VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ KATEDRA

Elektroninių dokumentų interoperabilumo Europos Sąjungoje tyrimas

Research into the interoperability of electronic documents within the European Union

Magistro baigiamasis darbas

Atliko: Markas Šišlo (parašas)

Darbo vadovas: doc. dr. Antanas Mitašiūnas (parašas)

Darbo recenzentas: doc. dr. Saulius Ragaišis (parašas)

Vilnius – 2016

PADĖKOS

Norėčiau išreikšti padėką savo darbo vadovui docentui daktarui Antanui Mitašiūnui už skirtą dėmesį ir suteiktą pagalbą viso tyrimo metu. Taip pat norėčiau padėkoti UAB „Asseco Lietuva“ organizacijai, ypatingai Programinių produktų departamento vadovui Jonui Juškiui, už suteiktą galimybę įgauti elektroninių parašų ir elektroninių dokumentų žinių, atliekant praktines užduotis.

SANTRAUKA

Šiame darbe yra nagrinėjama oficialių elektroninių dokumentų interoperabilumo Europos Sąjungoje problema. Elektroninių dokumentų interoperabilumo problema yra sprendžiama bendru atveju, kai elektroninis dokumentas yra sudaromas ir pasirašomas kelių ES šalių atstovų. Mokslinėje literatūroje yra pateiktas problemos sprendimo metodas: yra siūloma integruoti nacionalines elektroninių dokumentų platformas bei formuoti atskirus dokumento egzempliorius kiekvienai šaliai, tačiau šio metodo praktinio įgyvendinimo galimybių tyrimo rezultatai nėra skelbiami. Siekiant pagrįsti technologinio sprendimo galimumą, šiame magistro darbe buvo apibrėžta programų sistemos architektūra, suformuluoti reikalavimai sistemos išoriniams servisams, nustatytos sistemos įgyvendinimo sąlygos bei sukurtas elektroninių dokumentų sudarymo posistemės prototipas, pagrindžiantis pasiūlytos architektūros tinkamumą. Tyrimo metu gautos technologinio sprendimo įgyvendinimo žinios sudaro prielaidas elektroninių dokumentų tarpvalstybinio interoperabilumo tolimesniems tyrimams bei programinės įrangos plėtrai.

Raktiniai žodžiai: elektroninis dokumentas, oficialus elektroninis dokumentas, elektroninių dokumentų interoperabilumas, elektroninis parašas, elektroninių dokumentų nacionalinė platforma.

SUMMARY

In this thesis, the interoperability of official e-documents within the European Union is analysed. The general case of e-documents interoperability problem, when a single e-document is prepared and signed by multiple parties, is considered in this work. Scientific articles provide general principles to the solution: it is suggested to integrate national platforms of e-documents and create separate document exemplars for each signatory party; however, the feasibility studies of practical implementation of this approach are not published. In order to justify the feasibility of the technological solution, the system architecture, the requirements for external system services, and conditions for system implementation were presented in this master thesis. The prototype of e-documents creation subsystem, which justifies the feasibility of the proposed architecture, was implemented. The knowledge of technological solution implementation, gained during this research, provides conditions for the development of signing software and future research in the field of cross-border e-documents interoperability.

Keywords: e-document, official e-document, e-document cross-border interoperability, electronic signature, e-document national platform.

TURINYS

ĮVADAS

Dokumentai – yra daugelio organizacijų verslo procesų pagrindas [Pan08]. Dokumentai yra naudojami patvirtinant sprendimus ir fiksuojant veiklos rezultatus. Viešojo sektoriaus organizacijos naudoja oficialius dokumentus, kurie turi būti rengiami pagal šalies teisės aktų apibrėžtus reikalavimus. Per paskutinį dešimtmetį ES šalių narių valstybinių institucijų veiklos procesai perėjo į elektroninę erdvę, plačiai pradėtos naudoti specialios sistemos, skirtos oficialių dokumentų valdymui. Daugelyje ES šalių įvyko perėjimas prie oficialių elektroninių dokumentų naudojimo, buvo sukurtos specifikacijos, nustatančios reikalavimus oficialiems elektroniniams dokumentams [PRS11].

ES narių elektroninių dokumentų infrastruktūra buvo formuojama, remiantis nacionaline dokumentų valdymo teisėkūra. Valstybėse, kur elektroninių dokumentų platforma[1] buvo kuriama naujai, neprisirišant prie esamo paveldo, pavyko sukurti unikalią elektroninių dokumentų platformą [RBM+12, LPR09]. Kitose ES narėse, kur per kelis dešimtmečius įsigalėjo nusistovėję dokumentų tvarkymo principai, buvo panaudoti standartiniai elektroninių dokumentų naudojimo sprendimai [MB15]. Esamos nacionalinės elektroninių dokumentų platformos susiformavo šalių vidinių poreikių tenkinimui.

Šiandien ES teisės aktais yra siekiama panaikinti daugelį egzistuojančių kliūčių, trukdančių steigti verslą bei teikti arba gauti paslaugas kitose ES valstybėse, todėl tampa svarbu suteikti galimybes atlikti visas administracines procedūras elektroninėmis priemonėmis. Tačiau nacionalinės elektroninių dokumentų platformos nėra tam kurtos ir nėra pritaikytos. Todėl visai natūralu, kad jos netinka dokumentų naudojimui tarpvalstybiniu mastu. Oficialūs ES šalių elektroniniai dokumentai vaidina svarbų vaidmenį įgyvendinant elektroninės valdžios paslaugų tarpvalstybinį interoperabilumą, tačiau dėl nacionalinių elektroninių dokumentų specifikacijų skirtumų oficialių elektroninių dokumentų panaudojimas tarptautiniame kontekste yra komplikuotas, atsiranda taip vadinama Europos Sąjungos elektroninių dokumentų interoperabilumo problema [PRS11]. Ši problema yra viena iš pagrindinių kliūčių siekiant elektroninės valdžios paslaugų interoperabilumo, kas yra vienas iš ES strateginių tikslų [MB15]. Su elektroninių dokumentų interoperabilumo problema gali susidurti kiekvienas ES pilietis savo kasdieninėje veikloje, dėl šios problemos dažnai yra neįmanoma pasinaudoti informacinių technologijų teikiamais privalumais.

[1] Remiantis [MB15] straipsnyje pateikta medžiaga, nacionalinę elektroninių dokumentų platformą galima būtų apibrėžti kaip ES ir nacionalinių teisės aktų, standartų ir programinės įrangos visumą, kuri apibrėžia elektroninių dokumentų naudojimą šalies viduje.

Elektroninių dokumentų interoperabilumo problema turi kelis aspektus, sąlygojančius galimus problemos sprendimus. Jeigu būtų galimas problemos sprendimas teisinėmis priemonėmis, tai pakaktų Europos Sąjungoje nustatyti vieną standartinę elektroninio dokumento specifikaciją, pavyzdžiui, PDF formato pagrindu. Tačiau šalys turi skirtingas nacionalines teisėkūros sistemas ir jų suvienodinimo klausimas yra panašus į nacionalinių kalbų suvienodinimo klausimą, tai yra to tiesiog nereikia daryti.

Jeigu pakaktų tik patikrinti elektroninio dokumento parašų galiojimą, tai galima būtų apsiriboti skirtingų nacionalinių platformų dokumentų tikrinimo paslaugų sistemos įgyvendinimu arba pasinaudojimu dokumento sudarytojo pateiktomis darbo su tuo elektroniniu dokumentu priemonėmis ar paslaugomis. Esant daugiau sudarytojų, kiekvienas dokumento sudarytojas privalo disponuoti dokumento egzemplioriumi.

Kadangi grynai teisinis elektroninių dokumentų interoperabilumo sprendimas nėra galimas ir kadangi, kaip taisyklė, svarbiausi dokumentai yra rengiami kelių sudarytojų, šiame darbe yra ieškomas technologinis elektroninių dokumentų interoperabilumo problemos sprendimas, apimant visą elektroninių dokumentų gyvavimo ciklą ir esant kelių dokumento sudarytojų scenarijui.

Mokslinėse publikacijose [BBM+15, MR12] yra pateiktas metodas, kuris apibrėžia bendrus principus, kaip gali būti išspręsta elektroninių dokumentų interoperabilumo problema, taikant kelių pasirašančiųjų scenarijų. Tačiau netgi ir egzistuojant sprendimo metodui, atsakymas į klausimą „koks turi būti problemos technologinis sprendimas?“ nėra trivialus. Sprendimas turi būti pakankamai lankstus ir paprastas galutinio naudotojo atžvilgiu, bei įgalinti plečiamumą, t.y. naujų nacionalinių elektroninių dokumentų platformų palaikymą. Apibrėžiant technologinį sprendimą, turi būti atsižvelgta į tai, kad skirtingų šalių elektroninių dokumentų platformos yra didžiąja dalimi nesuderinamos, skiriasi reikalavimai elektroninio dokumento konteineriui, turininiu, metaduomenims. Tačiau iš kitos pusės, sprendimas neturi remtis vien tik nacionalinių elektroninių dokumentų paslaugų integravimu, turi būti siekiama minimizuoti veiksmų, kurie yra vykdomi nacionalinių elektroninių dokumentų paslaugų sistemų, aibę ir daugiau elektroninio dokumento sudarymo ir pasirašymo veiksmų vykdyti per centrinę sistemą. Šiame magistro darbe yra ieškomas elektroninių dokumentų interoperabilumo problemos technologinis sprendimas, kuris atsižvelgia į visas šias sąlygas.

Magistro **darbo tikslas** yra pagrįsti elektroninių dokumentų interoperabilumo Europos Sąjungoje problemos technologinio sprendimo galimumą, kad leisti kelių ES šalių atstovams sukurti ir pasirašyti bendrą oficialų elektroninį dokumentą ir pripažinti jį galiojančiu pagal kiekvienos šalies nacionalinės specifikacijos reikalavimus.

Tikslui pasiekti yra apibrėžti penki uždaviniai:

1. Išgryninti elektroninių dokumentų interoperabilumo problemą, jos kontekstą, priežastis ir esamą situaciją.
2. Ištirti problemos sprendimo strategijas, nustatyti tinkamiausius sprendimo metodus.
3. Nustatyti reikalavimus, kuriuos turi tenkinti elektroninių dokumentų interoperabilumo problemos technologinis sprendimas.
4. Apibrėžti elektroninių dokumentų interoperabilumo technologinio sprendimo architektūrą, reikalavimus išorinėms sistemos bei įgyvendinimo sąlygas.
5. Pagrįsti apibrėžto technologinio sprendimo įgyvendinamumą, realizuojant jo prototipą.

Magistro darbas yra sudarytas iš dviejų pagrindinių dalių: pirmoje – yra atliekama elektroninių dokumentų interoperabilumo problemos analizė, nagrinėjamos sprendimo strategijos, nustatomi reikalavimai technologiniams sprendimui; antroje dalyje yra pateikti technologinio įgyvendinamumo tyrimo rezultatai – sistemos apribojimai, programų sistemos architektūra, reikalavimai nacionalinėms elektroninių dokumentų sistemoms bei elektroninių dokumentų sudarymo posistemės prototipo aprašymas.

Didžiausią įtaką šiam elektroninių dokumentų interoperabilumo problemos Europos Sąjungoje sprendimo tyrimui turėjo A. Mitašiūno ir S. Ragaišio straipsnis „Elektroninių dokumentų interoperabilumo sprendimai akademinėje aplinkoje“ [MR12], kuriame yra pateikti elektroninių dokumentų interoperabilumo problemos sprendimo metodai esant kelių elektroninio dokumento sudarytojų scenarijui. Taip pat, vykdant technologinio įgyvendinamumo tyrimą, buvo atsižvelgta į praktinio įgyvendinamumo pagrindimo metodiką, kuri buvo naudojama ES pilotinio projekto SPOCS [SPOCS11] rėmuose.

1. ELEKTRONINIŲ DOKUMENTŲ INTEROPERABILUMO PROBLEMOS ANALIZĖ

1.1. Elektroninio dokumento sąvoka

Pradedant nagrinėti elektroninių dokumentų interoperabilumo problemą, svarbu yra išgryninti elektroninio dokumento sąvoką.

Pavyzdžiui, Europos Parlamento ir Tarybos reglamentas dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje [EPT14] apibrėžia elektroninį dokumentą kaip "bet kokį turinį, saugomą elektronine forma". Pagal šį apibrėžimą, elektroninis dokumentas gali būti tiek tekstas, tiek ir garso ar vaizdo įrašas. Ši sąvoka yra labai bendra; dažnai tam tikrų ES šalių teisėkūroje yra naudojamas siauresnis elektroninio dokumento apibrėžimas. Pavyzdžiui, pagal 2010 metų Lietuvos Respublikos archyvų ir dokumentų įstatymą [LRS10], elektroniniu dokumentu yra vadinamas "juridinio ar fizinio asmens norminių teisės aktų nustatyta tvarka informacinių technologijų priemonėmis sudarytas, patvirtintas ar gautas dokumentas, pasirašytas teisinę galią turinčiu elektroniniu parašu". Šiuo atveju elektroniniam dokumentui yra taikomi papildomi reikalavimai: dokumentas turi būti pasirašytas teisinę galią turinčiu elektroniniu parašu, o jo struktūra yra reglamentuojama teisės aktais. Tokio tipo reikalavimus tenkinantys elektroniniai dokumentai yra dažnai laikomi oficialiais elektroniniais dokumentais.

Svarbu yra išskirti dvi elektroninio dokumento sampratas: elektroninis dokumentas - kaip turinys, saugomas elektronine forma, ir oficialus elektroninis dokumentas – teisinę galią turintis elektroninis dokumentas, kuris yra prilyginamas rašytiniam pasirašytam dokumentui.

Elektroninio dokumento sąvoka šiame darbe yra naudojama siaurąja prasme, t.y. visur, kur yra vartojama sąvoka „elektroninis dokumentas“, yra laikoma, kad tai yra oficialus elektroninis dokumentas.

1.2. Elektroninių dokumentų interoperabilumo problemos sprendimo strategijos

Teisinę galią turintis dokumentas – tai pranešimas, kuris yra skirtas tam tikram adresatui, kuriam yra svarbūs dokumente užfiksuoti teisiniai santykiai. Dokumentai yra rengiami ne asmeniniam naudojimui, bet apsikeitimui su kitais. Todėl viena pagrindinių dokumento savybių yra jo interoperabilumas. Elektroninių dokumentų interoperabilumas – tai galėjimas perduoti elektroninį dokumentą iš pradinės aplinkos į adresato aplinką taip, kad adresato aplinkoje elektroninis dokumentas būtų priimtas ir pripažintas.

Egzistuoja dvi priešingos elektroninių dokumentų interoperabilumo strategijos:

- nacionalinių platformų **suvienodinimas** (unifikavimas), įgyvendinant bendrą elektroninių dokumentų platformą;
- egzistuojančių nacionalinių elektroninių dokumentų skirtingų platformų **integravimas** [RBM+12].

Šiuo metu Europos Sąjungoje dominuoja elektroninių dokumentų platformų unifikavimo kelias. Galutinis šios strategijos tikslas yra apibrėžti bendrus visoms šalims elektroninių dokumentų techninių artefaktų standartus (vieną arba kelis) ir sukurti bendrus įrankius darbui su šiuos standartus tenkinančiais elektroniniais dokumentais. Siekiant šio tikslo, yra sukurti tarpvalstybiniai elektroninių parašų formatų ir pasirašytų duomenų objektų bei jų parašų konteinerių standartai, kuriais įpareigota naudotis atliekant tarpvalstybinį apsikeitimą elektroniniais dokumentais. Pavyzdžiui, Europos Sąjungos teisės aktai [EK14] reikalauja iš valstybių narių priimti ir apdoroti elektroninius dokumentus pasirašytus CAdES, PAdES ir XAdES parašų formatais bei sudarytus pagal ASiC konteinerio specifikacija. Tačiau, nepaisant šių Europos Sąjungos iniciatyvų, elektroninių dokumentų interoperabilumo problema lieka aktuali, elektroninių dokumentų naudojimas tarpvalstybiniame lygmenyje yra gana ribotas.

Unifikavimo strategijos kritikai teigia, kad pagrindinis jos trūkumas yra nepilnas elektroninio dokumento esybės supratimas. Anot jų, elektroninio dokumento koncepcija turi atitikti rašytinio dokumento reikalavimus [BBM+15] tam, kad rašytinis ir elektroninis dokumentai turėtų vienodą teisinę galią. Todėl, kad elektroninis dokumentas yra ne tik techninis, bet ir teisinis artefaktas [MB15]. Bandymas spręsti elektroninių dokumentų interoperabilumo problemą technologinio sprendimo unifikavimo būdu, pritaikant pradinę ir adresato aplinkas vienam elektroninių dokumentų formatui, pavyzdžiui PDF, reikalauja ir teisinių normų unifikavimo, kas yra sunkiai įgyvendinama, nes kiekviena Europos Sąjungos narė turi suverenią teisę apibrėžti savo nacionalinius elektroninius dokumentus. Atsižvelgiant į tai, tampa aišku, kad interoperabilumo problema negali būti pilnai išspręsta suvienodinant nacionalines elektroninių dokumentų platformas.

Todėl yra siūloma kita elektroninių dokumentų interoperabilumo įgyvendinimo strategija – nacionalinių platformų integravimas. Aprašant šiuos strategijos principus, galima panaudoti tokią analogiją – nacionalinės elektroninių dokumentų platformos gali būti palygintos su skirtingomis kalbomis, kurios yra naudojamos įvairiose ES šalyse. Kiekviena šalis gali nepriklausomai pasirinkti savo valstybinę kalbą (arba kelias kalbas), analogiškai skirtingos valstybės savarankiškai apibrėžia savo nacionalines elektroninių dokumentų platformas. Tuo atveju, kai skirtingų šalių atstovai nori susikalbėti, jie neprivalo mokytis tam tikros vienos bendros kalbos, jie gali

pasinaudoti vertėjo pagalba. Taip pat, kai yra norima įgyvendinti skirtingų šalių elektroninių dokumentų platformų interoperabilumą, nėra būtina visas valstybes įpareigoti naudotis vienu bendru standartu, galima realizuoti centrinę elektroninių dokumentų sudarymo ir pasirašymo sistemą, per kurią vyktų komunikavimas tarp šalių nacionalinių platformų.

Galima teigti, kad integravimo strategija yra perspektyvesnis ir realistiškesnis būdas spręsti elektroninių dokumentų interoperabilumo problemą nei suvienodinimo strategija. Kituose apžvalgos skyriuose bus nagrinėjamos integravimo strategijos įgyvendinimo sąlygos bei metodai.

1.3. Elektroninių parašų ir elektroninių dokumentų reglamentavimas ES

Integravimo strategijos pagrindinis siekis yra integruoti nacionalines elektroninių dokumentų platformas, tačiau tai turi būti daroma atsižvelgiant į egzistuojančius tarptautinius standartus bei teisės aktus. Tarptautiniai standartai padeda apibrėžti principus, kuriais remiantis turi būti atliekami sukūrimo, pasirašymo ir tikrinimo veiksmai su skirtingų šalių elektroniniais dokumentais. Todėl svarbu yra nustatyti, kokie egzistuoja Europos Sąjungos teisės aktai ir juos įgyvendinantys standartai elektroninių dokumentų ir elektroninių parašų srityje.

1.3.1. Elektroninių parašų ir elektroninių dokumentų konteinerių standartai

Europos Parlamentas ir Taryba 1999 metų gruodžio 13 dieną išleido direktyvą „Dėl Bendrijos elektroninių parašų reguliavimo sistemos“ [EPT99], kuri nustato elektroninio parašo teisinį pripažinimą bei teisinius pagrindus skatinti elektroninio parašo interoperabilumą.

Direktyva apibrėžia saugaus elektroninio parašo sąvoką: „saugus elektroninis parašas – tai elektroninis parašas, atitinkantis šiuos reikalavimus:

a) vienareikšmiškai susijęs su pasirašančiu asmeniu;

b) leidžia nustatyti pasirašančio asmens tapatybę;

c) sukurtas priemonėmis, kurias pasirašantis asmuo gali kontroliuoti tik savo valia;

d) susijęs su pasirašytais duomenimis taip, kad bet koks šių duomenų pakeitimas yra pastebimas“ [EPT99].

Vienas svarbiausių Direktyvos teiginių yra tai, kad „saugūs elektroniniai parašai, paremti kvalifikuotais sertifikatais ir sukurti saugia parašo formavimo įranga[2], yra teisiškai lygiaverčiai rašytiniams parašams“ [EPT99].

Pagal Direktyvos elektroninių parašų standartizavimo iniciatyvą (EESSI) trys elektroninių parašų formatų standartai CAdES [ETSI12b], XAdES [ETSI10a] ir PAdES [ETSI09a] buvo sukurti įgyvendinant Direktyvos reikalavimus saugiems elektroniniams parašams.

[2] Tokie parašai yra dažnai vadinami „kvalifikuotais elektroniniais parašais“.

CAdES [ETSI12b] – tai standartas, aprašantis CMS (angl. Cryptographic message syntax) sintaksės praplėtimą, kad CMS sintaksė elektroninis parašas atitiktų saugaus elektroninio parašo reikalavimus. CMS – tai kriptografiškai apsaugotų pranešimų standartas. CAdES standartu pasirašyti duomenys gali būti saugomi tiek atskirai (atskirtasis) nuo parašo, tiek ir įtraukti į parašo objektą (apvelkantysis parašas).

XAdES standartas [ETSI10a] – tai XML parašo (angl. XML Signature) standarto [W3C13] apribojimų ir praplėtimų rinkinys, kad XML elektroninis parašas atitiktų saugaus elektroninio parašo reikalavimus. Egzistuoja trys XAdES elektroninio parašo ir pasirašomų duomenų išsidėstymo rūšys (elektroninio parašo topologijos): XAdES parašas gali būti saugomas atskirai nuo pasirašytų duomenų (atskirtasis parašas), įtrauktas į pasirašytą dokumentą (apvilktasis parašas) bei patys pasirašyti duomenys gali būti įtraukti į parašo XML struktūrą (apvelkantysis parašas).

PAdES standartas [ETSI09a] – tai PDF standarto (ISO 32000-1:2008 [ISO08]) apribojimų ir praplėtimų rinkinys, kad PDF parašas atitiktų saugaus elektroninio parašo reikalavimus. Skirtingai nuo CAdES ir XAdES, PAdES ne praplečia elektroninio parašo sintaksę, o nurodo reikalavimus dokumento konteineriui, kuriame yra saugomas elektroninis parašas.

2011 metais buvo išleistas ASiC elektroninių dokumentų konteinerių tarptautinis standartas [ETSI11a], kurio tikslas yra padidinti interoperabilumą tarp ES šalių, atliekant apsikeitimą elektroninių dokumentų konteineriais, sukurtais ZIP formato pagrindu.

Įsigaliojus elektroninių parašų ir ASiC konteinerio standartams ir pradėjus juos naudoti įgyvendinant nacionalines elektroninių dokumentų platformas, paaiškėjo, kad XAdES, CAdES, PAdES ir ASiC standartai gali būti ir yra interpretuojami skirtingais būdais. Todėl 2012 ir 2013 metais buvo išleisti šių standartų baziniai profiliai [ETSI12c, ETSI13a, ETSI13b, ETSI13c], kurie apibrėžia bendrą savybių rinkinį, kuriuo turi pasižymėti elektroniniai parašai ir ASiC konteineriai, kai jie yra naudojami tarpvalstybinių komunikacijų kontekste.

Europos Komisijos sprendimas 2014/148/EU [EK14] reikalauja, kad valstybės narės galėtų technologinėmis priemonėmis apdoroti elektroninius dokumentus pasirašytus XAdES, CAdES ir PAdES elektroniniais parašais arba apibrėžtus pagal ASiC standartą.

Šiuo atveju, svarbu yra atskirti elektroninio parašo, elektroninio dokumento konteinerio ir elektroninio dokumento sąvokas. Elektroninis parašas yra vienas iš elektroninio dokumento atributų, ir negali būti tapatinamas su elektroniniu dokumentu. Elektroninio dokumento konteineris apibrėžia konteinerio fizinę struktūrą, tačiau nenusako kitų elektroninio dokumento atributų (pavyzdžiui, turinio ir metaduomenų). Elektroninio dokumentų konteinerio ir elektroninių parašų standartai neapibrėžia pilnai elektroninio dokumento esybės. Iš to seka, kad elektroninių

parašų ir elektroninio dokumento konteinerio standartizavimas negali išspręsti elektroninių dokumentų interoperabilumo problemos, nes lieka nereglamentuotos kitos elektroninio dokumento dalys (turinys ir metaduomenys).

1.3.2. TSL sąrašai

Viena iš pirmųjų problemų, su kuriomis buvo susidurta, siekiant elektroninių dokumentų interoperabilumo Europos Sąjungoje, tapo elektroninių parašų tikrinimas tarpvalstybiniu mastu. Turi egzistuoti galimybė patikrinti elektroninio parašo, kuris buvo sukurtas kitos šalies piliečio, galiojimą. Pagrindiniu iššūkiu tapo sertifikatų leidėjų patikimumo nustatymas. Didelis skaičius sertifikatų paslaugų tiekėjų, kurie pradėjo veikti remiantis Parašų Direktyva [EPT99], lėmė chaotinę situaciją nustatant sertifikatų patikimumą. Problemos priežastis buvo sertifikatų išdavimo griežtų taisyklių, kurios būtų priimtos visų sertifikatų paslaugų teikėjų, stoka [PRS11].

Tam, kad palengvinti sertifikatų patikimumo nustatymą, Europos Komisija paskelbė sprendimą dėl Patikimų paslaugų būsenų sąrašo – TSL (angl. Trust Service Status List) paskelbimo [EK09]. Šį sąrašą sudaro prižiūrimų/akredituotų Sertifikatų paslaugų teikėjų patikimos paslaugos (pavyzdžiui, kvalifikuotų sertifikatų išdavimas arba sertifikato tikrinimas per OCSP protokolą). Sąraše yra nurodyti Patikimų paslaugų teikėjai, kurie teikdami savo paslaugas, veikia pagal pripažintą schemą. TSL sąrašai yra skelbiami XML ir PDF formatų failų pavidalu. XML formato TSL sąrašai gali būti automatiškai apdorojami ir gali būti įtraukti į elektroninio parašo tikrinimo sistemų lokalius Patikimų sertifikatų paslaugų teikėjų sąrašus.

Galima teigti, kad TSL sąrašų standartizavimas ir sukūrimas didžiąja dalimi išsprendė elektroninių parašų tarpvalstybinio tikrinimo problemą [MB15].

1.4. Elektroninių dokumentų tipai

Nacionalinių elektroninių dokumentų integravimo sprendimai negali būti įgyvendinti be tikslių žinių apie nacionalines platformas. Reikalavimai integravimo sprendimams tiesiogiai priklauso nuo palaikomų elektroninių dokumentų formatų aibės. Todėl svarbu yra suvokti Europos Sąjungoje naudojamų nacionalinių elektroninių dokumentų įvairovę, nustatyti jų skirtumus ir panašūmus, suklasifikuoti skirtingų šalių elektroninius dokumentus. Ši informacija yra svarbi siekiant nustatyti, kokių formatų elektroniniai dokumentai yra plačiausiai naudojami Europos Sąjungos šalyse, ir kokių formatų elektroniniams dokumentams turi būti teikiamas svarbiausias prioritetas įgyvendinant integravimo sprendimus.

Skirtingose ES valstybėse yra naudojami įvairių tipų elektroniniai dokumentai, skiriasi jų struktūra bei naudojimo būdai. Pavyzdžiui, A. Mitašiūnas ir A. Bykovskij skirsto elektroninius

dokumentus Europos Sąjungoje į penkis tipus (1 lentelė. Skirtingų elektroninių dokumentų tipų naudojimas ES šalyse [MB15]:

- Grindžiamus elektroninių parašų standartais;
- Grindžiamus programiniais produktais;
- Grindžiamus ISO standartizuotais dokumentų procesorių formatais;
- Grindžiamus ASiC specifikacija;
- Grindžiamus nacionalinėmis elektroninių dokumentų specifikacijomis.

1 lentelė. Skirtingų elektroninių dokumentų tipų naudojimas ES šalyse [MB15]

E-documents based on:				
Signature standards	Software products	ISO standardized formats of document processors	ASIC specification	National e-document specification
PKCS#7/CMS files **BG, IT, RO**, AT, CZ, DE, GR, HR, PL XMLDSig files **CZ**, DE XAdES files **EE** (DDOC), **ES, PL**, BG, DE, ES, LT CAdES files BG, DE, ES, IT, PL	Binary MS Office documents **BG, GR** XML-based documents LT, DE, PL	Signed PDF documents **AT, BG, CZ, FR, GB, GR, PL, PT**, BE, DE, DK, ES, HR, HU, IE, IT, LV, RO, SE, SI, SK Signed MS Office documents **BG**, FR, BE, CZ Signed Open Office documents BE, FR	ASiC approved as a national legal act **EE** (BDOC) ASiC-compliant documents BE	ASiC-based spec. **LT** (ADOC V2.0) ODF based spec. **LT** (ADOC-V1.0) PDF-based spec. **LT** (PDF-LT-V1.0), **AT** (PDF-AS) OOXML-based spec. **LV** (EDOC) XML-based spec. **ES** (documento-e), **HU** (e-szigno)

Kiekvieno tipo elektroniniai dokumentai pasižymi tam tikromis unikaliomis savybėmis. Pavyzdžiui, vienų elektroninių dokumentų naudojimas priklauso nuo konkretaus programinio produkto, kiti dokumentai yra savarankiškos esybės, kurios gali būti naudojamos skirtinguose kontekstuose. Taip pat skiriasi elektroninių dokumentų turinio struktūros sudėtingumas: vieni elektroniniai dokumentai gali saugoti turinį, sudarytą iš didelio skaičiaus priedų ir pridedamų dokumentų, kiti dokumentai palaiko tik primityvios struktūros turinį (pavyzdžiui, turinį sudarytą iš vienos XML formato rinkmenos). Toliau šiame darbe kiekvienas elektroninio dokumento tipas bus apžvelgtas detaliau.

1.4.1. Elektroniniai dokumentai, grindžiami elektroninių parašų standartais

Šio tipo elektroniniai dokumentai tiesiogiai remiasi elektroninių parašų standartais. Egzistuoja nemažai Europos Sąjungos šalių, naudojančių elektroninius dokumentus, kurių

struktūra tiesiogiai remiasi XAdES, CAdES arba XML-DSIG [W3C13] (standartas skirtas apibrėžti skaitmeninio parašo sukūrimo ir atvaizdavimo taisykles pagal XML sintaksę) bei CMS [IETF98] standartais (1 lentelė. Skirtingų elektroninių dokumentų tipų naudojimas ES šalyse [MB15]). Tokiuose dokumentuose pasirašyti duomenys yra dažnai įtraukti į elektroninio parašo struktūrą (apvelkantysis parašas) arba elektroninis parašas ir pasirašyti duomenys yra saugomi nepriklausomuose vieno XML failo elementuose (pavyzdžiui, tokie atskirti parašai yra naudojami Estijos DDOC [ASS04] dokumentuose).

Nacionaliniuose ir ES teisės aktuose dažnai yra pastebimas tam tikras neapibrėžtumas dėl elektroninio parašo ir elektroninio dokumento sąvokų. Nacionaliniuose teisės aktuose elektroninių dokumentų, grindžiamų elektroniniais parašais, formatai kartais yra apibrėžiami kaip elektroninių parašų formatai. Tačiau elektroninis dokumentas ir elektroninis parašas nėra ekvivalenčios esybės, koncepciniu požiūriu elektroninis dokumentas negali būti pakeistas elektroniniu parašu [MB15].

Nepaisant to, kad šio tipo elektroniniai dokumentai remiasi viešai pasiekiamais elektroninių parašų standartais, skirtingų šalių programiniai įrankiai gali nevienodai interpretuoti ir taikyti šiuos standartus. Todėl daugumos elektroninių parašų rinkmenų pilnas tikrinimas gali būti atliktas tik naudojantis ta pačia įranga, kuri buvo naudojama sukuriant šią rinkmeną [MB15].

1.4.2. Elektroniniai dokumentai, grindžiami programiniais produktais

Elektroniniai dokumentai, grindžiami programiniais produktais – tai dokumentai, kurie yra sukurti panaudojant nacionaliniu mastu pripažintą programinę įrangą. Dažniausiai tokių elektroninių dokumentų tikrinimas ir pasirašymas yra galimas tik panaudojant konkretų programinį produktą. Šio tipo elektroninių dokumentų specifikacijos yra uždaros, todėl elektroninių dokumentų interoperabilumas šalies viduje yra užtikrinamas per tam tikros programinės įrangos išplatinimą. Elektroninių dokumentų, grindžiamų programiniai produktais, tarpvalstybinis interoperabilumas yra komplikuotas dėl skirtingų įrankių ir standartų skirtingose šalyse.

Elektroninių dokumentų, grindžiamų programiniais produktais, specifikacijos pavyzdžiu gali būti Lietuvoje naudotos „Justa GE“ programinės įrangos specifikacija [SSC08]. Justa GE elektroninio dokumento struktūra remiasi XAdES elektroninių parašų standartu, tačiau esminis skirtumas nuo elektroninių dokumentų, grindžiamų elektroninių parašų standartais, yra tai, kad elektroninį dokumentą aprašanti specifikacija yra uždara. Todėl Justa GE elektroninių dokumentų naudojimas yra galimas tik disponuojant „Justa GE“ programine įranga.

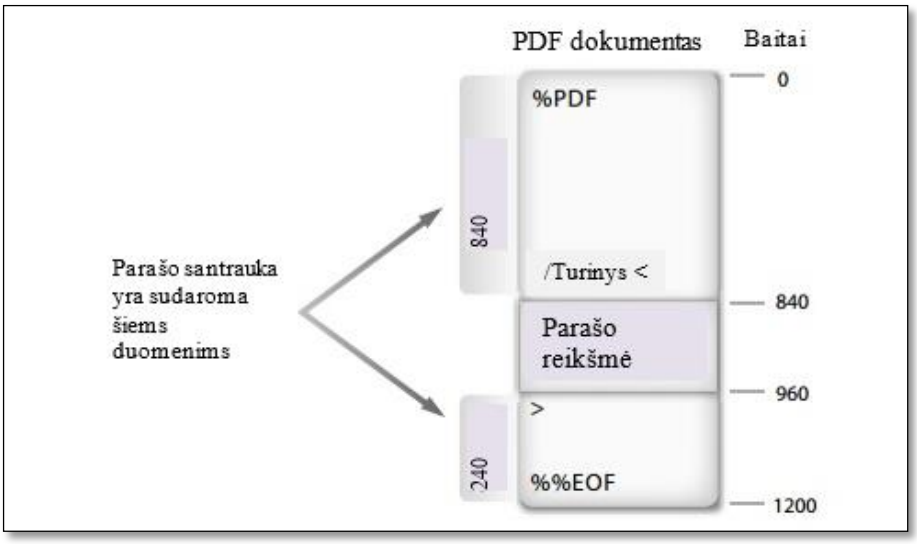
1.4.3. Elektroniniai dokumentai, grindžiami ISO standartizuotais dokumentų procesorių formatais

Elektroniniai dokumentai, grindžiami ISO standartizuotais dokumentų procesorių formatais – tai dokumentai, kurie gali būti peržiūrėti ir pasirašyti pasinaudojant tokiais ISO elektroninių dokumentų procesoriais, kaip Adobe PDF (standartas ISO 32000-1:2008 [ISO08]), MS Word ir Open Office.

Labiausiai paplitęs Europos Sąjungos šalyse yra pasirašomų PDF elektroninių dokumentų formatas (1 lentelė. Skirtingų elektroninių dokumentų tipų naudojimas ES šalyse [MB15]]). Pagrindinės to priežastys yra tai, kad:

- PDF formatas yra nepriklausomas nuo operacinės sistemos, programinės ir techninės įrangos;
- PDF dokumentai yra naudojami kaip popierinių dokumentų analogai;
- Egzistuoja didelis skaičius laisvai pasiekiamų PDF apdorojimo programų;
- PDF dokumentai yra plačiai naudojami verslo srityje.

Pasirašytas elektroninis dokumentas turi tokią sandarą (1 pav. PDF dokumento elektroninio parašo sudarymas [ISO08]): parašas ir elektroninį parašą aprašantys duomenys yra saugomi PDF dokumento duomenų struktūroje, kuri yra vadinama parašo žodynu (angl. signature dictionary). Parašo reikšmė yra užkoduota elektroninio parašo dvejetainio objekto pavidalu, kuris yra apibrėžtas panaudojant kriptografinių pranešimų sintaksę arba susijusius formatus (pavyzdžiui, PKCS#7 [IETF98] arba CAdES [ETSI09a]). Sudarant elektroninį parašą, yra formuojama pasirašomų rinkmenos dalių santrauka. PDF atveju, kai parašas yra integruotas į dokumentą, santrauka yra sudaroma iš visos rinkmenos duomenų, išskyrus pačią parašo reikšmę.



1 pav. PDF dokumento elektroninio parašo sudarymas [ISO08]

PAdES [ETSI09b] – tai standartas, kuris detalizuoja elektroninio parašo saugojimo PDF dokumente aspektus. Pavyzdžiui, pagal PAdES standartą PDF dokumente elektroniniai parašai yra saugomi pagal CAdES [ETSI09a] standarto reikalavimus.

Teoriškai elektroniniai dokumentai, grindžiami ISO standartizuotais dokumentų procesorių formatais, gali būti nagrinėjami, kaip alternatyva spręsti elektroninių dokumentų interoperabilumo problemos standartizavimo keliu. Tačiau PDF, MS Word ir Open Office dokumentų standartai, neapibrėžia reikalavimų elektroniniams dokumentams. Todėl, tiktai naudojantis specialia programine įranga, galima atlikti skirtingų šalių PDF elektroninių dokumentų pasirašymą bei tikrinimą. Iš to seka, kad elektroninių dokumentų, grindžiamų ISO standartizuotais dokumentų procesorių formatais ir elektroninių dokumentų, grindžiamų programiniais produktais, tarpvalstybinio interoperabilumo galimybės yra beveik ekvivalenčios.

Šią situaciją gerai iliustruoja Austrijos elektroniniai dokumentai PDF-AS, kurie turi unikalias savybes, tokias kaip pasirašančio asmens vizualus parašo blokas (2 pav. Austrijos vizualus elektroninio parašo blokas [LPR10]). Šis blokas, yra naudojamas tam, kad suteikti galimybę patikrinti elektroninio dokumento popierinės kopijos tikrumą. Parašo blokas yra sudarytas iš logotipo, skaitmeninio parašo reikšmės, pasirašančiojo informacijos, nuorodos į parašo tikrinimo pasaugų servisą ir kitų parašo atributų. Nepaisant to, kad PDF-AS elektroninis dokumentas yra sukurtas remiantis atvira PDF specifikacija, tačiau šių elektroninių dokumentų tikrinimas ir pasirašymas gali būti vykdomas tik pasinaudojant specializuota programine įranga, kuri atsižvelgia į vizualaus parašo bloko egzistavimą.

Parašo reikšmė	pzqm4cIZNMe0GQ8Z3PNDNmZprqVpkVWTrJ1Lva6gwRXXgfynXN6wLUcZuprm7Mco	
SIGNATURINFORMATIONEN A-SIT Herbert Leitold	Pasirašantis asmuo	Herbert Leitold
	Data/laikas	2009-10-26T00:11:27Z
	Išdavėjo sertifikatas	C=AT,O=Hauptverband ðsterr. Sozialvers.,CN=VSig CA 2
	Serijinis nr.	171850794265883555445726185650817446368O1
	Metodas	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parametras	etsi-bka-1.001256515887-4157159809854-19618-0-6356-13943
Patikrinimas	Validavimo servisas:	http://www.signature-verification.gv.at

2 pav. Austrijos vizualus elektroninio parašo blokas [LPR10]

1.4.4. Elektroniniai dokumentai, grindžiami ASiC specifikacija

Elektroniniai dokumentai, grindžiami ASiC specifikacija – tai elektroniniai dokumentai, kurių struktūra tiesiogiai remiasi ASiC konteinerio standartu [ETSI12a].

ASiC standartas apibrėžia ZIP konteinerio struktūrą, siekiant nustatyti bendrą būdą susieti duomenų objektus su saugiais elektroniniais parašais arba laiko žymomis. Duomenys ASiC konteineryje gali būti pasirašyti CAdES arba XAdES formatų atskirtaisiais elektroniniais parašais (angl. detached electronic signatures).

ASiC standartas apibrėžia du konteinerių tipus: paprastąjį (ASiC-S) ir išplėstinį (ASiC-E). Paprastasis ASiC konteineris (ASiC-S) susieja vieną ar daugiau elektroninių parašų su vienu duomenų objektu. Išplėstinis ASiC konteineris (ASiC-E) palaiko kelių duomenų objektų pasirašymą, kurių kiekvienas gali būti pasirašytas vienu ar daugiau elektroninių parašų. Su kiekvienu duomenų objektu gali būti susieti atitinkami metaduomenys, kurie gali būti apsaugoti konteineryje saugomais parašais. ASiC-E tipo konteineris gali būti suprojektuotas keliais būdais: draudžiant visas paskesnes konteinerio modifikacijas arba leidžiant papildomų duomenų objektų ir parašų įtraukimą į konteinerį, nepažeidžiant ankstesnių parašų.

Svarbu yra pažymėti, kad ASiC standartas neapibrėžia reikalavimų pasirašomų rinkmenų formatui. Tačiau norint turėti galimybę vizualizuoti elektroninį dokumentą, yra būtina apriboti dokumento turinio formatų aibę – pavyzdžiui, naudoti tik ISO standartizuotus formatus. Taip pat ASiC standartas neaprašo reikalavimų dokumento metaduomenims. Neturint, pavyzdžiui, dokumento registracijos duomenų (registracijos numerio ir datos) dažnai yra neįmanoma užtikrinti elektroninio dokumento teisinės galios. Taigi, koncepciniu požiūriu, elektroninio dokumento konteineris negali pilnai apibrėžti elektroninio dokumento [MB15].

Elektroninių dokumentų, grindžiamų ASiC specifikacija, pavyzdžiu gali būti Estijos BDOC V2.1 [ECS14] elektroniniai dokumentai. BDOC V2.1 specifikacija buvo sukurta verslui Baltijos šalyse, o Estijoje yra naudojama, kaip oficiali. BDOC V2.1 konteinerio struktūra atitinka išplėstinio ASiC konteinerio su XAdES parašu reikalavimus. Tačiau, kaip ir ASiC konteinerio standartas, BDOC V2.1 specifikacija nepateikia reikalavimų elektroninio dokumento turiniui bei dokumento metaduomenims.

1.4.5. Elektroniniai dokumentai, grindžiami nacionalinėmis elektroninių dokumentų specifikacijomis

Elektroninių dokumentų, grindžiamų nacionalinėmis specifikacijomis, struktūra yra aprašyta detaliomis nacionalinėmis specifikacijomis. Svarbu pažymėti, kad šio tipo elektroniniai dokumentai yra skirtingos struktūros – tai gali būti tiek ZIP, tiek PDF, tiek ir XML formato rinkmenos. Tačiau bendra yra tai, kad šių dokumentų visos trys pagrindines sudedamosios dalys (elektroninio dokumento turinys, dokumento metaduomenys ir elektroninis parašas) yra standartizuotos.

Elektroninio dokumento turinys – tai elektroninio dokumento dalis, kurioje tekstine, vaizdine ar kitokia forma pateikiama informacija [LAD06]. Reikalavimai elektroninio dokumento turiniui skirtingose šalyse nėra vienodi. Vienos specifikacijos griežtai apriboja elektroninio dokumento turinio formatų aibę (Lietuvos elektroniniai dokumentai ADOC-V1.0 [LAD09] ir ADOC-V2.0 [LVA14b]), tuo tarpu kitos specifikacijos leidžia įtraukti į elektroninį dokumentą bet

kokio formato turinio rinkmenas (Vengrijos „e-Dossier“ [Mic11] ir Latvijos EDOC-V2.0 [EUSO14] specifikacijos). Skiriasi ir įvairių šalių elektroninių dokumentų turinio struktūra. Pavyzdžiui, ADOC specifikacijos turinio rinkmenos yra skirstomos į tris tipus: pagrindinis turinys, dokumento priedai ir pridedami elektroniniai dokumentai, tuo tarpu Vengrijos „e-Dossier“ ir Latvijos EDOC-V2.0 specifikacijos palaiko tik vienos rūšies (pagrindinio turinio) rinkmenas.

Elektroninio dokumento metaduomenys apibrėžia dokumento sandarą, formatą ir aprašo viso dokumento gyvavimo ciklo įgyvendinimą: sudarymą, naudojimą ir saugojimą. Metaduomenų pavyzdžiai yra dokumento kūrėjo, dokumento tipo, dokumento autentifikavimo ir tikrinimo informacija. Nacionalinės elektroninių dokumentų specifikacijos skirtingais būdais apibrėžia metaduomenis elektroniniame dokumente. Jeigu Lietuvos elektroniniai dokumentai (ADOC-V1.0, ADOC-V2.0 ir PDF-LT [LVA14a]) turi griežtai apibrėžtą metaduomenų struktūrą, tai Latvijos EDOC-V2.0 specifikacijos dokumentų metaduomenų aibė gali būti plečiama per naudotojo sukurtus metaduomenų šablonus.

Elektroninis parašas – tai duomenys, kurie yra prijungiami ar logiškai susiejami su dokumento turiniu bei metaduomenimis ir yra naudojami elektroninio dokumento teisinės galios patvirtinimui. Elektroninio dokumento formatas nustato, kokio standarto elektroniniai parašai yra naudojami. Jeigu elektroninis dokumentas yra sudarytas XML rinkmenos (Vengrijos „e-Dossier“ specifikacija) arba ZIP konteinerio (Lietuvos ADOC-V1.0 ir ADOC-V2.0 bei Latvijos EDOC-V2.0 specifikacijos) pagrindu, tai elektroninis parašas yra XAdES standarto [ETSI10a]. Tais atvejais, kai elektroninio dokumento specifikacija remiasi PDF formatu (Lietuvos PDF-LT specifikacija), yra naudojamas PAdES [ETSI09a] standarto elektroninis parašas.

Svarbiausi elektroninių dokumentų specifikacijų pavyzdžiai yra Lietuvos ADOC ir PDF-LT specifikacijos. Daugelyje mokslinių straipsnių [BBM+15, MR12, MB15, RBM+12] šios specifikacijos yra pateikiamos kaip pavyzdys, kaip standartizavimo keliu galima pasiekti elektroninių dokumentą interoperabilumą šalies viduje.

ADOC specifikacija – tai teisės aktas, kuris apibrėžia elektroninio dokumento formato bei reikalavimus ADOC dokumentų kūrimo ir tikrinimo programinei įrangai. ADOC dokumentas gali būti sukurtas naudojantis bet kokia programine įranga, kuri palaiko ADOC formato dokumento sudarymą. Tokiu atveju yra įgyvendinamas principas, kad „elektroninio dokumento apibrėžimas yra svarbesnis nei programinio produkto kūrimas“ [MB15].

PDF-LT specifikacija išskiria iš pasirašytų PDF dokumentų aibės poaibį PDF dokumentų, kurie atitinka Lietuvos elektroninio dokumento reikalavimus. Kitais žodžiais, PDF-LT specifikacija nurodo, kokie PDF dokumentai yra elektroniniai dokumentai. Pavyzdžiui, PDF-LT

specifikacija reikalauja, kad PDF dokumentas atitiktų PDF/A-2 standartą, taip pat PDF-LT konteineryje turi būti saugomi elektroninio dokumento metaduomenys [LVA14a].

1.5. Elektroninių dokumentų platformų integravimo sprendimai

Keli plačios apimties pilotiniai projektai buvo įgyvendinti Europos Sąjungoje, kurių vienas iš tikslų buvo surasti optimaliausius elektroninių dokumentų interoperabilumo sprendimus. Vienas iš tokių pilotinių projektų buvo SPOCS projektas. Šis projektas yra svarbus tuo, kad jo rėmuose buvo įgyvendinti nacionalinių elektroninių dokumentų platformų integravimo sprendimai.

SPOCS pilotinis projektas yra skirtas įgyvendinti Paslaugų direktyvos [EPT06] reikalavimus. Beveik kiekviena transakcija SPOCS projekto rėmuose reikalauja elektroninių dokumentų panaudojimo, todėl viena iš projekto užduočių buvo sukurti interoperabilią platformą, reikalingą tarpvalstybiniam apsikeitimui elektroniniais dokumentais. Įgyvendinant šią užduotį, buvo išleista specifikacija, kurioje pateikiama daugiasluoksnio elektroninių dokumentų konteinerio formato koncepcija [SPOCS11]. Formato pavadinimas – OCD (angl. Omnifarious Container for eDocuments). Konteinerio viduje yra saugomi skirtingų formatų elektroniniai dokumentai kartu su jų kontekstine informacija (metaduomenimis). Tiek visas konteineris, tiek atskiri jo elementai gali būti pasirašyti elektroniniu parašu. Daugiasluoksnis elektroninio dokumento konteineris – tai tarsi pasirašytas vokas, į kurį galima įdėti skirtingo formato elektroninius dokumentus, kurių turinys ir struktūra yra aprašyti pagal apibrėžtą formą.

Elektroninių dokumentų interoperabilumo problemos kontekste yra svarbus OCD konteinerio turinio dalies (įdėtų elektroninių dokumentų) tikrinimo procesas. Į OCD konteinerį gali būti įtraukti dviejų rūšių elektroniniai dokumentai: OCD konteinerio elektroninių dokumentų formatai, pasirašyti XAdES, CAdES arba PAdES elektroniniais parašais, arba nacionalinių specifikacijų elektroniniai dokumentai. Nacionaliniai elektroniniai dokumentai yra tikrinami panaudojant papildomus modulius, kurie gali būti pridėti dinamiškai, neatliekant bazinio programinio kodo pakeitimų.

SPOCS konteineryje saugomų elektroninių dokumentų tikrinimas vyksta tokia tvarka: pagal OCD metaduomenyse saugomą informaciją (elektroninio dokumento identifikatorius ir turinio tipas (angl. content-type)), kiekvienam konteineryje esančiam elektroniniam dokumentui yra tikrinama ar egzistuoja išorinė tikrinimo paslauga, atliekanti parašų galiojimo tikrinimą konkretaus tipo dokumentui. Jeigu tokia išorinė paslauga egzistuoja – yra vykdoma užklausa, pateikiamas OCD konteinerio turinys. Išorinė verifikavimo paslauga atlieka dokumento galiojimo tikrinimą ir grąžina rezultatą (pranešimą apie sėkmingą tikrinimą arba klaidą). Tuo atveju, kai konkrečiam dokumentui išorinės tikrinimo paslaugos neegzistuoja, yra naudojamos vidinės tikrinimo

paslaugos. Taip pat yra tikrinamas pasirašiusio asmens sertifikato autentiškumas. Yra nustatoma: ar sertifikato leidėjo sertifikatas yra įtrauktas į lokaliai saugomų patikimų sertifikatų sąrašą. Jeigu ne, tai tikrinamas sertifikato leidėjo egzistavimas konkrečios šalies Patikimų paslaugų sąraše (TSL).

SPOCS projekto rėmuose buvo išdėstyti elektroninių dokumentų tikrinimo interoperabilumo problemos sprendimo baziniai principai (tokie kaip nacionalinių servisų naudojimas elektroninio dokumento tikrinimui bei jų integravimas per centrinę sistemą). Taip pat, remiantis šiais principais, buvo sukurtas prototipas, kuris patvirtina pateikto sprendimo įgyvendinamumą.

1.6. Interoperabilumo problemos sprendimo metodai

Priklausomai nuo elektroninių dokumentų naudojimo atvejų, gali egzistuoti skirtingi elektroninių dokumentų interoperabilumo problemos sprendimo metodai. Mokslinėse publikacijose yra išskiriami dviejų tipų elektroninių dokumentų interoperabilumo sprendimai integravimo būdu – „vieno dokumento“ ir „atskirų egzempliorių“ metodai [BBM+15, MR12].

„Vieno dokumento“ metodas yra taikomas tais atvejais, kai yra vienas elektroninio dokumento sudarytojas, kuris pristato dokumentą į kitą šalį. Sudarytojas turi pateikti elektroninio dokumento gavėjui darbo su tuo dokumentu priemones ar paslaugas (tikrinimo, peržiūros ir turinio paėmimo paslaugas). Šis interoperabilumo problemos sprendimas yra pakankamai palankus šalims, kurios turi išvystytą nacionalinę elektroninių dokumentų platformą – sprendimo įgyvendinimas nereikalauja papildomų pastangų. Tačiau esminė šio sprendimo problema – tai būtinybė įtraukti užsienio šalių nacionalinių formatų palaikymą į dokumentų valdymo sistemas. Tokiu būdu, norint įgyvendinti užsienio elektroninių dokumentų vientisumą, autentiškumą, neišsigynimą bei galimybę naudoti ir saugoti juos ilgą arba begalinį laikotarpį, reikia integruoti užsienių šalių platformų paslaugas į dokumentų valdymo sistemas, ką realizuoti Europos Sąjungos mastu, esant dideliam nacionalinių platformų skaičiui, yra komplikuotas uždavinys. Todėl sistemoje gali būti saugomi tik trumpo galiojimo dokumentai, kas neleidžia pasinaudoti elektroninių dokumentų privalumais [MR12].

„Atskirų egzempliorių“ metodas yra taikomas tada, kai vienas elektroninis dokumentas turi būti pasirašytas skirtingų šalių atstovų. Šio atveju yra parengiami elektroninių dokumentų egzemplioriai pagal kiekvienos šalies nacionalinės elektroninių dokumentų platformos reikalavimus ir kiekvienas iš šių egzempliorių yra pasirašomas visų šalių atstovų. Kiekvienas iš pasirašytų dokumentų yra teisiškai galiojantis atitinkamo atstovo šalyje, nes elektroninis dokumentas yra išsaugotas šios šalies formatu ir šalys turi programinius įrankius darbui su savo

oficialiais elektroniniais dokumentais. Pagrindinis šio sprendimo privalumas yra tai, kad šalims, kurios dalyvavo dokumento sudaryme, nereikia palaikyti kitų šalių dokumentų formatų [MR12].

Galima teigti, kad „atskirų egzempliorių“ metodas yra perspektyviausiais būdas spręsti elektroninių dokumentų interoperabilumo problemą esant kelių dokumento sudarytojų ir pasirašančiųjų scenarijui [BBM+15]. Tačiau moksliniuose straipsniuose aprašomos yra tiktai sprendimo idėjos remiantis „atskirų egzempliorių“ metodu, praktinis sprendimo įgyvendinimas nėra aprašytas [MB15]. Pagrindinė užduotis yra pagrįsti galimumą tokio technologinio sprendimo, kuris būtų pakankamai lankstus ir paprastas atlikti kasdienines tarpvalstybinių elektroninių dokumentų sukūrimo ir pasirašymo operacijas.

1.7. Reikalavimai technologiniam sprendimui

Egzistuoja moksliniai straipsniai, pavyzdžiui [BBM+15], kuriuose yra aprašomi principiniai reikalavimai elektroninių dokumentų interoperabilumo problemos technologiniam sprendimui, kuris remiasi „atskirų egzempliorių“ metodu.

Sprendimo įgyvendinimas reikalauja pateikti naudotojo sąsają, per kurią gali būti pasirinktos:

1) šalys, kurios dalyvauja elektroninio dokumento pasirašyme;

2) elektroninių dokumentų specifikacijos, kurias palaiko nacionalinė elektroninių dokumentų platforma.

Kiekvienas elektroninio dokumento egzempliorius turi būti pasirašytas kiekvienos pasirašančiosios šalies. Kiekvienas pasirašantysis pasirašo visus dokumento egzempliorius vieną kartą aktyvuodamas savo saugų parašo kūrimo įrankį. Pasibaigus pasirašymo procedūrai, visos pasirašančiosios šalys gauna dokumento egzempliorių, atitinkantį nacionalinės elektroninių dokumentų platformos reikalavimus.

Turi būti palaikomas ASiC arba PDF/PAdES standartus atitinkančių elektroninių dokumentų konteinerių sudarymas bei pasirašymas. PDF/PAdES standartus atitinkantys elektroninių dokumentų konteineriai yra labiausiai paplitę ES šalyse [MB15] ir yra naudojami paprasto turinio dokumentams. ASiC standartas yra pagrindinis standartas Europos Sąjungoje, naudojamas sudėtingos turinio struktūros elektroniniams dokumentams sudaryti.

Pagal mokslinėje literatūroje publikacijose [MR12, BBM+15] pateiktą „atskirų egzempliorių“ metodo aprašymą buvo sudarytas struktūrizuotas kelių lygių reikalavimų technologiniam sprendimui sąrašas:

1. Parengti elektroninio dokumento egzempliorius pagal nacionalinių specifikacijų reikalavimus.
   1.1. Elektroninių dokumentų egzemplioriai privalo turėti vienodą turinį.

1.2. Elektroninių dokumentų egzempliorių metaduomenys turi būti užpildyti pagal nacionalinių specifikacijų reikalavimus.
1.3. Turi būti galimybė sudaryti skirtingų konteinerio tipų (ASiC ir PDF) elektroninio dokumento egzempliorius.
1.4. Turi egzistuoti galimybė praplėsti palaikomų nacionalinių specifikacijų aibę.
1.5. Elektroninių dokumentų egzemplioriai turi būti tinkami ilgalaikiam saugojimui.

2. Pasirašyti elektroninio dokumento egzempliorius, parengtus pagal nacionalinių specifikacijų reikalavimus.
2.1. Privatus raktas, vykdant pasirašymo veiksmą, turi būti aktyvuojamas tik vieną kartą.
2.2. Po pasirašymo elektroninių dokumentų egzemplioriai turi atitikti nacionalinių specifikacijų reikalavimus.
2.3. Turi būti galimybė pasirašyti skirtingų konteinerio tipų (ASiC arba PDF) elektroninio dokumento egzempliorius.

Kitame šio magistro darbo skyriuje bus pateiktas technologinis sprendimas, kuriuo yra siekiama pagrįsti šių reikalavimų įgyvendinamumą.

2. TECHNOLOGINIO SPRENDIMO PRAKTINIS ĮGYVENDINIMAS

Remiantis moksliniuose šaltiniuose pateikta informacija, buvo sudaryti reikalavimai elektroninių dokumentų interoperabilumo problemos technologiniam sprendimui (1.7. Reikalavimai technologiniam sprendimui). Šiame skyriuje yra siekiama atsakyti į klausimą: kaip šie reikalavimai gali būti įgyvendinti? Tuo tikslu yra pasiūlyti architektūriniai sprendimai, nustatytos technologinio sprendimo apribojimai.

2.1. Praktinio įgyvendinimo tyrimo pavyzdys

Atliekant praktinio įgyvendinimo tyrimą, svarbu yra atsižvelgti į tai, kaip kituose elektroninių dokumentų interoperabilumo tyrimuose buvo pagrindžiamas technologinio sprendimo galimumas. Todėl buvo išnagrinėtos SPOCS projekto [SPOCS11] veiklos, kurios buvo atliktos siekiant pagrįsti praktinį technologinio sprendimo įgyvendinamumą.

SPOCS projekto rėmuose buvo vykdomas interoperabilios tarpvalstybinės elektroninių dokumentų apsikeitimo platformos praktinio įgyvendinimo tyrimas. Buvo tiriamos bendros Europos Sąjungos elektroninio dokumentų apsikeitimo platformos realizavimo galimybės.

Pagrindinės tyrimo užduotys buvo:

- Apibrėžti elektroninio dokumento konteinerio bendrą specifikaciją, kuri įgalintų tarpvalstybinį apsikeitimą elektroniniais dokumentais.
- Sukurti programinę įrangą, palaikančią šios specifikacijos dokumentų sudarymą bei tikrinimą.

Siekiant nustatyti reikalavimus elektroninio dokumento konteinerio bendrai specifikacijai, pirmiausia, buvo surinkta informacija apie skirtingose ES šalyse šiuo metu naudojamus elektroninių dokumentų formatus. SPOCS projekte dalyvavusios valstybės narės ir kiti partneriai turėjo pranešti, kokius elektroninių dokumentų formatus bei kokias pasirašymo technologijas jie naudoja.

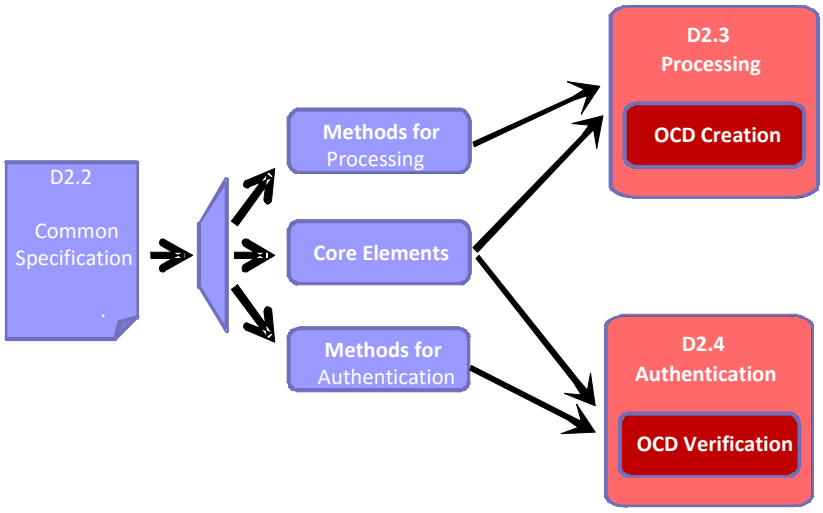
Kitame žingsnyje, pateikti elektroninių dokumentų formatai ir technologijos buvo įvertinti ekspertų ir pagal šiuos vertinimus buvo sudaryta elektroninių dokumentų tipų apžvalga. Remiantis apžvalgos rezultatais buvo nustatyti principiniai reikalavimai ir rekomendacijos elektroninio dokumento konteinerio bendrai specifikacijai. Pavyzdžiui, kad bendra elektroninio dokumento konteinerio specifikacija neturi orientuotis į fiksuoto skaičiaus elektroninio dokumento formatų palaikymą.

Atsižvelgiant į šiuos reikalavimus bei apžvelgtus elektroninių dokumentų standartus ir formatus buvo apibrėžta elektroninio dokumento konteinerio bendra specifikacija.

Specifikacija yra sudaryta iš trijų dalių:

- elektroninio dokumento konteinerio loginės struktūros;
- elektroninio dokumento konteinerio taikymo metodų (šioje dalyje, pavyzdžiui, yra aprašomas kaip turi būti vykdomas elektroninio dokumento konteinerio tikrinimas bei sudarymas);
- elektroninio dokumento konteinerio panaudojimo profilių (šioje dalyje yra nurodoma kaip elektroninio dokumento konteinerio struktūros elementai ir taikymo metodai yra naudojami vykdant SPOCS projekto scenarijus).

Remiantis elektroninio dokumento konteinerio bendra specifikacija buvo realizuoti konteinerio apdorojimo (angl. processing) ir autentifikavimo (angl. authentication) atviro kodo programinės įrangos moduliai (3 pav. SPOCS projekto praktinio įgyvendinimo tyrimo metodikos schema [SPOCS12]). Apdorojimo modulis įgyvendina konteinerio sukūrimo funkcionalumą, o autentifikavimo modulis vykdo dokumento tikrinimo veiksmus. SPOCS projekto darbo rezultatų dokumentuose [SPOCS12] buvo aprašytas kiekvieno modulio įgyvendintas funkcionalumas, pateikta jo architektūra bei dokumentuotos išorinės ir vidinės modulio sąsajos.



3 pav. SPOCS projekto praktinio įgyvendinimo tyrimo metodikos schema [SPOCS12]

SPOCS projekto rėmuose apibrėžti praktinio įgyvendinimo tyrimo principai yra pritaikyti šiame darbe vykdant elektroninių dokumentų interoperabilumo problemos technologinio sprendimo įgyvendinamumo pagrindimą.

2.2. Technologinio sprendimo galimumo pagrindimo principai

Siekiant pagrįsti elektroninių dokumentų interoperabilumo problemos technologinio sprendimo galimumą, turi būti žinoma, kaip patenkinti kiekvieną jo (technologinio sprendimo)

reikalavimą. Tai reiškia, kad kiekvienam reikalavimui turi būti pasiūlytas atitinkamas projektinis sprendimas, kuris pagrindžia konkretaus reikalavimo įgyvendinamumą.

Tam tikriems reikalavimams, be projektinių sprendimų, yra būtina apibrėžti papildomas įgyvendinimo sąlygas. Pavyzdžiui, norinti patenkinti reikalavimą 2.2 („Po pasirašymo elektroninių dokumentų egzemplioriai turi atitikti nacionalinių specifikacijų reikalavimus“), yra būtina nustatyti reikalavimus išorinėms sąsajoms, kurias turi pateikti nacionalinės elektroninių dokumentų sistemos įtrauktos į pasirašymo procesą.

Taip pat, kartais vien tik remiantis projektinio sprendimo egzistavimu negalima teigti, kad tam tikras reikalavimas yra įgyvendinamas. Pavyzdžiui, reikalavimas 1.1 teigia, kad „Elektroninių dokumentų egzemplioriai privalo turėti bendrą turinį“, tačiau šis reikalavimas gali būti patenkintas tik jeigu visų egzempliorių turinio struktūra yra vienoda. Vieni architektūriniai sprendimai yra taikomi esant paprastos turinio struktūros egzemplioriams, kiti architektūriniai sprendimai yra naudojami norint sudaryti sudėtingos turinio struktūros elektroninių dokumentų egzempliorius. Todėl svarbu yra identifikuoti tokius atvirus klausimus ir pateikiant projektinius sprendimus, nurodyti jų įgyvendinimo sąlygas. Pavyzdžiui, šiame darbe aprašytas architektūrinis sprendimas tenkina reikalavimą 1.1 („Elektroninių dokumentų egzemplioriai privalo turėti bendrą turinį“), jeigu yra rengiami tik paprastos turinio struktūros, sudarytos iš vienos rinkmenos, elektroninio dokumento egzemplioriai.

Taigi, siekiant pagrįsti technologinio sprendimo galimumą, turi būti nustatyti trys dalykai:

- elektroninių dokumentų sukūrimo ir pasirašymo sistemos architektūra;
- reikalavimai nacionalinėms elektroninių dokumentų paslaugų sistemoms;
- sistemos įgyvendinimo apribojimai.

Papildomai pagrindimas numato programų sistemos prototipo sukūrimą, kuris yra reikalingas norint patvirtinti, kad pateikti projektavimo sprendimai gali būti įgyvendinti panaudojant egzistuojančias technologijas.

2.3. Sistemos apribojimai

Technologinis elektroninių dokumentų sprendimas yra projektuojamas atsižvelgiant į eilę apribojimų, kurie nustato sistemos įgyvendinimo sąlygas. Pagrindiniai apribojimai yra tokie:

1. Elektroninio dokumento egzemplioriai yra paprastos turinio struktūros.

Elektroninio dokumento egzemplioriaus turinys turi būti sudarytas iš vienos rinkmenos. Jeigu ši sąlyga nėra tenkinama, t.y. jeigu yra kuriami sudėtingos turinio struktūros elektroninio dokumento egzemplioriai, kai turinys yra sudarytas iš kelių skirtingų tipų rinkmenų, mažėja sistemos palaikomų specifikacijų aibė. Pavyzdžiui, elektroniniai dokumentai, kurie yra grindžiami

PDF specifikacija yra paprastos struktūros, o elektroniniai dokumentai, grindžiami ASiC standartu, palaiko tiek paprastą, tiek ir sudėtingą turinio struktūrą. Norint sudaryti vieno elektroninio dokumento kelis egzempliorius, kurių vienas yra PDF formato, o kitas atitinka ASiC standartą, yra būtina kurti tik paprastos turinio struktūros elektroninio dokumento egzempliorius.

2. Elektroninio dokumento turinio rinkmena yra PDF/A-2 formato.

Siekiant, kad sistema palaikytų PDF formato elektroninio dokumento egzempliorių sudarymą – elektroninio dokumento turinys turi būti PDF formato. Norint palaikyti visą elektroninio dokumento ciklą, įskaitant ir archyvavimą, būtina taikyti papildomus reikalavimus PDF formato turinio rinkmenoms. Pavyzdžiui, apriboti interaktyvaus turinio saugojimo PDF dokumente galimybes bei įtraukti visus būtinus resursus (tokius, kaip šriftai arba paveikslėliai) į PDF rinkmenos struktūrą. Tokius reikalavimus atitinka PDF/A standarto dokumentai. Šis standartas yra skirtas PDF formato rinkmenų ilgalaikiam archyviniam saugojimui. PDF/A-2 – tai PDF/A standarto versija, kuri remiasi ISO 32000-1 standartu [ISO08]. Taip pat PDF/A-2 apibrėžia reikalavimus skaitmeniniams parašams atsižvelgiant į PDF saugių elektroninių parašų – PAdES [ETSI09b] profilius. Egzistuoja nacionalinių elektroninių dokumentų specifikacijų, kurios reikalauja, kad turinio rinkmena atitiktų PDF/A-2 standartą (pavyzdžiui Lietuvos PDF-LT [LVA14a] specifikacija). Todėl po pateikimo tam, kad įgalinti elektroninio dokumento egzempliorių ilgalaikį saugojimą, elektroninio dokumento turinio rinkmena yra konvertuojama į PDF/A-2 formatą

3. Pasirašymui yra naudojamas stacionarus pasirašymo būdas.

Mobilus pasirašymo būdas nebus naudojamas, nes paketinio pasirašymo technologija, kuri yra naudojama kelių elektroninio dokumento egzempliorių pasirašymui vieną kartą aktyvuojant privatųjį raktą, nepalaiko mobilaus pasirašymo būdo. Taip pat mobilaus pasirašymo palaikymas reikalautų skirtingų ES šalių mobilaus pasirašymo paslaugų tiekėjų įtraukimo į pasirašymo procesą, kas praktiškai yra komplikuotas uždavinys. Todėl pasirašymui yra naudojamas stacionarus pasirašymo būdas, kai skaitmeninį parašą formuojantis įrenginys yra prijungtas prie pasirašančio asmens kompiuterio.

4. Elektroniniai parašai yra XAdES [ETSI12c] arba PAdES [ETSI13b] formatų.

Remiantis ES nacionalinių elektroninių platformų apžvalgą [MB15], didžioji dauguma nacionalinių elektroninių dokumentų platformų naudoja elektroninius dokumentus pasirašytus XAdES arba PAdES elektroniniais parašais. Europos Sąjungos teisės aktai [EK14] reikalauja iš valstybių narių priimti ir apdoroti elektroninius dokumentus pasirašytus PAdES, XAdES arba CAdES parašais. Elektroniniai dokumentai pasirašyti CAdES elektroniniu parašu nebus

nagrinėjami vykdant ši tyrimą, tačiau technologinis sprendimas turi būti praplečiamas taip, kad ateityje įgalinti CAdES parašo naudojimą.

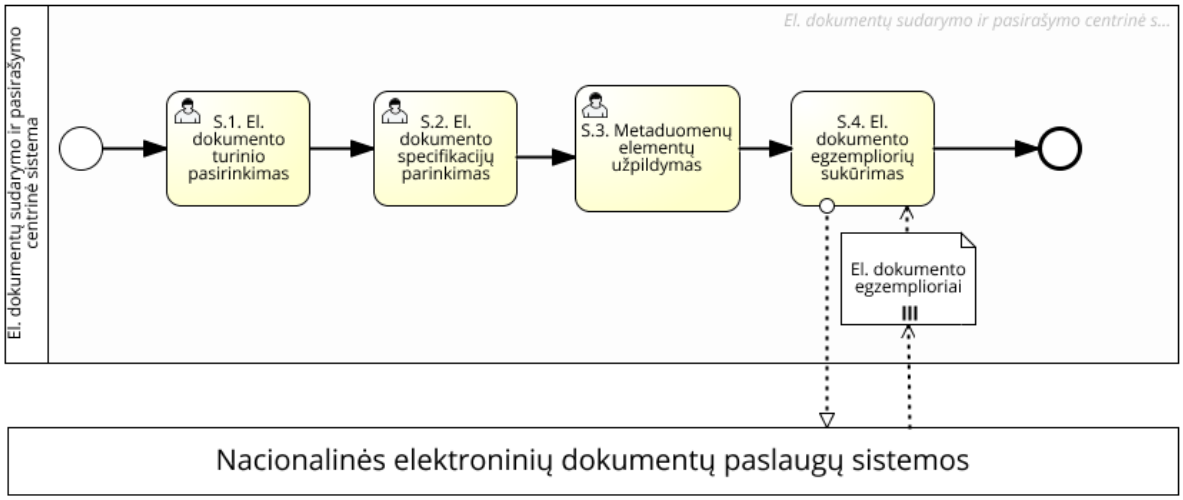
2.4. Veiklos procesai

Remiantis reikalavimais elektroninių dokumentų interoperabilumo problemos technologiniam sprendimui (žr. 1.7 Reikalavimai technologiniam sprendimui), buvo sudaryti elektroninio dokumento egzempliorių sudarymo ir pasirašymo veiklų procesai. Procesai apibrėžia naudotojų ir sistemos veiksmus, reikalingus sukurti ir pasirašyti elektroninio dokumento egzempliorius. Kiekvienas proceso veiksmas turi unikalų identifikatorių, kuris yra sudarytas iš proceso identifikatoriaus ir veiksmo eilės numerio. Pavyzdžiui, pirmas sudarymo proceso veiksmas turi identifikatorių S.1 (S – proceso identifikatorius, 1 - veiksmo eilės numeris).

2.4.1. Sudarymo procesas

Sudarymo proceso paskirtis yra suformuoti elektroninio dokumento egzempliorių rinkinį.

Elektroninio dokumento egzempliorių rinkinys yra formuojamas tokia tvarka (4 pav. Elektroninio dokumento egzempliorių sudarymo proceso diagrama).



4 pav. Elektroninio dokumento egzempliorių sudarymo proceso diagrama

S.1. Elektroninio dokumento turinio pasirinkimas

Pirmiausia sudarytojas pateikia pagrindinę elektroninio dokumento dalį – dokumento turinį. Atsižvelgiant į technologinio sprendimo apribojimus, elektroninio dokumento turinys – tai viena rinkmena, kuri atitinka PDF/A-2 standartą.

2. Elektroninių dokumentų specifikacijų parinkimas

Pateikęs elektroninio dokumento turinio rinkmeną, naudotojas nurodo, į kokių specifikacijų elektroninio dokumento egzempliorius ši turinio rinkmena turi būti įtraukta. Naudotojas iš pateikto sąrašo pasirenka šalį ir šios šalies elektroninio dokumento specifikaciją.

S.3. Metaduomenų elementų užpildymas

Egzistuoja elektroninių dokumentų specifikacijų, kurios be turinio ir elektroninio parašo papildomai saugo kontekstinę informaciją apie dokumentą, tokia dokumento informacija yra vadinama dokumento metaduomenimis. Metaduomenų pavyzdžiai yra dokumento registracijos numeris, registracijos data arba sudarytojo duomenys.

Elektroninio dokumento metaduomenų užpildymas yra viena pagrindinių elektroninių dokumentų interoperabilumo sprendimo technologinių problemų. Įvairios (netgi vienos šalies) specifikacijos apibrėžia skirtingus elektroninio dokumento metaduomenų rinkinius. Vieni metaduomenys (pavyzdžiui dokumento sudarytojo vardas ir pavardė) yra įtraukti į skirtingų specifikacijos metaduomenų rinkinius, tačiau dauguma nacionalinių specifikacijų metaduomenų neturi atitikmenų kitų specifikacijų metaduomenų rinkiniuose. Todėl naudotojui, norinčiam sudaryti kelis elektroninio dokumento egzempliorius, kurie yra skirtingų specifikacijų, tenka užpildyti kiekvieno egzemplioriaus metaduomenis atskirai. Šis sprendimas yra tinkamas, tuo aspektu, kad suteikia geras sąlygas naujų platformų integravimui (nacionalinės elektroninių dokumentų platformos turi pateikti tik tai konfigūraciją, kuri aprašo konkrečios elektroninio dokumento specifikacijos metaduomenų rinkinius). Tačiau naudotojo atžvilgiu šis sprendimas nėra efektyvus, nes jam reikalinga užpildyti kiekvieno elektroninio dokumento egzemplioriaus metaduomenis atskirai. Tokiu atveju, esant penkiems elektroninio dokumento egzemplioriams, naudotojui gali tekti penkis kartus įvesti savo vardą ir pavardę.

Siekiant išspręsti šią problema gali būti išnagrinėtas kitas elektroninio dokumento metaduomenų užpildymo metodas, kuris remiasi tuo, kad centrinėje sistemoje yra saugomi elektroninio dokumento metaduomenų šablonai. Metaduomenų šablonai – tai metaduomenų rinkiniai, kurie apibrėžia kokie metaduomenys turi būti užpildyti sudarant skirtingų rūšių tarpvalstybinius elektroninius dokumentus. Pavyzdžiui, dokumento metaduomenų šablonas gali būti sudarytas iš sudarytojo vardo, pavardės, antraštės ir dokumento rūšies.

Remiantis „metaduomenų šablonų“ metodu, nacionalinės elektroninių dokumentų platformos turi kiekvienam elektroninio dokumento metaduomenų šablonui pateikti konfigūracija, kurioje nurodo sąryšius tarp specifikacijos ir šablono metaduomenų. Pavyzdžiui, kad „sudarytojo“ metaduomuo nacionalinėje specifikacijoje atitinka „autoriaus“ metaduomenį šablone. Jeigu tokie sąryšiai yra nustatyti, tokiu atveju naudotojui nereikia tų pačių metaduomenų

įvesti kiekvienam egzemplioriui, šablone apibrėžtus metaduomenis naudotojas užpildo vieną kartą, o unikalius nacionalinių specifikacijų metaduomenis, užpildo kiekvienam egzemplioriui atskirai.

Toks metaduomenų užpildymo būdas yra efektyvus iš naudotojo pusės, tačiau turi svarbių trūkumų. Pagrindinis jų yra tai, kad sudėtingėja naujų nacionalinių platformų palaikymas ir integravimas į centrinę sistemą. Atsiranda papildomi reikalavimai nacionalinėms elektroninių dokumentų platformoms: jos turi pateikti kiekvienam elektroninio dokumento metaduomenų šablonui konfigūraciją, kurioje būtų apibrėžti sąryšiai tarp konkretaus šablono ir specifikacijos metaduomenų. Metaduomenų šablonų skaičius nėra fiksuotas – kiekvienam atskiram dokumento sudarymo atvejui gali būti reikalingas atskiras metaduomenų šablonas. Tokiu atveju, šalių nacionalinės elektroninių dokumentų platformos turės prisitaikyti prie naujų elektroninio dokumento metaduomenų šablonų atsiradimo ir pastoviai pateikti naujas specifikacijų ir šablono metaduomenų sąryšių konfigūracijas.

Esant fiksuotam palaikomų nacionalinių specifikacijų skaičiui, kai yra tiksliai apibrėžta naujų metaduomenų šablonų ir jų sąryšių konfigūracijų sukūrimo ir pateikimo centrinei sistemai tvarka, „metaduomenų šablonų“ metodas gali būti tinkamas. Tačiau šiame magistro darbe yra nagrinėjamas atvejis, kai palaikomų specifikacijų aibė nėra fiksuota ir elektroninių dokumentų šablonų tipai nėra griežtai apibrėžti. Tokiu atveju, metaduomenų užpildymas panaudojant metaduomenų šablonus yra komplikuotas, atsiranda stipri centrinės sistemos priklausomybė nuo nacionalinių platformų. Nacionalinės platformos turi reaguoti į naujų šablonų atsiradimą ir formuoti specifikacijų ir metaduomenų sąryšių konfigūracijas kiekvienam elektroninio dokumento metaduomenų šablonui. Esant dideliam skaičiau nacionalinių platformų ir neapibrėžtam skaičiui metaduomenų šablonų, tokios tvarkos palaikymas yra praktiškai neįgyvendinamas uždavinys.

Todėl, apibrėžiant technologinį sprendimą, elektroninio dokumento egzempliorių sudarymo atveju buvo nuspręsta atsisakyti metaduomenų šablonų naudojimo ir pildyti kiekvieno egzemplioriaus metaduomenis atskirai.

Taigi, naudotojas, norėdamas sudaryti elektroninio dokumento egzempliorius, kuriems reikia užpildyti metaduomenis, turėtų įvesti metaduomenis kiekvienam egzemplioriui atskirai, t.y. kiekvienam elektroninio dokumento egzemplioriui turi būti sugeneruota atitinkama metaduomenų HTML forma, kurią užpildo naudotojas. Metaduomenų laukų privalomumas yra patikrinimas.

S.4. Elektroninio dokumento egzempliorių sukūrimas

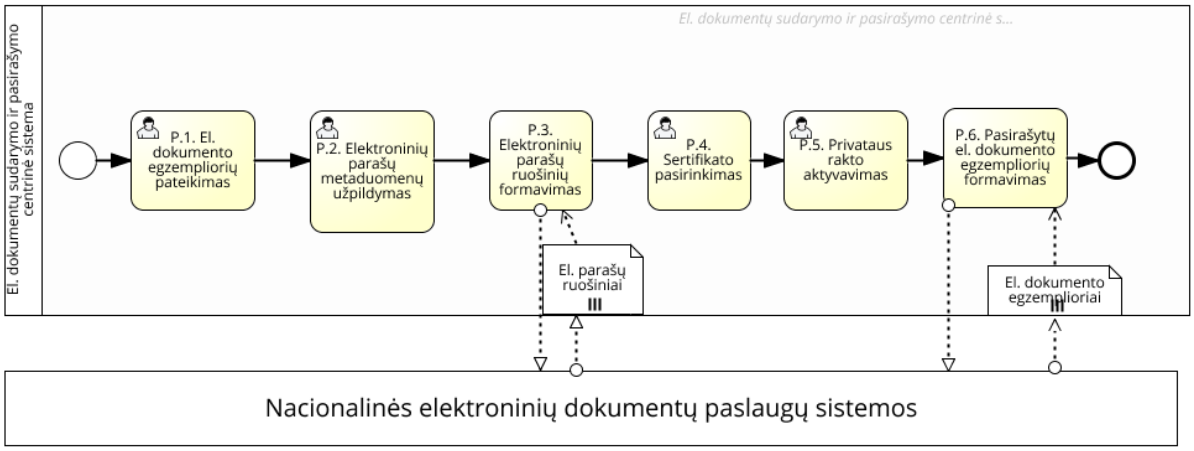
Siekiant užbaigti egzempliorių sudarymo procesą, turint elektroninio dokumento egzempliorių metaduomenis bei turinį, reikia šias elektroninio dokumento dalis įtraukti į elektroninio dokumento egzempliorių konteinerius. Skirtingų elektroninio dokumento

egzempliorių konteinerių tipai nėra vienodi, t.y. vienas elektroninio dokumento egzempliorius gali būti ASiC standarto konteineris, kitas egzempliorius gali būti PDF konteineris, o trečias egzempliorius gali būti sudarytas pagal unikalius nacionalinius konteinerio reikalavimus. Todėl elektroninių dokumento egzempliorių sudarymas reikalauja nacionalinių elektroninių dokumentų paslaugų sistemų įtraukimo, kad kiekvienas egzempliorius būtų sukurtas nacionalinės sistemos atsižvelgiant į nacionalinės specifikacijos reikalavimus. Nacionalinės elektroninių dokumentų paslaugų sistemos gauna iš centrinės sistemos dokumento turinį ir egzemplioriaus metaduomenis bei grąžina centrinei sistemai užpildytą elektroninio dokumento konteinerį.

Elektroninių dokumentų egzempliorių sudarymo proceso rezultatas – tai elektroninio dokumento egzempliorių rinkinys, kur visi egzemplioriai turi bendrą turinį bei kiekvienas egzempliorius yra sukurtas pagal nacionalinės specifikacijos reikalavimus.

2.4.2. Pasirašymo procesas

Elektroninių dokumentų pasirašymo proceso paskirtis yra papildyti kiekvieną elektroninio dokumento egzempliorių pasirašančiųjų asmenų elektroniniais parašais (5 pav. Elektroninio dokumento egzempliorių pasirašymo proceso diagrama).



5 pav. Elektroninio dokumento egzempliorių pasirašymo proceso diagrama

P.1. Elektroninio dokumento egzempliorių pateikimas

Pasirašymo procesas prasideda tuo, kad pasirašantysis pateikia elektroninių dokumentų pasirašymo posistemei elektroninio dokumento egzempliorių rinkinį ir nurodo, kokiai nacionalinei specifikacijai priklauso kiekvienas egzempliorius.

Elektroninio dokumento egzempliorių rinkinys galėtų būti įtrauktas į konteinerį (elektroninio dokumento egzempliorių konteinerį), kuriame yra saugomi elektroninio dokumento egzemplioriai bei papildomi metaduomenys apie kiekvieną egzempliorių. Šie metaduomenys gali būti efektyviai panaudoti vykdant pasirašymo procesą. Pavyzdžiui, egzempliorių specifikacijų reikšmės gali būti ištrauktos iš elektroninio dokumento egzempliorių konteinerio metaduomenų;

tokiu atveju, pateikiant egzempliorių rinkinį, pasirašančiajam nereikėtų nurodyti kiekvieno egzemplioriaus specifikacijos. Elektroninio dokumento egzempliorių konteineris gali būti naudingas siekiant automatiškai apdoroti elektroninių dokumentų egzempliorių rinkinį. Elektroninio dokumento egzempliorių konteineris gali būti įgyvendintas remiantis OCD [SPOCS11] konteinerio specifikacija, tačiau ši specifikacija nėra pilnai pritaikyta tarpvalstybiniam elektroninių dokumentų pasirašymo procesui. Šio darbo rėmuose elektroninio dokumento egzempliorių konteinerio struktūros apibrėžimas ir pakuotės formavimo procesas nėra detalizuojamas.

Pasirašantysis turi turėti galimybę susipažinti su elektroninio dokumento egzempliorių turiniu ir metaduomenimis prieš juos pasirašant. Naudotojas galės pasižiūrėti per centrinę sistemą elektroninio dokumento turinį (PDF/A-2 rinkmeną), o elektroninio dokumento egzempliorių struktūros ir metaduomenų vizualizacija yra vykdoma nukreipiant naudotoją į nacionalinių elektroninių dokumentų platformų sistemas.

P.2. Elektroninių parašų metaduomenų užpildymas

Egzistuoja elektroninių dokumentų specifikacijų (pavyzdžiui, ADOC 2.0 [LVA14b]), kurios reikalauja, kad pasirašantysis įvestų parašo metaduomenis (pavyzdžiui, parašo paskirtį, pasirašančio asmens vardą pavardę bei pareigas). Parašo metaduomenys yra apsaugomi skaitmeninu parašu ir negali būti keičiami.

Elektroninių parašų metaduomenų užpildymas yra atliekamas analogiškai kaip ir elektroninio dokumentų egzempliorių metaduomenų užpildymas vykdant elektroninio dokumento egzempliorių sudarymo procesą. Pasirašantysis norėdamas pasirašyti elektroninio dokumento egzempliorius, kuriems reikia įvesti parašo metaduomenis, turėtų užpildyti parašo metaduomenis kiekvienam egzemplioriui atskirai. Taip pat kaip ir nurodant sudarymo metaduomenis, kiekvienam elektroninio dokumento egzemplioriui turi būti sugeneruota atitinkama metaduomenų HTML forma, kurią užpildo naudotojas.

Tačiau, atsižvelgiant į tai, kad toks naudotojo darbo su sistema būdas yra neefektyvus, gali būti išnagrinėtas parašo metaduomenų užpildymo būdas, kai pasirašančiojo asmens vardas ir pavadė (metaduomuo, kuris yra nurodomas atliekant praktiškai kiekvieną pasirašymo veiksmą) yra įvedami vieną kartą visiems elektroninio dokumento egzemplioriams. Skirtingai nuo kitų parašo metaduomenų vardas ir pavardė yra metaduomuo, kurio reikšmė nepriklauso nuo elektroninio dokumento specifikacijos reikalavimų, t.y. vardas ir pavardė nesikeičia priklausomai nuo to, kokios šalies elektroninio dokumento egzempliorius yra pasirašomas (pavyzdžiui, parašo metaduomens „pasirašymo paskirtis“ reikšmės ADOC 2.0 ir PDF-AS elektroninio dokumento egzemplioriuose gali skirtis). Kitas svarbus dalykas yra tai, kad pasirašančio asmens vardas ir

pavardė yra PAdES elektroninio parašo sudedamoji dalis, todėl šis metaduomuo gali būti įtrauktas į elektroninį parašo ruošinį centrinės sistemos, kuri atpažįsta PAdES parašo struktūrą. XAdES parašo atveju, vardas ir pavardė nėra XAdES formato parašo dalis, todėl šis metaduomuo gali būti įtrauktas į elektroninio dokumento egzempliorių tik tai panaudojant nacionalinius servisus. Tai reiškia, kad kartu su nacionalinės specifikacijos elektroninio parašo metaduomenimis, nacionalinėms elektroninių dokumentų paslaugų sistemoms reikia papildomai pateikti bendrus elektroninio parašo metaduomenis (vienas iš kurių yra pasirašančiojo asmens vardas ir pavardė). Todėl tam, kad įgalinti vienkartinį pasirašančio asmens vardo ir pavardės įvedimą, reikia, kad nacionalinės elektroninių dokumentų paslaugų sistemos galėtų apdoroti ne tik nacionalinius, tačiau ir bendrus elektroninio parašo metaduomenis. Toks sprendimas nustato papildomus reikalavimus nacionalinėms elektroninių dokumentų paslaugų sistemoms, tačiau vienas iš pagrindinių šio technologinio sprendimo pagrindimo siekių yra minimizuoti veiksmų, kuriuos atlieka nacionalinės pasaugų sistemos, aibę. Todėl, formuojant technologinį sprendimą, buvo nuspręsta vienkartinio pasirašančiojo asmens vardo ir pavardės įvedimo funkcionalumo atsisakyti, siekiant netaikyti papildomų reikalavimų nacionalinėms elektroninių dokumentų paslaugų sistemoms.

P.3. Elektroninių parašų ruošinių formavimas

Naudotojui pasirinkus elektroninio dokumento egzempliorius, įvedus elektroninių parašų metaduomenis bei patvirtinus pasirašymo veiksmą, prasideda elektroninių parašų ruošinių formavimas. Jis vykdomas elektroninių dokumentų pasirašymo posistemės ir nereikalauja naudotojo įtraukimo.

Aprašant šį veiksmą, yra svarbu apibrėžti skaitmeninio parašo, elektroninio parašo bei elektroninio parašo ruošinio sąvokas. Skaitmeninis parašas – tai duomenys dvejetainiu pavidalu sudaryti iš kriptografinės pasirašomų duomenų santraukos panaudojant privatųjį raktą. Elektroninis parašas – tai duomenų struktūra apibrėžta pagal standartą (pavyzdžiui, PAdES arba XAdES), kurioje yra saugoma parašo informacija bei skaitmeninio parašo reikšmė. Elektroninio parašo ruošinys – tai elektroninis parašas, į kuri nėra įtraukta skaitmeninio parašo reikšmė bei pasirašančio asmens sertifikato informacija.

Svarbu pabrėžti, kad elektroninio parašo ruošinyje yra saugomi pasirašomi duomenys, tarp kurių yra ir pasirašomi elektroninio dokumento egzemplioriaus metaduomenys. Pasirašomų elektroninio dokumento egzemplioriaus metaduomenų struktūrą bei išsidėstymą elektroninio konteinerio viduje nustato nacionalinės elektroninių dokumentų specifikacijos. Įvairios nacionalinės specifikacijos skirtingai apibrėžia pasirašomus elektroninio dokumento metaduomenis, todėl ruošinio turinys ir struktūra priklauso nuo nacionalinių specifikacijų ypatumų. Iš to seka, kad elektroninio parašo ruošinys negali būti sukurtas centrinės sistemos, o

turi būti formuojamas nacionalinių elektroninių dokumentų paslaugų sistemų. Ruošinys gali būti sudarytas pagal PAdES arba XAdES standartą. Nacionalinės elektroninių dokumentų paslaugų sistemos elektroninio parašo ruošinį formuoja tokia tvarka:

1. Nacionalinės elektroninių dokumentų paslaugų sistemos iš centinės sistemos gauna elektroninio parašo metaduomenis bei elektroninio dokumento egzemplioriaus konteinerį.
2. Elektroninio parašo metaduomenys yra įdedami į elektroninio dokumento konteinerį.
3. XAdES parašo atveju, yra suskaičiuojamos visų pasirašomų elektroninio dokumento pakuotės elementų (turinio bei metaduomenų) santraukos ir kartu su santraukų skaičiavimo algoritmais yra įtraukiamos į XAdES ruošinio struktūrą. PAdES parašo atveju, pasirašomų metaduomenų santraukos nėra įtraukiamos į parašo struktūrą (6 pav. PAdES elektroninio parašo ruošinio pavyzdys).
4. Centrinei sistemai yra grąžinamas elektroninio parašo ruošinys, elektroninio dokumento egzempliorius papildytas parašo metaduomenimis bei, PAdES parašo atveju – pasirašomi duomenys dvejetainiu pavidalu.

```
<<
/Type /Sig
/Filter /Adobe.PPKLite
/SubFilter /ETSI.CAdES.detached
/Name (Vardas Pavardenis)
/Reason (signature)
/LTUd_Role (Position)
/LTUd_SignerNotes ()
/M (D:20150918145420+03'00')
/Contents <30820445060924864886F70D010702A08204363082....>
/ByteRange [0 111695 119297 662]
>>
```

6 pav. PAdES elektroninio parašo ruošinio pavyzdys

P.4. Sertifikato pasirinkimas

Naudotojas turi pamatyti sertifikatų sąrašą ir pasirinkti sertifikatą, kuriuo jis nori pasirašyti elektroninio dokumento egzempliorius. Šiame magistro darbe nėra analizuojamas mobilus pasirašymas, yra nagrinėjamas tik stacionarus pasirašymo būdas. Norint gauti sertifikato duomenis reikalinga prieiga prie naudotojo operacinės sistemos, kuri komunikuoja su parašo formavimo įrenginiais. Naudotojo kompiuteryje turi būti įdiegta programinė įranga, kuri atlieka komunikavimą tarp pasiekiamos per naršyklę elektroninio dokumento pasirašymo posistemės ir

parašo formavimo įrenginio. Po sertifikato pasirinkimo jo reikšmė yra įtraukiama į elektroninio parašo ruošinį.

P.5. Privataus rakto aktyvavimas

Naudotojas aktyvuoja savo privatųjį raktą įvesdamas PIN kodą. Kelių elektroninio dokumento egzempliorių duomenys yra pasirašomi vienu naudotojo privataus rakto aktyvavimo veiksmu. Tai yra pasiekiama per paketinio pasirašymo technologiją (angl. signing in bulk), kuri yra įgyvendinta tam tikrų ES šalių nacionalinėse elektroninių dokumentų pasirašymo sistemose [BBM+15]. Šio magistro darbo rėmuose paketinio pasirašymo technologijos veikimo principai nėra analizuojami, yra laikoma, kad technologija yra jau įgyvendinta ir gali būti panaudota elektroninio dokumento egzempliorių rinkinio pasirašymui.

Po privataus rakto aktyvavimo yra suformuojama skaitmeninio parašo reikšmė, kuri yra įtraukiama į elektroninio parašo ruošinį. Šis veiksmas yra vykdomas centrinės sistemos, kuri geba apdoroti XAdES ir PAdES elektroninių parašų ruošinius

P.6. Pasirašytų elektroninio dokumento egzempliorių formavimas

Po to, kai elektroniniai parašai yra suformuoti, jais reikia papildyti kiekvieną elektroninio dokumento egzempliorių. Elektroninio dokumento egzempliorių struktūra nėra žinoma centrinei sistemai, todėl elektroninių dokumentų egzempliorių papildymas elektroniniais parašais yra vykdomas nacionalinių sistemų. Kiekvienam elektroninio dokumento egzemplioriui per tinklines paslaugas yra vykdoma užklausa į nacionalinę elektroninių dokumentų sistemą, kuriai turi būti pateiktas elektroninis parašas ir atitinkamas elektroninio dokumento egzempliorius. Nacionalinės elektroninių dokumentų sistemos grąžina pasirašytus elektroninio dokumento egzempliorius, kuriuos pasirašantysis gali persisiųsti į savo kompiuterį.

2.4.3. Reikalavimų ir procesų veiksmų matrica

Kiekvienas pasirašymo ir sudarymo procesų žingsnis yra skirtas realizuoti konkrečius reikalavimus elektroninių dokumentų interoperabilumo problemos technologiniam sprendimui (žr. 1.7 Reikalavimai technologiniam sprendimui). Tam, kad būtų susieti reikalavimai ir sistemos architektūrinius elementai buvo sudaryta reikalavimų ir proceso veiksmų matrica (2 lentelė. Reikalavimų ir procesų veiksmų matrica).

2 lentelė. Reikalavimų ir procesų veiksmų matrica

Reikalavimai	**Proceso veiksmai**
1.1. Elektroninių dokumentų egzemplioriai privalo turėti vienodą turinį.	S.1

1.2. Elektroninių dokumentų egzempliorių metaduomenys turi būti užpildyti pagal nacionalinių specifikacijų reikalavimus.	S.3
1.3. Turi būti galimybė sudaryti skirtingų konteinerio tipų elektroninio dokumento egzempliorius.	S.2, S.4
1.4. Turi egzistuoti galimybė praplėsti palaikomų nacionalinių specifikacijų aibę.	S.3
1.5. Turi būti palaikomas sukurtų elektroninių dokumentų ilgalaikis saugojimas.	S.1
2.1. Privatus raktas, vykdant pasirašymo veiksmą turi būti aktyvuojamas tik vieną kartą.	P.5
2.2. Po pasirašymo elektroninių dokumentų egzemplioriai turi atitikti nacionalinių specifikacijų reikalavimus.	P.2, P.3, P.6
2.3. Turi būti galimybė pasirašyti skirtingų konteinerio tipų (ASiC arba PDF) elektroninio dokumento egzempliorius.	P.3

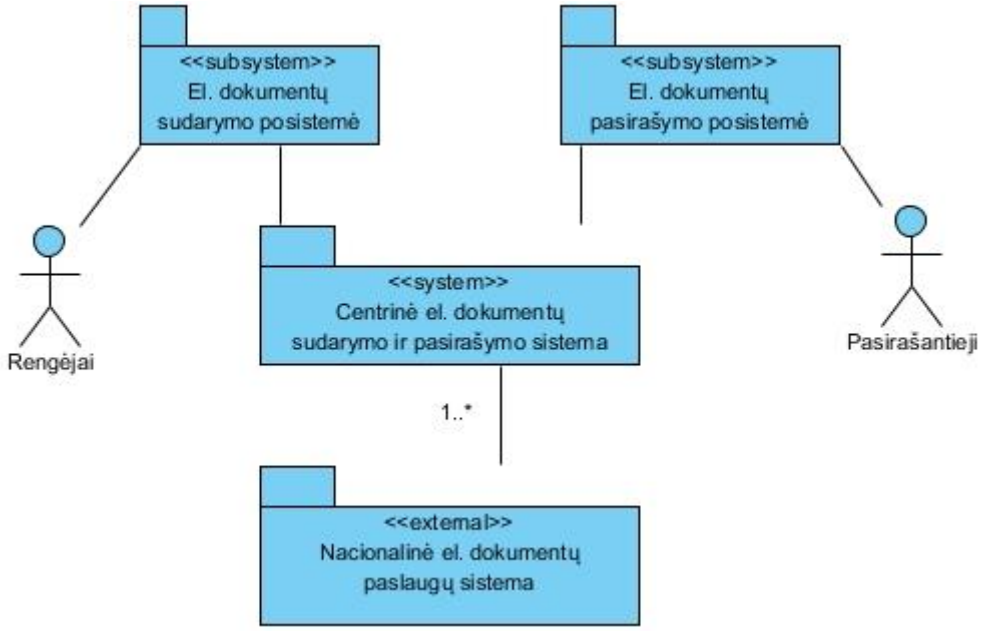
2.5. Sistemos architektūra

2.5.1. Apimties apibrėžimas

Elektroninių dokumentų sukūrimo ir pasirašymo sistema yra skirta sukurti ir pasirašyti elektroninio dokumento egzempliorius, kurie atitinka nacionalinių elektroninių dokumentų platformų reikalavimus. Tai yra centrinė Europos Sąjungos sistema, ji apibrėžia sąsajas, kurias realizuoja nacionalinės elektroninių dokumentų paslaugų sistemos. Komunikuojant su šiomis sistemomis, yra atliekami sukūrimo ir pasirašymo veiksmai. Nacionalinių sistemų, su kuriomis yra integruota centrinė sistema, aibė gali būti plečiama. Nacionalinės elektroninių paslaugų sistemos atlieka tik nacionalinei platformai specifinius elektroninio dokumento sukūrimo ir pasirašymo veiksmus, visos bendros skirtingoms platformoms elektroninio dokumento sukūrimo ir pasirašymo funkcijos yra vykdomos centrinėje sistemoje.

Centrinė sistema turi būti pasiekiama naudotojams per naršyklę.

Centrinės sistemos ribos ir su ja susijusios išorinės esybės yra pavaizduotos konteksto diagramoje (7 pav. Centrinės elektroninių dokumentų sukūrimo ir pasirašymo sistemos konteksto diagrama).



7 pav. Centrinės elektroninių dokumentų sukūrimo ir pasirašymo sistemos konteksto diagrama[3]

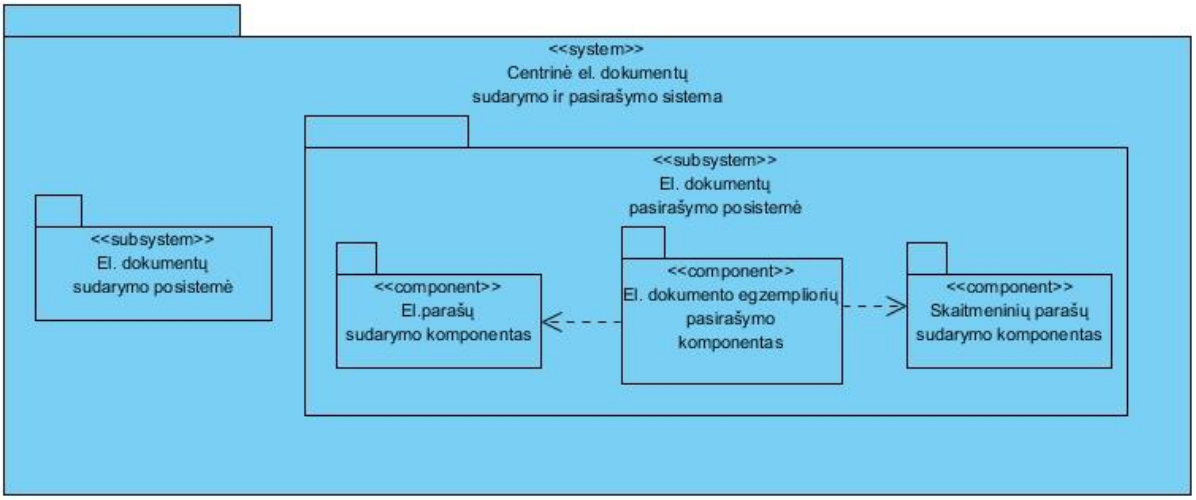
2.5.2. Sistemos loginiai komponentai

Centrinė elektroninių dokumentų pasirašymo ir sudarymo sistema yra sudaryta iš dviejų posistemių: elektroninių dokumentų sudarymo posistemės ir elektroninių dokumentų pasirašymo posistemės (8 pav. Sistemos loginių komponentų diagrama).

Elektroninių dokumentų sudarymo posistemės paskirtis yra iš pateikto elektroninio dokumento turinio ir metaduomenų suformuoti elektroninių dokumentų egzempliorius pagal nacionalinių elektroninių dokumentų specifikacijų reikalavimus.

Elektroninių dokumentų pasirašymo posistemės paskirtis yra pasirašyti pateiktus elektroninio dokumento egzempliorius, kad po pasirašymo kiekvienas egzempliorius atitiktų nacionalinių elektroninių dokumentų specifikacijų reikalavimus pasirašytiems dokumentams.

[3] Tokia konteksto diagramos notacija yra apibrėžiama [Mas07, 89].



8 pav. Sistemos loginių komponentų diagrama

Elektroninių dokumentų pasirašymo posistemė yra sudaryta iš trijų komponentų (8 pav. Sistemos loginių komponentų diagrama):

- Elektroninio dokumento egzempliorių pasirašymo komponentas;
- Elektroninių parašų sudarymo komponentas;
- Skaitmeninių parašų sudarymo komponentas.

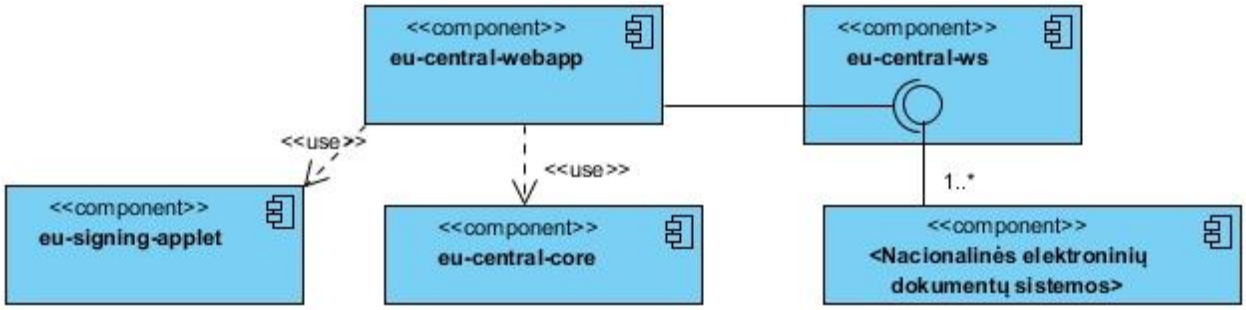
Elektroninio dokumento egzempliorių pasirašymo komponentas: pateikia naudotojui grafinę sąsaja, per kurią yra vykdomas pasirašymo procesas; suformuoja parašo metaduomenis; komunikuoja su nacionalinėmis elektroninių dokumentų sistemomis ir užpildo elektroninių dokumentų egzempliorius elektroniniais parašais.

Elektroninių parašų sudarymo komponentas atlieka elektroninių parašų ruošinių užpildymą sertifikato bei skaitmeninio parašo reikšmėmis.

Skaitmeninių parašų sudarymo komponentas komunikuoja su operacine sistema, pateikia pasirašančio asmens sertifikato reikšmę bei inicijuoja skaitmeninio parašo formavimo procesą.

2.5.3. Sistemos konstravimo vaizdas

Sistemos loginių komponentų reikalavimai yra įgyvendinti panaudojant penkis modulius: eu-central-webapp, eu-signing-applet, eu-central-core, eu-central-ws ir Nacionalinių elektroninių dokumentų paslaugų sistemų modulis (9 pav. Sistemos modulių diagrama).



9 pav. Sistemos modulių diagrama

eu-central-webapp modulis yra skirtas pateikti naudotojo grafinę sąsają, vykdyti komunikavimą tarp centrinės sistemos ir nacionalinių elektroninių dokumentų paslaugų sistemų bei atlikti skirtingų specifikacijų metaduomenų užpildymą.

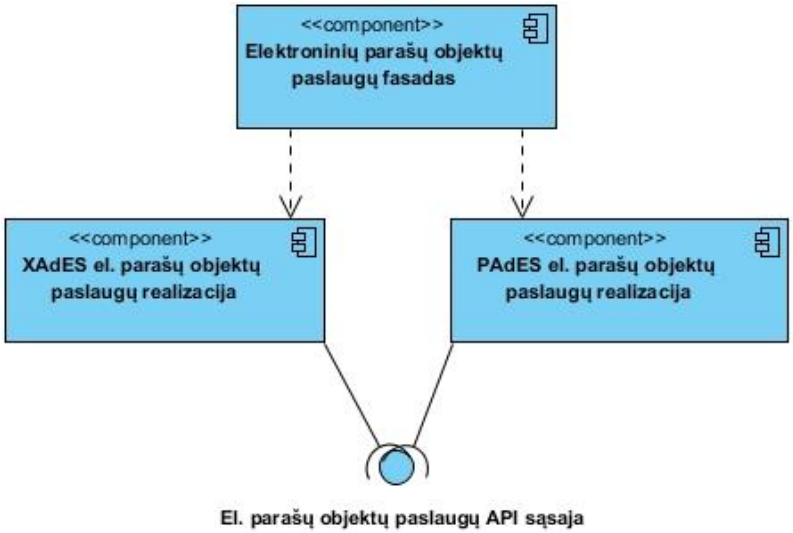
Elektroninio dokumento egzemplioriams, kuriems yra reikalaujama, kad prieš sudarymo ir pasirašymo veiksmus būtų užpildyti metaduomenys, eu-central-webapp modulyje yra dinamiškai sugeneruojamos kiekvieno egzemplioriaus metaduomenų HTML formos. Tai yra atliekama tokiu būdu: šalys, kurių elektroninių dokumentų specifikacijose turi būti įrašyti metaduomenys, turi pateikti centrinei sistemai specifikacijų metaduomenų rinkinius XML schemos pavidalu. Šie metaduomenų rinkiniai yra saugomi centrinėje sistemoje ir priklausomai nuo pasirinktų elektroninių dokumentų specifikacijų, sudarant elektroninio dokumento egzempliorius arba įrašant parašo metaduomenys, iš jų yra generuojamos HTML formos. Metaduomenų HTML formos užpildymo rezultatas yra išsaugomas XML rinkmenos pavidalu ir perduodamas į nacionalines sistemas elektroninio dokumento egzempliorių sudarymo arba pasirašymo metu.

Eu-central-webapp modulio funkcionalumas apima tiek pasirašymo, tiek ir sudarymo posistemių funkcionalumą.

eu-central-core modulyje turi būti įgyvendintos vidinės centrinės sistemos paslaugos. Vidinių paslaugų funkcionalumas apima komunikavimą su sistemos duomenų baze[4] bei elektroninių parašų formavimą (t.y. elektroninių parašų užpildymą sertifikato bei skaitmeninio parašo reikšmėmis).

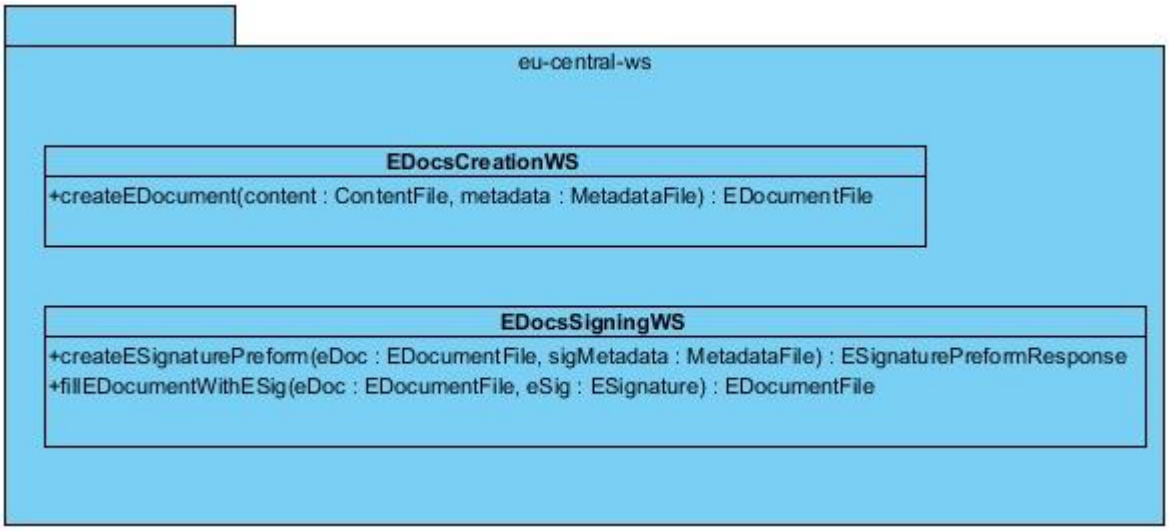
Veiksmus su elektroniniais parašais aprašo bendra API sąsaja, kurią realizuoja specifinės PAdES ir XAdES formatų paslaugų klasės. Kokią paslaugų klasę naudoti yra nustatoma pagal elektroninio parašo formato pavadinimą panaudojant fasado projektavimo šabloną (10 pav. Elektroninių parašų paslaugų struktūra).

[4] Sistemos duomenų bazėje yra saugoma informacija apie palaikomas elektroninių dokumentų specifikacijas.



10 pav. Elektroninių parašų paslaugų struktūra

eu-central-ws modulis pateikia sąsajas (angl. interfaces), kurias įgyvendina nacionalinės elektroninių dokumentų paslaugų sistemos ir kurias naudoja *eu-central-webapp* modulis vykdydamas pasirašymo ir elektroninių dokumentų egzempliorių sudarymo procesus (11 pav. Elektroninių dokumentų sudarymo ir pasirašymo sąsajos).



11 pav. Elektroninių dokumentų sudarymo ir pasirašymo sąsajos

Trys sąsajos (angl. interfaces) aprašytos **eu-central-ws** modulyje turi būti įgyvendintos kiekvienos nacionalinės elektroninių dokumentų paslaugų sistemos:

- Elektroninio dokumento egzemplioriaus sudarymo funkcija (EDocsCreationWS.createEDocument), kuri suformuoja elektroninį dokumentą iš pateikto turinio ir metaduomenų.
- Elektroninio parašo ruošinio formavimo funkcija (EDocsSigningWS.createESignaturePreform), kuris sukuria elektroninio parašo ruošinį iš elektroninio dokumento egzemplioriaus ir parašo metaduomenų (jeigu jie yra būtini pagal

nacionalinės specifikacijos reikalavimus). Elektroninio parašo ruošinys turi atitikti XAdES [ETSI10a] arba PAdES [ETSI09a] elektroninių parašų formatų reikalavimus. Funkcija grąžina elektroninio parašo ruošinį, elektroninio dokumento egzempliorių, kuris yra papildytas parašo metaduomenimis bei PAdES parašo atveju funkcija papildomai grąžina pasirašomus duomenis dvejetainiu pavidalu.

- Elektroninio dokumento užpildymo elektroniniu parašu funkcija (EDocsSigningWS.fillEDocumentWithESignature), kuri suformuoja pasirašytą elektroninio dokumento egzempliorių. Pasirašymo proceso metu sudarytas elektroninis parašas yra įtraukiamas į elektroninio dokumento struktūrą.

eu-signing-applet modulis komunikuoja su operacine sistema ir pateikia eu-central-webapp moduliui skaitmeninio parašo bei pasirašančio asmens sertifikato reikšmes. Šios funkcijos bus įgyvendintos panaudojant serverio programėlę (angl. applet). Serverio programėlė turės naudotojo grafinę sąsają, kuri bus reikalinga slaptojo PIN kodo įvedimui ir sertifikato pasirinkimui. Modulis operuos dvejetainiais duomenimis, jos veikimas nepriklausys nuo elektroninių parašų formatų. Komunikacija tarp serverio programėlės ir eu-central-webapp modulio bus vykdoma per tinklines paslaugas.

Serverio programėlės alternatyva, įgyvendinant komunikavimą su operacine sistema, buvo pasirinkta todėl, kad kitas variantas – taikomosios programos naudojimas, turi labai svarbų trūkumą – sudėtinga įgyvendinti sąsają tarp naršyklės ir taikomosios programos. Todėl, pavyzdžiui, jeigu naudotojas vidury pasirašymo uždarys laikomosios programos langą, naršyklė negaus apie tai informacijos ir pasirašymo procesas naršyklėje nebus atšauktas.

Nacionalinių elektroninių dokumentų paslaugų sistemų modulis nepriklauso centrinei sistemai, šis modulis apima visas nacionalines elektroninių dokumentų paslaugų sistemas, kurios realizuoja eu-central-ws sąsajas. Nacionalinės elektroninių dokumentų paslaugos turi būti pasiekiamos per tinklines paslaugas (angl. web-services), panaudojant SOAP protokolą. Nes SOAP tinklinių paslaugų protokolas įgalina apibrėžti griežtai nustatytą pranešimų formatą, bei turi geresnes saugumo ir transakcijų valdymo charakteristikas, nei kiti komunikavimo tarp sistemų būdai.

2.6. Reikalavimai nacionalinėms paslaugų sistemoms

Tam, kad tam tikros nacionalinės elektroninių dokumentų specifikacijos būtų palaikomos centrinės elektroninių dokumentų sukūrimo ir pasirašymo sistemos, nacionalinės elektroninių dokumentų paslaugų sistemos turi atitikti konkrečius reikalavimus.

Kiekviena nacionalinė paslaugų sistema turi pateikti tinklines paslaugas elektroninių dokumentų sudarymo ir pasirašymo veiksmams. Nacionalinės elektroninių dokumentų sistemos turi realizuoti EDocsCreationWS ir EDocsSigningWS sąsajas (angl. interfaces) apibrėžtas eu-central-ws modulyje (žr. Sistemos konstravimo vaizdas). Taip pat centrinei sistemai turi būti nurodytas adresas, per kurį būtų pasiekiamos nacionalinės elektroninių dokumentų paslaugų sistemos tinklinės paslaugos.

Nacionalinių elektroninių dokumentų specifikacijų, kurioms yra reikalaujama užpildyti elektroninio dokumento sudarymo bei parašo metaduomenis, sudarymo ir parašo metaduomenų XSD schemos turi būti pateiktos centrinei sistemai. Šios schemos gali būti panaudotos apdorojant per tinklines paslaugas atsiųstus metaduomenų XML failus.

Nacionalinėje elektroninių dokumentų platformoje turi būti įgyvendintos taikomosios žiniatinklio sistemos (angl. web-applications), kurios vizualizuoja elektroninio dokumento struktūrą (turinį, metaduomenis, elektroninius parašus). Nuorodos į šias elektroninių dokumentų vizualizavimo paslaugų sistemas turi būti pateiktos centrinei sistemai.

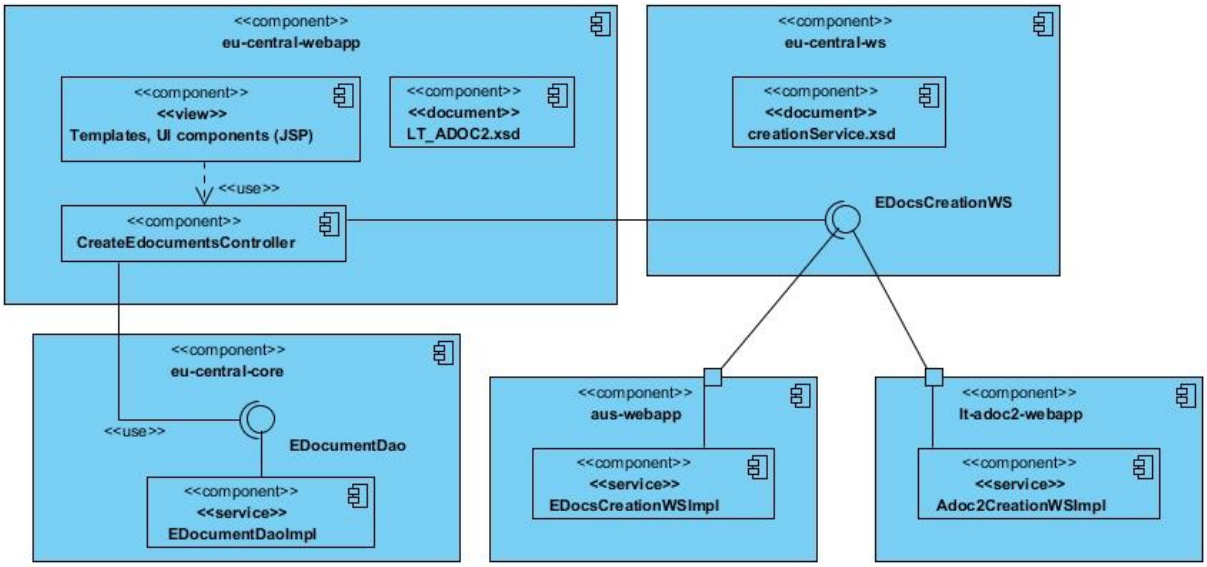
2.7. Elektroninių dokumentų sudarymo posistemės prototipas

Šiame skyriuje yra pateiktas vienos iš dviejų posistemių, elektroninių dokumentų sudarymo posistemės, prototipo aprašymas. Prototipas yra reikalingas norint patvirtinti, kad pateikti projektavimo sprendimai gali būti įgyvendinti panaudojant egzistuojančias programų sistemų kūrimo technologijas.

Prototipas pateikia keturių iš penkių sistemos modulių realizacijas (nebuvo įgyvendintas serverio programėlės – eu-signings-applet modulis). Prototipo realizacija apima visus elektroninių dokumentų egzempliorių sudarymo proceso žingsnius, įskaitant komunikavimą su nacionalinėmis sistemomis per tinklines paslaugas (12 pav. Elektroninių dokumentų sudarymo posistemės prototipo komponentų diagrama). Buvo sukurtos dviejų šalių – Austrijos (PDF-AS, aus-webapp modulis) ir Lietuvos (ADOC 2.0, lt-adoc2-webapp modulis), nacionalinių elektroninių dokumentų paslaugų sistemų realizacijos, kurios suformuoja elektroninių dokumentų egzempliorius pagal šių specifikacijų reikalavimus. Taip pat eksperimentiniais tikslais panaudojant prototipą buvo sudaryti ir PDF-LT specifikacijos elektroninio dokumento egzemplioriai.

ADOC 2.0, PDF-AS ir PDF-LT specifikacijos buvo pasirinktos tam, kad atskleisti sistemos palaikomų specifikacijų įvairovę. ADOC 2.0 specifikacija remiasi ASiC standartu bei turi papildomus nacionalinius dokumento metaduomenų reikalavimus. PDF-AS specifikacija – tai Austrijos elektroninių dokumentų specifikacija, atitinkanti daugelį ES šalių specifikacijų, kurios

yra grindžiamos PDF standartu. PDF-LT specifikacija remiasi PDF/A-2 standartu bei turi papildomų dokumento metaduomenų reikalavimų.



12 pav. Elektroninių dokumentų sudarymo posistemės prototipo komponentų diagrama

Prototipo realizacija buvo paremta Java 8 programavimo kalba. Dinaminiam HTML puslapių formavimui buvo panaudota JSP (JavaServer Pages) technologija. Naudotojo užklausos žiniatinklio serveryje (angl. web-server) yra apdorojamos naudojantis Spring MVC technologija. Spring karkasas (angl. Spring framework) yra naudojamas deklaratyviam priklausomybių tarp naudojamų komponentų valdymui. Sistema buvo įdiegta Apache Tomcat 8 serveryje. Sistemos surinkimui buvo naudojamas Apache Maven įrankis.

Elektroninių dokumentų egzempliorių metaduomenų rinkinio formavimas ir užpildymas yra vykdomas tokia tvarka:

1. Elektroninių dokumentų egzempliorių specifikacijų metaduomenų (sudarymo arba pasirašymo) XSD schemos yra išsaugomos failinėje sistemoje.
2. Iš šių XSD schemų, panaudojant atviro kodo XSD generavimo įrankį „xsd-forms“[5], yra generuojamos kiekvieno egzemplioriaus metaduomenų HTML formos.
3. Metaduomenų užpildymo rezultatas yra išsaugomas XML pavidalu.
4. Metaduomenys yra persiunčiami į nacionalines sistemas kaip XML rinkmenos.
5. Nacionalinėse elektroninių dokumentų paslaugų sistemose metaduomenų esybės yra generuojamos iš gautos XML rinkmenos panaudojant metaduomenų XSD schemą.

Prototipe buvo naudojamos ADOC 2.0 specifikacijos metaduomenų XSD schemos ištraukos. Svarbu pabrėžti, kad „xsd-forms“ įrankis palaiko tik poaibį XSD savybių, iš tam tikrų

[5] Nuoroda į šio įrankio saugyklą: https://github.com/davidmoten/xsd-forms

XSD schemų nėra įmanoma sugeneruoti HTML formos. Todėl XSD schemos turi atitikti konkrečius reikalavimus.

Informacija apie centrinės sistemos palaikomas specifikacijas yra saugoma duomenų bazėje (duomenų bazė buvo realizuota panaudojant hsqldb technologiją). Kiekviena palaikoma specifikacija yra aprašoma per: unikalų specifikacijos identifikatorių, tinklinių paslaugų adresą ir sudarymo metaduomenų XSD schemą. Įvedus naujos specifikacijos duomenis į duomenų bazę yra įmanoma, nesustabdant sistemos veikimo, dinamiškai įtraukti naują specifikaciją į palaikomų specifikacijų sąrašą.

REZULTATAI IR IŠVADOS

Šiame magistro darbe yra pagrįstas elektroninių dokumentų interoperabilumo problemos ne teisinio, o technologinio sprendimo galimumas.

Magistro darbe buvo išnagrinėtas elektroninių dokumentų interoperabilumo problemos kontekstas, priežastys ir esama jos sprendimo situacija. Elektroninių dokumentų interoperabilumas gali būti pasiektas unifikuojant (teisinėmis priemonėmis) arba integruojant (technologinėmis priemonėmis) nacionalines elektroninių dokumentų platformas.

Magistro darbe buvo sudarytos skirtingų elektroninių dokumentų tipų bei elektroninių dokumentų ir parašų reglamentavimo Europos Sąjungoje apžvalgos. Taip pat buvo išnagrinėti mokslinėse publikacijose aprašyti elektroninių dokumentų interoperabilumo problemos sprendimų metodai. Vienas iš šių metodų („atskirų egzempliorių“ metodas) buvo pasirinktas kaip labiausiai tinkamas spręsti elektroninių dokumentų interoperabilumo problemą technologinėmis priemonėmis, taikant kelių dokumento pasirašančiųjų asmenų scenarijų. Remiantis elektroninio dokumento atskirų egzempliorių metodu, darbe buvo suformuluoti reikalavimai technologiniam sprendimui. Atsižvelgiant į šiuos reikalavimus, buvo pasiūlytas ir išbandytas elektroninių dokumentų sudarymo ir pasirašymo tarpvalstybinio interoperabilumo praktinis įgyvendinimas. Pagrindinė užduotis buvo atrasti tokius sprendimus, kurie būtų pakankamai lankstūs ir paprasti sudaryti ir pasirašyti skirtingų šalių elektroninio dokumento egzempliorius.

Atliekant elektroninių dokumentų interoperabilumo Europos Sąjungoje tyrimą, buvo gauti tokie rezultatai:

1. Nustatyti reikalavimai elektroninio dokumento interoperabilumo problemos technologiniam sprendimui;
2. Sudaryta elektroninių dokumentų sukūrimo ir pasirašymo programų sistemos architektūra;
3. Nustatyti sistemos apribojimai;
4. Apibrėžti reikalavimai sistemos išorinėms paslaugoms (nacionalinėms elektroninių dokumentų paslaugų sistemoms);
5. Sukurtas elektroninių dokumentų sudarymo posistemės prototipas.

Apibendrinant tyrimo rezultatus, buvo padarytos tokios išvados:

1. Elektroninių dokumentų interoperabilumas Europos Sąjungoje gali būti pasiektas integruojant elektroninių dokumentų nacionalines platformas.
2. „Atskirų egzempliorių“ metodas gali būti sėkmingai pritaikytas įgyvendinant praktinį elektroninių dokumentų interoperabilumo problemos sprendimą.

3. Technologinis elektroninių dokumentų interoperabilumo problemos sprendimas yra sėkmingai įgyvendinamas panaudojant šiuolaikines programų sistemų kūrimo technologijas bei pritaikant jau egzistuojančius sprendimus (paketinis pasirašymas bei nacionalinės elektroninių dokumentų paslaugos).
4. Šiame darbe pateiktos technologinio sprendimo įgyvendinimo žinios sudaro prielaidas elektroninių dokumentų tarpvalstybinio interoperabilumo tolimesniems tyrimams bei programinės įrangos plėtrai.

ŠALTINIAI

[ASS04] AS Sertifitseerimiskeskus. DigiDoc Format Specification 1.3.0, 2004-05-12. [žiūrėta2014-05-14]. Prieiga per internetą: <http://www.id.ee/public/DigiDoc_format_1.3.pdf>

[BBM+15] J. Besson, A. Birštūnas, A. Mitašiūnas, A. Stočkus. SignaTM – Towards Electronic Document Cross-Border Interoperability. In: Applied Computer Systems. Vol.17, Riga, 2015, pp.46-52.

[IETF98] Internet Engineering Task Force. PKCS #7: Cryptographic Message Syntax (RFC 2315), Version 1.5, March 1998. [žiūrėta 2015-05-14]. Prieiga per internetą: http://www.ietf.org/rfc/rfc2315.txt

[EK09] Europos Komisijos 2009 m. spalio 16 d. sprendimas 2009/767/EB, kuriuo pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje nustatomos priemonės procedūroms, atliekamoms naudojantis elektroninėmis priemonėmis ir kontaktinių centrų paslaugomis, palengvinti. Europos Sąjungos oficialusis leidinys L274, 2009-10-20, p. 36-37.

[EK14] EUROPOS KOMISIJOS SPRENDIMAS kuriuo iš dalies keičiamas Sprendimas 2011/130/ES, kuriuo nustatomi būtinieji dokumentų, kompetentingų institucijų pasirašomų elektroniniu būdu pagal Europos Parlamento ir Tarybos direktyvą 2006/123/EB dėl paslaugų vidaus rinkoje, tarptautinio tvarkymo reikalavimai, OJ 2014/148/EU, 2014.

[EPT06] EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA dėl paslaugų vidaus rinkoje 2006/123/EB, 2006.

[EPT14] EUROPOS PARLAMENTO IR TARYBOS REGLAMENTAS dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje 910/2014, 2014.

[EPT99] EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA dėl Bendrijos elektroninių parašų reguliavimo sistemos 1999/93/EB, 1999.

[ETSI09a] European Telecommunications Standards Institute. TS 102 778. Electronic Signatures and Infrastructures (ESI), PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES, Version 1.1.1, June 2009. [žiūrėta 2016-01-10]. Prieiga per internetą: <http://www.etsi.org/deliver/etsi_ts/102700_102799/10277801/01.01.01_60/ts_10277801v010101p.pdf>

[ETSI10a] European Telecommunications Standards Institute. TS 101 903. XML Electronic Signatures and Infrastructures (ESI), Advanced Electronic Signatures (XAdES), 1.4.2, December 2010.
[žiūrėta 2016-05-15]. Prieiga per internetą:
<http://www.etsi.org/deliver/etsi_ts%5C101900_101999%5C101903%5C01.04.02_60%5Cts_101903v010402p.pdf>

[ETSI11a] European Telecommunications Standards Institute. TS 102 918 V1.1.1. Electronic Signatures and Infrastructures (ESI), Associated Signature Containers (ASiC),

February 2011.
[žiūrėta 2015-05-24] Prieiga per internetą:
<http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.01.01_60/ts_102918v010101p.pdf>

[ETSI12a] European Telecommunications Standards Institute. TS 102 918 V1.2.1. Electronic Signatures and Infrastructures (ESI), Associated Signature Containers (ASiC), February 2012.
[žiūrėta 2015-05-24] Prieiga per internetą:
<http://www.etsi.org/deliver/etsi_ts/102900_102999/102918/01.02.01_60/ts_102918v010201p.pdf>

[ETSI12b] European Telecommunications Standards Institute. TS 102 733. Electronic Signatures and Infrastructures (ESI), CMS Advanced Electronic Signatures (CAdES), Version 2.1.1, March 2012.

[ETSI12c] European Telecommunications Standards Institute. TS 103 171. Electronic Signatures and Infrastructures (ESI), XAdES Baseline Profile, Version 2.1.1, March 2012.

[ETSI13a] European Telecommunications Standards Institute. TS 103 173. Electronic Signatures and Infrastructures (ESI), CAdES Baseline Profile, Version 2.2.1, April 2012.

[ETSI13b] European Telecommunications Standards Institute. TS 103 172. Electronic Signatures and Infrastructures (ESI), PAdES Baseline Profile, Version 2.2.2, April 2012.

[ETSI13c] European Telecommunications Standards Institute. TS 103 174 V2.2.1. Electronic Signatures and Infrastructures (ESI), ASiC Baseline Profile, Version 2.2.1, June 2012.

[EUSO14] EUSO Ltd. EDOC elektroniskā paraksta formāts 2.0, Version 0.95, November 2014. [žiūrėta 2016-04-04]. Prieiga per internetą:
<https://www.eparaksts.lv/files/edoc_2_0_specifikacija_v0_95_4a34d.pdf>

[ECS14] Estonian Centre For Standartization. EVS 821:2014. BDOC V2.1 - Format for Digital Signatures, 2014. [žiūrėta 2016-03-28]. Prieiga per internetą:
<http://www.id.ee/public/bdoc-spec212-eng.pdf>

[LAD06] Lietuvos archyvų departamento patvirtintos Elektroninių dokumentų valdymo taisyklės, Nr. V-12. Valstybės žinios, Nr. 10, 2006-01-26.

[LAD09] Lietuvos archyvų departamento patvirtinta Elektroniniu parašu pasirašyto elektroninio dokumento specifikacija ADOC-V1.0, 2009-09-07, Nr. V-60.

[LPR10] H. Leitold, R. Posch, T. Rössler. Reconstruction of electronic signatures from eDocument printouts. Emerging Challenges for Security, Computers & Security, 2010 Jul, Vol.29(5), pp.523-532.

[LRS10] Lietuvos Respublikos Seimas. Lietuvos Respublikos dokumentų ir archyvų įstatymas XI-917, 2010-06-18. [žiūrėta 2016-04-04]. Prieiga per internetą:
https://www.e-tar.lt/portal/lt/legalAct/TAR.5E8A7FF89480

[LVA14a] Lietuvos vyriausiojo archyvaro patvirtinta Elektroninio dokumento PDF-LT-V1.0 specifikacija, 2014-08-29, Nr. VE(1.3 E)-42.

[LVA14b] Lietuvos vyriausiojo archyvaro patvirtinta Elektroninio dokumento specifikacija ADOC-V2.0, 2014-12-29, Nr. (1.3 E)VE-57.

[Mas07] S. Maskeliūnas. Programų sistemų architektūra ir projektavimas. Mokomoji medžiaga, 2007. Prieiga per internetą: <http://www.mif.vu.lt/~donatas/PSArchitekturaProjektavimas/Knyga/BPD/PSAPKnyga.pdf>

[MB15] A. Mitašiūnas, A. Bykovskij. Lithuanian National Platform of Electronic Documents: Towards Cross-Border Interoperability. In: eChallenges e-2015 Conference Proceedings, 2015.

[MR12] A. Mitašiūnas, S. Ragaišis. Electronic documents interperability solutions in academic environment. INTEL-EDU 2012 : 3rd international workshop on intelligent educational systems and technology-enhanced learning : selected papers, Riga, October 10-12, 2012. pp. 21-34.

[Mic11] Microsec Ltd. Specification of the e-Dossier Format, Version 1.2, February 2011. [žiūrėta 2016-04-04]. Prieiga per internetą: <https://e-szigno.hu/tudasbazis/specification-of-the-e-dossier-format.html>

[NWB06] Thomas Neubauer, Edgar Weippl, Stefan Biffl. Digital Signatures with Familiar Appearance for e-Government Documents: Authentic PDF, In: First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society, California, USA, 2006, pp. 723-731.

[Pan08] M. Pankowska. National frameworks' survey on standardization of e-government documents and processes for interoperability. In: J. Theor. Appl. Electron. Commer. Res., 2008, pp. 64-82.

[PRS11] A. Papadakis, K. Rantos, A. Stasis. Promoting e-gov services: e-Document interoperability across EU. In: Proceedings of the 15th Panhellenic Conference on Informatics, Kastoria, 2011, pp.304-308.

[Ran11] K.Rantos. Digital Signatures: How close is Europe to truly interoperable solutions? Proceedings of the 12th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security - CMS 2011, Springer-Verlag (LNCS 7025), Gent, 2011, pp.155-162.

[RBM+12] S. Ragaisis, A. Birstunas, A. Mitasiunas, A. Stockus. Electronic Archive Information System. In: Proc. DB&Local Proceedings, Žara, Vilnius, 2012, pp.107-114.

[SPOCS11] SPOCS Simple Procedures Online for Cross-border Services. D2.2 Standard Document and Validation Common Specifications, 2011-07-04. [žiūrėta 2014-04-27]. Prieiga per internetą: <http://www.eu-spocs.eu/index.php?option=com_processes&task=streamFile&id=18&fid=1223>

[SPOCS12] SPOCS Simple Procedures Online for Cross-border Services. D2.4 Open Source Authentication Module, 2012-12-11. [žiūrėta 2016-05-23]. Prieiga per internetą: <http://joinup.ec.europa.eu/site/spocs/eDocuments/references/D2.4_Open_source_authentication_module.zip>

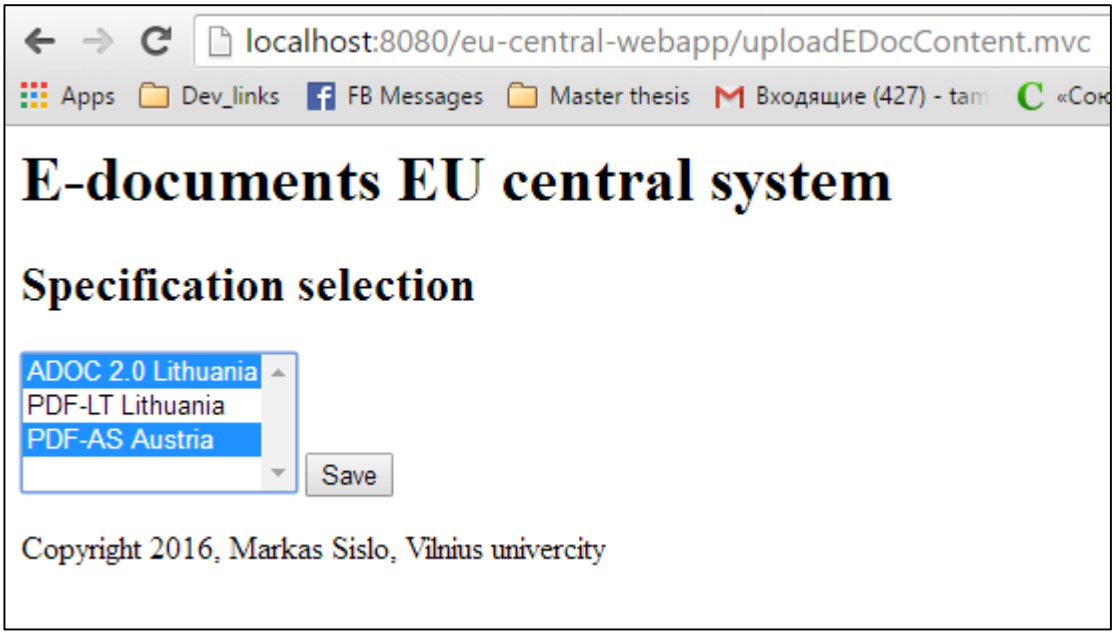
[SSC08] Skaitmeninio sertifikavimo centras. „Justa GE“ Diegimo instrukcija Windows OS, Versija 1.0.0, 2008.

[W3C13] World Wide Web Consortium (W3C). XML Signature Syntax and Processing Version 1.1, 2013-03-11. [žiūrėta 2014-03-22] Prieiga per internetą: <http://www.w3.org/TR/xmldsig-core1/>

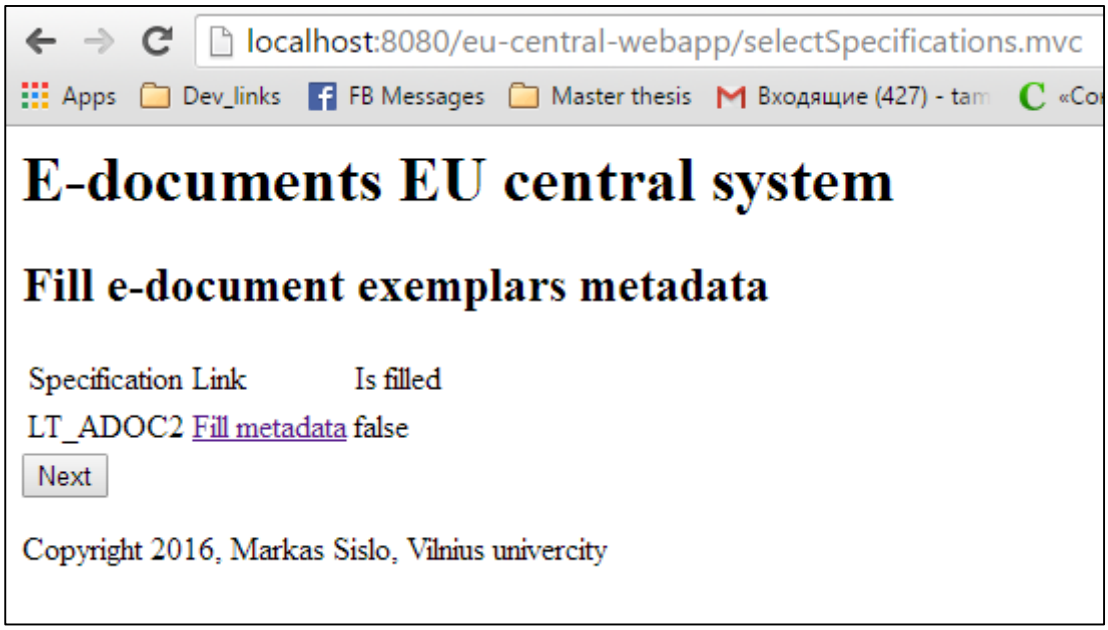
PRIEDAI

1 priedas. Elektroninių dokumentų sudarymo posistemės prototipo ekrano kopijos

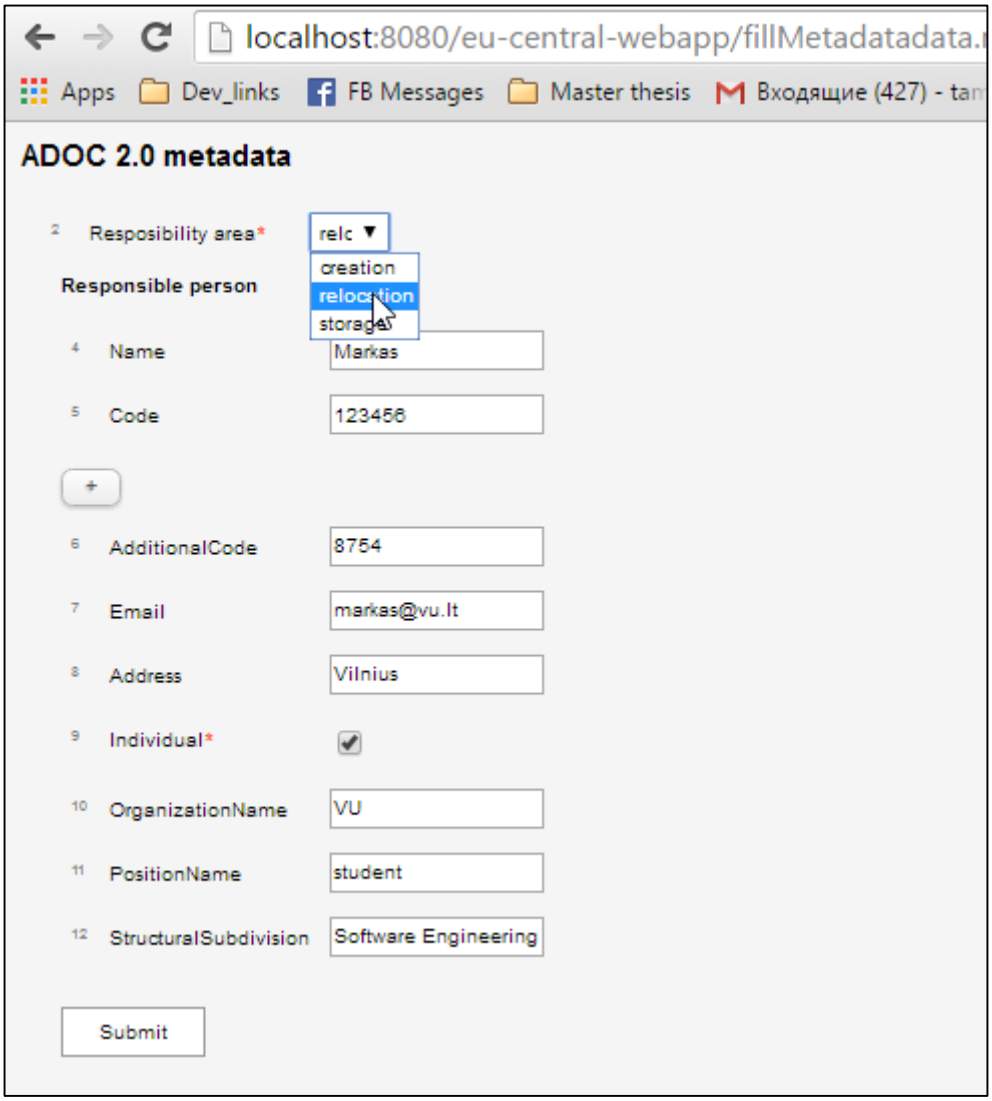
13 pav. Elektroninio dokumento turinio pasirinkimo puslapis



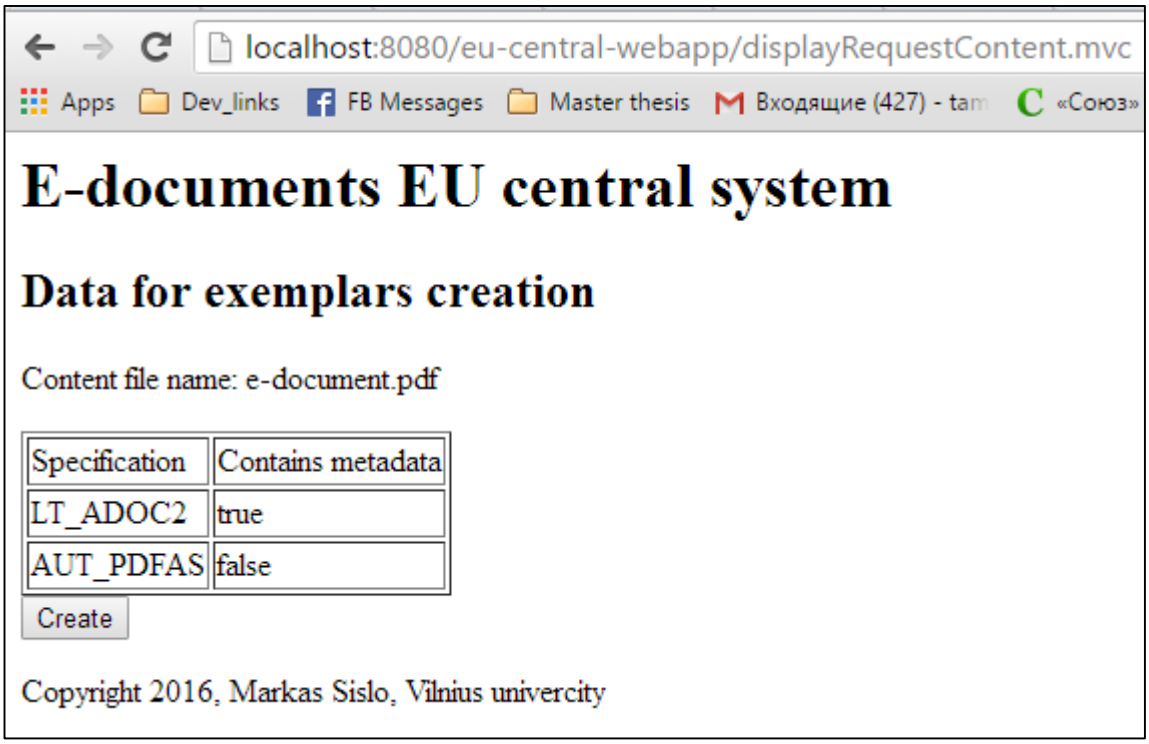
14 pav. Elektroninių dokumentų specifikacijų parinkimo puslapis



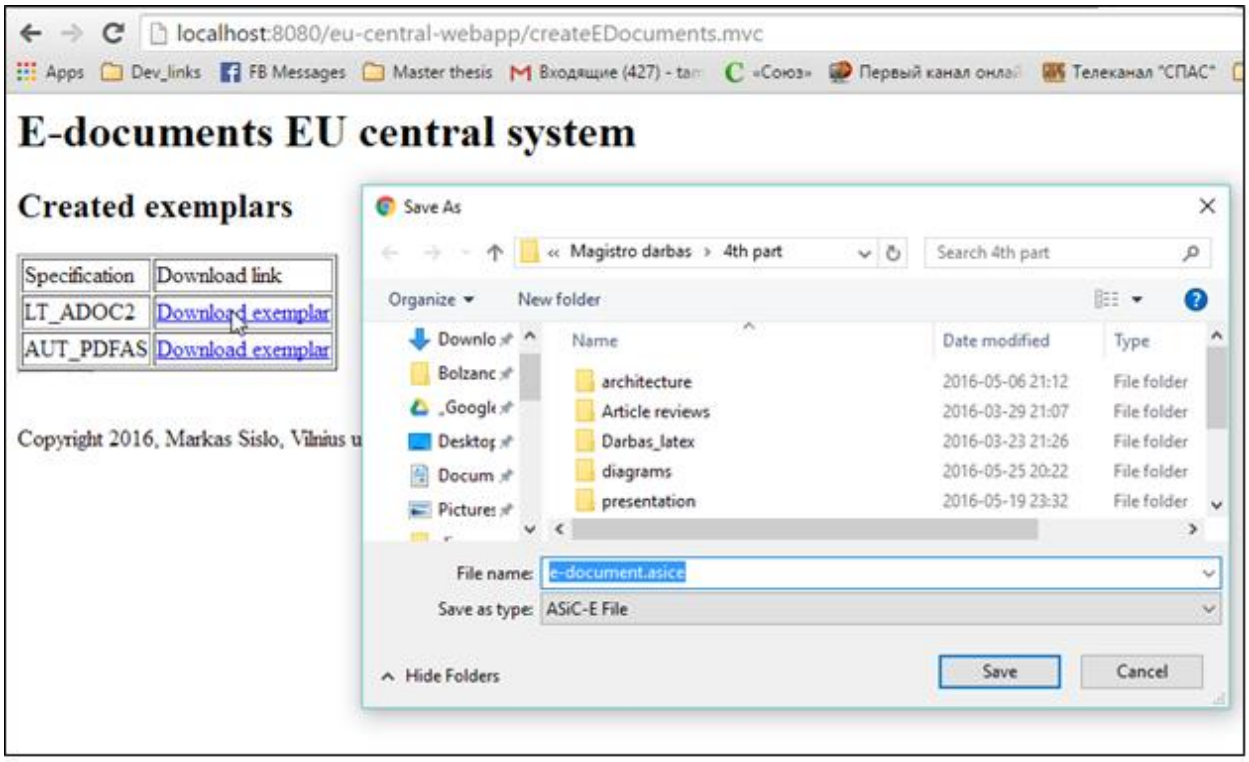
15 pav. Metaduomenų elementų užpildymas. Specifikacijų, kurioms reikia užpildyti metaduomenis sąrašas.



16 pav. ADOC 2.0 metaduomenų ištraukos užpildymo forma



17 pav. Informacija apie elektroninio dokumento egzempliorius iki sukūrimo



18 pav. Sudarytų elektroninio dokumento egzempliorių sąrašas