valdymo sistemos, informacija yra valdoma ir tvarkoma taip, kad padėtų žmonėms vykdyti jų veiklą, padėtų sėkmingiau vykti procesams ir sąveikoms, o ne tik būtų duomenų pertvarkymas.

Įstaigos raštvedybos organizavimo tikslai yra laiku ir kokybiškai parengti dokumentus, tvarkyti ir valdyti juos taip, kad galima būtų greitai jais pasinaudoti, užtikrinti skaidrią, efektyvią veiklą, administravimo ir atsiskaitymo gebėjimus. Visa svarbi veiklos informacija atsispindi dokumentuose. Kiekviena įstaiga dirba su didesniu ar mažesniu dokumentų srautu. Reikia organizuoti jų saugojimą, greitai surasti reikiamą dokumentą, užtikrinti jų rengimo ir atsakymo kontrolę, laiduoti dokumentų saugumą. Dažnai įmonės dokumentacijos tvarkymas atidedamas. Tačiau dokumentams besikaupiant tampa vis sudėtingiau atrasti reikiamą dokumentą, sugaištamas brangus laikas. Dokumentų valdymo sistemos pagalba įmonėje vykstantys procesai bei sąveikos yra vykdomi žymiai greičiau, kas neabejotinai mažina darbo laiko sąnaudas ir klaidų tikimybes. Taip pat dokumentų valdymo sistemos pagalba maksimizuojamas darbuotojų indėlis į įmonės valdymą, palengvinamas jų komunikavimas bei bendradarbiavimas, užtikrinamas veiksmų koordinavimas [1].

Terminas „document management" angliškoje literatūroje yra plačiai paplitęs. Lietuvių kalboje, kai kalbama apie dokumentus, naudojami žodžiai „valdymas" ir „tvarkymas". Daugelyje sričių „management" verčiamas kaip „valdymas". Dokumentų valdymo sistema (angl. document management system, DMS) skirta plačiam dokumentų tvarkymo spektrui – nuo jų paruošimo iki sunaikinimo. Tobulėjant šiuolaikinėmis technologijoms, vis daugiau įmonių atsisako įprasto įmonės administravimo ir pereina prie vadinamo „be popierinio" įmonės valdymo, kuris užtikrina efektyvesnį darbą, mažesnius administravimo kaštus bei mažina ar net visai panaikina geografinio įmonės darbuotojų išsidėstymo reikšmę. Dokumentų valdymo sistema (DVS), tai vartotojui orientuota sistema, jungianti dokumentus ir jų valdymo logiką, darbuotojų prieigos teises ir įmonės kontaktus bendroje sistemoje.

2.2.2. XML.

Dauguma sistemų naudoja skirtingų formatų duomenis, todėl atsiranda įvairių problemų ir sunkumų perduodant duomenis iš vienos sistemos į kitą. Šiai problemai spręsti reikia naudoti tokį duomenų struktūros aprašą, kurį suprastų visos sistemos – toks aprašas turėtų būti universalus. Šiuo metu labiausiai išvystytas ir plačiai naudojamas duomenų aprašymo standartas yra XML (eXtensible Markup Language). Dabartinė (antroji) XML versija 1.0 yra W3C (World Wide Web Consortium) pasiūlyta rekomendacija. XML gali būti panaudota tiek keistis duomenimis, tiek duomenims saugoti. XML dokumentai gali būti naudojami pačiose įvairiausiose srityse: elektroninėje

komercijoje, bendraujant su verslo partneriais ar organizacijos viduje integruojant programinę įrangą bei duomenų bazes [19].

Naudojant XML galima sukurti duomenų struktūras, kurios aprašo jose esančių duomenų turinį, neatsižvelgiant į tai, kaip turinys bus pavaizduotas. Nors XML griežtai specifikuoja sintaksę, tačiau leidžia laisvai apibrėžti XML dokumentų prasmę. XML leidžia susikurti savitą gramatiką arba naudotis jau sukurta gramatika, pavyzdžiui, tokia, kuri naudojama konkrečioje probleminėje srityje (pvz., prekyboje, matematikoje, chemijos pramonėje ir kt.). Gramatikai apibrėžti naudojami du formatai: XML schema arba dokumento tipo apibrėžtis – DTD. Dabartinis XML schemos standartas yra W3C pasiūlyta rekomendacija. W3C kuria standartus ir technologijas, kurios atitinka informacijos pateikimo internete keliamus reikalavimus [19].

XML schema aprašo XML dokumentų struktūrą. Ji nusako elementus, kurie gali būti naudojami XML dokumentuose. Jei XML dokumentas naudoja schemą, tai neaprašytų elementų negalima vartoti. Kitaip tariant, XML schema aprašo gramatiką, kurios laikydamiesi XML dokumentai yra teisingi. XML dokumentų tikrinimas reiškia, kad išoriniai duomenys turi laikytis taisyklių, kurios yra aprašytos XML schemoje. Schema užtikrina, kad XML dokumentas yra tokio formato, kokio tikimasi. XML schema yra galinga ir sudėtinga XML dokumentų struktūros kūrimo ir tos struktūros gramatikos patvirtinimo priemonė. XML schemos dokumentai aprašo konkretų XML dokumento tipą, nurodo apribojimus šio tipo dokumento duomenims, pateikia žymes ir atributus, naudojamus to tipo dokumentuose, sąryšius tarp šių XML dokumento elementų. XML schema, kaip ir XML dokumentas, yra hierarchinės medžio tipo struktūros. šakninis kiekvienos XML schemos elementas yra <schema>.

Vienas pagrindinių XML technologijos privalumų – tai galimybė konvertuoti XML duomenis iš vienos formos į kitą, naudojantis bendrinėmis priemonėmis. Technologija, kuri padeda tai atlikti, vadinama XSLT (angl. eXtensible Stylesheet Language for Transformations) – išplečiama stilių kalba transformacijoms. XSL stilių lentelė – tai transformavimo instrukcijų rinkinys, kuriomis išeitinis XML dokumentas verčiamas kitu dokumentu (nebūtinai XML). Norint atlikti XSLT transformacijas reikalingas XSLT procesorius, kuris transformuoja išeities XML dokumento duomenis, susiedamas juos su XSL stilių lentelės šablonais. Egzistuoja problema, kad XSLT procesoriai yra ganėtinai lėti, todėl kartais reikia griebtis įvairių priemonių norint generuoti dokumentus realiu laiku.

2.2.3. XML pasirašymas

Visų pirma skaitmeninis parašas – tai tam tikras kodas pridedamas prie dokumento, iš kurio nustatoma ar dokumentas buvo pakeistas po pasirašymo ar ne. Skaitmeniniam parašui realizuoti naudojama maišos funkcija ir asimetrinė kriptografija, t.y. du skirtingi raktai (privatus ir viešasis), iš kurių vienas naudojamas informacijos užšifravimui, o kitas – iššifravimui.

Labiausiai paplitęs RSA algoritmas. Jis naudojamas šioms funkcijoms realizuoti:

1. Šifravimas/ iššifravimas
2. Skaitmeninis parašas
3. Raktų apsikeitimas

Šifravimas bendruoju atveju susideda iš trijų pagrindinių dalių: raktų generavimo, šifravimo, iššifravimo.

Raktų generavimo schema:

1. Sugeneruojami du pirminiai skaičiai p ir q;
2. Apskaičiuojama sandauga: $n = pq$ ir $\varphi(n) = (p-1)(q-1)$;
3. Atsitiktinai pasirenkamas toks skaičius e ($1 < e < \varphi(n)$), su kuriuo $(e, \varphi) = 1$ (tarpusavyje pirminiai);
4. Suskaičiuojamas d: $d = e^{-1} \bmod \varphi(n)$;
5. Viešasis raktas VR = (n, e)
6. Privatusis raktas PR = d.

Siuntėjas ir gavėjas privalo žinoti reikšmę n. Siuntėjas norėdamas užšifruoti tekstą, taip pat turi žinoti ir reikšmę e, o gavėjas – reikšmę d. Taigi viešasis raktas KU={e, n}, o privatus raktas KR={d, n}. Informacijos šifravimui gali būti naudojamas arba viešasis arba privatus raktas (priklausomai nuo siekiamo tikslo) tuomet dešifravimui bus naudojamas priešingas raktas, nei buvo panaudotas užšifravime.

Jei norima užtikrinti konfidencialumą, informacija šifruojama gavėjo viešuoju raktu. Informaciją dešifruoti galės tik gavėjas, nes jis vienintelis turi privatų raktą.

Šifravimas:

Jei turimas teksto blokas M, tuomet šifruoto teksto blokas C gaunamas:

$C = M^e \bmod n$

Iššifravimas

Iššifruoto teksto M gavimas, turint šifruotą pranešimą C ir privatų raktą d

$M = C^d \bmod n$

Skaitmeninis parašas.

Jei norima užtikrinti siuntėjo autentiškumą ir siunčiamų duomenų vientisumą, naudojamas skaitmeninis (elektroninis) parašas. Tokiu atveju teksto santrauka šifruojama siuntėjo privačiu raktu – gaunamas skaitmeninis parašas. Skaitmeninis parašas pridedamas prie siunčiamos informacijos, ir norint patikrinti ar tekstas nebuvo pakeistas po pasirašymo, reikia:

- ✓ Naudojant tą patį maišos algoritmą, kurį naudojo siuntėjas suskaičiuoti teksto santrauką
- ✓ Iššifruoti siuntėjo atsiųstą parašą (užšifruotą teksto santrauką) su siuntėjo viešuoju raktu
- ✓ Palyginti suskaičiuotą santrauką su dešifruota. Jei santraukos sutampa – vadinasi parašas tikras, ir tai reiškia kad informacija po pasirašymo nebuvo pakeista ir siuntėjas yra tas asmuo, kuriuo dedasi.

Patikrinti siuntėjo skaitmeninį parašą gali visi, turintys siuntėjo viešąjį raktą. Tačiau pasirašyti gali tik siuntėjas (privataus rakto savininkas).

Raktų apsikeitimas.

Asimetrinėje kriptografijoje naudojami ilgesni raktai nei simetrinėje (kai šifravimui ir dešifravimui naudojamas tas pats raktas) ir simetrinio šifravimo algoritmai dirba žymiai greičiau už asimetrinius. Todėl didesnės apimties duomenų šifravimui paprastai naudojama simetrinė kriptografija, o norint pasikeisti simetriniais raktais, gali būtu naudojamas RSA algoritmas [2].
Siuntėjas užšifruoja simetrinį raktą gavėjo viešuoju raktu. Tokiu atveju pranešimą iššifruoti galės tik gavėjas (privataus rakto savininkas).

Maišos funkcija.

Norimam informacijos fragmentui pasirašyti suskaičiuojama maišos funkcija (santrauka), tam paprastai naudojamas SHA1, MD5 ar MD4 algoritmas. Maišos funkcija priima kintamo dydžio pranešimą *M* ir suskaičiuoja fiksuoto dydžio maišos kodą H(*M*), kartais dar vadinamą pranešimo santrauka. Maišos kodas yra visų pranešimo bitų funkcija. Kelių bitų pasikeitimas pranešime

pakeičia maišos kodą. Maišos funkcijos rezultatas - gaunama fiksuoto ilgio santraukos reikšmė (pvz. 160, 256, 384 ar 512 bitų ilgio seka), nepriklausomai nuo įeinančių duomenų apimties.

Maišos funkcijos reikšmė šifruojama pasinaudojant siuntėjo privačiu raktu – gaunamas skaitmeninis parašas. Norint gavėjui patikrinti ar gauta informacija nebuvo pakeista po pasirašymo, jis turi turėti siuntėjo viešąjį raktą. Užtikrinimui, kad paskelbtas viešasis raktas tikrai priklauso konkrečiam asmeniui, pasitelkiama trečioji patikima šalis (angl. *third trusted party – TTP*) - sertifikavimo centras (SC), kuris išduoda skaitmeninį sertifikatą.

Sertifikavimo centro atliekamos funkcijos [3]:

- ✓ Sugeneruoti asimetrinių raktų poras (PR, VR) vartotojams (nebūtina funkcija);
- ✓ Registruoti asmenis, prašančius sudaryti sertifikatus, patikrinti jų identifikacinius ir kitus dokumentus, kurių reikia sertifikatui sudaryti;
- ✓ Sudaryti sertifikatus;
- ✓ Tvarkyti sertifikatų duomenis;
- ✓ Laiku stabdyti arba nutraukti sertifikatų galiojimą, gavus atitinkamą prašymą;
- ✓ Teikti nebegaliojančių sertifikatų duomenis parašo naudotojams anksčiau sukurtiems parašams tikrinti;
- ✓ Atlikti kitas teisės aktų nustatytas funkcijas.

Skaitmeniniame sertifikate saugoma informacija:

- ✓ Vartotojo (sertifikato savininko) vardas
- ✓ Vartotojo viešasis raktas, atitinkantis jo turimą privatųjį raktą;
- ✓ Sertifikato galiojimo pradžios ir pabaigos terminai;
- ✓ Sertifikatą sudariusio SC ir jo buveinės bei šalies identifikatoriai;
- ✓ Sertifikato, kurį suteikia SC identifikatorius;
- ✓ Sertifikato naudojimo paskirtis;
- ✓ Sertifikavimo centro (SC) e. parašas

Sertifikatų centras, išduodamas sertifikatą, pasirašo jį su savo privačiu raktu. Gavėjas, priėmęs pasirašytą informaciją, priklausomai nuo to, ar sertifikavimo centras, siuntėjui išdavęs sertifikatą įtrauktas į patikimų sąrašą gavėjo sistemoje, pasitiki siuntėjo sertifikatu arba ne.

XML parašas (XML parašo standartai: XMLDSig, XADES) – yra W3C rekomendacija, nusakanti XML parašų sintaksę. XML parašų teikiamos paslaugos [4]:

- ✓ Informacijos integralumas (vientisumas)
- ✓ Pasirašytos informacijos autentifikacija
- ✓ Pasirašiusiojo autentifikacija

Šios paslaugos suteikiamos bet kokiam duomenų tipui, esančiam tame pačiame XML dokumente kur yra parašas, arba už jo ribų [4].

XML Parašas gali būtu trijų tipų [4]:

1. Atskirtas (angl. detached) – parašas naudojamas pasirašyti informaciją, esančią ne tame pačiame XML dokumente, kur yra parašas.
2. Įtrauktas (angl. enveloped) – parašas naudojamas pasirašyti dalį to XML dokumento, kuriame yra pats parašas. Parašas integruojamas į esančius XML duomenis.
3. Gaubiantis (angl. enveloping) – toks parašas, kai parašas savyje turi visus pasirašytus duomenis

Atskirtas (angl. detached) XML parašas.

XML failo, kuriame naudojamas atskirtas parašas struktūra[4]:

```
[s01] <Signature Id="MyFirstSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
[s02]   <SignedInfo>
[s03]   <CanonicalizationMethod Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
[s04]   <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
[s05]   <Reference URI="http://www.w3.org/TR/2000/REC-xhtml1-20000126/">
[s06]     <Transforms>
[s07]       <Transform Algorithm="http://www.w3.org/2006/12/xml-c14n11"/>
[s08]     </Transforms>
[s09]     <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
[s10]     <DigestValue>dGhpcyBpcyBub3QgYSBzaWduYXR1cmUK.../DigestValue>
[s11]   </Reference>
[s12] </SignedInfo>
[s13]   <SignatureValue>...</SignatureValue>
[s14]   <KeyInfo>
[s15a]    <KeyValue>
[s15b]      <DSAKeyValue>
[s15c]        <P>...</P><Q>...</Q><G>...</G><Y>...</Y>
[s15d]      </DSAKeyValue>
[s15e]    </KeyValue>
[s16]   </KeyInfo>
[s17] </Signature>
```

[s02-12] Elementas < SignedInfo > nusako informaciją, kuri yra pasirašyta. Algoritmai, naudojami apskaičiuojant < SignatureValue > yra įtraukiami į pasirašytą informaciją, tuo tarpu pats <SignatureValue > elementas yra už < SignedInfo > ribų.

[s03] Elementas < CanonicalizationMethod > aprašo algoritmą, kuris naudojamas kanonizuoti (angl. „canonicalize“) elementui < SignedInfo > prieš apskaičiuojant santrauką (reikalingą parašui formuoti).

[s04] Elementas < SignatureMethod > nusako algoritmą, kuris naudojamas < SignedInfo > esančiai informacijai transformuoti į < SignatureValue > elemente saugomą informaciją, t.y. šiame elemente nusakoma maišos algoritmo ir raktų generavimo algoritmo kombinacija, pvz. „RSA-SHA1“. Algoritmų pavadinimai yra pasirašomi, norint išvengti galimų atakų prieš „silpnesnius“ algoritmus.

[s05-11] < Reference > elementas aprašo sritį (objektą), kuri turi būti pasirašyta. Naudojant šį elementą, tikrinamas parašas.

[s14-16] < KeyInfo > elementas nusako raktą, kuris naudojamas parašo teisingumo patikrinimui. Šis elementas yra neprivalomas (jo gali ir nebūti) dėl tokių priežasčių: pasirašęs asmuo gali nenorėti atskleisti informacijos apie raktą visoms dokumentą naudojančioms šalims ar informacija gali būti žinoma tik programinei įrangai, ir nereikia jos rodyti atvirai.
Šis elementas < KeyInfo > yra už < SignedInfo > srities ribų, todėl, jei norima pasirašyti ir šį elementą, reiktų tai nurodyti < Reference > elemente.

Įtrauktas (angl. enveloped) XML parašas [5]
Šio XML parašo tipo pagrindinis skirtumas nuo Atskirto (angl. detached) XML parašo yra tai kad pasirašoma informacija yra tame pačiame dokumente kaip ir XML parašas, ir parašas įtraukiamas į dokumento turinį.

Jei turimas XML dokumentas:

```
<Envelope xmlns="urn:envelope">
</Envelope>
```

Tuomet parašas bus įterpiamas į pačio dokumento struktūrą:

```
<Envelope xmlns="urn:envelope">
<Signature> … </Signature>
</Envelope>
```

XML failo, kuriame naudojamas įtrauktas (angl. enveloped) parašas, struktūra[5]:

```
<Envelope xmlns="urn:envelope">
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod
           Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>uooqbWYa5VCqcJCbuymBKqm17vY=</DigestValue>
      </Reference>
    </SignedInfo>
<SignatureValue>
KedJuTob5gtvYx9qM3k3gm7kbLBwVbEQRl26S2tmXjqNND7MRGtoew==
    </SignatureValue>
    <KeyInfo>
      <KeyValue>
        <DSAKeyValue>
          <P>
/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTxe
Eu0ImbzRMqzVDZkVG9xD7nN1kuFw==
          </P>
          <Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>
          <G>Z4RxsnqC9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/
XPaF5Bpsy4pNWMOHCBiNU0NogpsQW5QvnlMpA==
          </G>
          <Y>qV38IqrWJG0V/
mZQvRVi1OHw9Zj84nDC4jO8P0axi1gb6d+475yhMjSc/
BrIVC58W3ydbkK+Ri4OKbaRZlYeRA==
         </Y>
        </DSAKeyValue>
      </KeyValue>
    </KeyInfo>
  </Signature>
</Envelope>
```

Gaubiantis (angl. enveloping) XML parašas [6]

Šis XML parašo tipas panašus į įtrauktą (angl. enveloped) parašą. Pagrindinis skirtumas, kad priešingai nei turint įtrauktą (angl. enveloped) parašą, visa informacija šiuo atveju „apvelkama“ <Signature > </Signature > elementu, o informacija, kuri turi būti pasirašoma (Objekto ID), nurodoma <Reference> elemente:

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
```

```
<Reference URI="#_18958953">
</Reference>
</SignedInfo>
<SignatureValue>
KedJuTob5gtvYx9qM3k3gm7kbLBwVbEQRl26S2tmXjqNND7MRGtoew==
</SignatureValue>
…
<Object Id="_18958953" MimeType="text/xml">
<Object>
</Signature>
```

XML parašo tikrinimas:

XML parašo tikrinimo metu, skaičiuojama <Reference> elementuose nurodytų objektų santraukos funkcijos (pagal <DigestMethod> elemente nurodytą santraukos funkcijos algoritmą), ir jos lyginamos su <Reference> elementuose saugomomis <DigestValue> reikšmėmis.

Papildoma XML parašo galimybė [9]:

Svarbi XML parašo savybė – galimybė saugoti keletą skaitmeninių parašų viename XML dokumente. Tai leidžia daugeliui vartotojų pasirašyti tą patį XML dokumentą. Kiekvieną kartą pasirašant dokumentą, ankstesni parašai gali būti įtraukiami į naująjį parašą.

2.2.4. XMLDSig standarto ypatumai.

Dėl XML specifikos, duomenis, skirtus pasirašyti, privaloma versti kanoniniu pavidalu, tam kad būtų gautas kuo paprastesnis ir nuo situacijos nepriklausantis pavidalas. [14]

Duomenys, santraukos apskaičiavimui turi būti tokie pat ir pasirašant ir kiekvieną kartą tikrinant parašą. Tam gali reikti atmesti įtraukto parašo reikšmę, XML kode esančius komentarus, suvienodinti kodo stilių, pritaikyti to paties tipo eilučių pabaigos simbolius, kodų lentelę ir t.t. [14]

Bazinė XMLDSig parašo struktūra [15]:

```
<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI? >
      (<Transforms>)?
      <DigestMethod>
      <DigestValue>
    </Reference>)+
  </SignedInfo>
  <SignatureValue>
```

(<KeyInfo>)?
(<Object ID?>)*
</Signature>

Kur simboliai: „*“, „?“ reiškia elemento kartojimąsi:
„?“ - nulį arba vieną kartą,
„*“ - nulį arba daugiau kartų.

Reiktų pastebėti, kad dokumentas nepasirašomas įprastu būdu, skaičiuojant dokumento turinio santrauką ir apdorojant parašo algoritmu, o pasirašomas XML kodas - „SignedInfo“ turinys, susijęs tik su pasirašomo dokumento turiniu. Tam taikomas sprendimas: iš pradžių sukuriamas „SignedInfo“ elementas, kurioje Reference elementais išvardijami dokumentai bei jų turinio santraukos, o paskui visa „SignedInfo“ apdorojama santraukos algoritmu, pasirašoma ir parašo reikšmė patenka į „SignatureValue“ elementą.[14]

Parašo tikrinimas vadinamas „core validation“. Jį sudaro 2 etapai: nuorodos tikrinimas (dokumentų santraukų tikrinimas) ir parašo tikrinimas (SignatureValue reikšmės tikrinimas).
Nuorodos tikrinimo etapai:

1. Pasirašytų duomenų išgavimas
2. Santraukos apskaičiavimas nurodytu metodu
3. Gautos santraukos palyginimas su su pasirašytos informacijos nuorodoje esančia santrauka

Parašo tikrinimo etapai:

1. Imama rakto informacija iš rakto informacijos elemento „KeyInfo“ arba iš išorinio šaltinio.
2. Pagal nurodytą metodą, apskaičiuojamas pasirašytos informacijos elemento kanoninis pavidalas, kuris kartu su rakto informacija naudojamas parašo reikšmei patikrinti.

Parašui tikrinti būtinas viešasis raktas, jis gali būti saugomas elemente „KeyInfo“ arba šio elemento gali nebūti (pasirinktinai).
„KeyInfo“ elemente saugomi raktai (išskaidytuose elementuose). Jei naudojamas RSA algoritmas, tuomet KeyInfo Elementas atrodo šitaip:

<KeyInfo>
<KeyValue>
<RSAKeyValue>

```
                    <Modulus>e6g4wertg...</Modulus>
                    <Exponent>fahger46qer...</Exponent>
                </RSAKeyValue>
            </KeyValue>
            <X509Certificate>uhJGsfg356weqr...</X509Certificate>
</KeyInfo>
```

Elemente „RSAKeyValue“ matomi askiri RSA algoritmo parametrai:

„Modulus“ – n *(RSA plačiau aprašomas analizės dalyje)*

„Exponent“ – e *(RSA plačiau aprašomas analizės dalyje)*

Elemente „X509Certificate“ gali būti saugomas visas X509 standarto sertifikatas ASN.1 DER formatu. Šis elementas neprivalomas.

Elementas „Object“ neprivalomas, jis paprastai naudojamas gaubiančio parašo atveju, kai visa informacija „apvelkama“ „Signature“ elementu. Tuomet „object“ elemente saugoma pats dokumento turinys. Galimi ir kiti „object“ elemento panaudojimo atvejai – tačiau jie nėra apibrėžti standarte.

2.2.5. XAdES standarto ypatumai.

XAdES iš esmės yra praplėstas XMLDSig standartas. Pagal teikiamas funkcijas, XadES skirstomas į sekančias formas (eiliškumas: nuo mažiausiai funkcijų turinčios formos XAdES, iki daugiausiai funkcijų turinčios XAdES-A):

XAdES
XAdES - T
XAdES - C
XAdES - X
XAdES – X - L
XAdES - A

Bazinėje XAdES formje, lyginant su XMLDSig standartu, išplečiamas „Object“ elementas, jame atsiranda elementai [16]:

```
<QualifyingProperties>
  <SignedProperties>
    <SignedSignatureProperties>
     (SigningTime)
```

```
      (SigningCertificate)
      (SignaturePolicyIdentifier)
      (SignatureProductionPlace)?
      (SignerRole)?
     </SignedSignatureProperties>
     <SignedDataObjectProperties>
      (DataObjectFormat)*
      (CommitmentTypeIndication)*
      (AllDataObjectsTimeStamp)*
      (IndividualDataObjectsTimeStamp)*
     </SignedDataObjectProperties>
    </SignedProperties>
    <UnsignedProperties>
     <UnsignedSignatureProperties>
      (CounterSignature)*
     </UnsignedSignatureProperties>
    </UnsignedProperties>
   </QualifyingProperties>
```

Kur simboliai: „*“, „?“ reiškia elemento kartojimąsi:

„?“ - nulį arba vieną kartą,

„*“ - nulį arba daugiau kartų.

Bazinė XAdES forma užtikrina autentifikaciją ir vientisumą.

Pagrindinių elementų aprašymai:

SigningTime - Pasirašymo laikas pagal kompiuterio sisteminį laikrodį (atitinkantis ISO 8601 formatą)

SigningCertificate - Pasirašant naudotas sertifikatas. Reiktų pastebėti, kad sertifikatas yra tarp pasirašomų elementų, kad jo nebūtų galima pakeisti kitu sertifikatu su tais pačiais raktais, tačiau kitokia sertifikato informacija (savininko vardu, pavarde ir kt.).

SignaturePolicyIdentifier – parašo politika, nurodoma tiek žmogui skaitomu tekstu, tiek programai suprantamu identifikatoriumi.

SignatureProductionPlace – Pasirašančiojo buvimo vieta pasirašymo metu. T.y. adresas, kur atskirais elementais galima nurodyti valstybe, miestą, pašto kodą ir pan.

SignerRole – Pasirašančiojo vaidmuo juridiniu atžvilgiu, pvz. pareigos

DataObjectFormat – aprašomas dokumento formatas (pavadinimu, standartu ar pan.)

CommitmentTypeIndication – Įsipareigojimas, susijęs su parašo sukūrimo tikslu

AllDataObjectsTimeStamp, IndividualDataObjectsTimeStamp – laiko žyma, įrodanti pasirašomo turinio egzistavimą tam tikru laiko momentu.
CounterSignature – saugomi parašai, kurie galioja tik kartu su pagrindiniu parašu. T.y. saugomas visas hierarchinis parašų medis, o ryšiai tarp parašų realizuojami žymų ir atributų reikšmėmis.

XAdES – T prideda laiko žymą, kad išvengti parašo išsiginamumo. Ji patvirtina, kad parašas egzistavo prieš joje nurodytą laiką. Jei tuo metu pasirašančiojo sertifikatas galiojo ir nebuvo atšauktas, parašą galima laikyti galiojančiu net tuomet, kai šios dvi sąlygos nebetenkinamos. Šią paslaugą realizuoja laiko žymos serveris, kuriam nusiunčiama apskaičiuota duomenų santrauka. Tarp atsakymo duomenų bus parašu apsaugotos santraukos kopija ir laiko reikšmė.

Lyginant su bazine XAdES forma, atsiranda elementas:

```
(SignatureTimeStamp)
```

XAdES – C pridedamos parašo nuorodos į duomenis, kurios palengvina parašo tikrinimą. Ši forma taikoma tuomet, kai duomenis archyvuoja VRI (angl. „PKI“) paslaugų tiekėjas. Forma reikalinga vėlesnio tikrinimo procedūrai, kurią reglamentuoja ETSI standartas. Standartas išskiria pradinį ir vėlesnį tikrinimą. Pradinio tikrinimo atveju surenkami ir išsaugomi duomenys, reikalingi ilgalaikiam parašo galiojimui. Tai daroma vienintelį kartą, iš kart po parašo sukūrimo. Vėlesnis tikrinimas – tai įprastinis xml parašo tikrinimas įprastu būdu, atliekamas neribotą skaičių kartų. Procesą palengvina pradinio patikrinimo metu surinkti duomenys.

Lyginant su XAdES - T forma, atsiranda elementai:

```
(CompleteCertificateRefs)
(CompleteRevocationRefs)
```

XAdES – X pridedama laiko žyma, apsauganti nuorodas į parašo tikrinimo duomenis, o jei reikia ir „Signature“ elementą.

Lyginant su XAdES - C forma, atsiranda elementai:

```
(SigAndRefsTimeStamp)
(RefsOnlyTimeStamp)
```

XAdES – X - L prideda parašo tikrinimo duomenis. Kitaip nei XAdES – C formoje, saugomos ne nuorodos į duomenis, bet patys duomenys. Tai praverčia tokiais atvejais, kai negalima pasinaudoti VRI paslaugų tiekėjo archyvais.

Lyginant su XAdES - X forma, atsiranda elementai:

```
(CertificatesValues)
(RevocationValues)
```

XAdES – A prideda papildomas laiko žymas, apsaugančias parašus nuo kriptografinių duomenų susilpnėjimo. Pvz. jei pažeidžiamas algoritmas, būtų užtikrinama, kad pasirašymo metu jis dar buvo tinkamas naudoti.

Lyginant su XAdES – X - L forma, atsiranda elementai:

```
(ArchiveTimeStamp)
```

Kiekvienam „ArchiveTimeStamp“ elementui reikalinga santrauka, kuri apskaičiuojam iš visos XAdES – X – L formos.

2.3. Panašių sistemų (Lietuvos ir tarptautiniu mastu) analizė.

Šios analizės tikslas išnagrinėti šiuo metu egzistuojančias sistemas, bent dalinai galinčias išspręsti šiame darbe iškeltus uždavinius. Pagal iškeltą darbo tikslą (sukurti dokumentų valdymo sistemą, kuri būtų pritaikyta XML duomenų tipo pasirašymui ir apdorojimui) tiriamos egzistuojančios sistemos išskaidytos į du tipus:

1. Universalios dokumentų valdymo sistemos – apimančios įvairių dokumentų tipų valdymą organizacijose, kuriose reikia apriboti dokumentų pasiekiamumą tam tikriems asmenims, arba priešingai – dokumentai turi būti pasiekiami visiems; reikia pasiekti visus dokumentus

iš bet kurios vietos, naudojant tik interneto naršyklę; ar esant kitokiems dokumentų valdymo poreikiams. Kadangi tolimesniame tyrime bus nagrinėjamas tik XML duomenų tipas, todėl universalios dokumentų valdymo sistemos (DVS) apžvelgiamos tik bendru aspektu, norint išnagrinėti ir palygint tarpusavyje jų galimybes – tai nulems tikslesnį būsimos sistemos vaizdą.

2. XML duomenų tipo pasirašymo programinė įranga – programos pritaikytos darbui su XML duomenų tipu ir teikiančios galimybę pasirašyti šį duomenų tipą, naudojant skaitmeninį (elektroninį) parašą.

2.3.1. Universalios dokumentų valdymo sistemos.

2.3.1.1. STATISTICA, StatSoft

STATISTICA dokumentų valdymo sistemos paketo savybės [10]:

- ✓ Labai paprasta ir lengvai naudojama
- ✓ Lanksti, pagal vartotojo poreikius pritaikoma vartotojo sąsaja
- ✓ Elektroniniai parašai
- ✓ Išsamus sistemos auditas
- ✓ Optimizuota paieška
- ✓ Dokumentų palyginimo įrankiai
- ✓ Apsauga
- ✓ Atitinka FDA 21 CFR Part 11 reikalavimus
- ✓ Atitinka ISO 9000 (9001, 14001) dokumentacijos reikalavimus
- ✓ Atvira architektūra ir suderinamumas su rinkos standartais

STATISTICA dokumentų valdymo sistema skirta įvairaus dydžio organizacijoms. Pagal poreikius, skiriamos dvi STATISTICA versijos: „Enterprise“ ir „Entry Level“. Pirmoji skirta didelėms organizacijoms, o antroji rekomenduojama ten kur numatoma 5 – 10 vienu metu su sistema dirbančių asmenų.

Sistemoje vartotojai autentifikuojami ir autorizuojami (pagal nustatytas vartotojų grupes). Dokumentai saugojami duomenų bazėse. Naudojama Microsoft SQL Server, tačiau galima prisijungti ir naudoti kitas jau egzistuojančias organizacijoje duomenų bazes. Sistema dokumentus gali automatiškai saugoti dviem formatais: pdf (peržiūrai) ir originaliu failo formatu (redagavimui).

Sistemoje gali būti naudojamas elektroninis parašas, kuris papildomai identifikuoja dokumento savininką. Kiekvieną kartą užsaugant pakeistą dokumentą, sukuriama nauja dokumento versija, o senesnės versijos taip pat išsaugomos. Išsaugant dokumentą, kartu išsaugomi ir reikalingi metaduomenys. Dokumentas gali būti užrakintas, kad niekas negalėtų sukurti naujos dokumento versijos. Galimi įvairūs sistemos nustatymai, pvz. prieš įkeliant tam tikrus dokumentus jie privalo būti pasirašyti ar pan.

2.3.1.2. „doQuments“ , Softonic [11, 12]

Yra 3 galimos programinės įrangos versijos: „Standard“, „Professional“, „Enterprise“, pasirenkama priklausomai nuo organizacijos dydžio ir poreikių.

doQuments programinio paketo savybės:

- ✓ Centralizuotas dokumentų saugojimas, valdymas, paieška
- ✓ Platus dokumentų formatų palaikymas (nuskanuoti dokumentai, Microsoft Office™ dokumentai, vaizdo rinkmenos ir t.t.
- ✓ Kelių tipų dokumentų išsaugojimas viename įraše
- ✓ Metaduomenų apie dokumentą saugojimas
- ✓ Indeksuojant dokumentus, vartotojas gali užpildyti ne tik sistemos nustatytus metaduomenų įrašus, bet ir susikurti naujus. Pvz.: vartotojui reikia išsaugoti informaciją apie tai, kas ir kodėl pakeista dokumente. Vartotojas susikuria naują metaduomenų įrašą Keitimai, ir jame išsaugo reikalingą informaciją.

2.3.1.3. „DocLogix 2009“ , [13, 12]

UAB "DocLogix" sukurta dokumentų valdymo sistema „DocLogix 2009“ turi tokias funkcijas bei savybes [13, 12]:

- ✓ Vartotojo sąsajai naudojama interneto naršyklė
- ✓ Dokumentų ir įrašų valdymas
- ✓ Vartotojų grupių bendradarbiavimas
- ✓ Informacijos paieška
- ✓ Standartinės ataskaitos
- ✓ Organizacijos bei asmenų kontaktinių duomenų tvarkymas
- ✓ Sistemos administravimas

- ✓ Procesų valdymas
- ✓ Intuityvi vartotojo sąsaja
- ✓ Dokumentų registracija
- ✓ Naujo dokumento kūrimo vedlys
- ✓ Duomenų tikrinimas
- ✓ Versijų kontrolė
- ✓ Specializuoti klasifikatoriai (Custom classifiers)
- ✓ Skenavimas
- ✓ Sinchronizuojamas dokumentų skenavimas ir konvertavimas į PDF formatą
- ✓ PDF konverteris
- ✓ Pranešimai
- ✓ Duomenų filtravimo sistema
- ✓ El. laiškų ir jų priedų valdymas
- ✓ Integracija su Windows Explorer
- ✓ Sistemos modulių ir jų turinio valdymas
- ✓ Dienos paveikslėlis

Vartotojas tiesiai DocLogix sistemoje gali pasirašyti dokumentus elektroniniu parašu, juos išsiųsti elektroniniu paštu, patikrinti gautų dokumentų elektroninių parašų galiojimą.
DocLogix – vienintelė sistema [13], įgalinanti naudotis ir atpažinti bet kurios Europos Sąjungos šalies elektroninio parašo formatus.

2.3.2. XML duomenų tipo pasirašymo programinė įranga.

2.3.2.1. 602XML Filler, „Software602“

Tai nemokama kompanijos „Software602“ programinė įranga, skirta elektroninių formų pildymui. Programinės įrangos palaikomi failų formatai: .fo, .xml, .zfo. Failų formatai fo, zfo gali būti eksportuoti pdf formatu ar išsiųsti elektroniniu paštu.
Pagrindinė šios programos funkcija – minėtų failų formatų pasirašymas elektroniniu parašu. Tačiau norint tai padaryti reikia turėti viešojo rakto sertifikatą (programoje nėra numatytos sertifikatų kūrimo funkcijos). Yra galimybė patikrinti ar pasirašyto XML dokumento parašas tikras.
Programos trūkumas – programos aplinkoje negalima pildyti XML formato bylų (XML leidžiama tik pasirašyti).

XML pasirašymas:

1. Sukuriamas XML failas:

```
<?xml version="1.0"?>
<konfiguracija>
</konfiguracija>
```

2. Pasirašytas XML failas:

```
<?xml version="1.0"?>
<dsig:Signature Id="_52908198" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
<dsig:SignedInfo>
<dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/><dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1"/><dsig:Reference URI="#_52908203"><dsig:Transforms><dsig:Transform
Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</dsig:Transforms><dsig:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>0cJN/DBzv/PoDby8dEb+ecapRX8=</dsig:DigestValue>
</dsig:Reference></dsig:SignedInfo><dsig:SignatureValue> ...
</dsig:SignatureValue>
<dsig:KeyInfo><dsig:X509Data>
<dsig:X509Certificate> ... </dsig:X509Certificate>
</dsig:X509Data></dsig:KeyInfo>
<dsig:Object Id="_52908203" MimeType="text/xml">
<konfiguracija></konfiguracija>
<dsig:SignatureProperties><dsig:SignatureProperty
Target="#_52908198"><fm:systeminfo datetime="2009-01-20T21:58:43Z"
xmlns:fm="http://software602.cz/forms"/>
</dsig:SignatureProperty></dsig:SignatureProperties>
</dsig:Object>
</dsig:Signature>
```

Kaip matome iš pasirašyto XML dokumento, visa informacija yra elemento < Signature > viduje, ir pasirašomas objektas, kurio ID=52908203. Taigi pasirašymui į XML, naudojamas gaubiantis (angl. enveloping) XML parašas.

Ši programinė įranga palaiko „daugybinį pasirašymą“ t.y. viename XML dokumente gali būti pasirašoma ne vieną kartą (visais pasirašymo atvejais gali būti pasirašoma naudojant tą patį viešojo rakto sertifikatą, arba skirtingus).

Pasirašymui naudojamas XMLDSig standartas, papildomai <Object> elemente saugoma pasirašymo data ir laikas (lokalaus kompiuterio). XAdES standartas nepalaikomas.

2.3.2.2. XML Signer, „Secure Soft“ [7]

Internetu pasiekiama tik demonstracinė programos „XML Signer“ versija. Pagrindinė programos funkcija XML dokumentų pasirašymas, naudojant X.509 sertifikatus. Programos privalumas –

galimybė pasirašyti neribotą skaičių XML dokumentų, vienu pasirinkimu (nurodant XML failų direktoriją). Pasirašymui reikalingas viešojo rakto sertifikatas (programoje tokio sertifikato generavimas nenumatytas, tačiau kompanijos internetiniame puslapyje užsiregistravus išduodamas sertifikatas). Pasirinkus XML failų, kuriuos reikia pasirašyti direktoriją, visi failai pasirašomi ir išsaugomi su „signed“ antrašte.

Programinė įranga suteikia galimybę tikrinti parašą.

XML pasirašymas:

1. Sukuriamas XML failas:

```
<?xml version="1.0"?>
<konfiguracija>
</konfiguracija>
```

2. Pasirašytas XML failas:

```
<?xml version="1.0"?>
<konfiguracija>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference Id="2009.01.21 00:23:02" URI="" Type="This is a demo version">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
</Transforms><DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>IvlktNzKsdiDW86wlEEwuSn26xk=</DigestValue></Reference>
</SignedInfo><SignatureValue>...</X509Certificate></X509Data>
</KeyInfo>
</Signature>
</konfiguracija>
```

Kaip matome iš pasirašyto XML dokumento, suformuotas parašas yra integruotas į dokumento informaciją, taigi pasirašymui į XML, programa „XML Signer“ naudoja įtrauktą (angl. enveloped) – XML parašą.

Parašas atitinka XMLDSig standartą, XAdES išplėtimas nepalaikomas.

2.3.2.3. Microsoft InfoPath [8]

InfoPath® - tai Microsoft Office sistemos programa, kuri gali padėti lanksčiai ir efektyviai rinkti informaciją įvairiomis, dinamiškomis formomis. Kaip teigia produktą sukūrusi kompanija, galima žymiai efektyviau bendrai naudotis informacija su savo komandos nariais arba organizacijos

darbuotojais, ją pakartotinai naudoti bei tikslingai pritaikyti gerinant verslo sprendimų priėmimą ir bendradarbiavimą.

Surinkta informacija gali būti integruota į daugelį verslo procesų, nes InfoPath® palaiko bet kokią kliento nustatytą XML schemą bei gali būti integruota į tinklapio paslaugas. Tokiu būdu InfoPath® gali padėti įmonės darbuotojams tiesiogiai prieiti prie organizacijos informacinės sistemos ir naudotis ja, taip plėtojant verslą.

Programa pritaikyta formų (saugomų .xsn formatu) pildymui. Užpildytos formos duomenys saugomi XML formatu.

Galimas ir atvirkštinis būdas: generuoti formą pagal XML failo turinį arba XML schemą (.xsd formato failą). Tokiu būdu elementai iš XML dokumento „tempimo“ (angl. „drag and drop“) principu tiesiog išdėstomi formoje, ir atsidarius formą „pildymo režimu“ šie laukai pildomi, o jų turinys saugomas XML dokumente.

Yra galimybė pasirašyti XML dokumentą. Pasirašymui naudojamas įtrauktas (angl. enveloped) XML parašas. Taip pat yra galimybė pasirašyti XML dokumentą keletą kartų (nesvarbu ar naudojant tą patį sertifikatą, su kuriuo buvo pasirašyta pirmąjį kartą, ar su kitu). Visi parašai saugomi <signatures> elemente:

```
<konfiguracija>
      <signatures>
            <Signature>.. </Signature>
            <Signature>.. </Signature>
      </signatures>
</konfiguracija>
```

Parašas suformuojamas pagal XMLDSig standartą, taip pat naudojamas išplėstas <Object> elementas, kuriame saugoma papildoma informacija apie parašą, tačiau nesilaikant XAdES standarto. XAdES standartas bus naudojamas tik 2010-ųjų metų InfoPath versijoje [20].

XML pasirašymo programinės įrangos palyginimas

602XML Filler, „Software602“

Privalumai:

- ✓ Daugybinis pasirašymas (daugiau nei vienas XML parašas viename dokumente)

- ✓ Nemokama

Trūkumai:

- ✓ Nėra galimybės pildyti XML failus programos aplinkoje

XML Signer, „Secure Soft“

Privalumai:

- ✓ Galimybė pasirašyti visus XML dokumentus nurodžius tik direktoriją

Trūkumai:

- ✓ Nepalaiko daugybinių XML parašų (daugiau nei vieno XML parašo tame pačiame XML dokumente)
- ✓ Nėra galimybės redaguoti, ar peržiūrėti XML dokumento turinį.

Microsoft InfoPath [8]

Privalumai:

- ✓ Suderinamumas (su kitomis MS Office programomis)
- ✓ Microsoft Office programiniam paketui būdinga aplinka
- ✓ Formų generavimas iš XML dokumentų arba XSD schemų
- ✓ XML dokumentų redagavimas
- ✓ Daugybinis pasirašymas (palaiko daugiau nei vieno parašą viename XML dokumente)

Trūkumai:

- ✓ Nėra galimybės pasirašyti XML dokumentą, kuris buvo sukurtas ne su „InfoPath“ programine įranga.
- ✓ Generuojant formą iš XML dokumento, nėra galimybės ją pasirašyti, jei XML dokumente nebuvo numatytas <signatures> elementas.

2.4. Siekiamos sistemos apibrėžimas

Numatomos sistemos pagrindinės funkcijos turėtų apimti XML dokumentų valdymą (kūrimą, saugojimą MS Sql server duomenų bazėje, redagavimą), pasirašymą skaitmeniniu parašu, parašo tikrinimą (tikrinimas remsis viešojo rakto sertifikatais), taip pat planuojamos realizuoti bendros dokumentų valdymo funkcijos, tokios kaip senų dokumentų versijų saugojimas, sistemos įvykių registravimas ir pan.

Realizacijos rezultatas – klientinė programa.

2.5. Analizės išvados

Atlikus universalių dokumentų valdymo sistemų ir XML pasirašymo programinės įrangos analizę, paaiškėjo dokumentų valdymo sistemų (DVS) siūlomi sprendimai, nustatyti trūkumai - XML duomenų tipo apdorojimo ir pasirašymo srityse. Apžvelgus ir eksperimentiškai ištyrus XML pasirašymo programinę įrangą, ir pasirašytų XML dokumentų struktūrą, išaiškėjo esminiai programinės įrangos pasirašymo principai – naudojamų XML parašų tipai:

- ✓ 602XML Filler, „Software602“ - naudojamas gaubiantis (angl. enveloping) XML parašas
- ✓ XML Signer, „Secure Soft“ - naudojamas įtrauktas (angl. enveloped) – XML parašas
- ✓ Microsoft InfoPath [8] – naudojamas įtrauktas (angl. enveloped) – XML parašas

Išsiaiškinti galimi daugybinio pasirašymo (kelių parašų viename XML dokumente) realizavimo būdai, tiek naudojant „gaubiantį“ XML parašą, tiek „įtrauktą“.

3. Pasirašytų XML dokumentų saugojimo ir judėjimo PĮ reikalavimų specifikacija.

3.1. Funkciniai reikalavimai.

Panaudojimo atvejai.

1 Pav. Sistemos funkcijų panaudojimo atvejai

Panaudojimo atvejai detaliai aprašomi lentelėse (1 - 17).

Eilinio vartotojo (pvz. dėstytojo) funkcijos:

- ✓ Prisijungimas prie sistemos
- ✓ Slaptažodžio keitimas

Veiksmai su duomenų šablonais (XML schemomis)

- ✓ Duomenų įvedimo šablonų sudarymas / išsaugojimas
- ✓ Duomenų šablono redagavimas
- ✓ Duomenų šablono naikinimas

Veiksmai su XML dokumentais:

- ✓ Naujų XML dokumentų kūrimas (pagal DB saugomą XML schemą)
- ✓ Duomenų importavimas iš xml failų
- ✓ XML dokumentų importavimas iš DB (redagavimui, papildymui)
- ✓ XML dokumentų pasirašymas
- ✓ XML dokumentų išsaugojimas (xml formato failo pavidalu)
- ✓ XML dokumentų užkrovimas į DB (lygiagrečiai į 2 DB)
  Į pirmąją DB užkraunami tam tikri laukai iš XML dokumento
  Į antrąją DB užkraunami pasirašyti XML dokumentai
- ✓ XML dokumentų tapatumo kontrolė (susidedanti iš XML dokumento parašo patikrinimo ir XML dokumente esančių duomenų sulyginimo su kitoje DB esančiais duomenimis)
- ✓ Duomenų sinchronizacija

Sistemos administratoriaus galimi veiksmai:

- ✓ Prisijungimas prie sistemos
- ✓ Slaptažodžio keitimas

Sistemos vartotojų administravimas

- ✓ Sistemos vartotojų įtraukimas,
- ✓ Sistemos vartotojų peržiūra,
- ✓ Sistemos vartotojų šalinimas,
- ✓ Sistemos vartotojų atliktų veiksmų peržiūra

Veiksmai su duomenų šablonais (XML schemomis)

- ✓ Duomenų įvedimo šablonų sudarymas / išsaugojimas
- ✓ Duomenų šablono redagavimas
- ✓ Duomenų šablono naikinimas

Veiksmai su XML dokumentais:

- ✓ Naujų XML dokumentų kūrimas (pagal DB saugomą XML schemą)
- ✓ Duomenų importavimas iš xml failų
- ✓ XML dokumentų importavimas iš DB (redagavimui, papildymui)
- ✓ XML dokumentų pasirašymas
- ✓ XML dokumentų išsaugojimas (xml formato failo pavidalu)
- ✓ XML dokumentų užkrovimas į DB (lygiagrečiai į 2 DB)
  Į pirmąją DB užkraunami tam tikri laukai iš XML dokumento
  Į antrąją DB užkraunami pasirašyti XML dokumentai
- ✓ XML dokumentų tapatumo kontrolė (susidedanti iš XML dokumento parašo patikrinimo ir XML dokumente esančių duomenų sulyginimo su kitoje DB esančiais duomenimis)
- ✓ Duomenų sinchronizacija

1 Lentelė. Panaudojimo atvejis „Prisijungimas“

Panaudojimo atvejo numeris	1	**Panaudojimo atvejo pavadinimas**	Prisijungimas
Aprašymas	Sistemos administratorius turi prisijungti prie sistemos jam suteiktu pirminiu vartotojo vardu ir slaptažodžiu. Šiuos prisijungimo duomenis suteikia sistemos kūrėjai.		
Pirminiai reikalavimai	Administratorius privalo gauti pradinius prisijungimo duomenis, reikalingus prisijungti ir pradėti darbą su sistema. Slaptažodis turi tenkinti tam tikrus, jam iškeltus reikalavimus (ilgio, panaudotų simbolių ir pan.).		
Bendroji proceso eiga	➢ Atidarius pirmąjį sistemos langą, į atitinkamus laukus suvesti vartotojo vardą, bei slaptažodį. ➢ Nuspausti mygtuką „Prisijungti“.		
Rezultatai	➢ Jei prisijungimo vardas bei slaptažodis buvo įvesti teisingai ir vartotojas yra autentifikuojamas ir autorizuojamas, t.y. pagal jo prisijungimo duomenis jam priskiriamos teisės darbui su sistema. ➢ Jei vartotojo vardas ar slaptažodis buvo įvestas neteisingai, tuomet sistema praneš, kad įvesti duomenys nerasti arba įvesti neteisingai. Tuomet vartotojas galės vėl bandyti jungtis prie sistemos.		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

2 Lentelė. Panaudojimo atvejis „Slaptažodžio keitimas“

Panaudojimo atvejo numeris	2	**Panaudojimo atvejo pavadinimas**	Slaptažodžio keitimas
Aprašymas	Prisijungus prie sistemos, vartotojai turi galimybę pasikeisti jiems suteiktą (įvestą arba automatiškai sugeneruotą) slaptažodį.		
Pirminiai reikalavimai	Slaptažodžio pakeitimui, vartotojas turi būti prisijungęs prie sistemos.		
Bendroji proceso eiga	➢ Prisijungus prie sistemos, vartotojas pasirenka vartotojo nustatymų skiltį, tuomet pasirenka meniu punktą „slaptažodžio keitimas“. ➢ Įvedimo laukeliuose vartotojas įveda senąjį slaptažodį ir du kartus pakartoja naująjį, ir pasirenka meniu punktą „Pakeisti slaptažodį“.		

Rezultatai	➢ Jeigu senasis slaptažodis buvo įvestas teisingas, bei naujasis slaptažodis įvestas pagal slaptažodžio reikalavimus ir pakartotinai įvestas toks pat naujasis slaptažodis, tuomet paspaudus mygtuką „Pakeisti slaptažodį", ekrane atsiras informacinis pranešimas, kad slaptažodis sėkmingai pakeistas ir vartotojas galės toliau tęsti darbą. ➢ Jeigu bent viename iš teksto įvedimo laukų buvo įvesta netaisyklinga ar bloga informacija (senasis vartotojo slaptažodis yra neteisingas ar naujasis slaptažodis neatitinka slaptažodžio reikalavimų, ar naujasis slaptažodis, įvestas pakartotinai, nesutampa su pirmuoju įvestu naujuoju slaptažodžiu), tuomet, paspaudus mygtuką „Pakeisti slaptažodį", ekrane atsiras informacinis pranešimas, kad įvyko kažkuri iš išvardintų klaidų su informacijos įvedimu ir slaptažodis nebus pakeistas tol, kol nebus suvesta tinkama informacija.
Aktorius	Administratorius, eilinis vartotojas
Pastabos	-

3 Lentelė. Panaudojimo atvejis „Sistemos vartotojų įtraukimas"

Panaudojimo atvejo numeris	3	**Panaudojimo atvejo pavadinimas**	Sistemos vartotojų įtraukimas
Aprašymas	Administratorius turi galimybę įtraukti į sistemą naujus vartotojus, sukurdamas prisijungimo vardą ir sugeneruodamas arba įrašydamas slaptažodį.		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos administratoriaus teisėmis.		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą: „vartotojų administravimas", tuomet „įtraukti naują vartotoją", ir įvedimo laukeliuose suveda reikalingą informaciją apie naują vartotoją: Vardas, Pavardė, prisijungimo vardas, slaptažodis (gali būti sugeneruotas atsitiktinis slaptažodis pasirinkus atitinkamą meniu punktą), komentarai ir kita informacija.		
Rezultatai	Teisingai suvedus duomenis, taip pat, jei slaptažodis atitinka jam keliamus reikalavimus, sėkmingai sukuriamas naujas vartotojas.		
Aktorius	Administratorius		
Pastabos	-		

4 Lentelė. Panaudojimo atvejis „Sistemos vartotojų peržiūra"

Panaudojimo atvejo numeris	4	**Panaudojimo atvejo pavadinimas**	Sistemos vartotojų peržiūra
Aprašymas	Administratorius turi galimybę peržiūrėti visų sistemos vartotojų duomenis, aktyvumą (paskutinio prisijungimo datą ir laiką).		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos administratoriaus teisėmis.		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą: „vartotojų administravimas", tuomet „vartotojų peržiūra". Pasirinkęs konkretų vartotoją, pasirenka meniu punktą „detaliau" ir gali peržiūrėti visą apie vartotoją kaupiamą informaciją.		

Rezultatai	-
Aktorius	Administratorius
Pastabos	-

5 Lentelė. Panaudojimo atvejis „Sistemos vartotojų šalinimas“

Panaudojimo atvejo numeris	5	**Panaudojimo atvejo pavadinimas**	Sistemos vartotojų šalinimas
Aprašymas	Administratorius turi galimybę pašalinti sistemos vartotoją.		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos administratoriaus teisėmis.		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą: „vartotojų administravimas“, tuomet „vartotojų šalinimas“, pasirenka vartotoją, nuspaudžią mygtuką „šalinti vartotoją“ ir dar kartą patvirtinęs savo pasirinkimą, pašalina vartotoją iš sistemos.		
Rezultatai	Iš sistemos pašalintas vartotojas, t.y. pašalinta visa informacija apie vartotoją (užkrauti XML dokumentai neištrinami).		
Aktorius	Administratorius		
Pastabos	-		

6 Lentelė. Panaudojimo atvejis „Sistemos vartotojų atliktų veiksmų peržiūra“

Panaudojimo atvejo numeris	6	**Panaudojimo atvejo pavadinimas**	Sistemos vartotojų atliktų veiksmų peržiūra
Aprašymas	Administratorius turi galimybę peržiūrėti kitų sistemos vartotojų atliktus veiksmus		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos administratoriaus teisėmis.		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą: „vartotojų administravimas“, tuomet „Vartotojų atliktų veiksmų peržiūra“, ir matomi visų vartotojų atlikti veiksmai. Informaciją galima nufiltruoti pagal datą ar vartotoją.		
Rezultatai	-		
Aktorius	Administratorius		
Pastabos	-		

7 Lentelė. Panaudojimo atvejis „Duomenų įvedimo šablonų sudarymas / išsaugojimas“

Panaudojimo atvejo numeris	7	**Panaudojimo atvejo pavadinimas**	Duomenų įvedimo šablonų sudarymas / išsaugojimas
Aprašymas	Įvedimo šablonai sudaromi įrašius reikiamų laukų pavadinimus, reikiamu eiliškumu, nurodant įvedamų duomenų tipus		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos		

Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą, skirtą naujų šablonų sudarymui. Sukuria šakninį XML dokumento elementą; po šio veiksmo kuria visus kitus reikiamus elementus, kiekvienam elementui nurodydamas leistiną duomenų tipą. Užbaigus šablono kūrimą, įvedamas šablono pavadinimas, ir jis išsaugomas duomenų bazėje.
Rezultatai	Šablonas išsaugotas duomenų bazėje
Aktorius	Administratorius, eilinis vartotojas
Pastabos	-

8 Lentelė. Panaudojimo atvejis „Duomenų šablonų redagavimas“

Panaudojimo atvejo numeris	8	**Panaudojimo atvejo pavadinimas**	Duomenų šablonų redagavimas
Aprašymas	Duomenų šablonai gali būti redaguojami, keičiami elementų pavadinimai, tipai ar elementų eiliškumas, pridedama naujų elementų arba ištrinami seni.		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos Turi būti sukurtas duomenų šablonas		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą, skirtą šablonų redagavimui, pasirenka vieną iš šablonų ir pasirenka šablono redagavimo mygtuką. Atsidariusioje formoje gali keisti elementų pavadinimus, tipus, pridėti arba ištrinti elementus.		
Rezultatai	Duomenų šablonas modifikuojamas, t.y. senoji duomenų šablono versija ištrinama, ir vietoje jo, išsaugoma nauja šablono versija.		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

9 Lentelė. Panaudojimo atvejis „Duomenų šablonų naikinimas“

Panaudojimo atvejo numeris	9	**Panaudojimo atvejo pavadinimas**	Duomenų šablonų naikinimas
Aprašymas	Duomenų šablonai gali būti sunaikinti (ištrinti) iš DB		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos Turi būti sukurtas duomenų šablonas		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas, pasirenka meniu punktą: „Naikinti duomenų šabloną“, tuomet pasirenka šabloną, kuris turi būti ištrintas, ir patvirtina savo pasirinkimą.		
Rezultatai	Duomenų šablonas ištrintas iš DB.		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

10 Lentelė. Panaudojimo atvejis „Naujų XML dokumentų kūrimas“

Panaudojimo atvejo numeris	10	**Panaudojimo atvejo pavadinimas**	Naujų XML dokumentų kūrimas

Aprašymas	Vartotojas turi galimybę kurti naują xml dokumentą pagal duomenų bazėje saugomą duomenų šabloną (XML schemą (XSD)).
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos; Turi būti sukurtas duomenų šablonas
Bendroji proceso eiga	Vartotojas pasirenka meniu punktą „Kurti naują XML dokumentą", pagal duomenų bazėje saugomą XML schemą sudaroma forma su reikiamais laukais. Vartotojas suveda duomenis į šiuos laukus.
Rezultatai	Gaunama užpildyta forma, kurios duomenys išsaugomi XML formatu.
Aktorius	Administratorius, eilinis vartotojas
Pastabos	-

11 Lentelė. Panaudojimo atvejis „Duomenų importavimas iš xml failų"

Panaudojimo atvejo numeris	11	**Panaudojimo atvejo pavadinimas**	Duomenų importavimas iš xml failų
Aprašymas	Duomenys gali būti importuoti iš xml failų ir papildomi		
Pirminiai reikalavimai	XML failai turi atitikti jiems keliamus griežtus struktūros, elementų eiliškumo ir duomenų tipų reikalavimus.		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas, pasirenka meniu punktą: „Importuoti duomenis iš xml failo" tuomet patikrinama ar duomenų failas atitinka jam keliamus reikalavimus (ar atitinka XML schemą).		
Rezultatai	Jei duomenys iš xml failo atitinka duomenų šablono keliamus reikalavimus, tuomet duomenys atvaizduojami ekrane. Jei – ne – vartotojas informuojamas apie klaidas.		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

12 Lentelė. Panaudojimo atvejis „XML dokumentų importavimas iš DB (redagavimui,papildymui)"

Panaudojimo atvejo numeris	12	**Panaudojimo atvejo pavadinimas**	XML dokumentų importavimas iš DB (redagavimui, papildymui, peržiūrai)
Aprašymas	Duomenys gali būti importuoti tiek iš akademinės informacijos DB, tiek iš XML archyvo DB saugojamų pasirašytų XML dokumentų.		
Pirminiai reikalavimai	Iš DB nuskaityti duomenys turi atitikti jiems keliamus griežtus struktūros, elementų eiliškumo ir duomenų tipų reikalavimus;		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas, pasirenka meniu punktą: „Importuoti duomenis iš DB" tuomet pasirenka duomenų bazę, iš kurios turi būti importuoti duomenys, ir keletą parametrų nurodančių, kuriuos duomenis importuoti (modulio kodą, semestrą ir pan.)		
Rezultatai	Jei importuoto xml dokumento duomenys atitinka duomenų šablono keliamus reikalavimus, tuomet duomenys atvaizduojami ekrane. Jei – ne – vartotojas informuojamas apie klaidas.		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

13 Lentelė. Panaudojimo atvejis „XML dokumentų pasirašymas“

Panaudojimo atvejo numeris	13	**Panaudojimo atvejo pavadinimas**	XML dokumentų pasirašymas
Aprašymas	Sukurtas XML dokumentas pasirašomas pasirinkus meniu punktą „Pasirašyti XML dokumentą“ ir atsidariusiame lange pasirinkus vieną iš kompiuteryje įdiegtų skaitmeninių sertifikatų.		
Pirminiai reikalavimai	Kompiuteryje turi būti įdiegtas bent vienas skaitmeninis sertifikatas; Turi būti sukurtas XML dokumentas		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas, pasirenka duomenų šabloną, sukuria naują xml dokumentą arba importuoja duomenis iš failo arba duomenų bazės. Tuomet pasirenkamas meniu punktas, skirtas xml dokumento pasirašymui, atsivėrusiame lange pasirenkamas sertifikatas, su kurio privačiu raktu bus pasirašomas dokumentas.		
Rezultatai	Jei visi veiksmai įvykdyti sėkmingai, XML dokumentas pasirašomas, programa prie dokumento rodo atitinkamą ikoną, rodančią, kad dokumentas pasirašytas.		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

14 Lentelė. Panaudojimo atvejis „XML dokumentų išsaugojimas (xml formato failo pavidalu)“

Panaudojimo atvejo numeris	14	**Panaudojimo atvejo pavadinimas**	XML dokumentų išsaugojimas (xml formato failo pavidalu)
Aprašymas	Sukurtas XML dokumentas gali būti išsaugotas kaip xml formato failas		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos; Turi būti sukurtas XML dokumentas;		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas sukuria naują xml dokumentą arba importuoja duomenis iš failo arba duomenų bazės. Tuomet pasirenkamas meniu punktas „Išsaugoti kaip failą“, pasirenkama direktorija, kurioje bus išsaugotas failas, failo vardas ir pasirenkamas mygtukas „Išsaugoti“.		
Rezultatai	XML dokumentas išsaugotas xml formato faile		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

15 Lentelė. Panaudojimo atvejis „XML dokumentų užkrovimas į DB (lygiagrečiai į 2 DB)“

Panaudojimo atvejo numeris	15	**Panaudojimo atvejo pavadinimas**	XML dokumentų užkrovimas į DB (lygiagrečiai į 2 DB)
Aprašymas	Sukurto XML dokumento duomenys gali būti „užkrauti“ į duomenų bazes. T.y. vienoje duomenų bazėje xml dokumento duomenys saugomi atskiruose laukuose; kitoje duomenų bazėje saugomi pasirašyti XML dokumentai. Duomenys neišvengiamai saugomi abiejose DB (t.y. vartotojas neturi pasirinkimo saugoti duomenis tik vienoje iš dviejų DB).		

Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos; Turi būti sukurtas duomenų šablonas; Turi būti sukurtas XML dokumentas;
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas, pasirenka duomenų šabloną, sukuria naują xml dokumentą arba importuoja duomenis iš failo arba duomenų bazės. Tuomet pasirenkamas meniu punktas „Užkrauti duomenis į DB". Jei XML dokumentas nebuvo pasirašytas, vartotojas bus apie tai perspėtas ir programa pasiūlys pasirinkti sertifikatą, kuris bus naudojamas pasirašymui
Rezultatai	Duomenys išsaugoti dviejose DB. Pirmoje saugomi atskirais laukais, antroje pasirašytų XML dokumentų pavidalu
Aktorius	Administratorius, eilinis vartotojas
Pastabos	Duomenų įrašymui turėtų būti naudojamos transakcijos, kadangi nepavykus įrašymui į vieną iš DB, įrašymas į kitą DB privalo būti atšauktas.

16 Lentelė. Panaudojimo atvejis „XML dokumentų tapatumo kontrolė"

Panaudojimo atvejo numeris	16	**Panaudojimo atvejo pavadinimas**	XML dokumentų tapatumo kontrolė
Aprašymas	Vartotojas turi galimybę patikrinti akademinės informacijos DB saugomų duomenų ir XML archyvo DB saugomų duomenų tapatumą. Tapatumo kontrolė susideda iš dviejų etapų: 1. XML dokumento parašo tikrinimo 2. Pasirašytame XML dokumente saugomų duomenų ir kitoje DB saugomų duomenų sulyginimo		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos; Turi būti užkrauti duomenys: XML archyvo DB: Pasirašytas XML dokumentas Akademinės informacijos DB: XML dokumento duomenys atskiruose laukuose		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą „XML dokumentų tapatumo kontrolė", naujai atsidariusiame lange iš sąrašo pasirenkami duomenys, kurių tapatumas turėtų būti patikrintas, ir pasirenkamas tapatumo kontrolės vykdymo mygtukas.		
Rezultatai	Galimi rezultatai: duomenys sutampa arba duomenys nesutampa		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

17 Lentelė. Panaudojimo atvejis „Duomenų sinchronizacija“

Panaudojimo atvejo numeris	17	**Panaudojimo atvejo pavadinimas**	Duomenų sinchronizacija
Aprašymas	Atlikus duomenų tapatumo kontrolę ar kitokiu būdu nustačius duomenų nesutapimus duomenų bazėse, vartotojas turi galimybę sinchronizuoti duomenis. Sinchronizacijos metu nuskaitomi reikiami duomenys iš XML dokumentų archyvo DB ir įrašomi į akademinės informacijos DB.		
Pirminiai reikalavimai	Vartotojas turi būti prisijungęs prie sistemos; Turi būti užkrauti duomenys: XML archyvo DB: Pasirašytas XML dokumentas Akademinės informacijos DB: XML dokumento duomenys atskiruose laukuose		
Bendroji proceso eiga	Prisijungęs prie sistemos vartotojas pasirenka meniu punktą „Duomenų sinchronizacija“, naujai atsidariusiame lange iš sąrašo pasirenkami duomenys, kurie turėtų būti sinchronizuoti (pasirenkamas modulio kodas, semestras ir pan.)		
Rezultatai	Galimi rezultatai: duomenys sinchronizuoti (suvienodinti) arba nepavyksta to padaryti ir vartotojas informuojamas apie klaidą.		
Aktorius	Administratorius, eilinis vartotojas		
Pastabos	-		

3.2. Nefunkciniai reikalavimai

Reikalavimai sistemos išvaizdai

18 Lentelė. Reikalavimai sistemos išvaizdai

Reikalavimo numeris	1	**Reikalavimo pavadinimas**	Reikalavimai vartotojo sąsajai
Aprašymas	Sistemos vartotojų sąsaja (angl. GUI – Graphical User Interface) realizuojama lietuvių kalba, paprasta, suprantama, lengvai valdoma meniu pagalba, neperkrauta nereikalingais elementais, esami elementai aiškiai ir patogiai išdėstyti, rezultatų atvaizdavimas aiškus, paprastas.		
Pagrindimas	Sistemos vartotojai nebus specialiai paruošti (apmokyti) sistemos naudojimui		
Tinkamumo kriterijus:	Sistemos naudojimui nereikalingas specialus pasiruošimas, t.y. intuityvus funkcijų valdymas		
Pastabos	-		

Reikalavimai vykdymo charakteristikoms

19 Lentelė. Reikalavimai vykdymo charakteristikoms

Reikalavimo numeris	2	**Reikalavimo pavadinimas**	Reikalavimai vykdymo charakteristikoms
Aprašymas	Duomenų užkrovimas lygiagrečiai į dvi duomenų bazes vykdomas lygiagrečiai, t.y. be vartotojo įsikišimo		
Pagrindimas	Sistemos vartotojai neturi turėti galimybės išvengti duomenų užkrovimo į vieną iš dviejų duomenų bazių		
Tinkamumo kriterijus:	Vieno mygtuko paspaudimu duomenys atskirais laukais saugomi pirmoje DB ir pasirašytais xml saugomi kitoje DB		
Pastabos	-		

Reikalavimai sistemos charakteristikoms

20 Lentelė. Reikalavimai sistemos charakteristikoms

Reikalavimo numeris	3	**Reikalavimo pavadinimas**	Reikalavimai sistemos charakteristikoms
Aprašymas	XML dokumente saugomiems duomenims turi būti užtikrintas duomenų nekintamumas (vientisumas). Bet kokie dokumento pokyčiai po sukūrimo turi būti pastebimi. Turi būti žinoma XML dokumentą sukūrusio subjekto tapatybė ir kiek įmanoma sumažinta suklastojamumo galimybė.		
Pagrindimas	Sistemos pagrindinėms funkcijoms užtikrinti, reikalinga bent viena duomenų kopija, kuri išliktų nepakitusi nuo duomenų sukūrimo. Ši duomenų kopija bus laikoma saugia, etalonine, su kuria bus lyginamos kitos duomenų kopijos.		
Tinkamumo kriterijus:	Duomenys saugomi pasirašyto XML dokumento pavidalu.		
Pastabos	-		

Reikalavimai veikimo sąlygoms

21 Lentelė. Reikalavimai veikimo sąlygoms

Reikalavimo numeris	4	**Reikalavimo pavadinimas**	Reikalavimai veikimo sąlygoms
Aprašymas	Veikimo aplinkoje privalo būti įdiegtas Microsoft .NET Framework 3.5 klasių bibliotekos karkasas.		
Pagrindimas	Kuriama sistema naudos standartines MS .NET Framework 3.5 klases.		
Tinkamumo kriterijus:	Įdiegtas Microsoft .NET Framework 3.5 klasių bibliotekos karkasas.		
Pastabos	-		

22 Lentelė. Reikalavimai veikimo sąlygoms

Reikalavimo numeris	5	**Reikalavimo pavadinimas**	Reikalavimai veikimo sąlygoms
Aprašymas	Kiekvieno vartotojo kompiuteryje privalo būti įdiegtas bent vienas asmeninis skaitmeninis sertifikatas ir vartotojui priklausytų jį atitinkantis privatus raktas; Kiekvieno vartotojo kompiuteryje privalo būti tų vartotojų viešojo rakto sertifikatai, kurių parašai bus tikrinami.		
Pagrindimas	Parašo tikrinimui reikalingas viešasis pasirašiusiojo raktas, kuris saugomas skaitmeniniame sertifikate.		
Tinkamumo kriterijus:	Įdiegtas bent vienas sertifikatas, kurio privatus raktas priklauso vartotojui. Įdiegti kitų sistemos vartotojų skaitmeniniai sertifikatai.		
Pastabos	-		

Reikalavimai sistemos priežiūrai

23 Lentelė. Reikalavimai sistemos priežiūrai

Reikalavimo numeris	6	**Reikalavimo pavadinimas**	Reikalavimai sistemos priežiūrai
Aprašymas	Visos klaidos, nenumatyti atvejai registruojami "registracijos žurnale" (angl. Event Log)		
Pagrindimas	Sistemos darbo teisingumui užtikrinti, visi nenumatyti atvejai, iškilusios klaidos turi būti registruojamos ir prieinamos sistemos vartotojui		
Tinkamumo kriterijus:	Kiekvienas sistemos vartotojas turi galimybę peržiūrėti sistemoje (klientinėje programoje) iškilusias klaidas ir informacinius pranešimus registracijos žurnale.		
Pastabos	-		

Reikalavimai saugumui

24 Lentelė. Reikalavimai saugumui

Reikalavimo numeris	7	**Reikalavimo pavadinimas**	Reikalavimai saugumui
Aprašymas	Sistemos administratorius užtikrina, kad visi sistemoje dirbantys vartotojai, kuriems administratorius suteikė prisijungimo duomenis, turi teisę atlikti eilinio vartotojo rolei priskirtus veiksmus.		
Pagrindimas	Prisijungusiems vartotojams prieinami visi duomenys		
Tinkamumo kriterijus:	Sistemos administratorius privalo pašalinti vartotoją, kuris neturi ar dėl kažkokių priežasčių neteko teisės atlikti veiksmus sistemoje.		
Pastabos	-		

25 Lentelė. Reikalavimai saugumui

Reikalavimo numeris	8	**Reikalavimo pavadinimas**	Reikalavimai saugumui
Aprašymas	Kiekvienas sistemos vartotojas užtikrina savo skaitmeninio sertifikato privataus rakto saugumą		
Pagrindimas	Turi būti užtikrinta, kad tik teisėtas skaitmeninio sertifikato savininkas galės pasirašyti dokumentus su jam išduotu privačiu raktu, priešingu atveju atsiranda galimybė suklastoti duomenis.		
Tinkamumo kriterijus:	Vartotojo privatus raktas saugomas		
Pastabos	-		

Kultūriniai-politiniai reikalavimai
Kultūriniai-politiniai reikalavimai nekeliami

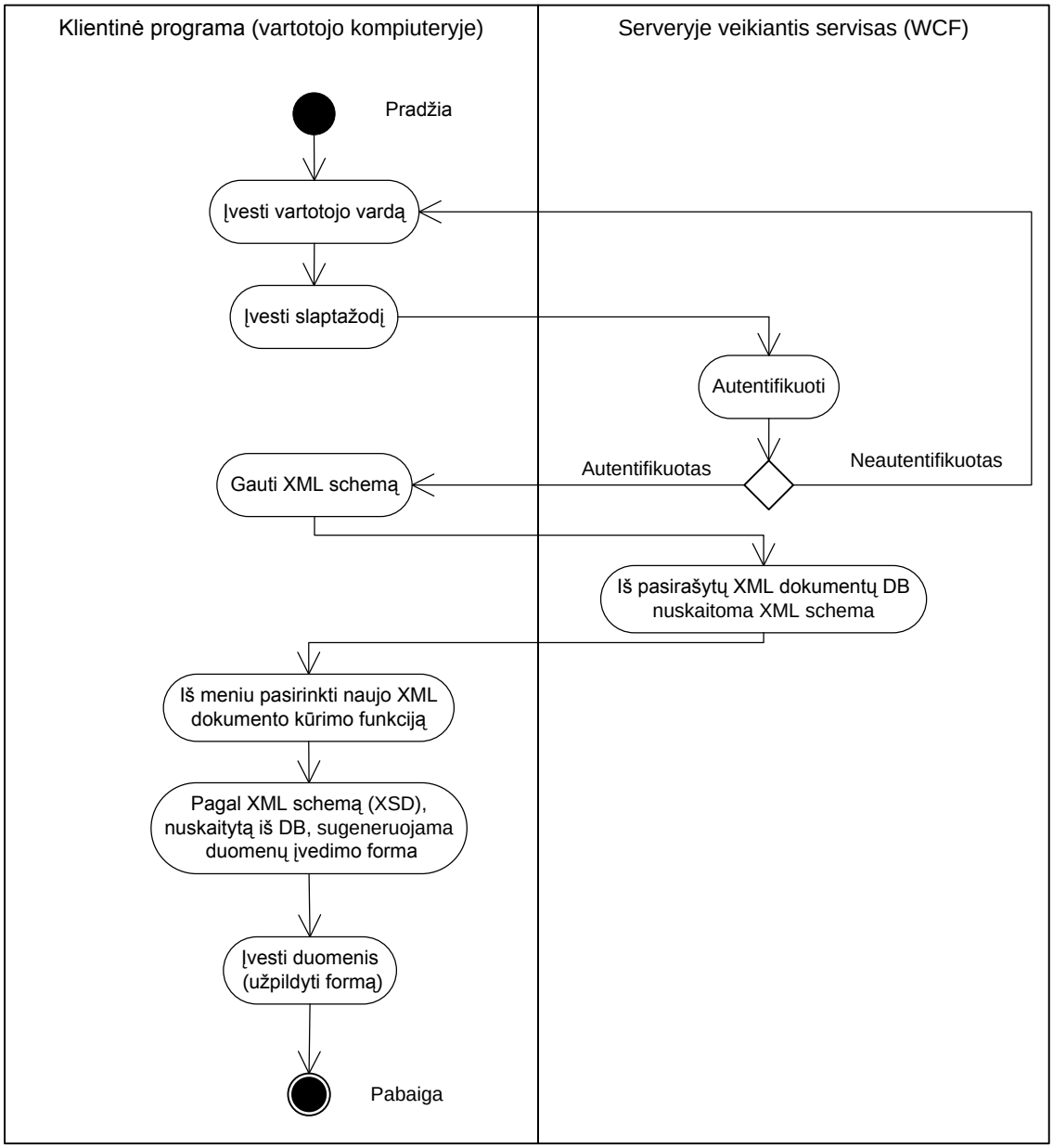
Teisiniai reikalavimai
Teisiniai reikalavimai nekeliami

4. Pasirašytų XML dokumentų saugojimo ir judėjimo PĮ projektas

4.1. Veiklos diagramos.

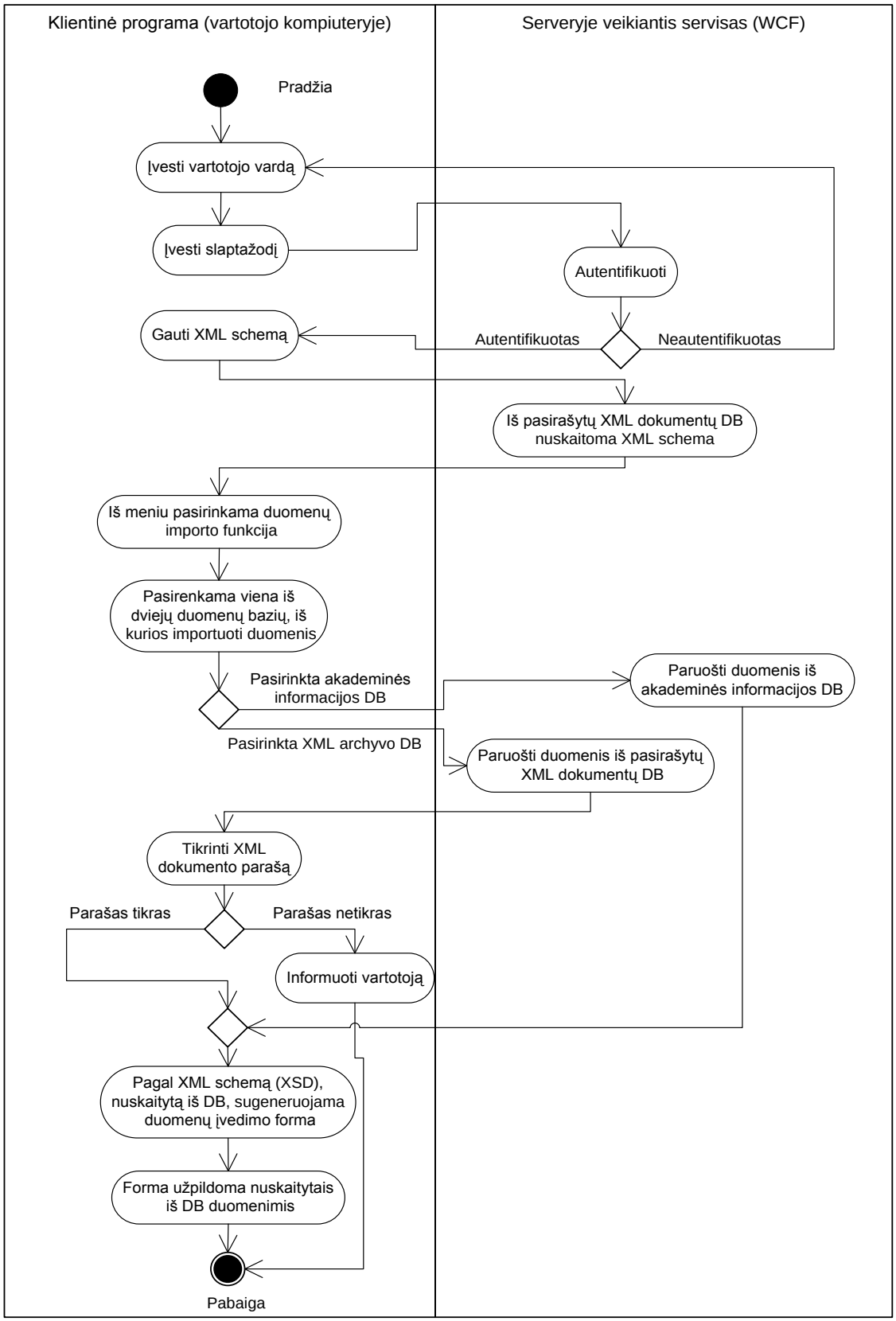
Šioje dalyje pateikiami pagrindinių sistemos funkcijų algoritmai veiklos (angl. „Activity“) UML diagramomis.

4.1.1. Naujų XML dokumentų kūrimas



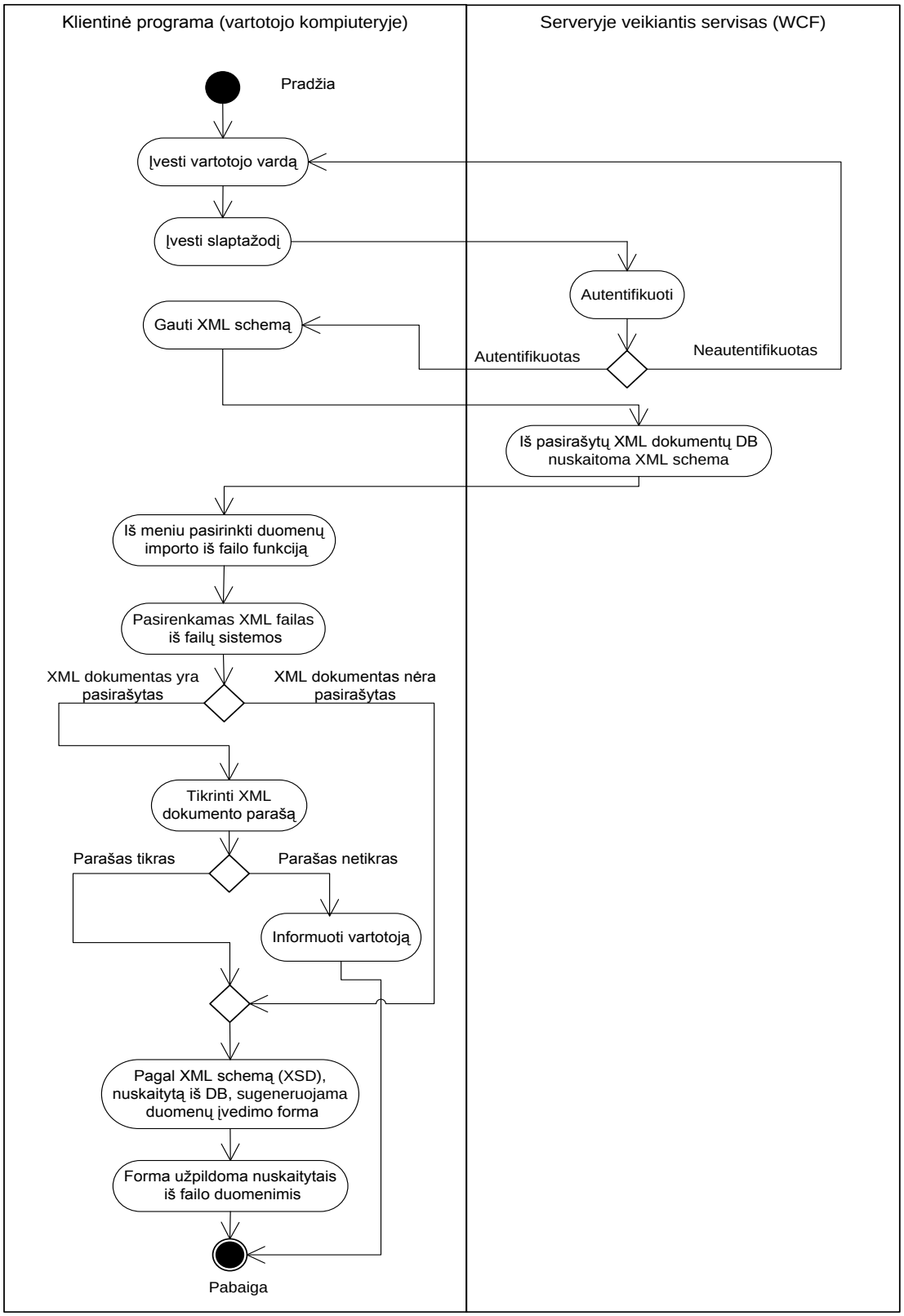
2 Pav. Naujų XML dokumentų kūrimo veiklos diagrama

4.1.2. XML dokumentų importavimas iš DB (redagavimui, papildymu, peržiūrai)



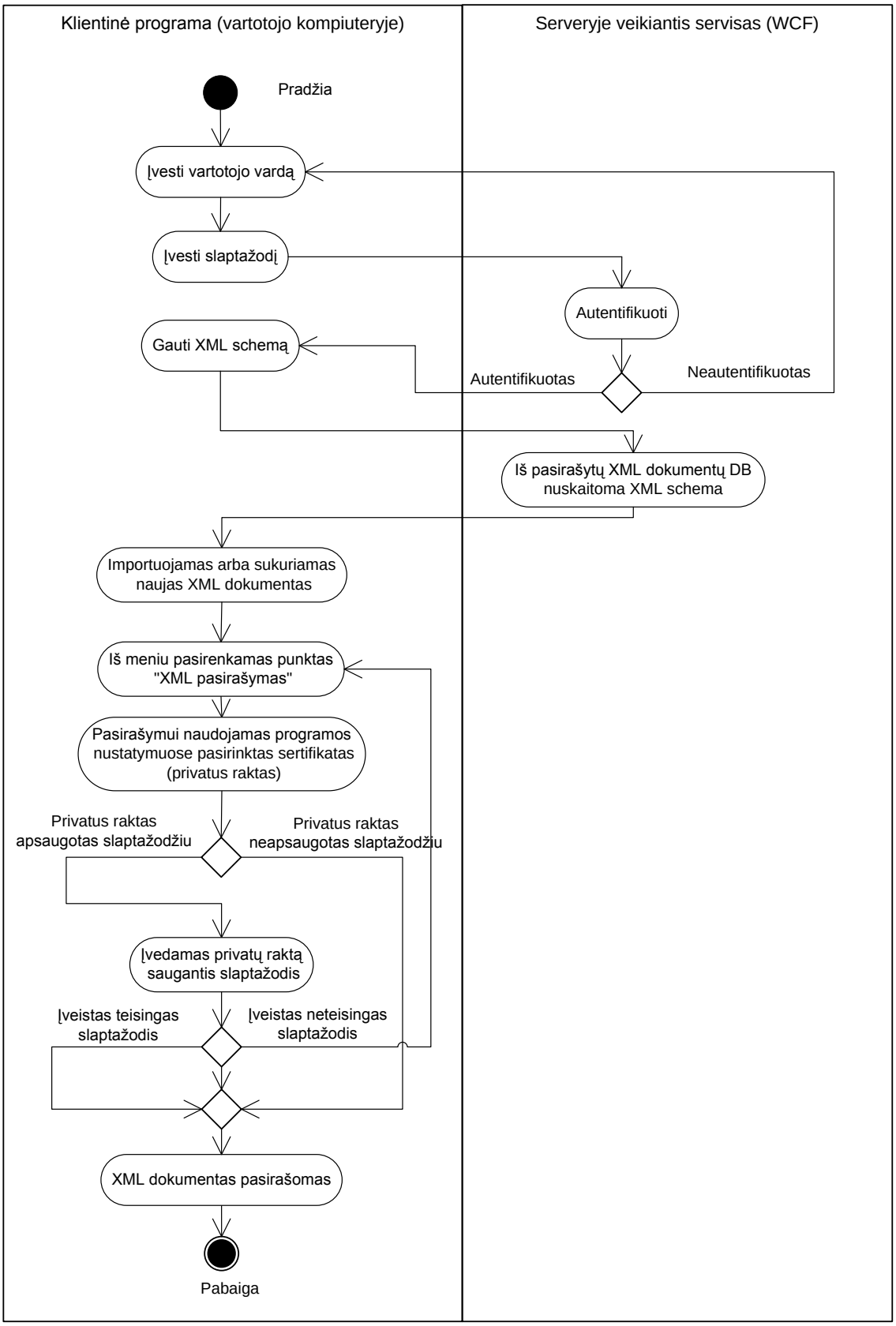
3 Pav. XML dokumentų importavimo iš DB veiklos diagrama

4.1.3. Duomenų importavimas iš xml failo



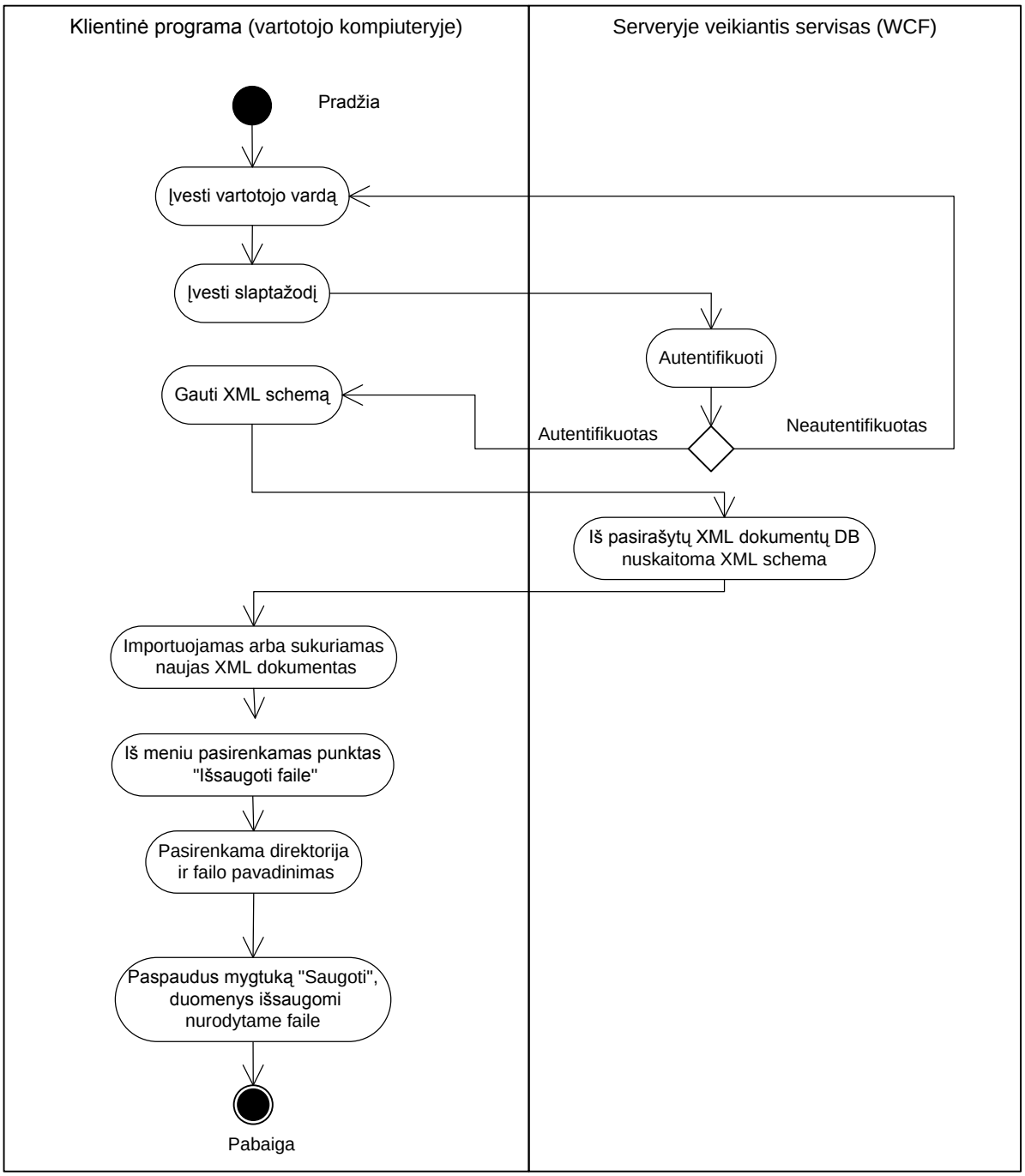
4 Pav. Duomenų importavimo iš xml failo veiklos diagrama

4.1.4. XML dokumentų pasirašymas



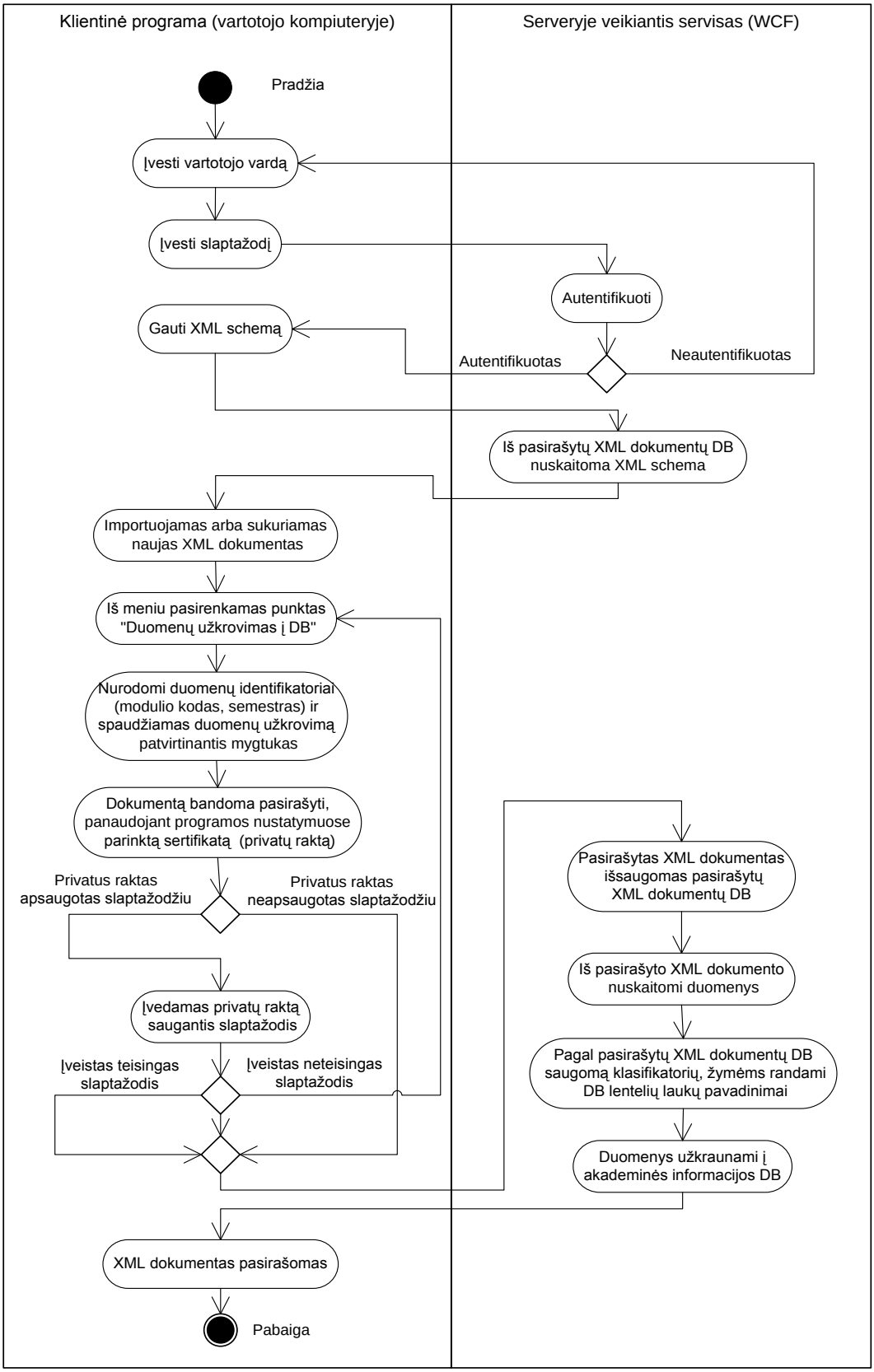
5 Pav. XML dokumentų pasirašymo veiklos diagrama

4.1.5. XML dokumentų išsaugojimas (xml formato failo pavidalu)



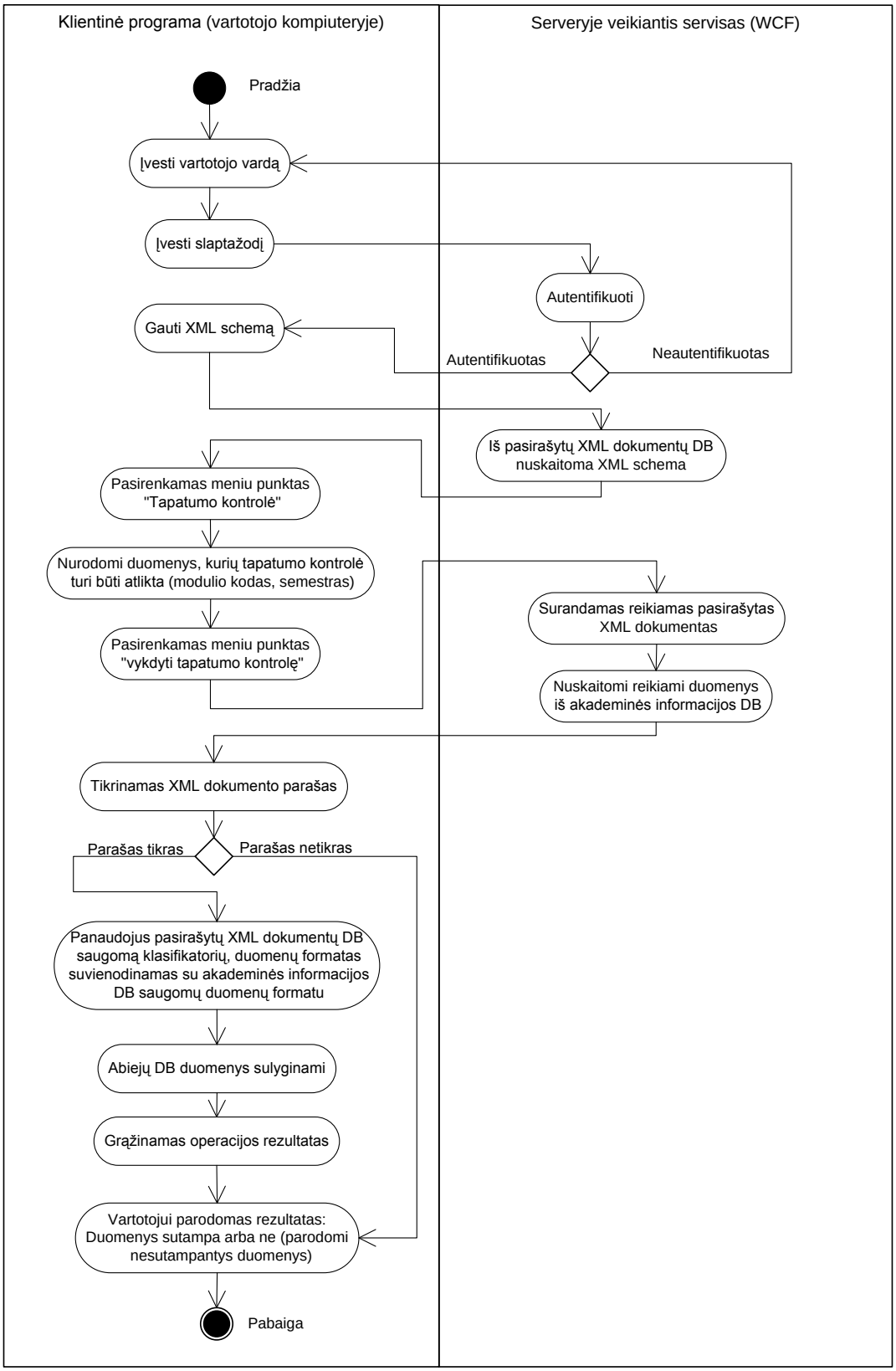
6 Pav. XML dokumento išsaugojimo faile veiklos diagrama

4.1.6. XML dokumentų užkrovimas (į DB)



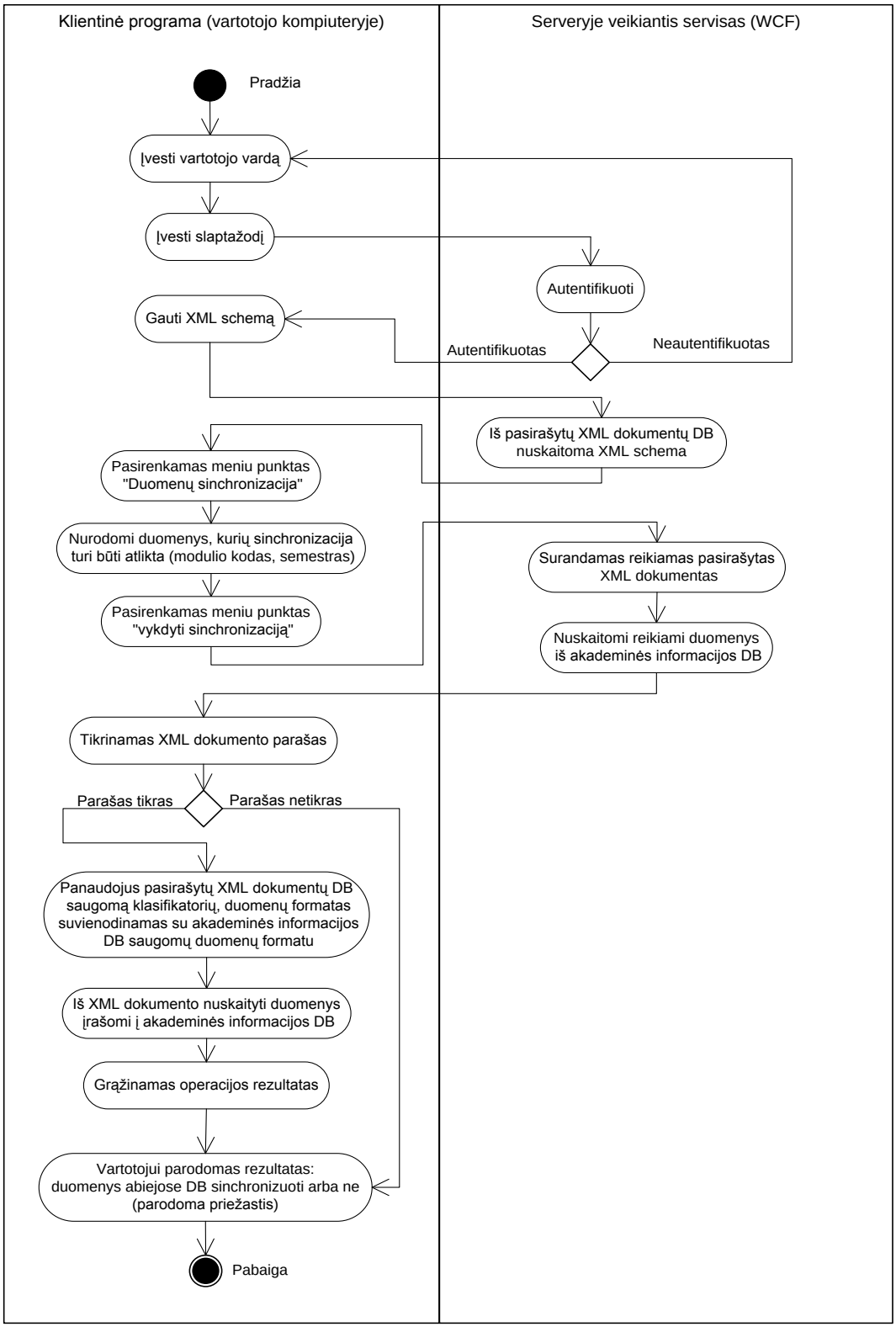
7 Pav. XML dokumento užkrovimo į DB veiklos diagrama

4.1.7. Pasirašytų XML dokumentų ir akademinės informacijos DB saugomų duomenų tapatumo kontrolė



8 Pav. Duomenų tapatumo kontrolės veiklos diagrama

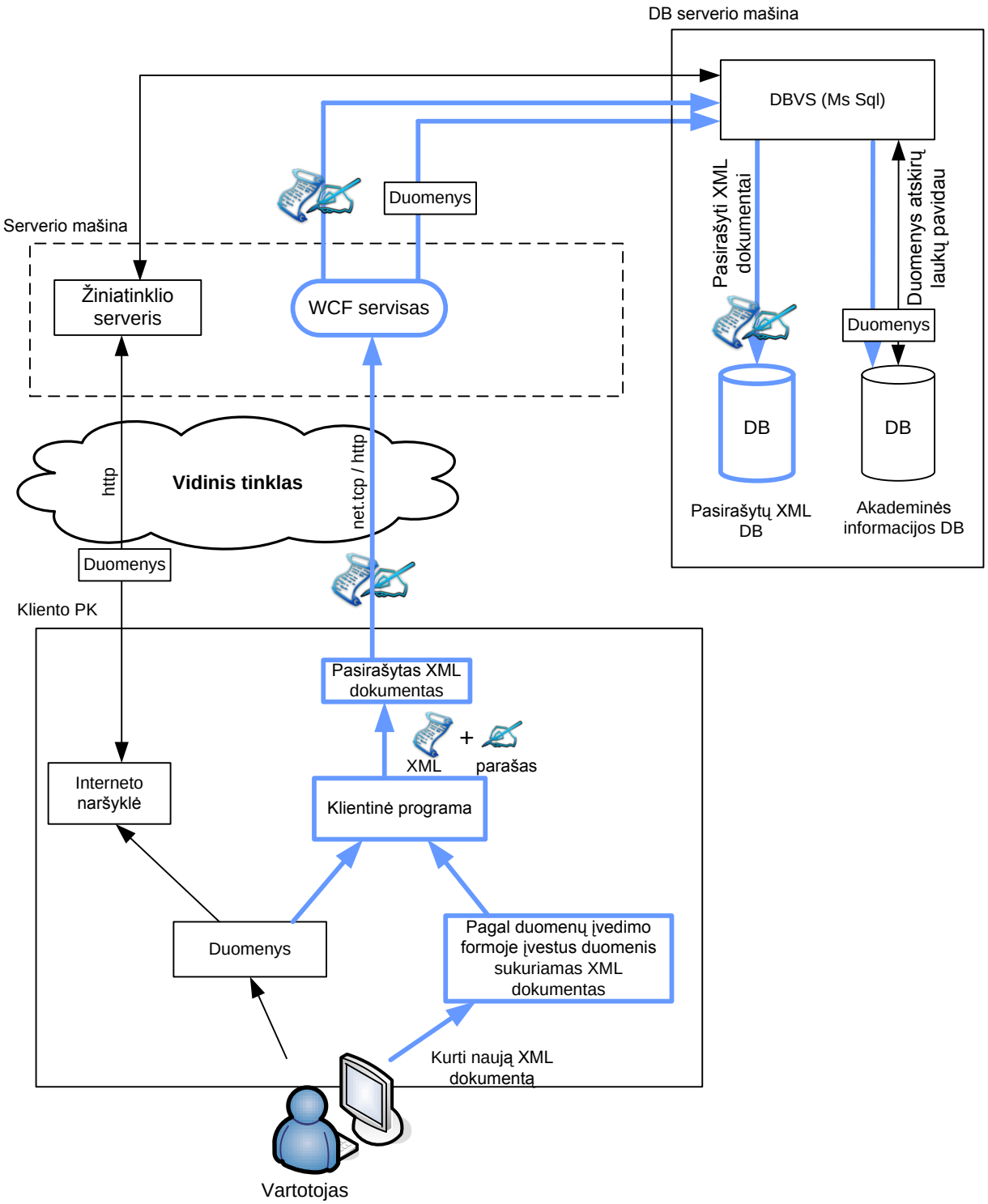
4.1.8. Duomenų sinchronizacija



9 Pav. Duomenų sinchronizacijos veiklos diagrama

4.2. Sistemos konteksto schema

Sistemos konteksto schema. Paryškintoji dalis vaizduoja kuriamą sistemą (10 pav.)



10 pav. Pasirašytų XML dokumentų saugojimo ir judėjimo programinės įrangos konteksto schema

Schemoje pavaizduota senoji akademinės informacijos sistema ir sukurta „Pasirašytų XML dokumentų saugojimo ir judėjimo programinė įranga“ (sukurtos sistemos komponentai paryškinti).
Akademinės informacijos sistemos pagrindiniai komponentai schemoje:
Kliento kompiuteris: *Interneto naršyklė, duomenys*
Serverio mašina: *Žiniatinklio (angl.Web) serverio programa*
DB serverio mašina: *duomenų bazės valdymo sistema (DBVS), akademinės informacijos duomenų bazė.*
Sukurtos sistemos „Pasirašytų XML dokumentų saugojimo ir judėjimo programinė įranga“ pagrindiniai komponentai schemoje:
Kliento kompiuteris: *klientinė programa*
Serverio mašina: *WCF servisas*
DB serverio mašina: *pasirašytų XML duomenų bazė*

Sukurta sistema sudaryta iš neribojamo skaičiaus klientinių programų ir 2 duomenų bazių. Norint apriboti klientinių programų ir duomenų bazių sąveiką, taip pat duomenų vientisumui ir autentifikacijai užtikrinti, duomenims „keliaujant“ tarp klientinės programos ir duomenų bazių, kaip priemonė pasitelkiama Microsoft WCF (angl. „Windows Communication Foundation“) technologija.

WCF (Windows komunikacijų pagrindo) servisas.

Tai technologija, supaprastinanti aplikacijų bendravimą tarpusavyje. WCF serviso privalumas, kad jis gali bendrauti su klientinėmis programomis naudojant SOAP pranešimus, todėl jis gali būti suderintas su kitomis platformomis (pvz. J2EE aplikacijomis). Jei bendrauja WCF servisas ir klientinė programa, veikianti .NET pagrindu, galima optimizuoti jų bendravimą, koduojant SOAP pranešimus dvejetainiu formatu.[17]

Kadangi WCF ir klientinių programų bendravimas paremtas SOAP protokolu, todėl saugumui tarp WCF ir klientinių programų užtikrinti, gali būti naudojami SOAP protokolui skirti metodai:

- ✓ WS-Security
- ✓ WS-SecureConversation

- ✓ WS-Trust
- ✓ WS-Federation

Kadangi SOAP pranešimas yra XML dokumentas, sudarytas iš dviejų dalių:

- ✓ antraštės (angl. „Header“),
- ✓ pranešimo kūno (angl. „Body“),

šių SOAP pranešimų vientisumui, siuntėjo autentifikacijai užtikrinti naudojami analogiški būdai kaip ir anksčiau aptartiems XML dokumentams – dokumento pasirašymas E. Parašu (*plačiau apie E-parašą rašoma analizės dalyje*).

Konfidencialumui užtikrinti naudojamas šifravimas (simetrinis), kai šifruojama tik informacija tarp žymių (angl. „tags“). [18]

Taigi, sistemos realizavimui bus naudojamas WCF servisas. Galimi 2 WCF realizavimo būdai:

1. „Lengvas“ klientas
2. „Sunkus“ klientas

Kiekvienas iš būdų turi privalumų ir trūkumų.

„Lengvo“ kliento privalumai – visa verslo logika (angl. „Business Logic“) veikia serveryje, o klientinė programa perduoda reikiamus duomenis WCF servisui, ir tik atvaizduoja tai, kokius rezultatus grąžina WCF servisas. Šis būdas patogus palaikant sistemą, kadangi atliekant sistemos pakeitimus, patobulinimus nereikia keisti klientinių programų, o keičiamas tik WCF servisas.

Sunkaus kliento privalumai: mažiau apkraunamas serveris, kadangi verslo logika veikia kliento kompiuteryje, o WCF servisas veikia kaip tarpininkas klientinei programai bendraujant su duomenų baze.

Pagal apibrėžtas sistemos funkcijas, priimtinesnis „sunkaus kliento“ modelis, kadangi skaitmeninių sertifikatų paieškos ir dokumentų pasirašymo funkcijos realizuojamos kliento dalyje. Tačiau neišvengiamai tam tikra dalis funkcijų privalo būti realizuotos serverio dalyje (pasirašyto XML dokumento vertimas į jį atitinkančios klasės objektą (angl. „Deserialization“)). Todėl privalo būti naudojamas kombinuotas variantas. WCF servisas - tarpininkas tarp klientinių programų ir duomenų bazių. Klientinė programa kreipdamasi į WCF servisą, perduoda tam tikrus parametrus, ir gauna atsakymą – tokiu būdu klientinė programa yra visiškai izoliuota nuo duomenų sluoksnio.

XML dokumento pasirašymas vykdomas klientinėje programoje, kadangi šiam veiksmui reikalingas pasirašančiojo privatus raktas.

Vartotojų prisijungimo duomenų saugumo užtikrinimas.

Vartotojų prisijungimo prie klientinės programos slaptažodžiai duomenų bazėje saugomi santraukų (angl. Hash, Digest) pavidalu.

Sukurtos sistemos idėja: sistema naudoja esamos (pvz. akademinės informacijos) sistemos duomenų bazę (ji nekeičiama) bet originali esamos sistemos vartotojo programa (aplikacija arba internetinė aplikacija) pakeičiama į naujai sukurtą klientinę programą.

Naudojant sukurtą klientinę programą, įrašant duomenis į esamos sistemos (akademinės informacijos) DB, jų kopijos pasirašomos su sistemos vartotojo skaitmeniniu parašu ir saugomos naujai suprojektuotoje pasirašytų XML dokumentų duomenų bazėje.

Atlikus bet kokius nesankcionuotus šių duomenų pakeitimus esamos sistemos duomenų bazėje – šie pakeitimai bus pastebėti, įvykdžius duomenų bazių tapatumo kontrolę, kuri sulygina pasirinktus duomenis esančius esamos sistemos DB su kitoje DB pasirašytuose XML dokumentuose saugomais duomenimis.

Bet kokie duomenų pakeitimai, atlikti pasirašytų XML dokumentų duomenų bazėje pastebimi patikrinus XML dokumentų parašus – jei parašas neatitinka pasirašytų duomenų – vadinasi buvo atlikti duomenų pakeitimai.

5. XML dokumentų tapatumo kontrolės užtikrinimo priemonių tyrimas

Sąvoka „tapatumas“ šiame kontekste turėtų būti suprantama kaip dviejų duomenų blokų (duomenų šaltinių) identiškumas, lygybė. Atitinkamai „tapatumo kontrolė“ suprantama, kaip priemonių, skirtų šių dviejų duomenų šaltinių identiškumui patikrinti ir valdyti, visuma.

Sistemos pagrindinės funkcijos: „tapatumo kontrolė“ veikimo užtikrinimui, reikalinga bent viena duomenų kopija, kuri išliktų nepakitusi nuo duomenų sukūrimo. Ši duomenų kopija laikoma saugia, etalonine, su kuria lyginamos kitos duomenų kopijos. Ji saugoma pasirašyto XML dokumento pavidalu, Saugaus Xml Archyvo („SXA“) duomenų bazėje.

Sistemos duomenų bazės.

Kuriama sistema naudoja 2 duomenų bazes, kurių duomenų tapatumas turi būti užtikrinamas:

- ✓ Akademinės Informacijos Sistemos („AIS“) DB, kurioje saugomi duomenys apie studentus, jų įvertinimus, modulius, dėstytojus ir kt.
- ✓ Saugaus XML Archyvo („SXA“) DB, kurioje duomenys saugomi pasirašytų XML dokumentų pavidalu.

Problemos aktualumas.

Esamoje, egzistuojančioje sistemoje, įvesti duomenys saugomi akademinės informacijos sistemos (AIS) reliacinėje duomenų bazėje. Atlikus tam tikrus duomenų pakeitimus duomenų bazėje, šie pakeitimai liktų nepastebėti.

Kuriamos sistemos uždavinys: užtikrinti duomenų nekintamumą (vientisumą) ir duomenis sukūrusio subjekto autentiškumą.

Uždavinys sprendžiamas sukuriant kitą duomenų bazę (SXA), kurioje, pasirašytų XML dokumentų pavidalu, saugoma tam tikra dalis AIS duomenų bazės duomenų. SXA duomenų bazėje duomenys negali būti pakeisti to nepastebėjus, kadangi po pakeitimų XML dokumente, parašas bus „netikras“.

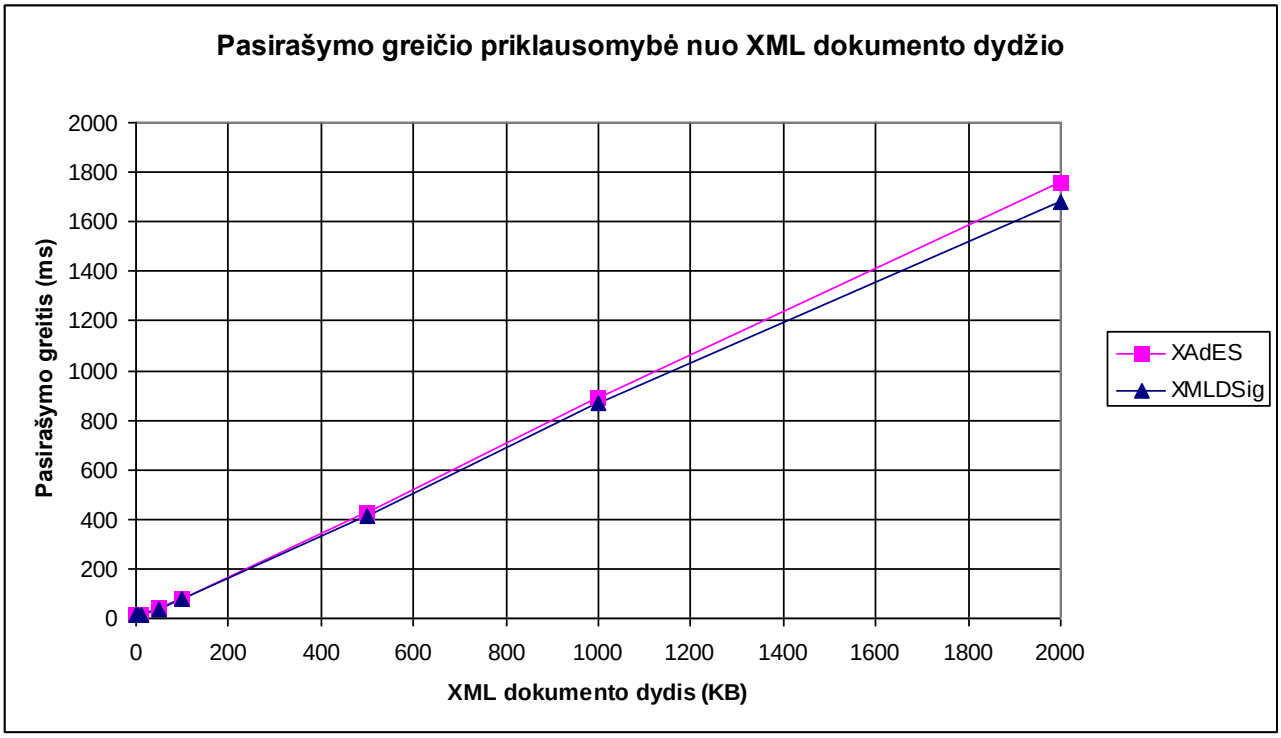
XML dokumentų parašus, jų elementus nusako standartai: XMLDSig ir XAdES. Priklausomai nuo jų teikiamų funkcijų, privalumų ir trūkumų turi būti pasirinktas vienas iš standartų, kuris tiksliau atitiktų parašui keliamus reikalavimus.

Eksperimento metu lyginamos sukurtos PĮ charakteristikos, vykdant pagrindines funkcijas su XMLDSig, ir XAdES standartais. Tyrimui atlikti, sukurta programinė įranga buvo pritaikyta darbui su šiais dviem XML parašų standartais.

Viena iš nagrinėjamų charakteristikų – parašo formavimo greitis.
Atlikti skaičiavimai su įvairiais XML dokumentų dydžiais (nuo 1KB iki 2000KB). Norint gauti kuo tikslesnius rezultatus, kiekviena pasirašymo procedūra (su tuo pačiu XML dokumentu) pakartota 10 kartų, 26 lentelėje pateikiamos vidutinės laiko reikšmės milisekundėmis.

26 Lentelė. XML dokumento pasirašymo greičio priklausomybė nuo dokumento dydžio

XML dokumento dydis (KB)		**1 KB**	**5KB**	**10KB**	**50KB**	**100KB**	**500KB**	**1000KB**	**2000KB**
Pasirašymo greitis (ms)	XMLDSig	10,9375	10,9375	12,5000	37,5000	78,1250	414,0625	867,1875	1681,2500
	XAdES	12,1500	14,0600	14,0625	42,1875	79,6875	425,0000	889,3750	1759,3750



11 pav. XML dokumento pasirašymo greičio priklausomybė nuo dokumento dydžio

Kaip minėta analitinėje darbo dalyje, XAdES standartas turi 6 sintaksės formas, eksperimento metu nagrinėta XAdES standarto bazinė forma, literatūroje dar vadinama XAdES-BES [21].

Kitoms XAdES formoms privalomas elementas - laiko žyma (angl. time stamp), jos generavimui reikalingas laiko žymos serveris [3]. Kadangi laiko žymos generavimas stipriai įtakotų skaičiavimus, todėl kitos XAdES standarto formos eksperimento metu nenagrinėjamos.
Atlikus eksperimentą, nustatyta, kad XML parašo, atitinkančio XAdES-BES standartą generavimas užtrunka vidutiniškai 1.096 karto ilgiau, lyginant su XMLDSig (27 lentelė).

27 lentelė. XMLDSig ir XAdES - BES parašų palyginimas pagal pasirašymo greitį

XML dokumento dydis (KB)		**1 KB**	**5KB**	**10KB**	**50KB**	**100KB**	**500KB**	**1000KB**	**2000KB**
Pasirašymo greitis (ms)	XMLDSig	10,9375	10,9375	12,5000	37,5000	78,1250	414,0625	867,1875	1681,2500
	XAdES	12,1500	14,0600	14,0625	42,1875	79,6875	425,0000	889,3750	1759,3750
XAdES/ XMLDSig		1,1109	1,2855	1,1250	1,1250	1,0200	1,0264	1,0256	1,0465

Vidutinė reikšmė	1,0956

Kita aktuali parašų charakteristika – xml parašo užimamas dydis atmintyje. Nagrinėjamas tik parašo elementas, neįtraukiant pasirašomo XML dokumento duomenų.
XMLDSig standarto parašas vidutiniškai reikalauja 1087 baitų (1.06KB) disko vietos
XAdES – BES standarto parašui vidutiniškai reikia 2170 baitų (2.11KB) disko vietos

28 lentelė. XMLDSig ir XAdES - BES parašų palyginimas pagal disko vietos poreikį

Duomenų užkrovimo operacijos vykdymų skaičius	**XMLDSig parašo dydis (KB)**	**XAdES - BES parašo dydis (KB)**	**Reikalaujamos disko vietos padidėjimas, naudojant XAdES-BES (MB)**
1	1,06152344	2,119140625	0,0010
10	10,6152344	21,19140625	0,0103
100	106,152344	211,9140625	0,1033
1000	1061,52344	2119,140625	1,0328
10000	10615,2344	21191,40625	10,3283
100000	106152,344	211914,0625	103,2829

Taigi, skaitmeniniam parašui formuoti panaudojus XAdES – BES standartą ir sukurtos programinės įrangos pagalba atlikus 100000 duomenų užkrovimų, duomenys reikalautų apie 103MB daugiau vietos, nei naudojant XMLDSig standartą.

Sukurtos programinės įrangos pagrindinės funkcijos (tapatumo kontrolės) veikimo korektiškumui patikrinti, atliekamas testas.

Tapatumo kontrolės tikrinimui reikalingi etapai:

1. XML dokumento sukūrimas panaudojus kitą programinę įrangą, pvz.: „MS Excel“ (suderinamumo su kita PĮ patikrinimas).
2. Programos paleidimas
3. Skaitmeninio sertifikato, naudojamo XML dokumento pasirašymui, pasirinkimas
4. Duomenų importavimas iš išorinio šaltinio
5. XML dokumento pasirašymas skaitmeniniu parašu ir pasirašytame XML dokumente saugomų duomenų įrašymas lygiagrečiai į 2 duomenų bazes (skirtingais formatais).
6. Duomenų pakeitimai :
   6.1. „AIS“ duomenų bazėje
   6.2. „SXA“ duomenų bazėje
7. Tapatumo kontrolės funkcijos vykdymas tarp skirtingose DB saugomų duomenų
8. Neatitikimų peržiūra
9. Duomenų sinchronizacijos (arba redagavimo ir duomenų užkrovimo) vykdymas

Sukurtos PĮ aplinkoje importuojami duomenys patikrinami, ar jie atitinka SXA DB saugomą XML schemą (t.y. ar yra reikiami laukai, ar atitinka jų duomenų tipai ir pan.). Norint kurti XML dokumentus, kurie bus importuojami į SXA, reiktų tai daryti pagal šią XML schemą.

MS Excel aplinkoje pagal minėtą XML schemą sukuriama duomenų įvedimo forma (12, 13 pav.) ir išsaugoma įprastiniu „xls“ arba „xlsx“ formatu.

Žiniaraštis	2009R124578
Mokslo metai	2009/2010
Semestras	R - rudens
Modulio kodas	T120B102
Modulio pavadinimas	Kompiuterių funkcionavimo pagrindai
Studijų forma	D-dieninė

12 pav. Duomenų apie žiniaraštį įvedimas MS Excel aplinkoje

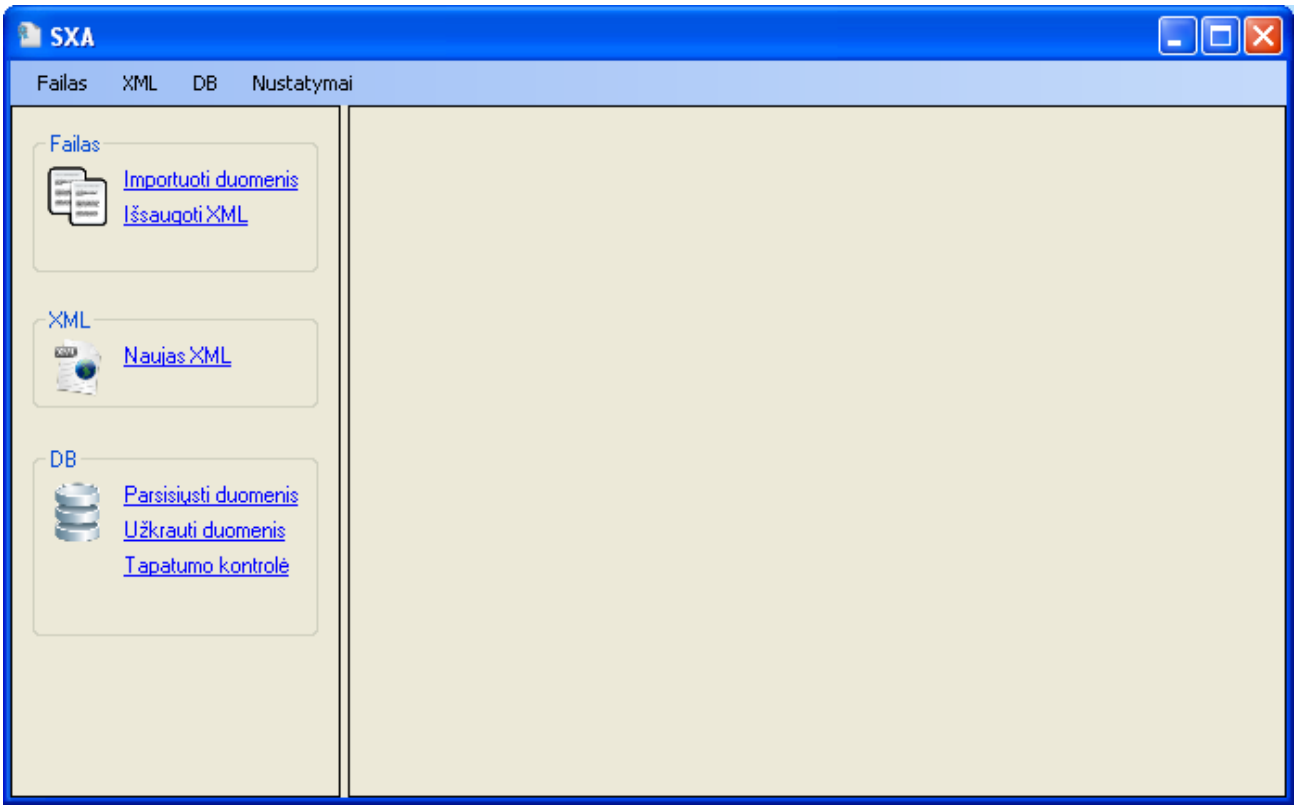
				Papildomi įvertinimai, kurių reikšmės neįtraukiamos saugant xml formatu. (Galima pridėti daugiau stulpelių)							
Stud bilieto nr	**Grupė**	**Studento vardas**	**Studento pavardė**	**Tarpinis atsiskaitymas nr1**	**Tarpinis atsiskaitymas nr2**	**Tarpinis atsiskaitymas nr3**	**Semestro įvertinimas**	**Semestro dėstytojo tabelio nr.**	**Egzamino pažymys**	**Egzamino dėstytojo tabelio nr**	**Egzamino data**
07482	IF-4/1	Rita	Kriūkienė	8	9	9	IS įskaityta	0386	9	0386	2010-01-26
01898	IF-4/1	Jonas	Noskovas	5	8	8	IS įskaityta	0386	7	0386	2010-01-26
32963	IF-4/2	Aurimas	Lisauskas	8	8	7	BR Išbraukta	0386			
10073	IF-4/2	Audrius	Jakubonis	8	9	5	IS įskaityta	0386	8	0386	2009-01-20
10996	IF-4/2	Darius	Tamelis	8	5	9	IS įskaityta	2101	7	0386	2009-01-20
00576	IF-4/1	Marijus	Šeporaitis	8	8	8	IS įskaityta	0386	8	0386	2009-01-20
00645	IF-4/1	Artūras	Šmaižys	7	9	7	IS įskaityta	0386	8	0386	2009-01-20
00740	IF-4/1	Anastasija	Gedgaudienė	8	8	5	IS įskaityta	2101	7	0386	2009-01-20
00771	IF-4/1	Aidas	Daugelė	5	8	9	IS įskaityta	0386	8	0386	2009-01-20
00797	IF-4/1	Eglė	Ivanauskaitė	8	9	8	IS įskaityta	0386	9	0386	2009-01-20
00838	IF-4/1	Giedrius	Keizikas	8	8	7	IS įskaityta	0386	8	0386	2009-01-20
00928	IF-4/1	Dmitrijus	Miškinas	7		5		0386	3		
01045	IF-4/1	Rimantas	Jasinskas	8		9		0386	4		
01086	IF-4/1	Saulius	Juškevičius	8		8		0386	4		
01134	IF-4/1	Jurgita	Grigalionienė	8		7		0386	4		
01242	IF-4/1	Valdas	Šulinskas	8		5		2101	3		
01440	IF-4/1	Saulius	Grigonis	7		9		0386	4		
01481	IF-4/1	Vytautas	Švykas	8		8		2101	4		
01492	IF-4/1	Irina	Irčinova	8		7		0386	4		
01534	IF-4/1	Neringa	Survilaitė-Bagdo	7		5		0386	3		
01538	IF-4/1	Vida	Gajauskaitė	8		9		0386	4		

13 pav. Studentų įvertinimų įvedimas MS Excel aplinkoje

MS Excel aplinkoje yra galimybė naudoti daugiau laukų, pvz. tarpiniams rezultatams saugoti, naudoti formules galutiniams rezultatams skaičiuoti ir pan. Išsaugant duomenis XML formatu, išsaugomos tik su XML schema susietų (angl. mapped) laukų reikšmės. Todėl vartotojas neapribojamas, ir gali savo nuožiūra pridėti papildomų duomenų, kurie reikalingi galutinio įvertinimo apskaičiavimui.

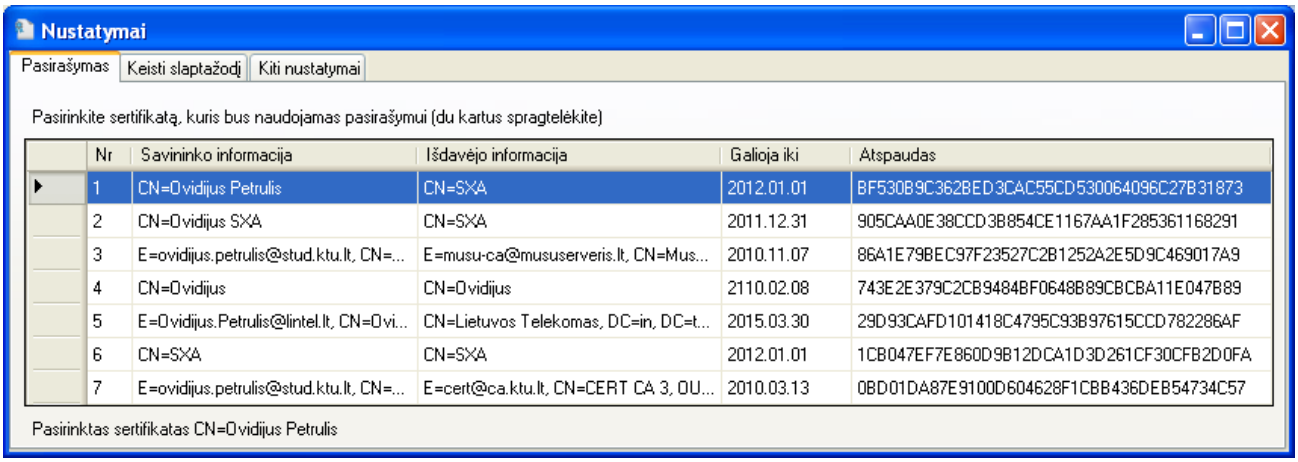
Suvedus duomenis, jie išsaugomi XML formatu, ir gali būti importuoti į sukurtą PĮ.

Paleidžiama programa. Programos langas pavaizduotas (14 pav.). Jei leidžiant programą parodomas įspėjamasis pranešimas, informuojantis, kad neveikia „SXA“ servisas, reiktų jį paleisti, nes priešingu atveju klientinė programa negalės vykdyti duomenų mainų su duomenų bazėmis, taip pat nuskaityti XML dokumentų validacijai reikalingos XML schemos.



14 pav. Klientinės programos langas

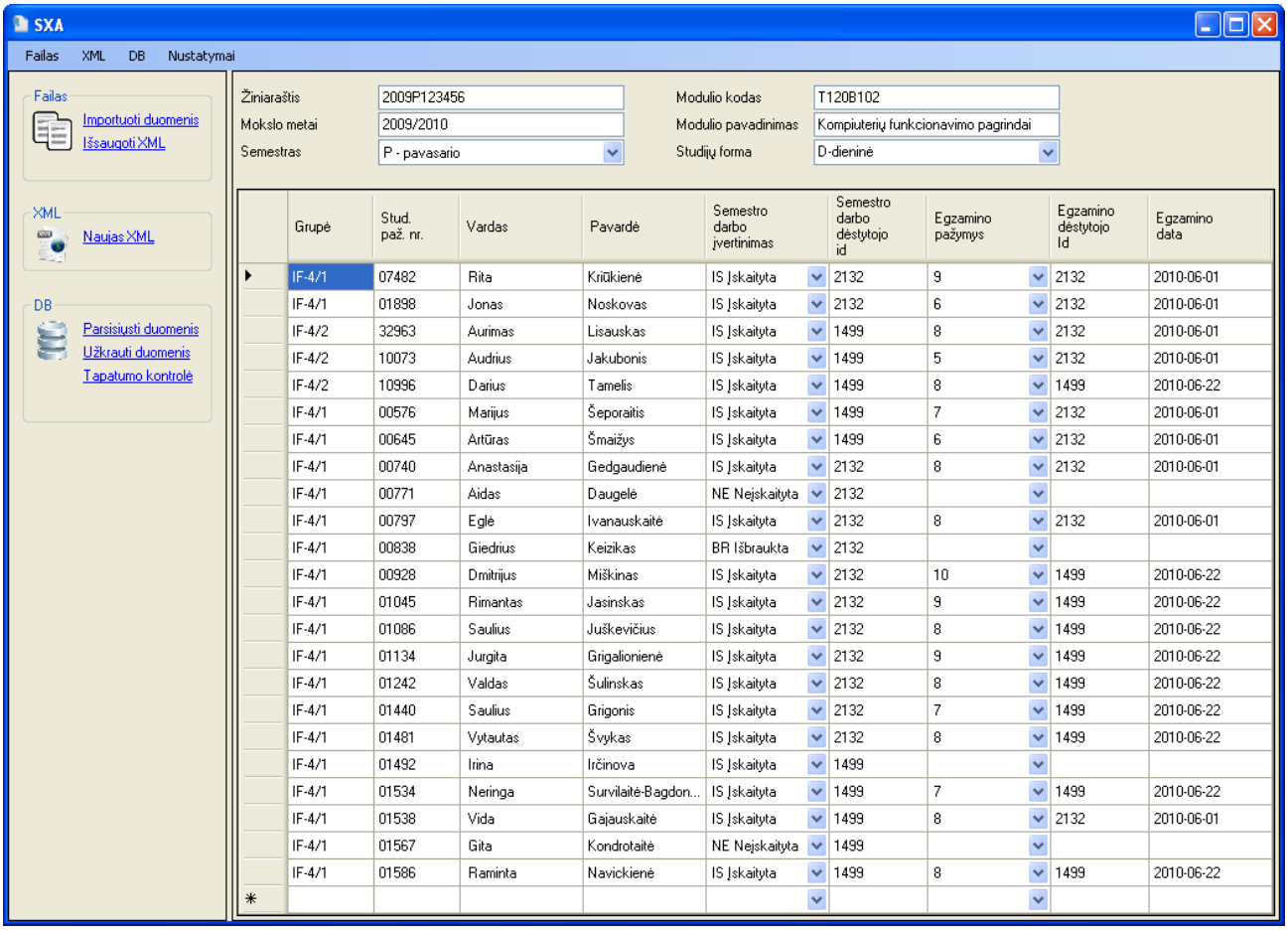
Skaitmeninio sertifikato pasirinkimas vykdomas pasirinkus meniu punktą „Nustatymai“ ir 2 kartus spragtelėjus ant sertifikatų sąraše pasirinkto sertifikato.



15 pav. Sertifikato, naudojamo pasirašymui, pasirinkimas

XML dokumentas gali būti kuriamas tuščioje formoje, arba duomenis galima importuoti (iš failo arba DB). Šiuo atveju duomenys importuojami iš išorinio šaltinio (MS Excel aplinkoje sukurto XML failo).

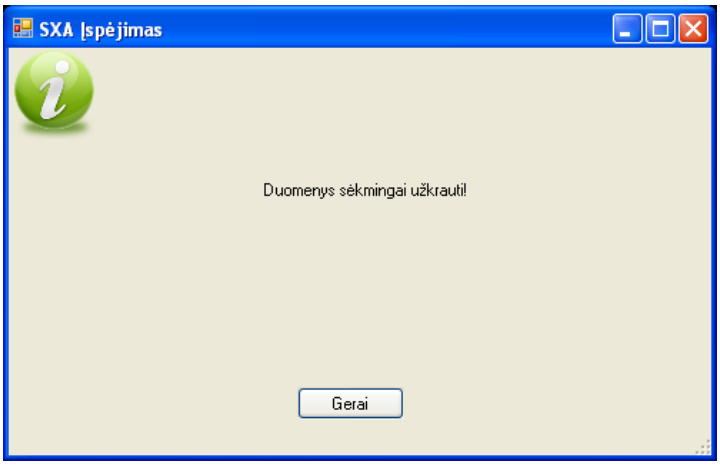
Importavus duomenis, jie gali būti keičiami programos lange



Grupė	Stud. paž. nr.	Vardas	Pavardė	Semestro darbo įvertinimas	Semestro darbo dėstytojo id	Egzamino pažymys	Egzamino dėstytojo Id	Egzamino data
IF-4/1	07482	Rita	Kriūkienė	IS Įskaityta	2132	9	2132	2010-06-01
IF-4/1	01898	Jonas	Noskovas	IS Įskaityta	2132	6	2132	2010-06-01
IF-4/2	32963	Aurimas	Lisauskas	IS Įskaityta	1499	8	2132	2010-06-01
IF-4/2	10073	Audrius	Jakubonis	IS Įskaityta	1499	5	2132	2010-06-01
IF-4/2	10996	Darius	Tamelis	IS Įskaityta	1499	8	1499	2010-06-22
IF-4/1	00576	Marijus	Šeporaitis	IS Įskaityta	1499	7	2132	2010-06-01
IF-4/1	00645	Artūras	Šmaižys	IS Įskaityta	1499	6	2132	2010-06-01
IF-4/1	00740	Anastasija	Gedgaudienė	IS Įskaityta	2132	8	2132	2010-06-01
IF-4/1	00771	Aidas	Daugelė	NE Nejskaityta	2132			
IF-4/1	00797	Eglė	Ivanauskaitė	IS Įskaityta	2132	8	2132	2010-06-01
IF-4/1	00838	Giedrius	Keizikas	BR Išbraukta	2132			
IF-4/1	00928	Dmitrijus	Miškinas	IS Įskaityta	2132	10	1499	2010-06-22
IF-4/1	01045	Rimantas	Jasinskas	IS Įskaityta	2132	9	1499	2010-06-22
IF-4/1	01086	Saulius	Juškevičius	IS Įskaityta	2132	8	1499	2010-06-22
IF-4/1	01134	Jurgita	Grigalionienė	IS Įskaityta	2132	9	1499	2010-06-22
IF-4/1	01242	Valdas	Šulinskas	IS Įskaityta	2132	8	1499	2010-06-22
IF-4/1	01440	Saulius	Grigonis	IS Įskaityta	2132	7	1499	2010-06-22
IF-4/1	01481	Vytautas	Švykas	IS Įskaityta	2132	8	1499	2010-06-22
IF-4/1	01492	Irina	Irčinova	IS Įskaityta	1499			
IF-4/1	01534	Neringa	Survilaitė-Bagdon...	IS Įskaityta	1499	7	1499	2010-06-22
IF-4/1	01538	Vida	Gajauskaitė	IS Įskaityta	1499	8	2132	2010-06-01
IF-4/1	01567	Gita	Kondrotaitė	NE Nejskaityta	1499			
IF-4/1	01586	Raminta	Navickienė	IS Įskaityta	1499	8	1499	2010-06-22

16 pav. Žiniaraščio duomenys

Pasirinkus meniu punktą „DB“, tuomet „Užkrauti duomenis“, sukuriamas XML dokumentas, dokumentas pasirašomas panaudojus nustatymuose parinktą sertifikatą ir pasirašytas XML dokumentas perduodamas „SXA“ servisui. Servisas iš pasirašyto XML dokumento nuskaito visus duomenis ir juos užkrauna į akademinės informacijos sistemos „AIS“ DB, jei duomenų užkrovimas sėkmingai įvykdytas, tuomet pasirašytas XML dokumentas užkraunamas į Saugaus XML Archyvo „SXA“ DB. Vartotojas informuojamas apie vykdytos operacijos rezultatą.



17 pav. Informacinis pranešimas apie sėkmingą duomenų užkrovimą

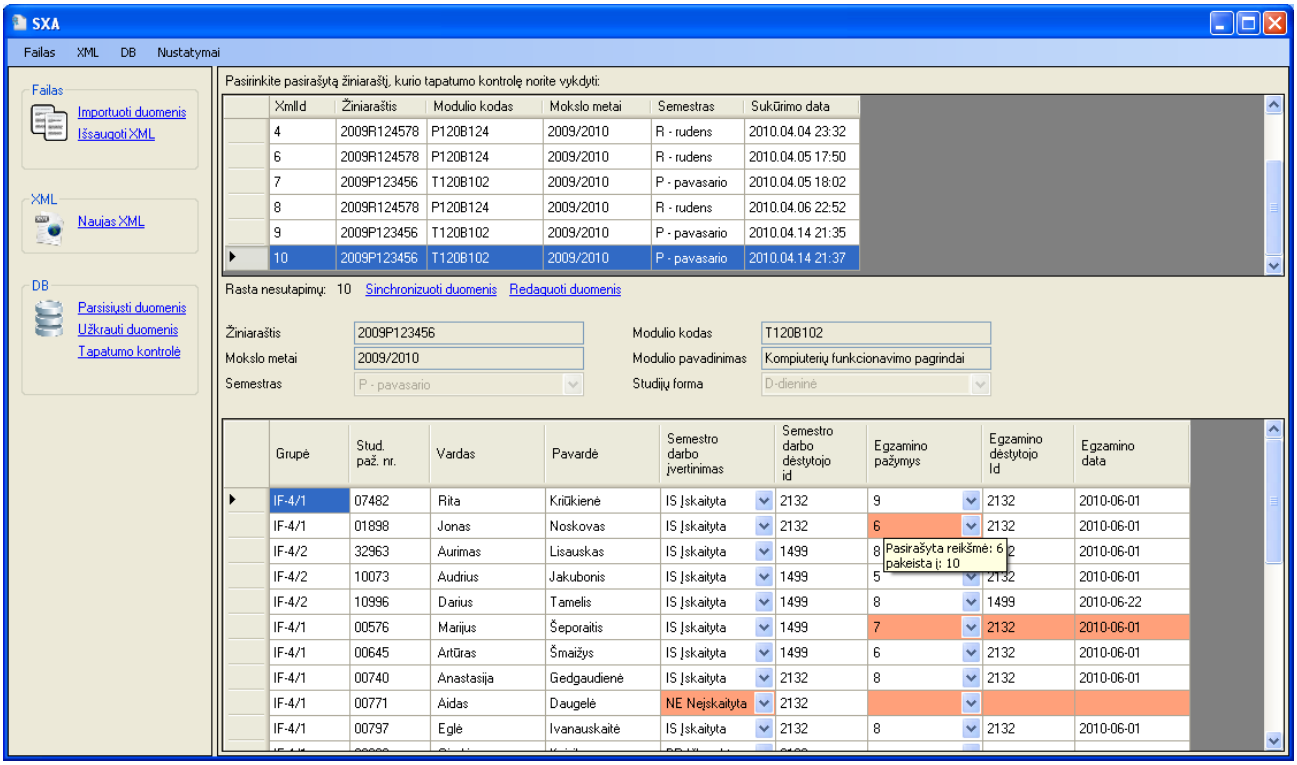
AIS duomenų bazėje atliekami duomenų pakeitimai:

- ✓ Pakeičiamas semestro darbo įvertinimas
- ✓ Pakeičiami keletas egzamino įvertinimų
- ✓ Pakeičiami keletas dėstytojo tabelio numerių
- ✓ Pakeičiamos keletas egzamino datų

Tapatumo kontrolė vykdoma pasirinkus meniu punktą „DB“, tuomet „Tapatumo kontrolė“. Pasirinkus minėtą meniu punktą vartotojui rodomi jo užkrauti į DB žiniaraščiai. Pasirinkus vieną iš žiniaraščių, vykdoma pasirinkto žiniaraščio tapatumo kontrolė:

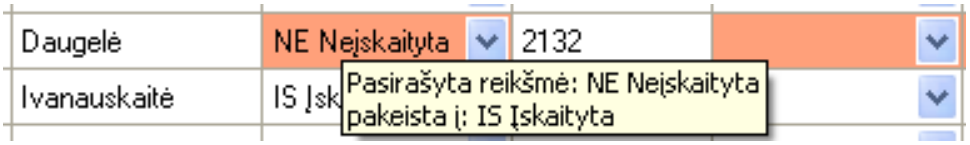
- ✓ iš „SXA“ duomenų bazės nuskaitomas pasirašytas XML dokumentas su reikiamo žiniaraščio duomenimis, patikrinama ar dokumentas nebuvo pakeistas po pasirašymo
- ✓ iš „AIS“ duomenų bazės nuskaitomi pasirinkto žiniaraščio duomenys
- ✓ suvienodinami nuskaitytų duomenų formatai
- ✓ duomenys sulyginami
- ✓ vartotojui atvaizduojami pasirašyto XML dokumento duomenys ir rasti nesutapimai su „AIS“ duomenų bazėje saugomais duomenimis.

Tapatumo kontrolės vykdymo rezultatų peržiūra (18 pav.).



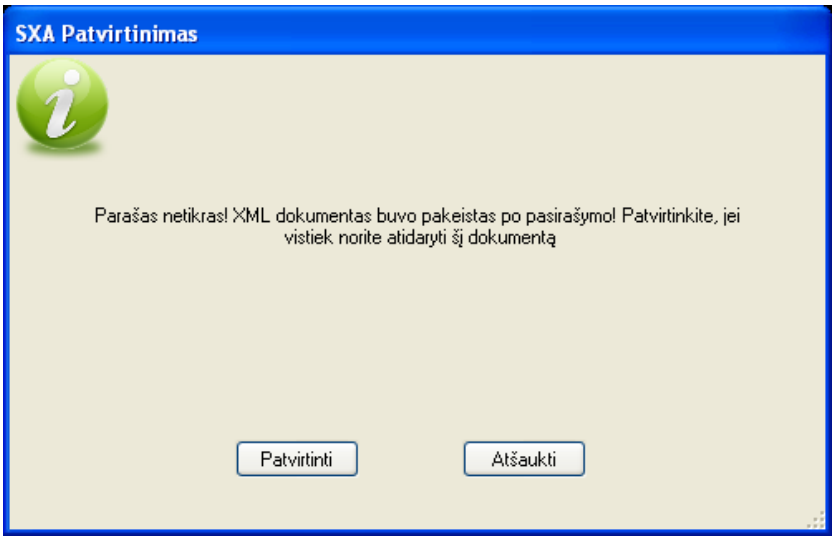
18 pav. Tapatumo kontrolės rezultatai

Įvykdžius tapatumo kontrolę, pateikiamos pasirašyto XML dokumento (žiniaraščio) reikšmės, o nesutapimai su akademinės informacijos sistemos „AIS“ DB saugomomis reikšmėmis pažymimi rausvai (18 pav.). Norint sužinoti, į kokią reikšmę buvo pakeista pradinė (pasirašytoji) reikšmė, pelės žymeklis užvedamas ant pasirinkto narelio (angl. cell) (19 pav.).



19 pav. Semestro įvertinimo nesutapimas, įvykužius tapatumo kontrolę

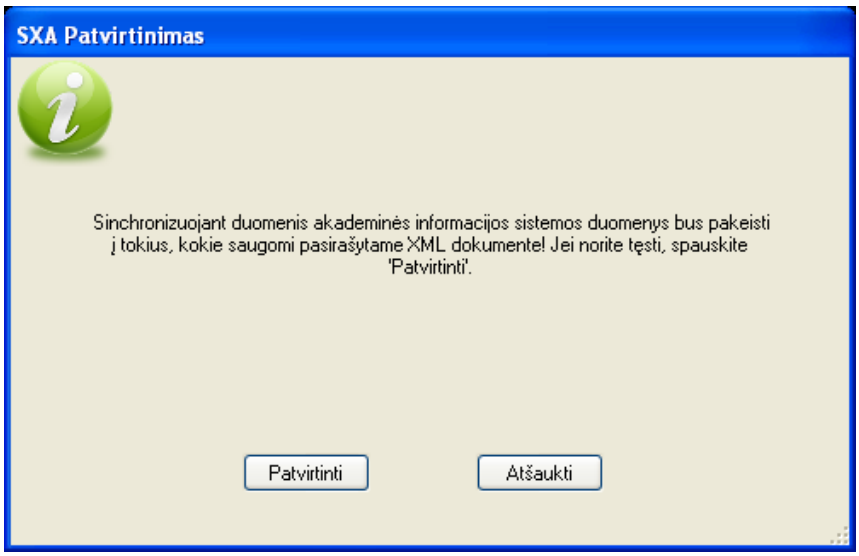
Atlikus pakeitimą „SXA“ duomenų bazėje saugomame XML dokumente, vykdant tapatumo kontrolę, vartotojas yra įspėjamas, kad pasirašytas XML dokumentas yra pakeistas po pasirašymo (parašas „netikras“) (20 pav.). Vartotojas gali pasirinkti ar vis tiek nori atidaryti pakeistą XML dokumentą.



20 pav. Įspėjimas apie pakeistą XML dokumentą po pasirašymo

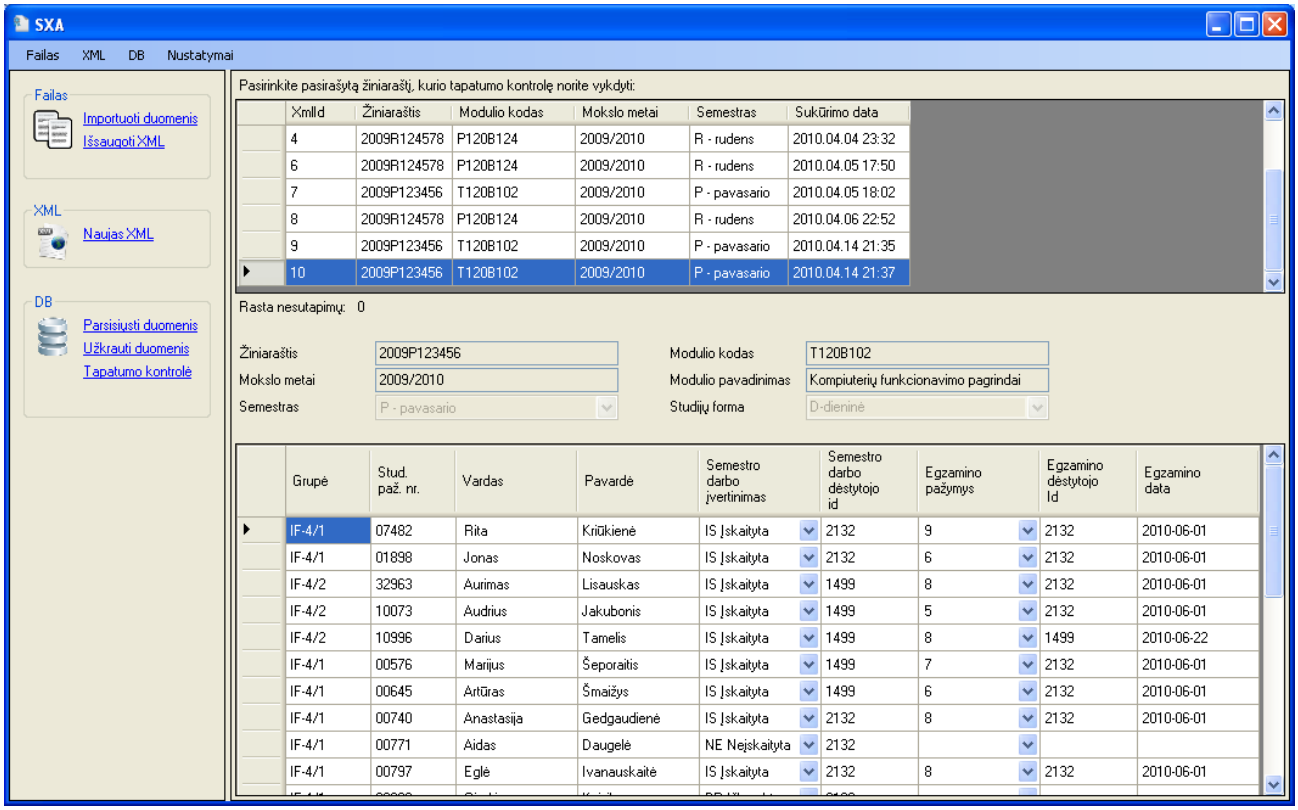
Duomenų sinchronizacijos vykdymas.

Duomenų sinchronizacijos metu, duomenys, saugomi akademinės informacijos DB pakeičiami, suvienodinami su reikšmėmis, saugomomis pasirašytame XML dokumente. Duomenų sinchronizacija vykdoma pasirinkus funkciją: „Sinchronizuoti duomenis“ (18 pav.). Pasirinkus sinchronizavimo funkciją, vartotojas įspėjamas apie būsimus veiksmus (21 pav.), o vartotojui patvirtinus savo pasirinkimą, žiniaraščio duomenys „AIS“ duomenų bazėje pakeičiami pagal saugomus pasirašytame XML dokumente.



21 pav. Duomenų sinchronizacijos patvirtinimas

Pakartotinai įvykdžius to paties žiniaraščio tapatumo kontrolę, nerandama nesutapimų, vadinasi sinchronizacija įvykdyta sėkmingai (22 pav.).



22 pav. Pakartotinė duomenų tapatumo kontrolė, po vykdytos sinchronizacijos

Sukurtos programinės įrangos pagalba pasirašius žiniaraštį su vieno studento įvertinimais, panaudojus XMLDSig standarto parašą, gaunamas xml dokumentas (23 pav.).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Statement Id="2009P123456">
  <AcademicYear>2009/2010</AcademicYear>
  <Semester>P - pavasario</Semester>
  <SubjectCode>T121B101</SubjectCode>
  <SubjectTitle>Kompiuterių elementai</SubjectTitle>
  <StudyForm>D-dieninė</StudyForm>
  <Students>
    <Student StudentCardId="00928">
      <GroupName>IF-4/1</GroupName>
      <StudentName> Dmitrijus</StudentName>
      <StudentSurname>Miškinas</StudentSurname>
      <SemesterWork>
        <SemesterEval>IS Įskaityta</SemesterEval>
        <SemesterLecturerId>2101</SemesterLecturerId>
      </SemesterWork>
      <Exam>
        <ExamMark>10</ExamMark>
        <ExamLecturerId>1499</ExamLecturerId>
        <ExamDate>2010-06-22</ExamDate>
      </Exam>
    </Student>
  </Students>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>BWTrOllBsbxtmf/hzl0rYZQBCr4=</DigestValue>
      </Reference>
    </SignedInfo>
<SignatureValue>T6JXWE71E5LP0vkKClyiU/JDQi7ejn1VhUlF/XXbmhxm3AX0H/zdSbpJcDKu5nO0opjt7wu3l8N3m+B
Z5cPvn3RTjcbHIFUqJvh+ttgtQ5u6A24QUGJ6O6eXDLMyCTW7XG5hSluBLQSEvYuR06+smF3u9gD/YTl2eSwN9tOlLjY=</
SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509IssuerSerial>
          <X509IssuerName>CN=SXA</X509IssuerName>
          <X509SerialNumber>109163669859787732389984170045939008721</X509SerialNumber>
        </X509IssuerSerial>
      </X509Data>
    </KeyInfo>
  </Signature>
</Statement>
```

23 pav. Sistemoje sukurto ir pasirašyto XML dokumento (XMLDSig standarto) pavyzdys

Pasirašius žiniaraštį su vieno studento įvertinimais, panaudojus XAdES-BES standarto parašą, gaunamas xml dokumentas (24 pav.).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Statement Id="2009P123456">
  <AcademicYear>2009/2010</AcademicYear>
  <Semester>P - pavasario</Semester>
  <SubjectCode>T121B101</SubjectCode>
  <SubjectTitle>Kompiuterių elementai</SubjectTitle>
  <StudyForm>D-dieninė</StudyForm>
  <Students>
    <Student StudentCardId="00928">
      <GroupName>IF-4/1</GroupName>
      <StudentName> Dmitrijus</StudentName>
      <StudentSurname>Miškinas</StudentSurname>
      <SemesterWork>
        <SemesterEval>IS Įskaityta</SemesterEval>
        <SemesterLecturerId>2101</SemesterLecturerId>
      </SemesterWork>
      <Exam>
        <ExamMark>10</ExamMark>
        <ExamLecturerId>1499</ExamLecturerId>
        <ExamDate>2010-06-22</ExamDate>
      </Exam>
    </Student>
  </Students>
  <Signature Id="S0" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#SignedProps" Type="http://uri.etsi.org/01903#SignedProperties">
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>gx+Bkm1DjyyzGV5v2nWKcy1e8ms=</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>BWTrOllBsbxtmf/hzl0rYZQBCr4=</DigestValue>
      </Reference>
    </SignedInfo>
<SignatureValue>gO+KCC4sl1tY3eKOp+Ar7myunNeKoJ3aJfIc6WQQ4TOIsbRzM0/larCpdEYeSY6WGpaucNGlZbRrw46
IbB96eRDFd7Fd7FEBI+XEsHtm5sq3w3vKE4FYO0U/WmPpRp2ir/zaHNJm1UaXJmP8ULiNf7SlnIPsKzOsw8kZi2uGMfQ=</
SignatureValue>
    <Object>
      <QualifyingProperties Target="#S0" xmlns="http://uri.etsi.org/01903/v1.1.1#">
        <SignedProperties Id="SignedProps">
          <SignedSignatureProperties>
            <SigningTime>2010-05-15T19:53:10.218Z</SigningTime>
            <SigningCertificate>
              <Cert>
                <CertDigest>
                  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
                  <DigestValue>v1MLnDYr7TysVc1TAGQJbCezGHM=</DigestValue>
                </CertDigest>
                <IssuerSerial>
                  <X509IssuerName>CN=SXA</X509IssuerName>
                  <X509SerialNumber>52202876C3F3B381480AB372DA3A44D1</X509SerialNumber>
                </IssuerSerial>
              </Cert>
            </SigningCertificate>
            <SignaturePolicyIdentifier />
          </SignedSignatureProperties>
          <SignedDataObjectProperties />
        </SignedProperties>
        <UnsignedProperties>
          <UnsignedSignatureProperties />
        </UnsignedProperties>
      </QualifyingProperties>
    </Object>
  </Signature>
</Statement>
```

24 pav. Sistemoje sukurto ir pasirašyto XML dokumento (XAdES-BES standarto) pavyzdys

Išvados.

Eksperimento metu panaudoti 2 XML parašų formavimo standartai: XMLDSig ir XAdES-BES. Remiantis atliktais skaičiavimais (27 lentelė) formuojant parašą pagal XAdES-BES standartą, tai atliekama vidutiniškai 1.096 karto ilgiau, nei formuojant parašą pagal XMLDSig standartą. Tai gali būti paaiškinama tuo, kad XAdES-BES atveju padaugėja atliekamų operacijų skaičius: papildomai įdedama nuoroda į <SignedProperties> elementą, todėl visam <SignedProperties> elementui skaičiuojama santrauka, kuri patenka tarp pasirašomų duomenų, taip pat skaičiuojama sertifikato, su kuriuo pasirašoma, santraukos funkcija ir generuojamas didesnis elementų skaičius.
Dėl papildomo XAdES parašo funkcionalumo išauga jo užimama vieta diske. Lyginant su XMLDSig standartu, vieno dokumento dydis vidutiniškai išauga 1.06KB, taigi, sukurtos programinės įrangos pagalba užkrovus 100000 XML dokumentų, XML dokumentams su XAdES-BES parašais, prireiktų apie 103MB daugiau vietos, nei XML dokumentams su XMLDSig parašais.
Tačiau XAdES standarto parašas turi privalumų prieš XMLDSig parašą: XAdES atveju pasirašomi naudoto sertifikato duomenys. Kaip minima literatūroje: „Sertifikatas yra pasirašomų savybių sąraše, kad nebūtų galima jo pakeisti kitu su tais pačiais raktais, tačiau skirtingais signataro rekvizitais ar skirtinga naudojimo paskirtimi (pvz., kai kurie universiteto darbuotojai yra ir dėstytojai, ir administratoriai). Tokio sukeitimo pavojus kyla sukompromitavus išdavėjo raktus. Apskritai vienodi raktai yra įprastas reiškinys, susijęs su didelėmis raktų generavimo sąnaudomis“.[14] Nors reiktų paminėti, kad XMLDSig atveju <KeyInfo> elemento informaciją taip pat įmanoma pasirašyti, įdėjus papildomą <Reference> elementą, rodantį į <KeyInfo> elementą.

Vienas pagrindinių XAdES parašo privalumų – galimybė pridėti papildomų elementų, tam tikroms parašo funkcijoms užtikrinti. Nagrinėjamu atveju svarbus išplečiamumas iki XAdES-T standarto. Kaip minėta analizės dalyje, XAdES-T standarto atveju prie dokumento pridedama laiko žyma, kuri gaunama iš tokią paslaugą teikiančio serverio. Ši žyma garantuotų parašo neišsiginamumą tam tikru laiko momentu, jeigu pasirašymo metu sertifikatas galiojo ir nebuvo atšauktų sertifikatų sąrašuose. Taigi XAdES-T parašas suteiktų galimybę ilgalaikiam xml dokumentų saugojimui, kadangi net ir pasibaigus sertifikato galiojimui, anksčiau pasirašyti dokumentai būtų laikomi galiojančiais. Laiko žyma gali būti dedama ne iš karto, o praėjus tam tikram laikui po pasirašymo.

Nepaisant šiek tiek didesnių laiko ir reikalaujamos atminties sąnaudų, kurių reikia XAdES parašui, dėl šio parašo privalumų pasirenkamas, ir sukurtoje programinėje įrangoje naudojamas būtent šis standartas.

Sukurtoje programinėje įrangoje yra galimybė importuoti duomenis iš XML failų. Šie failai gali būti sukurti su kita programine įranga, vienintelė sąlyga: jie turi atitikti XML schemą, saugomą „SXA“ duomenų bazėje. Būtent dėl šios importavimo galimybės ir paprastesnio suderinamumo su kita programine įranga, naudojamas įtrauktas (angl. enveloped) XML parašo tipas.

6. Išvados

1. Darbo metu išanalizuotos dokumentų valdymo sistemos bei XML duomenų tipo pasirašymo programinės įrangos paketai. Paaiškėjo dokumentų valdymo sistemų (DVS) siūlomi sprendimai, nustatyti trūkumai XML duomenų tipo apdorojimo ir pasirašymo srityse, taip pat įdiegus demonstracines XML pasirašymo programinės įrangos versijas, nustatyti naudojami XML parašų tipai ir parašų standartai.
2. Duomenų nekintamumo užtikrinimo duomenų bazėse problemai spręsti pasiūlytas sprendimas: į esamą sistemą integruojama papildoma Saugaus XML Archyvo (SXA) duomenų bazė, kurioje saugomi tie patys duomenys, kaip ir originalioje DB, tačiau pasirašytų XML dokumentų pavidalu. Tokiu atveju esama sistema ir jos duomenų bazė nekeičiama, o šalia sukuriama papildoma DB, vadinama SXA DB (Saugaus XML Archyvo DB) ir įdiegiama programinė įranga, skirta darbui su originalia sistemos DB ir naująja SXA DB.
3. Įdiegus pakeitimus esamoje sistemoje, viena duomenų kopija, kaip ir prieš pakeitimų įdiegimą, išsaugoma originalioje sistemos (akademinės informacijos sistemos „AIS“) DB, o kita duomenų kopija pasirašoma vartotojo skaitmeniniu parašu ir išsaugoma SXA duomenų bazėje. Atlikus bet kokius nesankcionuotus pakeitimus akademinės informacijos duomenų bazėje, jie pastebimi sulyginus duomenis su saugomais SXA DB. Atlikus bet kokius pakeitimus SXA duomenų bazėje, jie taip pat pastebimi, kadangi patikrinus parašą, matoma, kad jis neatitinka pasirašytų duomenų (parašas netikras).
4. Suprojektuota ir realizuota programinė įranga. Eksperimento metu sukurta PĮ pritaikyta darbui su XMLDSig ir XAdES-BES standartų parašais.
5. Pastebėta, kad XAdES-BES parašo generavimas užtrunka apytiksliai 10% ilgiau, lyginant su XMLDSig parašu, taip pat XAdES-BES parašas reikalauja apie 1.06 KB daugiau vietos nei XMLDSig. Tačiau naudojant XAdES-BES parašą, automatiškai pasirašoma naudojamo sertifikato informacija, todėl negalima pakeisti sertifikato į kitą, turintį identiškus raktus.
6. XAdES-BES parašo atveju gali būti pridėta laiko žyma, gauta iš šią paslaugą teikiančio serverio. Laiko žyma gali būti pridėta prie XML dokumento vėliau, t.y. praėjus tam tikram laikui po pasirašymo. Ši laiko žyma užtikrintų ilgalaikį pasirašytų XML dokumentų parašų galiojimą.
7. Dėl papildomo XAdES funkcionalumo ir lengvo išplečiamumo iki XAdES-T standarto parašo, pasirinktas XAdES standarto parašas.

7. Literatūra

[1]. Barauskas, V. Universali dokumentų valdymo sistema mažoms ir vidutinėms įmonėms: magistro darbas. [Interaktyvus] [žiūrėta 2009-01-18]. Prieiga per Internetą: <http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2006~D_20060112_051047-16407>

[2]. „Secret Key Exchange" [Interaktyvus] [žiūrėta 2009-01-18]. Prieiga per Internetą: <http://www.microsoft.com/technet/prodtechnol/windows2000serv/reskit/distrib/dsch_key_xihm.mspx?mfr=true>

[3]. Sakalauskas Eligijus et al. Kriptografinės sistemos. Kaunas, 2008. ISBN 978-9955-686-76-7.

[4] W3 konsorciumas. [Interaktyvus] [žiūrėta 2009-01-19] Prieiga per internetą: <http://www.w3.org/TR/xmldsig-core/>

[5] XML Digital Signature. [Interaktyvus] [žiūrėta 2009-01-18]. Prieiga per Internetą: http://java.sun.com/webservices/docs/2.0/tutorial/doc/XMLDigitalSignatureAPI7.html

[6] XML-Signature Syntax and Processing. [Interaktyvus] [žiūrėta 2009-01-19]. Prieiga per internetą: <http://tools.ietf.org/html/rfc3275>

[7] XML Signer. [Interaktyvus] [žiūrėta 2009-01-19]. Prieiga per Internetą: <http://www.signfiles.com/signxml.htm>

[8] Microsoft InfoPath® apžvalga. [Interaktyvus] [žiūrėta 2009-01-20]. Prieiga per Internetą: <http://www.microsoft.com/lietuva/office/infopath/prodinfo/overview.mspx>

[9] „About XML Signatures". [Interaktyvus] [žiūrėta 2009-01-20]. Prieiga per Internetą: <http://office.microsoft.com/en-gb/infopath/HP010967311033.aspx>

[10] „Statistica" document management system. [Interaktyvus] [žiūrėta 2009-01-20]. Prieiga per <Internetą: http://www.statsoft.com/products/documentmanagement.html>

[11] „doQuments 4.0" document management system. [Interaktyvus] [žiūrėta 2009-01-19]. Prieiga per Internetą: <http://doquments.en.softonic.com/>

[12] Sturis, R. Virtualios organizacijos dokumentų valdymo sistema: magistro darbas. [Interaktyvus] [žiūrėta 2009-01-20]. Prieiga per Internetą: <http://vddb.library.lt/obj/LT-eLABa-0001:E.02~2003~D_20040922_110119-93511>

[13] "DocLogix" dokumentų valdymo sistema. [Interaktyvus] [žiūrėta 2009-01-20]. Prieiga per <Internetą: http://www.doclogix.lt/index.php?mid=347&lang=lt>

[14] Sakalauskas, E.; Blažauskas, T.; Lukšys, K. Elektroninių dokumentų ir duomenų sauga. Kaunas, 2008.

[15] W3 konsorciumas. XMLDSig standartas. [Interaktyvus] [žiūrėta 2009-06-06]. Prieiga per internetą: <http://www.w3.org/TR/xmldsig-core/>

[16] W3 konsorciumas. XAdES standartas. [Interaktyvus] [žiūrėta 2009-06-06]. Prieiga per internetą <http://www.w3.org/TR/XAdES/>

[17] Microsoft WCF. [Interaktyvus] [žiūrėta 2009-06-08] Prieiga per internetą <http://msdn.microsoft.com/en-us/library/ms731082.aspx>

[18] WS security. [Interaktyvus] [žiūrėta 2009-06-06]. Prieiga per internetą <http://msdn.microsoft.com/en-us/library/ms977327.aspx>

[19] Vyšnauskaitė, R. Xml schemų sudarymo ir normalizavimo metodika: magistro darbas. [Interaktyvus] [žiūrėta 2009-01-19]. Prieiga per internetą: <http://vddb.library.lt/fedora/get/LT-eLABa-0001:E.02~2005~D_20050525_091727-93586/DS.005.0.02.ETD>

[20] „Digital Signature Support in InfoPath 2010", [Interaktyvus] [žiūrėta 2010-03-01]. Prieiga per internetą: <http://www.microsoftblog.co.in/?cat=376>

[21] Gudas A., „Elektroninio parašo standartai Lietuvoje", 10-osios Lietuvos jaunųjų mokslininkų konferencijos „Mokslas – Lietuvos ateitis" medžiaga. Vilnius, 2007.