



**VALSTYBĖS ĮMONĖS REGISTRŲ CENTRO
DIREKTORIUS**

**ĮSAKYMAS
DĖL ELEKTRONINIO DOKUMENTO SPECIFIKACIJOS PDF-RC-V1.0
PATVIRTINIMO**

2017 m. rugsėjo 5 d. Nr. v-220
Vilnius

Vadovaudamasis Elektroninių dokumentų specifikacijų reikalavimų aprašo, patvirtinto Lietuvos vyriausiojo archyvaro 2014 m. rugpjūčio 29 d. įsakymu Nr. VE(1.3 E)-41 „Dėl Elektroninių dokumentų specifikacijų reikalavimų aprašo patvirtinimo“, 4 punktu ir Lietuvos Respublikos nekilnojamojo turto kadastro nuostatų, patvirtintų 2015 m. gruodžio 2 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 1238 „Dėl Lietuvos Respublikos Vyriausybės 2002 m. balandžio 15 d. nutarimo Nr. 534 „Dėl Lietuvos Respublikos nekilnojamojo turto kadastro nuostatų patvirtinimo“ pakeitimo“, 63¹ punktu,

t v i r t i n u Elektroninio dokumento specifikaciją PDF-RC-V1.0 (pridedama).

Direktoriaus pavaduotojas teisių registrams,
atliekantis direktoriaus funkcijas

Vaidas Valikonis

SUDERINTA

Lietuvos vyriausiojo archyvaro tarnybos
2017 m. rugsėjo 1 d. raštu Nr. (6.2 E)V4-367

ELEKTRONINIO DOKUMENTO SPECIFIKACIJA PDF-RC-V1.0

I SKYRIUS

BENDROSIOS NUOSTATOS

1. Elektroninio dokumento specifikacija PDF-RC-V1.0 (toliau – Specifikacija) nustato elektroninių dokumentų, kurie išsaugomi PDF formatu, formato technines savybes, sudarymo saugia elektroninio parašo formavimo sistema, tikrinimo ir gyvavimo ciklo reikalavimus.

2. Specifikacija skirta sudaryti, tikrinti ir atvaizduoti nesudėtingos turinio struktūros (kaip nurodyta šios Specifikacijos 17 punkte) rašytiniams elektroniniams dokumentams su pridedamomis rinkmenomis, kuriose pateikiama *erdvinė ir rastrinė informacija*, ir kurių turinys, metaduomenys bei skaitmeniniai parašai yra išsaugoti PDF formato rinkmenoje.

3. Specifikacija parengta vadovaujantis Elektroninių dokumentų specifikacijų reikalavimų aprašu, patvirtintu Lietuvos vyriausiojo archyvaro 2014 m. rugpjūčio 29 d. įsakymu Nr. VE (1.3 E)-41 „Dėl Elektroninių dokumentų specifikacijų reikalavimų aprašo patvirtinimo“ su 2016 m. birželio 13 dienos pakeitimais, (toliau – Specifikacijų reikalavimų aprašas) Europos parlamento ir Tarybos reglamentu (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB (Specifikacijos 12 priedo 4 punktas), (toliau – Reglamentas) ir standartais bei rekomendacijomis, nurodytomis Specifikacijos 12 priede.

4. Specifikaciją atitinkantis dokumentas yra realizuojamas PDF/A-3 formato rinkmena, kuri atitinka Specifikacijos reikalavimus. Ši Specifikacija apibrėžia 2 reikalavimų lygmenis, pagal kuriuos turi būti rengiamas ir tikrinamas elektroninis dokumentas:

A lygmuo. Pagal šį lygmenį parengtas elektroninis dokumentas turi atitikti visus šioje Specifikacijoje rinkmenai keliamus reikalavimus. Toks dokumentas toliau vadinamas „A lygmens dokumentu“.

B lygmuo. Pagal šį lygmenį parengtas elektroninis dokumentas turi atitikti visus šioje Specifikacijoje rinkmenai keliamus reikalavimus, išskyrus tuos, kuriuose nurodyta, kad jie netaikomi B lygmens elektroniniam dokumentui. Toks dokumentas toliau vadinamas „B lygmens dokumentu“.

5. Atlikus esminius Specifikacijos pakeitimus, turi būti keičiamas Specifikacijos versijos numeris, o atlikus redakcinius Specifikacijos pakeitimus ar atnaujinus naudojamų algoritmų sąrašą, nurodytą Specifikacijos 7 priede, turi būti keičiamas redakcijos (angl. *revision*) numeris. Šios Specifikacijos redakcijos numeris yra 1.

6. Specifikacijoje vartojamos sąvokos ir santrumpos:

CADES – skaitmeninio parašo aprašymo kriptografinių pranešimų sintakse (CMS) standartas LST EN 319 122-1 V1.1.1:2016 (Specifikacijos 12 priedo 6 punktas; toliau – CAdES standartas).

CRL – sertifikatų, kurių galiojimas nutrauktas ar sustabdytas, sąrašas, atitinkantis RFC 5280 rekomendacijas (Specifikacijos 12 priedo 24 punktas).

Inkrementinis keitimas – (angl. *incremental update*) PDF rinkmenos keitimo ir papildymo būdas, kai nauji PDF objektai pridedami rinkmenos pabaigoje, nekeičiant jau esančių rinkmenoje objektų ir jų tvarkos (PDF-1.7 standarto 7.5.6 skyrius). Rinkmenos papildymas inkrementinio keitimo būdu nepažeidžia skaitmeninių parašų, kuriais iki papildymo rinkmena galėjo būti pasirašyta, vientisumo.

OCSP paslauga – sertifikatų galiojimo patikrinimo paslauga, atitinkanti RFC 6960 rekomendacijas (Specifikacijos 12 priedo 26 punktas).

PAdES – skaitmeninio parašo PDF rinkmenoje standartas LST EN 319 142-1 V1.1.1:2016 (Specifikacijos 12 priedo 7 punktas; toliau – PAdES standartas).

PAdES-B-B – PAdES standarte aprašytas skaitmeninio parašo formatas, atitinkantis PAdES standarto 6 skyriuje aprašytus B-B lygmens reikalavimus.

PAdES-B-LT – PAdES standarte aprašytas skaitmeninio parašo su elektronine laiko žyma ir parašo galiojimą patvirtinančiais duomenimis formatas, atitinkantis PAdES standarto 6 skyriuje aprašytus B-LT lygmens reikalavimus.

PAdES-B-LTA – PAdES standarte aprašytas ilgalaikio galiojimo skaitmeninio parašo su elektronine laiko žyma, parašo galiojimą patvirtinančiais duomenimis ir PDF dokumento laiko žyma formatas, atitinkantis PAdES standarto 6 skyriuje aprašytus B-LTA lygmens reikalavimus.

PAdES-B-T – PAdES standarte aprašytas skaitmeninio parašo su elektronine laiko žyma formatas, atitinkantis PAdES standarto 6 skyriuje aprašytus B-T lygmens reikalavimus.

PAdES parašas – skaitmeninis parašas, atitinkantis PAdES bazinio parašo PAdES-B-B, PAdES-B-T, PAdES-B-LT ar PAdES-B-LTA formatų reikalavimus.

Parašo galiojimą patvirtinantys duomenys – norminių teisės aktų nustatyta tvarka surinkti elektroniniai duomenys (sertifikatai, OCSP paslaugos atsakymai, CRL sąrašai), panaudoti skaitmeninį parašą patvirtinusio sertifikato galiojimui patikrinti. Šioje sąvokoje apibrėžti duomenys neapima elektroninių laiko žymų.

PDF – (angl. *portable document format*) kompiuterių rinkmenos formatas, aprašytas standartu LST ISO 32000-1:2009 (Specifikacijos 12 priedo 15 punktas; toliau – PDF-1.7 standartas).

PDF/A-3 formatas – PDF-1.7 standarto pagrindu sukurtas ilgalaikio saugojimo paskirties rinkmenos formatas, aprašytas standartu LST ISO 19005-3:2017 (Specifikacijos 12 priedo 14 punktas; toliau – PDF/A-3 standartas).

PDF dokumento katalogas – (angl. *document catalog*) pagrindinis PDF formato rinkmenos objektas, aprašomas PDF žodynu, kuriame saugomos nuorodos į kitus PDF rinkmeną sudarančius objektus (PDF-1.7 standarto 7.7.2 skyrius).

PDF dokumento laiko žyma – (angl. *document time-stamp*) į PDF formato rinkmeną įtraukta elektroninė laiko žyma, kurios santrauka skaičiuojama nuo visos PDF formato rinkmenos (išskyrus pačią elektroninę laiko žymą). PDF dokumento laiko žyma patvirtina, kad visi objektai, įtraukti į PDF formato rinkmeną prieš sudarant PDF dokumento laiko žymą, egzistavo iki PDF

dokumento laiko žymoje nurodyto laiko. PDF dokumento laiko žyma aprašoma PDF dokumento laiko žymos žodyne.

PDF dokumento laiko žymos žodynas – (angl. *document time-stamp dictionary*) PDF žodynas, kuriame saugoma PDF dokumento laiko žyma (PAdES standarto 5.4.3 skyrius).

PDF metaduomenų šaltinis – (angl. *metadata stream*) PDF duomenų šaltinio objektas, kuriame metaduomenys saugomi XMP specifikaciją atitinkančiu formatu ir atitinka PDF/A-2 standarto 6.6.2 skyriuje bei PDF-1.7 standarto 14.3.2 skyriuje nustatytus reikalavimus. PDF žodyne metaduomenų šaltinis nurodomas kaip to žodyno lauko „*Metadata*“ reikšmė.

PDF parašo formos lauko žodynas – (angl. *signature form field*) PDF žodynas, kurio laukuose saugoma skaitmeninio parašo atvaizdavimo informacija (PDF-1.7 standarto 12.7.4.5 skyrius) ir PDF parašo žodynas.

PDF parašo žodynas – (angl. *signature dictionary*) PDF žodynas, kurio laukuose saugomi skaitmeninio parašo duomenys (PDF-1.7 standarto 12.8 skyrius).

PDF puslapių medis – (angl. *page tree*) hierarchinės struktūros PDF puslapio objektų struktūra, PDF rinkmenoje aprašoma puslapių medžių ir puslapių žodynais, kuri kartu su nurodytais vektorinės grafikos ir teksto resursais aprašo kompiuterio ekrane, spausdintuve ar kitame įrenginyje atvaizduojamą informaciją (PDF-1.7 standarto 7.7.3 skyrius).

PDF žodynas – (angl. *dictionary object*) PDF objektas, kitų sudėtingų PDF objektų sudėtinė dalis, apibrėžiamas kaip lentelė, sudaryta iš PDF objektų porų – PDF žodyno laukų, nustatytu formatu aprašančių tų sudėtingų objektų atributus (PDF-1.7 standarto 7.3.7 skyrius).

PDF žodyno laukas – (angl. *dictionary entry*) sudėtinė PDF žodyno dalis, apibūdinanti vieną PDF žodyno atributą, susidedantį iš PDF objektų poros: rakto (vardo) ir nustatyto tipo reikšmės (PDF-1.7 standarto 7.3.7 skyrius).

Prefiksas – (angl. *prefix*) PDF žodyno lauko, XML arba XMP elemento, atributo ar reikšmių tipo vardo sudėtinė dalis, nurodoma vardo pradžioje, skirta vardo unikalumui užtikrinti ir (ar) vienareikšmei vardo naudojimo sričiai nustatyti. Prefiksas taip pat naudojamas kaip XML arba XMP elementus, atributus ir jų reikšmių tipus apibrėžiančios schemos URI santrumpa.

Saugi elektroninio parašo formavimo sistema – programinė ir techninė įranga, kurią sudaro kvalifikuotas elektroninio parašo kūrimo įtaisas ir elektroninio parašo formavimo taikomoji sistema, atitinkanti standarto ETSI TS 119 101 V1.1.1:2016 (Specifikacijos 12 priedo 11 punktas) reikalavimus arba ekvivalenčius reikalavimus saugioms elektroninio parašo formavimo taikomosioms sistemoms.

Skaitmeninis parašas (angl. *digital signature*) – duomenys, pridedami prie kitų duomenų, ar kriptografiškai transformuoti duomenys, leidžiantys nustatyti pastarųjų duomenų šaltinį, įrodyti jų integralumą ir apsaugoti nuo klastojimo. Skaitmeninis parašas gali būti tiek elektroniniu parašu, tiek elektroniniu spaudu.

URI – universalusis išteklį identifikatorius (angl. *uniform resource identifier*), kurio sandara atitinka RFC 3986 rekomendacijas (Specifikacijos 12 priedo 122 punktas), šioje Specifikacijoje naudojamas kaip XML arba XMP elementus, atributus ir jų reikšmių tipus apibrėžiančios schemos identifikatorius.

XML – (angl. *extensible markup language*) Pasaulinio tinklo konsorciūmo (angl. *The World Wide Web Consortium, W3C*) rekomenduojama bendrosios paskirties duomenų struktūrų ir jų turinio aprašomoji kalba (Specifikacijos 12 priedo 27 punktas).

XMP – (angl. *extensible metadata platform*) Adobe Systems korporacijos rekomenduojama plečiama metaduomenų kūrimo, nuskaitymo ir keitimosi jais platforma, aprašyta viešai paskelbta XMP specifikacija (Specifikacijos 12 priedo 30 punktas; toliau – XMP specifikacija), kuri yra sudėtinė PDF-1.7 standarto dalis.

Kitos šioje Specifikacijoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Reglamente (Specifikacijos 12 priedo 4 punktas), Lietuvos Respublikos dokumentų ir archyvų įstatyme, Specifikacijų reikalavimų apraše ir Elektroninių dokumentų valdymo taisyklėse, patvirtintose Lietuvos vyriausiojo archyvaro 2011 m. gruodžio 29 d. įsakymu Nr. V-158 „Dėl Elektroninių dokumentų valdymo taisyklių patvirtinimo“.

II SKYRIUS

ELEKTRONINIO DOKUMENTO STRUKTŪRA

7. Elektroninio dokumento loginę struktūrą sudaro šios dalys:

7.1. turinys, susidedantis iš vieno privalomo pagrindinio dokumento ir privalomos bent vienos pridėamos rinkmenos;

7.2. metaduomenys (tik nekeičiami);

7.3. bent vienas kvalifikuotas elektroninis parašas ar kvalifikuotas elektroninis spaudas.

8. Elektroninio dokumento pakuotė yra PDF formato rinkmena, sujungianti visas elektroninio dokumento dalis į visumą.

9. Elektroninio dokumento loginės struktūros dalys pakuotėje atvaizduojamos kaip PDF objektai. Fizinę elektroninio dokumento struktūrą sudaro PDF formato rinkmena, kurios:

9.1. PDF puslapių medyje yra atvaizduotas visas turinys, išskyrus pridėdamos rinkmenas. Turinio atvaizdavimo dalimi taip pat laikomi naudotojo darbui su PDF puslapių medžio struktūra palengvinti skirti dokumento struktūros, straipsnių, vardų, veiksmų objektai ir kiti su puslapiais susiję objektai;

9.2. metaduomenų šaltiniuose, susietuose su PDF dokumento katalogo ar PDF parašo formos laukų žodynais, ir Specifikacijoje nustatytyuose PDF parašo žodyno laukuose yra atvaizduoti elektroninio dokumento metaduomenys;

9.3. PDF parašų žodynuose (išskyrus žodyno laukus, kuriais aprašomi metaduomenys ir susieti metaduomenų šaltiniai) yra atvaizduoti elektroniniai parašai arba elektroniniai spaudai;

9.4. PDF įdėtinės rinkmenos aprašo žodyne (PDF-1.7 standarto 7.11.4 skyrius) yra atvaizduotos pridėdamos rinkmenos.

10. Elektroninio dokumento rinkmena, joje saugomas turinys ir metaduomenys turi atitikti Specifikacijoje keliamus reikalavimus, įskaitant PDF/A-3 standarto reikalavimus. Skaitmeniniai parašai turi atitikti Specifikacijoje keliamus reikalavimus, įskaitant PAdES standarto reikalavimus.

11. Šią Specifikaciją atitinkančiame elektroniniame dokumente negali būti:

11.1. keičiamų metaduomenų;

11.2. lygiagrečiuoju pasirašymo būdu sudarytų skaitmeninių parašų.

12. Ši Specifikacija draudžia elektroniniame dokumente naudoti XML architektūros formas (XFA formas – PDF/A-3 standarto 6.4.2 skyrius).

III SKYRIUS

ELEKTRONINIO DOKUMENTO PAKUOTĖ

13. Elektroninio dokumento pakuotė yra rinkmena, atitinkanti šiuos reikalavimus:

13.1. rinkmenos plėtinys yra PDF (MIME tipo žymuo – *application/pdf*);

13.2. rinkmenos antraštės eilutėje (angl. *header line*) nurodyta versija „1.7“ (PDF-1.7 standarto 7.5.2 skyrius);

13.3. rinkmena atitinka vieno pasirinkto suderinamumo su PDF/A-3 standartu lygio (PDF/A-3a, PDF/A-3b, PDF/A-3u) keliamus rinkmenos struktūros reikalavimus;

13.4. rinkmena neviršija PDF rinkmenai nustatytų apribojimų (PDF-1.7 standarto C priedas).

14. Šią Specifikaciją atitinkantis elektroninis dokumentas neturi būti šifruotas, apsaugotas slaptažodžiais, negali turėti naudojimo (kopijavimo, spausdinimo ar kitų) ribojimų – pakuotėje esančio pagrindinio PDF rinkmenos žodyno (angl. *file trailer dictionary*) laukas „**Encrypt**“ (PDF-1.7 standarto 7.7.5 skyrius) yra draudžiamas.

15. Kai naudojami šioje Specifikacijoje apibrėžti PDF parašo žodyno metaduomenų laukai „**LTUd_SignerNotes**“ ir (arba) „**LTUd_Role**“ (1 priedo 3 skyrius), PDF dokumento katalogo plėtinių žodyne (PDF dokumento katalogo žodyno laukas „**Extensions**“) turi būti aprašytas šioje Specifikacijoje apibrėžtų naujų PDF žodyno laukų prefiksas „LTUd“. Prefiksą aprašančio PDF žodyno (PDF-1.7 standarto 7.12.2 skyrius) lauke „**BaseLevel**“ turi būti nurodyta reikšmė „1.7“, „**ExtensionLevel**“ lauke – reikšmė „1“ (žr. Specifikacijos 3 priede pateiktą pavyzdį).

16. Elektroninio dokumento atitiktis Specifikacijai deklaruojama nurodant elektroninio dokumento specifikacijos identifikacinį žymenį metaduomenyse (Specifikacijos 1 priedas). Šią Specifikaciją atitinkančių elektroninių dokumentų specifikacijos identifikavimo žymuo turi būti „PDF-RC-V1.0“. B lygmens dokumentams atitiktis Specifikacijai deklaracija neprivaloma. Elektroninio dokumento atitiktis Specifikacijos redakcijai gali būti nurodyta dokumento atitikties specifikacijos redakcijai deklaracijos metaduomenyse (Specifikacijos 1 priedas).

IV SKYRIUS

TURINYS

17. Elektroninio dokumento turinį sudaro vienas privalomas pagrindinis dokumentas ir privaloma bent viena pridedama rinkmena.

18. Elektroninio dokumento turinys turi būti išsaugotas PDF/A-3 standarte aprašytu formatu. Šio formato rinkmenas gali suformuoti ir interpretuoti *Adobe Acrobat XI* versijos, *Adobe Reader XI* versijos (peržiūrėti), atvirojo kodo bibliotekos *iText 5* versijos (formuoti) ir kitų gamintojų programinė įranga. Pridedamas rinkmenas galima peržiūrėti:

18.1. JPG ir TIF su bet kuria paveikslėlių peržiūros priemone.

18.2. DWG, DXF, SHP, SID su programomis AutoCAD, NanoCAD, ArcGIS, QGIS.

18.3. DWF su programomis Internet Explorer, A360, Design Review.

19. Visas elektroninio dokumento turinys, išskyrus pridedamas rinkmenas, turi būti atvaizduotas viename PDF puslapių medžio žodyne, kuris nurodytas PDF dokumento katalogo

lauke „**Pages**“. Pridedamos rinkmenos turi būti atvaizduotos PDF dokumento katalogo lauko „**Names**“ žodyne „**EmbeddedFiles**“

20. Elektroninio dokumento turinyje turi būti tik statinė informacija. Kintančio vaizdo, garso ir trimatės grafikos objektai yra draudžiami (PDF/A-3 standarto 6.3.1 skyrius).

21. Elektroninio dokumento turinys turi būti pasirašytas bent vienu kvalifikuotu elektroniniu parašu arba kvalifikuotu elektroniniu spaudu, kurio paskirtis nurodyta šios Specifikacijos 49 punkte.

22. Draudžiama šalinti ar keisti pasirašyto elektroninio dokumento turinio objektus ir turinį pildyti naujais objektais (pvz., inkrementinio keitimo būdu), išskyrus atvejus, nurodytus Specifikacijos 91 punkte.

23. Pridedamų rinkmenų turinys yra pavaizduotas elektroninio dokumento turinyje.

24. Pridedama rinkmena negali būti savarankiškas elektroninis dokumentas.

25. Leistini rinkmenų tipai nurodyti Specifikacijos 11 priede.

26. Pridedamos rinkmenos turi būti deklaruotos laikantis PDF/A-3 standarto 6.8 skyriaus ir PDF-1.7 standarto 7.11.4 skyriaus reikalavimų.

27. Draudžiamos nuorodos į išorines rinkmenas.

28. PDF įdėtinės rinkmenos aprašo žodyno lauke „**AFRelationship**“ turi būti nurodyta reikšmė „**Source**“.

V SKYRIUS

METADUOMENYS

29. Metaduomenys yra duomenys, aprašantys elektroninio dokumento formatą, turinį, sudarymo, pasirašymo ir registravimo informaciją.

30. Visi elektroninio dokumento metaduomenys yra nekeičiami, jų autentiškumas ir vientisumas užtikrinami PAdES parašu. Metaduomenys po jų įtraukimo į PDF rinkmeną nekeičiami.

31. Metaduomenys skirstomi į šias grupes:

31.1. dokumento sudarymo metaduomenys – elektroninio dokumento sudarymo metu sukuriama metaduomenys. B lygmens elektroniniame dokumente šie metaduomenys neprivalomi ir gali būti pridedami po dokumento sudarymo inkrementinio keitimo būdu, kaip nurodyta Specifikacijos 91 punkte;

31.2. dokumento registravimo metaduomenys – metaduomenys, įrašomi į elektroninį dokumentą jo registravimo metu;

31.3. elektroninių parašų ir elektroninių spaudų metaduomenys – kiekvieno PAdES parašo formavimo metu sukuriama metaduomenys.

32. Elektroninio dokumento metaduomenys, jiems fiksuoti naudojamų XMP elementų ir PDF žodyno laukų vardai, reikšmių tipai, privalomumo ir kiti reikalavimai nurodyti Specifikacijos 1 priede.

33. Dokumento sudarymo metaduomenys turi būti fiksuojami XMP specifikaciją ir PDF/A-3 standarto 6.6.2 skyriaus reikalavimus atitinkančiu formatu PDF metaduomenų šaltinyje, susietame su PDF dokumento katalogo žodynu.

34. Dokumento registravimo metaduomenys turi būti fiksuojami XMP specifikaciją ir PDF/A-3 standarto 6.6.2 skyriaus reikalavimus atitinkančiu formatu PDF metaduomenų šaltinyje, susietame su PAdES parašu.

35. Elektroninių parašų ir elektroninių spaudų metaduomenys fiksuojami PDF parašo žodyno laukuose bei CAdES formato skaitmeninio parašo laukuose ir atributuose. Elektroninių parašų ir elektroninių spaudų metaduomenys ir jų reikšmių tipai apibrėžti Specifikacijos 1 priedo 3 skyriuje.

36. Specifikaciją atitinkančio elektroninio dokumento PDF dokumento katalogo žodynas privalo turėti lauką „**Metadata**“, kurio reikšmė yra metaduomenų šaltinis, apimantis šią informaciją:

36.1. PDF/A standarto versiją ir suderinamumo su standartu lygį identifikuojančius metaduomenis, aprašytus vadovaujantis PDF/A-3 standarto 6.6.4 skyriuje nustatytais reikalavimais;

36.2. PDF-RC-V1.0 XMP metaduomenų plėtinio schemą (Specifikacijos 2 priedas), jeigu yra naudojami metaduomenys iš „LTUD“ vardų zonos;

36.3. privalomuosius elektroninio dokumento sudarymo metaduomenis (Specifikacijos 1 priedo 1 skyrius).

37. Sudarant PAdES parašą, PDF parašo žodyne turi būti užpildyti privalomieji elektroninio parašo ar elektroninio spaudos metaduomenų laukai (Specifikacijos 1 priedo 3 skyrius).

38. Su PAdES parašu susieti dokumento registravimo metaduomenys (Specifikacijos 1 priedo 2 skyrius) saugomi metaduomenų šaltinio pavidalu PDF parašo formos lauko žodyno lauke „**Metadata**“.

39. Elektroniniame dokumente gali būti kitų PDF-1.7 ir PDF/A-3 standartuose bei XMP specifikacijoje apibrėžtų neprivalomų metaduomenų, kai jų įtraukimo būdas nepažeidžia šios Specifikacijos reikalavimų.

40. Elektroninis dokumentas, atsižvelgiant į jo gyvavimo ciklą, gali turėti ir kitų (papildomų) metaduomenų, kurie nėra apibrėžti šioje Specifikacijoje ir jos 39 punkte nurodytuose standartuose ir specifikacijose. Jeigu šie papildomi metaduomenys fiksuojami XMP formatu, elektroniniame dokumente turi būti pateikta ir naujus metaduomenų elementus bei jų reikšmių tipus aprašanti XMP metaduomenų plėtinio schema, sudaryta pagal PDF/A-3 standarto 6.6.2.3 skyriuje nustatytus reikalavimus. Jei papildomi metaduomenys fiksuojami PDF žodynų laukuose, naudojamų papildomų laukų vardų prefiksas turi būti apibrėžtas PDF dokumento katalogo žodyno plėtinių žodyne pagal PDF-1.7 standarto 7.12 skyriuje nustatytus reikalavimus.

41. Sudarant elektroninį dokumentą, PDF dokumento informacijos žodyno (PDF-1.7 standarto 14.3.3 skyrius) kurti nerekomenduojama. Jeigu šis žodynas kuriamas, PDF dokumento katalogo metaduomenų šaltinyje privalo būti nurodytos PDF žodyno laukus atitinkančios XMP metaduomenų reikšmės, atsižvelgiant į PDF/A-3 standarto 6.6.3 skyriuje pateiktą PDF žodyno laukų ir XMP metaduomenų atitikčių lentelę.

42. Elektroninio dokumento sudarymo ir tikrinimo priemonės privalo sudaryti ir patikrinti šioje Specifikacijoje apibrėžtus metaduomenis. Interaktyvios programinės priemonės privalo atvaizduoti Specifikacijoje apibrėžtus elektroninio dokumento metaduomenis. Kiti metaduomenys, kurių programinės priemonės nepalaiko, turi būti ignoruojami, išskyrus tuos atvejus, kai jų įtraukimo būdas pažeidžia šios Specifikacijos reikalavimus.

43. Elektroninio dokumento metaduomenys privalo būti pasirašyti PAdES parašu.

44. Pasirašyto elektroninio dokumento metaduomenis draudžiama šalinti, keisti ar pildyti (pvz., inkrementinio keitimo būdu), išskyrus šios Specifikacijos 91 punkte nurodytus atvejus.

VI SKYRIUS

ELEKTRONINIAI PARAŠAI IR ELEKTRONINIAI SPAUDAI

45. Elektroninis dokumentas pasirašomas PAdES parašu, kurio duomenys saugomi PDF parašo žodyno „**Contents**“ lauke saugomame CAdES formato skaitmeniniame paraše, kituose PDF parašo žodyno laukuose, PDF dokumento laiko žymų žodynuose ir DSS žodynuose.

46. PAdES parašu turi būti pasirašomi visi PDF rinkmenoje esantys duomenys, išskyrus paties skaitmeninio parašo reikšmę (PAdES standarto 1 dalis, 6.3 skyrius; PDF/A-3 standarto B priedas).

47. Elektroninis dokumentas pasirašomas tik daugiapakopiu pasirašymo būdu. Lygiagretusis pasirašymo būdas draudžiamas.

48. Elektroniniame dokumente galimi šie PAdES parašai:

48.1. kvalifikuoti elektroniniai parašai;

48.2. kvalifikuoti elektroniniai spaudai;

48.3. elektroniniai parašai ar elektroniniai spaudai, užtikrinantys duomenų autentiškumą ir vientisumą.

49. Elektroninių dokumentų pasirašymo, tvirtinimo, suderinimo ir kopijos tikrumo patvirtinimo paskirties (Specifikacijos 1 priedo 10 pastaba) PAdES parašai turi būti kvalifikuoti elektroniniai parašai arba kvalifikuoti elektroniniai spaudai.

50. Galimos tik šios elektroninio spaudo paskirtys: tvirtinimas, suderinimas, registravimas, gauto dokumento registravimas, archyvinis patvirtinimas, kopijos tikrumo patvirtinimas, autentiškumo (vientisumo) patvirtinimas (Specifikacijos 1 priedo 10 pastaba).

51. PAdES parašai turi būti kuriami vadovaujantis parašo taisyklėmis (jeigu jos yra), LST EN 319 102-1 V1.1.1:2016 (Specifikacijos 12 priedo 5 punktas) standarte aprašytais procedūromis ir laikantis PAdES standarte apibrėžtų reikalavimų.

52. Kvalifikuoti elektroniniai parašai turi būti sukurti naudojant saugią elektroninio parašo formavimo sistemą ir patvirtinti galiojančiu kvalifikuotu elektroninio parašo sertifikatu, atitinkančiu standartą LST EN 319 412-2 V2.1.1:2016 (Specifikacijos 12 priedo 8 punktas). Kvalifikuoti elektroniniai spaudai turi būti patvirtinti galiojančiu kvalifikuotu elektroninio spaudo sertifikatu, atitinkančiu standartą LST EN 319 412-3 V1.1.1:2016 (Specifikacijos 12 priedo 9 punktas).

53. Elektroniniame dokumente galimi tik PAdES-B-B, PAdES-B-T, PAdES-B-LT arba PAdES-B-LTA formato PAdES parašai. Atsižvelgiant į tai, kad PAdES standartas yra universalus ir numato alternatyvas, Specifikacijoje sukonkretinamas PAdES parašų elementų naudojimas konkrečiau taikymo atveju.

54. Elektroninio dokumento turinyje gali būti pridedama PAdES parašo buvimą atvaizduojanti informacija (PDF standarto 12.7.4.5 skyrius). Ji elektroniniame dokumente pridedama prieš PAdES parašo sudarymą ir gali būti sudaryta iš tekstinės ir (arba) grafinės informacijos (pvz., sertifikato duomenų).

55. Jeigu elektroninio dokumento turinyje pridedama PAdES parašo buvimą atvaizduojanti informacija:

55.1. ji negali uždengti dokumento turinį atvaizduojančios informacijos;

55.2. elektroniniame dokumente konkretaus PAdES parašo buvimas gali būti atvaizduotas ne daugiau kaip vieną kartą – PDF parašo žodynas gali būti susietas tik su vienu „Widget“ tipo PDF anotacijų žodynu (angl. *widget annotations dictionary*; PDF standarto 12.5.6.19 skyrius). PDF parašo ir PDF anotacijų žodynai susiejami PDF parašo formos lauko žodyne.

56. Elektroninis dokumentas gali būti papildytas PAdES parašais, modifikuojant PDF rinkmeną inkrementinio keitimo būdu, kaip tai aprašyta PDF-1.7 standarto 7.5.6 skyriuje.

57. Visi PDF rinkmenoje esantys skaitmeniniai parašai turi būti tvirtinamieji (angl. *approval*), kaip tai aprašyta PDF-1.7 standarto 12.8.1 skyriuje. Kiti šiame skyriuje aprašyti sertifikavimo (angl. *certification*) ir naudojimo teisių (angl. *usage rights*) skaitmeniniai parašai draudžiami.

58. Jeigu sudarant PAdES parašą užpildomas PDF parašo formos lauko pradinių reikšmių žodynas (angl. *signature field seed value dictionary*), apibrėžtas PDF-1.7 standarto 12.7.4.5 skyriuje, jame nurodyti ribojimai neturi prieštarauti šios Specifikacijos reikalavimams.

59. PDF parašo žodyno laukai turi būti užpildyti taip, kaip nurodyta šios Specifikacijos 5 priede.

60. PDF parašo žodyno „**Contents**“ lauke saugomi skaitmeninio parašo duomenys turi būti CAdES formato. CAdES formato skaitmeninio parašo atributų leistinumai ir privalomumas nurodytas PAdES standarto 5.2 ir 6.3 skyriuose bei sukonkretintas Specifikacijos 8 priede.

61. PDF parašo žodyno „**Contents**“ lauke saugomo CAdES formato skaitmeninio parašo duomenų struktūra, elementų privalomumo ir reikšmių pildymo reikalavimai nurodyti šios Specifikacijos 8 priede, algoritmai PAdES parašams formuoti pateikti Specifikacijos 7 priede.

62. PDF parašo žodyno „**Contents**“ lauke saugomo CAdES formato skaitmeninio parašo atributai turi būti užkoduoti naudojant DER koduotę.

63. Tam, kad būtų galima automatinėmis priemonėmis patikrinti PAdES parašą baigus galioti pasirašančiojo asmens sertifikatui (kai baigiasi sertifikato galiojimo terminas arba sertifikatas paskelbiamas negaliojančiu), į elektroninį dokumentą turi būti įtraukti parašo galiojimą patvirtinantys duomenys ir elektroninės laiko žymos.

64. Parašo galiojimą patvirtinantys duomenys turi būti išsaugoti PDF dokumento duomenų saugyklos žodyne (angl. *document security store dictionary*, *DSS*), kaip aprašyta PAdES standarto 5.4 skyriuje.

65. PDF formato rinkmenoje gali būti naudojamos dviejų rūšių elektroninės laiko žymos:

65.1. parašo laiko žyma, saugoma CAdES formato skaitmeninio parašo nepasirašomame elektroninės laiko žymos atribute „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 5.3 skyrius), patvirtinanti PAdES parašą, į kurį yra įtraukta, egzistavimą iki parašo laiko žymoje nurodyto laiko;

65.2. PDF dokumento laiko žyma, saugoma PDF dokumento laiko žymos žodyne, patvirtinanti visų iki jos sudarymo įtrauktų PAdES parašų, parašų tikrinimo duomenų ir elektroninių laiko žymų (tiek parašų laiko žymų, tiek PDF dokumento laiko žymų) egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko.

66. Visos elektroninės laiko žymos turi atitikti standartą LST EN 319 422 V1.1.1:2016 (Specifikacijos 12 priedo 10 punktas). Elektroninės laiko žymos turi būti gaunamos HTTP arba HTTPS protokolu pagal RFC 3161 rekomendacijas (Specifikacijos 12 priedo 213 punktas). Kvalifikuotuose elektroniniuose parašuose ir kvalifikuotuose elektroniniuose spauduose turi būti

naudojamos kvalifikuotos elektroninės laiko žymos, atitinkančios LST EN 319 422 V1.1.1:2016 standarto (Specifikacijos 12 priedo 10 punktas) 9 skyriaus reikalavimus.

67. CRL sąrašai turi atitikti RFC 5280 rekomendacijas (Specifikacijos 12 priedo 247 punktas) ir turi būti gaunami HTTP arba HTTPS protokolu.

68. OCSP paslaugų atsakymai turi atitikti RFC 6960 rekomendacijas (Specifikacijos 12 priedo 26 punktas) ir turi būti gaunami HTTP arba HTTPS protokolu.

69. PDF dokumento laiko žymos žodyno laukai turi būti užpildyti taip, kaip nurodyta šios Specifikacijos 6 priede.

70. Elektroniniame dokumente galimi einamieji, trumpalaikiai ir ilgalaikiai PAdES parašai.

71. Einamasis PAdES parašas yra PAdES-B-B formato skaitmeninis parašas be parašo laiko žymos, esantis PDF formato rinkmenoje, kurioje nėra nė vienos PDF dokumento laiko žymos, patvirtinančios PAdES parašo egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko.

72. Trumpalaikiai PAdES parašai gali būti dviejų tipų:

72.1. PAdES-B-T arba PAdES-B-LT formato skaitmeninis parašas su parašo laiko žyma, esantis PDF formato rinkmenoje, kurioje nėra nė vienos PDF dokumento laiko žymos, patvirtinančios parašo galiojimą patvirtinančių duomenų egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko (Specifikacijos 9 priedo 1 punktas);

72.2. PAdES-B-T arba PAdES-B-LT formato skaitmeninis parašas be parašo laiko žymos, esantis PDF formato rinkmenoje, kurioje yra PDF dokumento laiko žyma, patvirtinanti PDF parašo egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko, ir nėra nė vienos PDF dokumento laiko žymos, patvirtinančios parašo galiojimą patvirtinančių duomenų egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko (Specifikacijos 9 priedo 2 punktas).

73. Ilgalaikiai PAdES parašai gali būti dviejų tipų:

73.1. PAdES-B-LTA formato skaitmeninis parašas su parašo laiko žyma, esantis PDF formato rinkmenoje, kurioje yra parašo galiojimą patvirtinantys duomenys ir bent viena PDF dokumento laiko žyma, patvirtinanti parašo galiojimą patvirtinančių duomenų egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko (Specifikacijos 9 priedo 3 punktas);

73.2. PAdES-B-LTA formato skaitmeninis parašas be parašo laiko žymos, esantis PDF formato rinkmenoje, kurioje yra bent dvi PDF dokumento laiko žymos ir parašo galiojimą patvirtinantys duomenys. Pirmoji PDF dokumento laiko žyma turi patvirtinti PAdES parašo egzistavimą iki pirmojoje PDF dokumento laiko žymoje nurodyto laiko. Parašo galiojimą patvirtinantys duomenys turi būti įtraukti vėliau nei pirmoji PDF dokumento laiko žyma. Antroji PDF dokumento laiko žyma turi patvirtinti parašo galiojimą patvirtinančių duomenų egzistavimą iki antrojoje PDF dokumento laiko žymoje nurodyto laiko (Specifikacijos 9 priedo 4 punktas).

VII SKYRIUS

ELEKTRONINIO DOKUMENTO TIKRINIMAS

74. Elektroninio dokumento tikrinimas susideda iš:

74.1. elektroninio dokumento atitikties Specifikacijai tikrinimo;

74.2. elektroninio dokumento PAdES parašų galiojimo tikrinimo.

75. Elektroninio dokumento atitikties Specifikacijai tikrinimo metu turi būti patikrinta, ar elektroninis dokumentas atitinka visus šioje Specifikacijoje nustatytus elektroninio dokumento

pakuotės, struktūros, metaduomenų ir PAdES parašų formato reikalavimus, atsižvelgiant į reikalavimų lygmenis.

76. Jei PDF dokumento katalogo žodyno metaduomenų šaltinyje yra deklaruojama atitiktis „A“ reikalavimų lygmeniui (Specifikacijos 1 priedas), turi būti tikrinama elektroninio dokumento atitiktis Specifikacijos A lygmens reikalavimams. Visais kitais atvejais turi būti tikrinama elektroninio dokumento atitiktis Specifikacijos B lygmens reikalavimams.

77. PDF rinkmenos atitikties deklaruoto standarto (PDF/A-3) reikalavimams patikra neturi apsiriboti vien tik šios Specifikacijos 36.1 papunktyje nurodytų metaduomenų egzistavimo patikra.

78. Visų PAdES parašų galiojimo tikrinimas turi būti atliekamas vadovaujantis LST EN 319 102-1 V1.1.1:2016 standarte (Specifikacijos 12 priedo 5 punktas) aprašytomis procedūromis ir laikantis PAdES standarte apibrėžtų reikalavimų. Tikrinant kvalifikuotus elektroninius parašus, papildomai turi būti vadovujamasi Reglamento 32 straipsnio nuostatomis, o tikrinant kvalifikuotus elektroninius spaudus – Reglamento 40 straipsnio nuostatomis, reglamentuojančiomis kvalifikuotų elektroninių spaudų galiojimo patvirtinimą.

79. Jei PAdES parašas nėra kvalifikuotas elektroninis parašas ar kvalifikuotas elektroninis spaudas, jis turi būti patvirtintas elektroninio parašo arba elektroninio spaudos sertifikatu, išduotu patikimumo užtikrinimo paslaugų teikėjo, kuriuo PAdES parašo tikrintojas pasitiki.

80. PAdES paraše esančios elektroninės laiko žymos turi būti kvalifikuotos arba sukurtos patikimumo užtikrinimo paslaugų teikėjų, kuriais PAdES parašo tikrintojas pasitiki.

81. PAdES parašo galiojimą patvirtinantys duomenys turi būti sukurti kvalifikuoto patikimumo užtikrinimo paslaugų teikėjo, arba patikimumo užtikrinimo paslaugų teikėjo, kuriuo PAdES parašo tikrintojas pasitiki. Paslaugų teikėjas turi turėti teisę teikti parašo galiojimą patvirtinančius duomenis apie tikrinamą sertifikatą kaip tai yra nurodyta RFC 5280 (Specifikacijos 12 priedo 24 punktas) ir RFC 6960 (Specifikacijos 12 priedo 26 punktas) rekomendacijose.

82. Jeigu yra parašo laiko žyma ar PDF dokumento laiko žymos, patvirtinančios tikrinamo PAdES parašo egzistavimą iki jose nurodyto laiko, tai šiam PAdES parašui patvirtinti naudoti sertifikatai ir sertifikatų seka tikrinami anksčiausio laiko, nurodyto tose elektroninėse laiko žymose, atžvilgiu. Jeigu tokių elektroninių laiko žymų nėra, tai PAdES parašui patvirtinti naudoti sertifikatai ir sertifikatų seka tikrinami einamojo laiko atžvilgiu.

83. Jeigu yra PDF dokumento laiko žymos, patvirtinančios tikrinamo parašo galiojimą patvirtinančių duomenų egzistavimą iki jose nurodyto laiko, tai šie parašo galiojimą patvirtinantys duomenys tikrinami anksčiausio laiko, nurodyto tose elektroninėse laiko žymose, atžvilgiu. Jeigu tokių elektroninių laiko žymų nėra, tai parašo galiojimą patvirtinantys duomenys tikrinami einamojo laiko atžvilgiu.

84. Jeigu yra PDF dokumento laiko žymos, patvirtinančios tikrinamos elektroninės laiko žymos (tiek parašo laiko žymos, tiek PDF dokumento laiko žymos) egzistavimą iki jose nurodyto laiko, tai šią elektroninę laiko žymą patvirtinantis sertifikatas ir sertifikatų seka tikrinami anksčiausio laiko, nurodyto tose elektroninėse laiko žymose, atžvilgiu. Jeigu tokių elektroninių laiko žymų nėra, tai elektroninę laiko žymą patvirtinantis sertifikatas ir sertifikatų seka tikrinami einamojo laiko atžvilgiu.

85. Sertifikatų galiojimą patvirtinantys duomenys (OCSP paslaugos atsakymai ar CRL sąrašai) laikomi tinkamais PAdES parašui ar elektroninei laiko žymai tikrinti, jeigu atitinka bent vieną šių reikalavimų:

85.1. sertifikatų galiojimą patvirtinantys duomenys yra surinkti PAdES parašo ar elektroninės laiko žymos tikrinimo metu;

85.2. sertifikatų galiojimą patvirtinantys duomenys yra surinkti ir įtraukti į dokumentą ne anksčiau, nei buvo įtraukta anksčiausia iš elektroninių laiko žymų, patvirtinančių PAdES parašo egzistavimą iki jose nurodyto laiko (elektroninės laiko žymos tikrinimo atveju – ne anksčiau, nei buvo sukurta pati tikrinamoji elektroninė laiko žyma).

86. Kiekvienas PAdES parašas tikrinamas neatsižvelgiant į kitų elektroninio dokumento PAdES parašų galiojimą.

VIII SKYRIUS

SPECIFIKACIJOS REIKALAVIMŲ LYGMENYS

87. Pagal šią Specifikaciją sudarytas elektroninis dokumentas turi būti rengiamas pagal Specifikacijos 4 punkte apibrėžtus A arba B reikalavimų lygmenis.

Specifikacijos reikalavimų, skirtingai taikomų A ir B lygmens elektroniniams dokumentams, suvestinė pateikta Specifikacijos 10 priede.

88. Elektroniniame dokumente atitiktis reikalavimų lygmeniui turi būti deklaruojama `xmp:Identifier` elemente PDF dokumento katalogo metaduomenų šaltinyje, kaip nurodyta Specifikacijos 1 priedo 1 skyriuje. B lygmens elektroniniam dokumentui šis reikalavimas neprivalomas.

89. A lygmens dokumentas iš B lygmens dokumento formuojamas, papildant jį privalomais A lygmens metaduomenimis ir objektais inkrementinio keitimo būdu.

90. Bet kokie Specifikacijos leidžiami elektroninio dokumento turinio ar metaduomenų papildymai ir pakeitimai turi būti patvirtinti PAdES parašu, kuris apimtų visą rinkmeną, įskaitant visus atliktus papildymus ir pakeitimus.

91. Leidžiami tik šie dokumento pakuotės, turinio ir metaduomenų keitimo (inkrementinio keitimo būdu) atvejai:

91.1. elektroninio dokumento papildymas nauju PAdES parašu kartu su registravimo metaduomenimis arba be jų (Specifikacijos 56 punktas);

91.2. elektroninio dokumento papildymas parašo galiojimą patvirtinančiais duomenimis (DSS ir VRI žodynuose);

91.3. elektroninio dokumento papildymas nauja PDF dokumento laiko žyma;

91.4. turinio papildymas PAdES parašų buvimo atvaizdavimo informacija (Specifikacijos 55 punktas);

91.5. PDF dokumento katalogo plėtinių žodyno papildymas PDF žodyno laukų prefiksu „LTUd“ (Specifikacijos 15 punktas);

91.6. B lygmens elektroninio dokumento PDF dokumento katalogo žodyno metaduomenų šaltinio papildymas XMP metaduomenų plėtinio schema (Specifikacijos 36.2 papunktis);

91.7. B lygmens elektroninio dokumento PDF dokumento katalogo žodyno metaduomenų šaltinio papildymas dokumento sudarymo ir kitais metaduomenimis (Specifikacijos 36.3 papunktis, 39, 40 punktai);

91.8. dokumento sudarymo metaduomenyse `xmp:Identifier` reikšmių rinkinio papildymas arba pakeitimas nauja elektroninio dokumento atitikties reikalavimų lygmeniui deklaracijos reikšme (Specifikacijos 1 priedo 1 skyrius);

91.9. dokumento sudarymo metaduomenyse `xmp:Identifier` reikšmių rinkinio papildymas nauja elektroninio dokumento atitikties specifikacijos redakcijai deklaracijos reikšme (Specifikacijos 1 priedo 1 skyrius), jeigu jos nebuvo.

92. B lygmens elektroninį dokumentą pildant dokumento sudarymo metaduomenimis, juose rekomenduojama nurodyti `xmpMM:History` metaduomenis, kuriais būtų aprašyti atlikti papildymai. Šie „XMP Media Management“ schemos vardų zonoje (XMP specifikacijos 4 skyrius) apibrėžti standartiniai metaduomenys yra skirti informacinių išteklių valdymo sistemoms ir juos naudojant vadovaujamasi PDF/A-3 standarto 6.6.6 skyriumi ir XMP specifikacija (Specifikacijos 12 priedo 230 punktas).

IX SKYRIUS

BAIGIAMOSIOS NUOSTATOS

93. Dokumentų, kuriais remiantis parengta Specifikacija, sąrašas pateikiamas šios Specifikacijos 12 priede.

METADUOMENYS

I SKYRIUS DOKUMENTO SUDARYMO METADUOMENYS

Dokumento sudarymo metaduomenys nurodomi PDF dokumento katalogo žodyno metaduomenų šaltinyje. Šie metaduomenys neprivalomi B lygmens elektroniniame dokumente. Metaduomenų pavyzdys pateikiamas 4 priedo I skyriuje.

Metaduomuo	XMP vardas ¹	Tipas ²	Privalomas A lygmens dokumentui	Aprašas
Elektroninio dokumento specifikacijos identifikacinis žymuo	LTUd:standardVersion	Riboto pasirinkimo tekstas	Taip	Šią specifikaciją atitinkančiam elektroniniam dokumentui nurodoma reikšmė „PDF-RC-V1.0“.
Dokumento atitikties reikalavimų lygmeniui deklaracija	xmp:Identifier	Teksto reikšmių rinkinys	Taip	Atitiktis reikalavimų lygmeniui deklaruojama rinkinyje įdėjus reikšmę, kuria nurodomas lygmuo ir reikšmės kvalifikatorius. Deklaravimui turi būti naudojama reikšmės struktūra, pateikta šio priedo 6 pastaboje.
Dokumento atitikties specifikacijos redakcijai deklaracija			Ne	Atitiktis specifikacijos redakcijai deklaruojama rinkinyje įdėjus reikšmę, kuria nurodomas redakcijos numeris ir reikšmės kvalifikatorius. Deklaravimui turi būti naudojama reikšmės struktūra, pateikta šio priedo 7 pastaboje.
Dokumento sudarytojai	LTUd:authors	Asmens tipo reikšmių seka	Taip	Reikšmių seka, kuria aprašytas vienas ar daugiau juridinių ar fizinių asmenų, sudariusių dokumentą. Seka privalo turėti bent vieną reikšmę. Sudarytojų pavadinimų (LTUdEnt:name lauko) reikšmės turi būti pakartotos metaduomens dc:creator reikšmėje.
Adresatai	LTUd:recipients	Asmens tipo reikšmių seka	Taip, pagal pobūdį	Jeigu adresatai nurodomi, jie metaduomenyse fiksuojami reikšmių seka, kuria aprašytas vienas ar daugiau juridinių ar fizinių asmenų, nurodytų kaip adresatai. Nurodyta seka privalo turėti bent vieną reikšmę. Jei adresatai nenurodomi, metaduomens neturi būti iš viso.
Dokumento pavadinimas	dc:title	Tekstas skirtingomis kalbomis	Taip	Privaloma užpildyti reikšmę su atributo xml:lang reikšme „x-default“.

Metaduomuo	XMP vardas ¹	Tipas ²	Privalomas A lygmens dokumentui	Aprašas
Dokumento sudarytojų – juridinių asmenų – pavadinimai ar fizinių asmenų vardai ir pavardės	dc:creator	Pavadinimo tipo reikšmių seka	Taip	Dokumentą formuojanti priemonė turi užpildyti šį metaduomenį sudarytojų (LTUd:authors) pavadinimo (LTUdEnt:name lauko) reikšme. Dokumento metaduomenis skaitanti priemonė turi naudoti metaduomenų elemente LTUd:authors nurodytas reikšmes.
Dokumento kalbos	dc:language	Kalbos kodų rinkinys	Ne	Nurodoma, kokiomis kalbomis yra parengtas dokumentas. Lietuvių kalba sudarytiems dokumentams rekomenduojama nurodyti reikšmę „lt-LT“.
Dokumento egzemplioriaus identifikacinis žymuo	LTUd:documentCopyIdentifier	Tekstas	Ne	Metaduomuo skirtas to paties dokumento egzemplioriams (ne tapačioms kopijoms) atskirti, pvz., skirtingiems sutarties egzemplioriams Lietuvai ir Latvijai.
Dokumento parašų ir spaudų duomenys kopijoje	LTUd:originalSignatures	Parašo tipo reikšmių seka	Ne	Į dokumento elektroninę kopiją iš originalaus dokumento perkelti dokumento parašų ir spaudų metaduomenys.
Dokumento registravimo duomenys kopijoje	LTUd:originalRegistrations	Registracijos tipo reikšmių seka	Ne	Į dokumento elektroninę kopiją iš originalaus dokumento perkelti dokumento registracijos (LTUd:registration) metaduomenys.
Gauto dokumento registravimo duomenys kopijoje	LTUd:originalReceptions	Registracijos tipo reikšmių seka	Ne	Į dokumento elektroninę kopiją iš originalaus dokumento perkelti gauto dokumento registracijos (LTUd:reception) metaduomenys.
Dokumento gavėjai kopijoje	LTUd:originalReceivers	Asmens tipo reikšmių seka	Ne	Į dokumento elektroninę kopiją iš originalaus dokumento perkelti dokumento gavėjų (LTUd:receiver) metaduomenys.
Elektroninį dokumentą suformavusios priemonės pavadinimas ir versija	xmp:CreatorTool	Programinės įrangos pavadinimas	Ne	Rekomenduojamas reikšmės užpildymo formatas pateiktas reikšmės tipo apraše.

II SKYRIUS

DOKUMENTO REGISTRAVIMO METADUOMENYS

Dokumento registravimo metaduomenys nurodomi PDF parašo formos lauko žodyno metaduomenų šaltinyje. Šie metaduomenys neprivalomi B lygmens elektroniniame dokumente. Metaduomenų pavyzdžiai pateikiami 4 priedo II ir III skyriuose.

Metaduomuo	XMP vardas ¹	Tipas ²		Privalomas A lygmens dokumentui	Aprašas
Sudaryto dokumento registravimo duomenys	LTUd:registration	Registracija		Taip, jei registravimą nustato teisės aktai	Pildo elektroninio dokumento sudarytojas. Dokumente gali būti nulis ar daugiau metaduomenų. Viena PDF parašo formos lauko žodyno metaduomenų šaltinyje gali būti nurodytas ne daugiau kaip vienas metaduomuo.
Gauto dokumento registravimo duomenys	LTUd:reception	Registracija		Taip, jei registravimą nustato teisės aktai	Pildo elektroninio dokumento gavėjas. Dokumente gali būti nulis ar daugiau metaduomenų. Viena PDF parašo formos lauko žodyno metaduomenų šaltinyje gali būti nurodytas ne daugiau kaip vienas metaduomuo. Kai nurodomi gauto dokumento registracijos metaduomenys, tame pačiame metaduomenų šaltinyje turi būti nurodyti ir dokumento gavėjo metaduomenys (LTUd:receiver).
Dokumento gavėjas	LTUd:receiver	Asmuo		Taip, jei registravimą nustato teisės aktai	Pildo elektroninio dokumento gavėjas. Dokumente gali būti nulis ar daugiau metaduomenų. Viena PDF parašo formos lauko žodyno metaduomenų šaltinyje gali būti nurodytas ne daugiau kaip vienas metaduomuo.

III SKYRIUS

ELEKTRONINIŲ PARAŠŲ IR ELEKTRONINIŲ SPAUDŲ METADUOMENYS

Elektroninių parašų ir elektroninių spaudų metaduomenys nurodomi kiekvieno PDF parašo žodyno laukuose.

Metaduomuo	PDF parašo žodyno lauko raktas (vardas)	Tipas ⁸	Privalomas A lygmens dokumentui	Privalomas B lygmens dokumentui	Aprašas
Elektroninio parašo ar elektroninio spaudo paskirtis	Reason arba Contents lauke saugomame CAdES formato skaitmeninio parašo atributute ⁹	Tekstas (text string), ar objekto identifikatorius ¹⁰	Ne ¹¹	Ne ¹¹	Elektroninio parašo ar elektroninio spaudo paskirtį žyminčios reikšmės nurodytos šio priedo 10 pastaboje.

Metaduomuo	PDF parašo žodyno lauko raktas (vardas)	Tipas ⁸	Privalomas A lygmens dokumentui	Privalomas B lygmens dokumentui	Aprašas
Elektroninį parašą ar elektroninį spaudą sudaręs asmuo	Name	Tekstas (text string)	Taip, jei šių duomenų nėra sertifikate	Taip, jei šių duomenų nėra sertifikate	Jeigu elektroninį parašą sudariusio asmens vardas ir pavardė yra nurodyti ir sertifikate, ir šiame PDF parašo žodyno lauke, tai vardas ir pavardė turi sutapti. Jeigu jie nesutampa, naudojami duomenys iš sertifikato. Jeigu elektroninį spaudą sudariusio juridinio asmens pavadinimas yra nurodytas ir sertifikate, ir šiame PDF parašo žodyno lauke, tai pavadinimas turi sutapti. Jeigu jie nesutampa, naudojami duomenys iš sertifikato.
Elektroninį parašą sudariusio asmens pareigos	LTUd_Role	Tekstas (text string)	Taip, jei pasirašo viešo juridinio asmens atstovas	Ne	
Elektroninio parašo ar elektroninio spaudos sudarymo data (deklaruojama)	M¹²	Data (date)	Taip	Taip	
Elektroninį parašą sudariusio asmens pastaba	LTUd_SignerNotes	Tekstas (text string)	Taip, pagal pobūdį	Ne	Vizavimo pastaba, rezoliucijos tekstas, žyma apie užduoties įvykdymą ar kita.

Pastabos:

1. Lentelėje nurodyti XMP vardai, susidedantys iš XML prefikso ir elemento vardo (**prefix:local**), kaip tai apibrėžta XMP specifikacijos 2 skyriuje „Schemas and Namespaces“. Metaduomenų schemoms apibrėžti naudojamų XMP vardų prefiksų paaiškinimai pateikti šioje lentelėje:

Prefiksas	URI	XMP/XML schema
LTUd	http://archyvai.lt/pdf-ltud/2013/metadata/	Metaduomenų lentelėje aprašyta ir 2 priede apibrėžta XMP metaduomenų plėtinio schema.
dc	http://purl.org/dc/elements/1.1/	<i>Dublin Core</i> XMP metaduomenų schema, apibrėžta XMP specifikacijos 4 skyriuje „Dublin Core Schema“.
xmp	http://ns.adobe.com/xap/1.0/	XMP metaduomenų schema, apibrėžta XMP specifikacijos 4 skyriuje „XMP Basic Schema“.
rdf	http://www.w3.org/1999/02/22-rdf-syntax-ns#	XML schema, apibrėžta W3C rekomendacijose „RDF/XML sintaksės specifikacija (peržiūrėta)“ (Specifikacijos 12 priedo 28 punktas).
xmpidq	http://ns.adobe.com/xmp/Identifier/qual/1.0/	xmp:Identifier metaduomenų reikšmių kvalifikatorių schema, apibrėžta XMP specifikacijos 4 skyriuje „XMP Basic Schema“.

2. Toliau pateiktoje lentelėje aprašyti XMP metaduomenų reikšmių duomenų tipai:

Tipas	Aprašas
-------	---------

Tipas	Aprašas
Asmuo	Šių pastabų 3 punkte aprašyta metaduomenų plėtinio struktūra.
Registracija	Šių pastabų 4 punkte aprašyta metaduomenų plėtinio struktūra.
Parašas	Šių pastabų 5 punkte aprašyta metaduomenų plėtinio struktūra.
Loginis	Reikšmė, galinti įgyti tik dvi reikšmes: taip („True“) arba ne („False“).
Data	Datos arba datos ir laiko reikšmė aprašyta XMP specifikacijos 4 skyriuje „Basic Value Types“ apibrėžtu formatu. Datų formatai be dienos parametro („YYYY“ ir „YYYY-MM“) draudžiami. Jei nurodomas laikas, turi būti nurodyta ir laiko zona.
Tekstas	Unicode koduote užkoduotas tekstas, galintis būti tuščias (turintis 0 simbolių).
Programinės įrangos pavadinimas	Tekstinio tipo reikšmė, kurios rekomenduojamas užpildymo formatas: „Organizacija Programa Versija (tekstas; tekstas;...)“, čia: Organizacija – programinės įrangą sukūrusios organizacijos pavadinimas; Programa – programinės įrangos pavadinimas; Versija – konkreti programinės įrangos versija; tekstas – papildoma informacija, nurodanti operacinės sistemos versiją, įdiegtus komponentus, kita.
Riboto pasirinkimo tekstas	(angl. <i>closed choice</i>) Tekstinis laukas, kuriame leidžiama nurodyti tik apibrėžtą aibę reikšmių.
Tekstas skirtingomis kalbomis	(angl. <i>language alternative</i>) Alternatyvus tekstinio tipo reikšmių sąrašas. Kiekviena masyvo, aprašomo elementu rdf:Alt , reikšmė privalo turėti atributą xml:lang , kuriame turi būti nurodyta RFC 3066 rekomendacijos (Specifikacijos 12 priedo 19 punktas) atitinkanti kalbos kodo reikšmė arba reikšmė „x-default“ standartinei teksto reikšmei nurodyti.
Kalbos kodas	(angl. <i>locale</i>) Tekstinis laukas, kuriame nurodyta RFC 3066 rekomendacijos (Specifikacijos 12 priedo 19 punktas) atitinkanti kalbos kodo reikšmė.
Pavadinimas	Tekstas, juridinio asmens pavadinimas ar fizinio asmens vardas ir pavardė
Nurodyto tipo reikšmių seka	Nurodyto tipo reikšmių masyvas, aprašomas elementu rdf:Seq , kuriame elementų išdėstymo tvarka yra svarbi.
Nurodyto tipo reikšmių rinkinys	Nurodyto tipo reikšmių masyvas, aprašomas elementu rdf:Bag , kuriame elementų išdėstymo tvarka nėra svarbi.

3. Toliau pateiktoje lentelėje aprašyta **Asmens** tipo (prefiksas: *LTUdEnt*; URI: <http://archyvai.lt/pdf-ltud/2013/metadata/Entity/>) struktūra:

Laukas	XMP vardas	Tipas	Privalomas (nurodžius asmenį)			Pastabos
			Sudarytojui ir parašą ar spaudą sudariusiam asmeniui	Adresatui	Gavėjui	
Požymis: fizinis (taip) ar juridinis (ne) asmuo	LTUdEnt:individual	Loginis	Taip	Ne	Taip	
Juridinio asmens pavadinimas arba fizinio asmens vardas ir pavardė	LTUdEnt:name	Tekstas	Taip	Taip	Taip	Sudarytojų pavadinimų (LTUdEnt:name laukų) reikšmės turi būti pakartotos dokumento metaduomens dc:creator reikšmėje.

Laukas	XMP vardas	Tipas	Privalomas (nurodžius asmenį)			Pastabos
			Sudarytojui ir parašą ar spaudą sudariusiam asmeniui	Adresatui	Gavėjui	
Juridinio ar fizinio asmens kodas	LTUdEnt:code	Tekstas	Taip, jei juridinis asmuo	Ne	Taip, jei juridinis asmuo	Lauko reikšmės privalomumas turi būti tikrinamas atsižvelgiant į požymį, ar tai fizinis, ar juridinis asmuo.
Adresas	LTUdEnt:address	Tekstas	Ne	Ne	Ne	
El. pašto adresas	LTUdEnt:eMail	Tekstas	Ne	Ne	Ne	

4. Toliau pateiktoje lentelėje aprašyta Registracijos tipo
(prefiksas: *LTUdReg*; URI: <http://archyvai.lt/pdf-ltud/2013/metadata/Registration/>) struktūra:

Laukas	XMP vardas	Tipas	Privalomas (nurodžius registravimo duomenis)	Pastabos
Registravimo data	LTUdReg:date	Data	Taip	Jeigu data nurodoma su laiku, kaip tai apibrėžta XMP specifikacijoje, turi būti nurodyta ir laiko zona.
Registracijos numeris	LTUdReg:number	Tekstas	Taip	
Juridinio asmens kodas	LTUdReg:code	Tekstas	Ne	Kai yra keli dokumento sudarytojai, nurodomas juridinio asmens, užregistravusio dokumentą, kodas. Gautame dokumente rekomenduojama nurodyti gavėjo kodą.

5. Toliau pateiktoje lentelėje aprašyta Parašo tipo
(prefiksas: *LTUdSig*; URI: <http://archyvai.lt/pdf-ltud/2013/metadata/Signature/>) struktūra:

Laukas	XMP vardas	Tipas	Privalomas (nurodžius parašo ar spaudo duomenis)	Pastabos
Deklaruotas pasirašymo ar spaudo sukūrimo laikas	LTUdSig:signingTime	Data	Taip	Jeigu data nurodoma su laiku, kaip tai apibrėžta XMP specifikacijoje, turi būti nurodyta ir laiko zona.
Parašo ar spaudo paskirtis	LTUdSig:signingPurpose	Tekstas	Taip	Parašo ar spaudo paskirtį žyminčios reikšmės nurodytos šio priedo 10 pastaboje.

Laukas	XMP vardas	Tipas	Privalomas (nurodžius parašo ar spaudo duomenis)	Pastabos
Parašą ar spaudą sudaręs asmuo	LTUdSig:signer	Asmuo	Taip	Parašo atveju nurodomi pasirašančio fizinio asmens metaduomenys. Spaudo atveju nurodomi spaudą sukūrusio juridinio asmens metaduomenys.
Parašo ar spaudo galiojimo tikrinimo informacija	LTUdSig:validationInfo	Tekstas	Ne	Metaduomenyje nurodoma parašo ar spaudo galiojimo tikrinimo informacija: nustatytas parašo galiojimas, galiojimo tikrinimo būdas, data, galiojimo tikrinimą atlikusio asmens ar sistemos duomenys ir kt.

6. Toliau pateiktoje lentelėje aprašyta reikšmės, kuria `xmp:Identifier` elemente deklaruojama elektroninio dokumento atitiktis reikalavimų lygmeniui, struktūra:

Laukas	XMP vardas	Tipas	Pastabos
Dokumento atitiktis lygmuo	rdf:value	Tekstas	Leidžiamos reikšmės: „A“ - deklaruojama atitiktis A lygmeniui; „B“ - deklaruojama atitiktis B lygmeniui.
Kvalifikatorius	xmpidq:Scheme	Tekstas	Reikšmė „ <code>http://archyvai.lt/pdf-ltud/2013/level/</code> “.

7. Toliau pateiktoje lentelėje aprašyta reikšmės, kuria `xmp:Identifier` elemente deklaruojama elektroninio dokumento atitiktis specifikacijos redakcijai, struktūra:

Laukas	XMP vardas	Tipas	Pastabos
Specifikacijos redakcijos numeris	rdf:value	Tekstas	Reikšmė – specifikacijos redakcijos numeris.
Kvalifikatorius	xmpidq:Scheme	Tekstas	Reikšmė „ <code>http://archyvai.lt/pdf-ltud/2013/revision/</code> “.

8. Teksto ir datos duomenų tipai, skirti PDF žodyno reikšmėms fiksuoti, apibrėžti PDF-1.7 standarto 7.9.2 ir 7.9.4 skyriuose.

9. Jeigu CAdES formato skaitmeniniame paraše (saugomame PDF parašo žodyno lauke *Contents*) nėra parašo taisyklių identifikatoriaus atributo (objekto identifikatorius „`id-aa-ets-sigPolicyId`“), tai PAdES parašo paskirtis gali būti nurodyta tik PDF parašo žodyno lauke *Reason*. Jeigu CAdES formato skaitmeniniame paraše yra parašo taisyklių identifikatoriaus atributas, tai PAdES parašo paskirtis gali būti nurodyta tik CAdES formato skaitmeninio parašo atribute, kurio identifikatorius yra `id-aa-ets-commitmentType`. PAdES prašo paskirtis neturi būti nurodyta abejose vietose.

10. Galimos parašų ir spaudų paskirtys yra:

Parašo ar spaudo paskirtis	Identifikatorius nurodomas PDF parašo žodyno lauke <i>Reason</i> ir XMP metaduomenų šaltinyje	Identifikatorius nurodomas CAdES formato skaitmeninio parašo <i>commitment-type-indication</i> atribute	El. parašas ar el. spaudas privalo būti kvalifikuotas	Paskirtį galima nurodyti ir spaudui
pasirašymas	signature	id-cti-ets-proofOfOrigin (1.2.840.113549.1.9.16.6.1)	Privalo	Ne
tvirtinimas	confirmation	id-cti-ets-proofOfApproval (1.2.840.113549.1.9.16.6.5)	Privalo	Taip

PDF parašo žodyno lauko *Reason* reikšmė privalo būti nurodyta be kabučių mažosiomis raidėmis.

11. Jeigu elektroninio parašo paskirties reikšmės nėra arba ji nesutampa su nė viena iš čia išvardytųjų, laikoma, kad elektroninio parašo paskirtis yra pasirašymas (t.y., atitinka reikšmę „signature“). Jeigu elektroninio spaudo paskirties reikšmės nėra arba ji nesutampa su nė viena iš čia išvardytųjų, laikoma, kad elektroninio spaudo paskirtis yra tvirtinimas (t.y., atitinka reikšmę „confirmation“).

12. PDF rinkmenos suformavimo datos metaduomens (**xmp:CreateDate**) reikšmė nelaikytina elektroninio dokumento sudarymo data. Elektroninio dokumento sudarymo data laikytina dokumento registravimo data (jei dokumentas registruojamas) arba vėliausio pasirašymo ar tvirtinimo paskirties PAdES parašo sudarymo data (PDF parašo žodyno lauko „**M**“ reikšmė) (kai dokumentas nėra registruojamas).

XMP METADUOMENŲ PLĖTINIO SCHEMA

```
<rdf:RDF xmlns:rdf = "http://www.w3.org/1999/02/22-rdf-syntax-ns#">
  <rdf:Description rdf:about = ""
    xmlns:pdfaExtension = "http://www.aiim.org/pdfa/ns/extension/"
    xmlns:pdfaSchema = "http://www.aiim.org/pdfa/ns/schema#"
    xmlns:pdfaProperty = "http://www.aiim.org/pdfa/ns/property#"
    xmlns:pdfaType = "http://www.aiim.org/pdfa/ns/type#"
    xmlns:pdfaField = "http://www.aiim.org/pdfa/ns/field#">

    <!-- PDF/A XMP metaduomenų plėtinio schemas -->
    <pdfaExtension:schemas>
      <rdf:Bag>
        <rdf:li rdf:parseType="Resource">
          <pdfaSchema:schema>PDF-RC-V1.0 elektroninio dokumento metaduomenų plėtinio
          schema</pdfaSchema:schema>
          <pdfaSchema:namespaceURI>http://archyvai.lt/pdf-
          ltud/2013/metadata/</pdfaSchema:namespaceURI>
          <pdfaSchema:prefix>LTUd</pdfaSchema:prefix>
          <pdfaSchema:property>
            <rdf:Seq>
              <!-- Dokumento sudarymo metaduomenys (nurodomi dokumento katalogo
              metaduomenų šaltinyje) -->
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>standardVersion</pdfaProperty:name>
                <pdfaProperty:valueType>closed Choice of Text</pdfaProperty:valueType>
                <pdfaProperty:category>internal</pdfaProperty:category>
                <pdfaProperty:description>Elektroninio dokumento specifikacijos
                identifikatorius (pvz., PDF-RC-V1.0)</pdfaProperty:description>
              </rdf:li>
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>authors</pdfaProperty:name>
                <pdfaProperty:valueType>seq Entity</pdfaProperty:valueType>
                <pdfaProperty:category>external</pdfaProperty:category>
                <pdfaProperty:description>Dokumento sudarytojas (-
                ai)</pdfaProperty:description>
              </rdf:li>
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>recipients</pdfaProperty:name>
                <pdfaProperty:valueType>seq Entity</pdfaProperty:valueType>
                <pdfaProperty:category>external</pdfaProperty:category>
                <pdfaProperty:description>Dokumentu adresatas (-
                ai)</pdfaProperty:description>
              </rdf:li>
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>documentCopyIdentifier</pdfaProperty:name>
                <pdfaProperty:valueType>Text</pdfaProperty:valueType>
                <pdfaProperty:category>external</pdfaProperty:category>
                <pdfaProperty:description>Dokumentu egzemplioriaus
                identifikatorius</pdfaProperty:description>
              </rdf:li>
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>originalSignatures</pdfaProperty:name>
                <pdfaProperty:valueType>seq Signature</pdfaProperty:valueType>
                <pdfaProperty:category>external</pdfaProperty:category>
                <pdfaProperty:description>Originalaus dokumento parašų ir spaudų
                duomenys kopijoje</pdfaProperty:description>
              </rdf:li>
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>originalRegistrations</pdfaProperty:name>
```

```

    <pdfaProperty:valueType>seq Registration</pdfaProperty:valueType>
    <pdfaProperty:category>external</pdfaProperty:category>
    <pdfaProperty:description>Originalaus dokumento registracija (-os)
kopijoje</pdfaProperty:description>
  </rdf:li>
  <rdf:li rdf:parseType="Resource">
    <pdfaProperty:name>originalReceptions</pdfaProperty:name>
    <pdfaProperty:valueType>seq Registration</pdfaProperty:valueType>
    <pdfaProperty:category>external</pdfaProperty:category>
    <pdfaProperty:description>Gauto originalaus dokumento registracija (-
os) kopijoje</pdfaProperty:description>
  </rdf:li>
  <rdf:li rdf:parseType="Resource">
    <pdfaProperty:name>originalReceivers</pdfaProperty:name>
    <pdfaProperty:valueType>seq Entity</pdfaProperty:valueType>
    <pdfaProperty:category>external</pdfaProperty:category>
    <pdfaProperty:description>Originalaus dokumento gavėjas (-ai)
kopijoje</pdfaProperty:description>
  </rdf:li>
  <!-- Dokumento registravimo metaduomenys (nurodomi PDF parašo formas
lauko žodyno metaduomenų šaltinyje) -->
  <rdf:li rdf:parseType="Resource">
    <pdfaProperty:name>registration</pdfaProperty:name>
    <pdfaProperty:valueType>Registration</pdfaProperty:valueType>
    <pdfaProperty:category>external</pdfaProperty:category>
    <pdfaProperty:description>Sudaryto dokumento
registracija</pdfaProperty:description>
  </rdf:li>
  <rdf:li rdf:parseType="Resource">
    <pdfaProperty:name>reception</pdfaProperty:name>
    <pdfaProperty:valueType>Registration</pdfaProperty:valueType>
    <pdfaProperty:category>external</pdfaProperty:category>
    <pdfaProperty:description>Gauto dokumento
registracija</pdfaProperty:description>
  </rdf:li>
  <rdf:li rdf:parseType="Resource">
    <pdfaProperty:name>receiver</pdfaProperty:name>
    <pdfaProperty:valueType>Entity</pdfaProperty:valueType>
    <pdfaProperty:category>external</pdfaProperty:category>
    <pdfaProperty:description>Dokumento gavėjas</pdfaProperty:description>
  </rdf:li>
</rdf:Seq>
</pdfaSchema:property>
<!-- Metaduomenų reikšmių tipai -->
<pdfaSchema:valueType>
  <rdf:Seq>
    <!-- Asmens tipas -->
    <rdf:li rdf:parseType = "Resource">
      <pdfaType:description>Asmuo (sudarytojas, adresatas,
gavėjas)</pdfaType:description>
      <pdfaType:namespaceURI>http://archyvai.lt/pdf-
ltud/2013/metadata/Entity/</pdfaType:namespaceURI>
      <pdfaType:prefix>LTUdEnt</pdfaType:prefix>
      <pdfaType:type>Entity</pdfaType:type>
      <pdfaType:field>
        <rdf:Seq>
          <rdf:li rdf:parseType = "Resource">
            <pdfaField:name>individual</pdfaField:name>
            <pdfaField:valueType>Boolean</pdfaField:valueType>
            <pdfaField:description>Požymis: fizinis (taip) ar juridinis (ne)
asmuo</pdfaField:description>
          </rdf:li>
          <rdf:li rdf:parseType = "Resource">

```



```

        <pdfaField:name>name</pdfaField:name>
        <pdfaField:valueType>Text</pdfaField:valueType>
        <pdfaField:description>Juridinio asmens pavadinimas arba fizinio
asmens vardas ir pavardė</pdfaField:description>
    </rdf:li>
    <rdf:li rdf:parseType = "Resource">
        <pdfaField:name>code</pdfaField:name>
        <pdfaField:valueType>Text</pdfaField:valueType>
        <pdfaField:description>Juridinio ar fizinio asmens
kodas</pdfaField:description>
    </rdf:li>
    <rdf:li rdf:parseType = "Resource">
        <pdfaField:name>address</pdfaField:name>
        <pdfaField:valueType>Text</pdfaField:valueType>
        <pdfaField:description>Adresas</pdfaField:description>
    </rdf:li>
    <rdf:li rdf:parseType = "Resource">
        <pdfaField:name>eMail</pdfaField:name>
        <pdfaField:valueType>Text</pdfaField:valueType>
        <pdfaField:description>El. pašto adresas</pdfaField:description>
    </rdf:li>
</rdf:Seq>
</pdfaType:field>
</rdf:li>
<!-- Registracijos tipas -->
<rdf:li rdf:parseType = "Resource">
    <pdfaType:description>Sudaryto ar gauto dokumento registracija
</pdfaType:description>
    <pdfaType:namespaceURI>http://archyvai.lt/pdf-
ltud/2013/metadata/Registration/</pdfaType:namespaceURI>
    <pdfaType:prefix>LTUdReg</pdfaType:prefix>
    <pdfaType:type>Registration</pdfaType:type>
    <pdfaType:field>
        <rdf:Seq>
            <rdf:li rdf:parseType = "Resource">
                <pdfaField:name>date</pdfaField:name>
                <pdfaField:valueType>Date</pdfaField:valueType>
                <pdfaField:description>Registravimo data</pdfaField:description>
            </rdf:li>
            <rdf:li rdf:parseType = "Resource">
                <pdfaField:name>number</pdfaField:name>
                <pdfaField:valueType>Text</pdfaField:valueType>
                <pdfaField:description>Registracijos
numeris</pdfaField:description>
            </rdf:li>
            <rdf:li rdf:parseType = "Resource">
                <pdfaField:name>code</pdfaField:name>
                <pdfaField:valueType>Text</pdfaField:valueType>
                <pdfaField:description>Juridinio ar fizinio asmens
kodas</pdfaField:description>
            </rdf:li>
        </rdf:Seq>
    </pdfaType:field>
</rdf:li>
<!-- Parašo tipas -->
<rdf:li rdf:parseType = "Resource">
    <pdfaType:description>Originalaus parašo kopijoje
duomenys</pdfaType:description>
    <pdfaType:namespaceURI>http://archyvai.lt/pdf-
ltud/2013/metadata/Signature/</pdfaType:namespaceURI>
    <pdfaType:prefix>LTUdSig</pdfaType:prefix>
    <pdfaType:type>Signature</pdfaType:type>
    <pdfaType:field>

```

```

    <rdf:Seq>
      <rdf:li rdf:parseType = "Resource">
        <pdfaField:name>signingTime</pdfaField:name>
        <pdfaField:valueType>Date</pdfaField:valueType>
        <pdfaField:description>Deklaruotas pasirašymo ar spaudo sukūrimo
laikas</pdfaField:description>
      </rdf:li>
      <rdf:li rdf:parseType = "Resource">
        <pdfaField:name>signingPurpose</pdfaField:name>
        <pdfaField:valueType>Text</pdfaField:valueType>
        <pdfaField:description>Parašo ar spaudo
paskirtis</pdfaField:description>
      </rdf:li>
      <rdf:li rdf:parseType = "Resource">
        <pdfaField:name>signer</pdfaField:name>
        <pdfaField:valueType>Entity</pdfaField:valueType>
        <pdfaField:description>Paraša ar spauda sudaręs
asmuo</pdfaField:description>
      </rdf:li>
      <rdf:li rdf:parseType = "Resource">
        <pdfaField:name>validationInfo</pdfaField:name>
        <pdfaField:valueType>Text</pdfaField:valueType>
        <pdfaField:description>Parašo ar spaudo galiojimo tikrinimo
informacija</pdfaField:description>
      </rdf:li>
    </rdf:Seq>
  </pdfaType:field>
</rdf:li>
</rdf:Seq>
</pdfaSchema:valueType>
</rdf:li>
</rdf:Bag>
</pdfaExtension:schemas>

</rdf:Description>
</rdf:RDF>

```

PDF PARAŠO ŽODYNO LAUKŲ PREFIKSO UŽREGISTRAVIMO KATALOGO PLĖTINIŲ ŽODYNE PAVYZDYS

```
%PDF-1.7
<</Type /Catalog
  /Extensions
    <</LTUd
      <</BaseVersion /1.7
        /ExtensionLevel 1
      >>
    >>
  >>
>>
```

METADUOMENŲ PILDYMO PAVYZDŽIAI

I SKYRIUS DOKUMENTO SUDARYMO METADUOMENYS (nurodomi PDF katalogo žodyno metaduomenų šaltinyje)

```
<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"

    <!-- PDF/A standarto versija (3) ir suderinamumo lygis (A, B ar U) -->

    <rdf:Description rdf:about = ""
      xmlns:pdfaid = "http://www.aiim.org/pdfa/ns/id/"
      <pdfaid:part>3</pdfaid:part>
      <pdfaid:conformance>B</pdfaid:conformance>
    </rdf:Description>

    <!-- LTUd XMP metaduomenų plėtinio schema -->

    <rdf:Description rdf:about = ""
      xmlns:pdfaExtension = "http://www.aiim.org/pdfa/ns/extension/"
      xmlns:pdfaSchema = "http://www.aiim.org/pdfa/ns/schema#"
      xmlns:pdfaProperty = "http://www.aiim.org/pdfa/ns/property#"
      xmlns:pdfaType = "http://www.aiim.org/pdfa/ns/type#"
      xmlns:pdfaField = "http://www.aiim.org/pdfa/ns/field#"

      <!-- nurodomas 2 priede pateiktos schemas turinys -->

    </rdf:Description>

    <!-- Dokumento atitikties Specifikacijos reikalavimų lygmeniui (A arba B)
    deklaravimas ir dokumento atitikties specifikacijos redakcijai deklaravimas -->

    <rdf:Description rdf:about=""
      xmlns:xmp="http://ns.adobe.com/xap/1.0/"
      xmlns:xmpidq="http://ns.adobe.com/xmp/Identifier/qual/1.0/"
    <xmp:Identifier>
      <rdf:Bag>
        <rdf:li>
          <rdf:Description>
            <rdf:value>A</rdf:value>
            <xmpidq:Scheme>http://archyvai.lt/pdf-ltud/2013/level/</xmpidq:Scheme>
          </rdf:Description>
        </rdf:li>
        <rdf:li>
          <rdf:Description>
            <rdf:value>1</rdf:value>
            <xmpidq:Scheme>http://archyvai.lt/pdf-ltud/2013/revision/</xmpidq:Scheme>
          </rdf:Description>
        </rdf:li>
      </rdf:Bag>
    </xmp:Identifier>
  </rdf:Description>

  <!-- PDF-RC-V1.0 dokumento sudarymo metaduomenys -->

  <rdf:Description rdf:about=""
    xmlns:LTUd="http://archyvai.lt/pdf-ltud/2013/metadata/"
    xmlns:LTUdEnt="http://archyvai.lt/pdf-ltud/2013/metadata/Entity/"
```

```

    xmlns:LTUdSig="http://archyvai.lt/pdf-ltud/2013/metadata/Signature/"
<LTUd:standardVersion>PDF-RC-V1.0</LTUd:standardVersion>
<LTUd:authors>
  <rdf:Seq>
    <rdf:li rdf:parseType="Resource">
      <LTUdEnt:individual>False</LTUdEnt:individual>
      <LTUdEnt:name>UAB Sudarytojas pirmasis</LTUdEnt:name>
      <LTUdEnt:code>1234568</LTUdEnt:code>
      <LTUdEnt:address>Adreso g. 115, Miestas</LTUdEnt:address>
      <LTUdEnt:eMail>info@pirmasis.lt</LTUdEnt:eMail>
    </rdf:li>
    <rdf:li rdf:parseType="Resource">
      <LTUdEnt:individual>True</LTUdEnt:individual>
      <LTUdEnt:name>Sudarytojas Antrasis</LTUdEnt:name>
      <LTUdEnt:address>Medžiotojų g. 2, Kaimas</LTUdEnt:address>
    </rdf:li>
  </rdf:Seq>
</LTUd:authors>
<LTUd:recipients>
  <rdf:Seq>
    <rdf:li rdf:parseType="Resource">
      <LTUdEnt:name>UAB Adresatas pirmasis</LTUdEnt:name>
      <LTUdEnt:code>123456878</LTUdEnt:code>
    </rdf:li>
    <rdf:li rdf:parseType="Resource">
      <LTUdEnt:name>Adresatas Antrasis</LTUdEnt:name>
    </rdf:li>
  </rdf:Seq>
</LTUd:recipients>
<LTUd:documentCopyIdentifier>1/5</LTUd:documentCopyIdentifier>
<LTUd:originalSignatures>
  <rdf:Seq>
    <rdf:li rdf:parseType="Resource">
      <LTUdSig:signingTime>2016-11-30T11:32:18.254+02:00</LTUdSig:signingTime>
      <LTUdSig:signingPurpose>registration</LTUdSig:signingPurpose>
      <LTUdSig:signer rdf:parseType="Resource">
        <LTUdEnt:individual>False</LTUdEnt:individual>
        <LTUdEnt:name>UAB Žinoma įmonė</LTUdEnt:name>
        <LTUdEnt:code>120792080</LTUdEnt:code>
        <LTUdEnt:address>Adreso g. 23, Miestas</LTUdEnt:address>
        <LTUdEnt:eMail>info@zinomaimone.lt</LTUdEnt:eMail>
      </LTUdSig:signer>
    </rdf:li>
  </rdf:Seq>
</LTUd:originalSignatures>
</rdf:Description>
<rdf:Description rdf:about=""
  xmlns:dc="http://purl.org/dc/elements/1.1/">
  <dc:language>
    <rdf:Bag>
      <rdf:li>lt-LT</rdf:li>
    </rdf:Bag>
  </dc:language>
  <dc:title>
    <rdf:Alt>
      <rdf:li xml:lang="x-default">Dėl darbo grupės sudarymo</rdf:li>
      <rdf:li xml:lang="lt-LT">Dėl darbo grupės sudarymo</rdf:li>
    </rdf:Alt>
  </dc:title>
  <dc:creator>
    <rdf:Seq>
      <rdf:li>UAB Sudarytojas pirmasis</rdf:li>
      <rdf:li>Sudarytojas antrasis</rdf:li>
    </rdf:Seq>
  </dc:creator>

```

```

    </rdf:Seq>
  </dc:creator>
</rdf:Description>
<rdf:Description rdf:about=""
  xmlns:xmp="http://ns.adobe.com/xap/1.0/"
  <xmp:CreatorTool>Organizacija Programa 2.44.1 (Win XP)</xmp:CreatorTool>
</rdf:Description>

</rdf:RDF>
</x:xmpmeta>
<?xpacket end="w"?>

```

II SKYRIUS

SUDARYTO DOKUMENTO REGISTRAVIMO METADUOMENYS (nurodomi PDF parašo formos lauko žodyno metaduomenų šaltinyje)

```

<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/"
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"

    <rdf:Description rdf:about=""
      xmlns:LTUd="http://archyvai.lt/pdf-ltud/2013/metadata/"
      xmlns:LTUdReg="http://archyvai.lt/pdf-ltud/2013/metadata/Registration/"

        <LTUd:registration rdf:parseType="Resource">
          <LTUdReg:date>2011-11-30T21:32:18.254+02:00</LTUdReg:date>
          <LTUdReg:number>IV-1458</LTUdReg:number>
          <LTUdReg:code>1234568</LTUdReg:code>
        </LTUd:registration>
      </rdf:Description>

    </rdf:RDF>
  </x:xmpmeta>
<?xpacket end="w"?>

```

III SKYRIUS

GAUTO DOKUMENTO REGISTRAVIMO METADUOMENYS (nurodomi PDF parašo formos lauko žodyno metaduomenų šaltinyje)

```

<?xpacket begin="" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/"
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"

    <rdf:Description rdf:about=""
      xmlns:LTUd="http://archyvai.lt/pdf-ltud/2013/metadata/"
      xmlns:LTUdReg="http://archyvai.lt/pdf-ltud/2013/metadata/Registration/"
      xmlns:LTUdEnt="http://archyvai.lt/pdf-ltud/2013/metadata/Entity/"

        <LTUd:reception rdf:parseType="Resource">
          <LTUdReg:date>2011-11-30T21:32:18.301+02:00</LTUdReg:date>
          <LTUdReg:number>GR-24</LTUdReg:number>
          <LTUdReg:code>33397440</LTUdReg:code>
        </LTUd:reception>
        <LTUd:receiver rdf:parseType="Resource">
          <LTUdEnt:individual>False</LTUdEnt:individual>
          <LTUdEnt:name>UAB Gavėjas</LTUdEnt:name>
          <LTUdEnt:code>33397440</LTUdEnt:code>
          <LTUdEnt:address>Adreso g. 115, Miestas</LTUdEnt:address>
          <LTUdEnt:eMail>info@pirmasis.lt</LTUdEnt:eMail>
        </LTUd:receiver>
      </rdf:Description>

```

```
</rdf:RDF>  
</x:xmpmeta>  
<?xpacket end="w"?>
```

PDF PARAŠO ŽODYNO LAUKAI

Žodyno lauko raktas	Tipas ¹	Privalomumas	Aprašas
Type	Vardas (name)	Ne	Jeigu laukas nurodytas, reikšmė turi būti „Sig“.
Filter	Vardas (name)	Taip	Skaitmeninio parašo tikrinimo valdiklio vardas. Skaitmeniniam parašui tikrinti gali būti naudojamas ir kitas, nei nurodytas, valdiklis, jeigu jis palaiko „SubFilter“ lauke nurodytą skaitmeninio parašo formatą. Rekomenduojama nurodyti standartinio valdiklio vardą „Adobe.PPKLite“.
SubFilter	Vardas (name)	Taip	Reikšmė turi būti „ETSI.CAdES.detached“.
Contents	Baitų seka (byte string)	Taip	CAdES formato skaitmeninis parašas.
Cert	Masyvas arba baitų seka (array or byte string)	Draudžiamas	Pasirašyti naudoto sertifikato ir jo kelio sertifikatai turi būti nurodyti CAdES formato skaitmeninis paraše.
ByteRange	Masyvas (array)	Taip	Nurodo pasirašytų baitų intervalus. Turi nurodyti visą PDF rinkmeną, išskyrus šio PDF parašo žodyno „Contents“ lauką.
Reference	Masyvas (array)	Draudžiamas	Skaitmeninių parašų nuorodų žodynai.
Changes	Masyvas (array)	Ne	Pakeitimai atlikti po paskutinio Skaitmeninio parašo sukūrimo. Jeigu nurodytas, tai visos trys masyvo reikšmės turi būti „0“.
Name	Tekstas (text string)	Taip, jei šių duomenų nėra sertifikate	Metaduomens „Elektroninį parašą ar elektroninį spaudą sudaręs asmuo“ reikšmė (1 priedo 3 skyrius).
M	Data (date)	Taip	Metaduomens „Elektroninio parašo ar elektroninio spaudo sudarymo data (deklaruojama)“ reikšmė (1 priedo 3 skyrius).
Location	Tekstas (text string)	Ne	Parašo ar spaudo sudarymo vieta.
Reason	Tekstas (text string)	Ne	Metaduomens „Elektroninio parašo ar elektroninio spaudo paskirtis“ reikšmė (1 priedo 3 skyrius).
ContactInfo	Tekstas (text string)	Ne	Pasirašančiojo asmens ryšio duomenys.
R	Skaičius (integer)	Draudžiamas	Skaitmeninio parašo tikrinimo valdiklio versija.
V	Skaičius (integer)	Ne	PDF parašo žodyno formato versija. Jeigu laukas nurodytas, reikšmė turi būti „0“.
Prop_Build	Žodynas (dictionary)	Ne	Žodynas, kuriame pateikiama pasirašyti naudotos programinės įrangos techninė informacija.
Prop_AuthTime	Skaičius (integer)	Ne	Sekundžių skaičius, praėjęs po pasirašančiojo asmens tapatybės nustatymo iki skaitmeninio parašo sudarymo momento. Draudžiama lauką nurodyti, jeigu reikšmė nežinoma.

Žodyno lauko raktas	Tipas ¹	Privalomumas	Aprašas
Prop_AuthType	Vardas (name)	Ne	Pasirašančiojo asmens tapatybei nustatyti taikytas metodas. Galimos reikšmės yra: „PIN“, „Password“, „Fingerprint“. Draudžiama lauką nurodyti, jeigu reikšmė nežinoma.
LTUd_Role	Tekstas (text string)	Ne	Metaduomens „Elektroninį parašą sudariusio asmens pareigos“ reikšmė (1 priedo 3 skyrius).
LTUd_SignerNotes	Tekstas (text string)	Ne	Metaduomens „Elektroninį parašą sudariusio asmens pastaba“ reikšmė (1 priedo 3 skyrius).

Pastaba. ¹ Skliaustuose nurodyti standartiniai PDF objektų tipai yra aprašyti PDF-1.7 standarto 7.3 ir 7.9 skyriuose.

DOKUMENTO LAIKO ŽYMOŠ ŽODYNO LAUKAI

Žodyno lauko raktas	Tipas ¹	Privalomumas	Aprašas
Type	Vardas (name)	Ne	Jeigu laukas nurodytas, reikšmė turi būti „DocTimeStamp“.
Filter	Vardas (name)	Taip	PDF dokumento laiko žymos tikrinimo valdiklio vardas. PDF dokumento laiko žymai tikrinti gali būti naudojamas ir kitas, nei nurodytas, valdiklis, jeigu jis palaiko „SubFilter“ lauke nurodytą elektroninės laiko žymos formatą. Rekomenduojama nurodyti standartinio valdiklio vardą „Adobe.PPKLite“.
SubFilter	Vardas (name)	Taip	Reikšmė turi būti „ETSI.RFC3161“.
Contents	Baitų seka (byte string)	Taip	Elektroninė laiko žyma, atitinkanti RFC 3161 reikalavimus. Elektroninės laiko žymos „messageImprint“ elemente turi būti nurodyta santrauka, apskaičiuota nuo duomenų, kurių intervalai nurodyti „ByteRange“ lauke.
Cert	Masyvas arba baitų seka (array or byte string)	Draudžiamas	
ByteRange	Masyvas (array)	Taip	Nurodo intervalus baitų, nuo kurių apskaičiuota santrauka. Turi nurodyti visą PDF rinkmeną, išskyrus šios PDF dokumento laiko žymos žodyno „Contents“ lauką.
Reference	Masyvas (array)	Draudžiamas	
Changes	Masyvas (array)	Draudžiamas	
Name	Tekstas (text string)	Draudžiamas	
M	Data (date)	Draudžiamas	
Location	Tekstas (text string)	Draudžiamas	
Reason	Tekstas (text string)	Draudžiamas	
ContactInfo	Tekstas (text string)	Draudžiamas	
R	Skaičius (integer)	Draudžiamas	
V	Skaičius (integer)	Ne	Dokumento laiko žymos žodyno formato versija. Jeigu laukas nurodytas, reikšmė turi būti „0“.
Prop_Build	Žodynas (dictionary)	Ne	Žodynas, kuriame pateikiama programinės įrangos, naudotos dokumento laiko žymai įtraukti, techninė informacija.
Prop_AuthTime	Skaičius (integer)	Draudžiamas	
Prop_AuthType	Vardas (name)	Draudžiamas	

Pastaba. ¹ Skliaustuose nurodyti standartiniai PDF objektų tipai yra aprašyti PDF-1.7 standarto 7.3 ir 7.9 skyriuose.

PADES PARAŠUOSE NAUDOJAMI ALGORITMAI

PAdES parašuose gali būti naudojami tik šie algoritmai:

Algoritmas	Identifikatorius	Identifikatorių aprašantis dokumentas
Santraukos sudarymas (angl. <i>digest</i>)		
SHA256	id-sha256	RFC 4055 (Specifikacijos 12 priedo 23 punktas)
SHA384	id-sha384	RFC 4055
SHA512	id-sha512	RFC 4055
Pasirašymas (angl. <i>signature</i>)		
RSASwithSHA256	sha256WithRSAEncryption	RFC 3447 (Specifikacijos 12 priedo 21 punktas)
RSASwithSHA384	sha384WithRSAEncryption	RFC 3447
RSASwithSHA512	sha512WithRSAEncryption	RFC 3447
RSASSA-PSS ¹	id-RSASSA-PSS	RFC 3447
DSASwithSHA256	id-dsa-with-sha256	RFC 5758 (Specifikacijos 12 priedo 18 punktas)
ECDSASwithSHA256	ecdsa-with-SHA256	RFC 5758
ECDSASwithSHA384	ecdsa-with-SHA384	RFC 5758
ECDSASwithSHA512	ecdsa-with-SHA512	RFC 5758

Pastaba.¹ Algoritmas gali būti naudojamas tik kartu su šioje lentelėje nurodytu santraukos sudarymo algoritmu.

Algoritmai ir raktų ilgiai PAdES parašams formuoti parenkami pagal LST ETSI TS 119 312 (Specifikacijos 12 priedo 13 punktas) standarto vėliausią versiją.

Vėlesnė PDF-RC-V1.0 specifikacijos redakcija gali apibrėžti kitus leistinus algoritmus. PAdES parašų tikrinimui ir jų papildymui turi būti vadovaujamas algoritmais nurodytais naujausioje PDF-RC-V1.0 specifikacijos redakcijoje.

CAdES FORMATO SKAITMENINIO PARAŠO STRUKTŪRA

Šis priedas aprašo PAdES-B-B, PAdES-B-T, PAdES-B-LT ir PAdES-B-LTA formato PDF parašo žodyno lauke „**Contents**“ saugomo CAdES formato skaitmeninio parašo vidinę struktūrą.

CAdES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
ContentInfo ::= SEQUENCE {	Taip	1	
contentType ContentType ::= OBJECT IDENTIFIER,	Taip	1	Turi būti nurodyta reikšmė „id-signedData“.
content [0] EXPLICIT ANY DEFINED BY contentType	Taip	1	Turi būti saugomas „SignedData“ tipo elementas.
}			
„SignedData“ tipo elementas:			
SignedData ::= SEQUENCE {	Taip	1	
version CMSVersion,	Taip	1	Sintaksės versijos numeris. Reikšmė turi būti „1“ arba „3“ ir parenkama, kaip nurodyta RFC 5652 (Specifikacijos 12 priedo 25 punktas) 5.1 skyriuje.
digestAlgorithms DigestAlgorithmIdentifiers ::= SET OF	Taip	1	
DigestAlgorithmIdentifier,	Taip	1-N	Santraukos sudarymo algoritmai nurodyti 7 priede.
encapContentInfo EncapsulatedContentInfo ::= SEQUENCE {	Taip	1	
eContentType ContentType,	Taip	1	Turi būti nurodyta reikšmė „id-data“.
eContent [0] EXPLICIT OCTET STRING OPTIONAL	Draudžiamas	0	Draudžiamas, nes pasirašomieji duomenys yra CAdES formato skaitmeninio parašo išorėje.
}			
certificates [0] IMPLICIT CertificateSet OPTIONAL ::= SET OF	Taip	1	Privalo būti pasirašančiojo asmens X509 v3 sertifikatas.

CADES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
CertificateChoices ::= CHOICE { certificate Certificate, extendedCertificate [0] IMPLICIT ExtendedCertificate, v1AttrCert [1] IMPLICIT AttributeCertificateV1, v2AttrCert [2] IMPLICIT AttributeCertificateV2,other [3] IMPLICIT OtherCertificateFormat }		1-N	Privalo būti pasirašančiojo asmens sertifikatas. Gali būti nurodyti ir kiti sertifikatai, esantys pasirašančiojo asmens sertifikato sekoje. Jeigu pasirašančiojo asmens sertifikatas yra kvalifikuotas, rekomenduojama įtraukti visus sertifikato seką sudarančius sertifikatus iki sertifikato, nurodyto Europos Sąjungos šalies registruotų ir (ar) akredituotų paslaugų teikėjų sąraše (angl. <i>trusted services list</i> , <i>TSL</i>).
certificate Certificate,	Privalomas	1	X509 sertifikatas.
extendedCertificate [0] IMPLICIT ExtendedCertificate,	Draudžiamas	0	
v1AttrCert [1] IMPLICIT AttributeCertificateV1,	Draudžiamas	0	
v2AttrCert [2] IMPLICIT AttributeCertificateV2,	Draudžiamas	0	
.....other [3] IMPLICIT OtherCertificateFormat	Draudžiamas	0	
}			
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL	Draudžiamas	0	
„signerInfos“ tipo elementas:			
signerInfos ::= SET OF	Taip	1	CADES formato skaitmeniniame paraše turi būti tik vieno asmens skaitmeninio parašo informacija.
SignerInfo ::= SEQUENCE {	Taip	1	
version CMSVersion,	Taip	1	Sintaksės versijos numeris. Reikšmė turi būti „1“ arba „3“ ir parenkama, kaip nurodyta RFC 5652 (Specifikacijos 12 priedo 25 punktas) 5.3 skyriuje.
sid SignerIdentifier ::= CHOICE {	Taip	1	Pasirašančiojo asmens sertifikato identifikatorius.
issuerAndSerialNumber IssuerAndSerialNumber ::= SEQUENCE {	Ne	0-1	Sertifikatas identifikuojamas, nurodant sertifikate esantį jį išdavusios įstaigos pavadinimą (angl. <i>distinguished name</i>) ir sertifikato serijos numerį.
issuer Name, -- X.509 Name	Taip	1	
serialNumber CertificateSerialNumber ::= INTEGER	Taip	1	
}			
subjectKeyIdentifier [0] SubjectKeyIdentifier ::= OCTET STRING	Ne	0-1	Sertifikatas identifikuojamas pagal sertifikato raktinį identifikatorių, kuris parenkamas, kaip nurodyta RFC 5652 5.3 skyriuje.

CAdES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
<code>},</code>			
<code>digestAlgorithm DigestAlgorithmIdentifier,</code>	Taip	1	Santraukos sudarymo algoritmai nurodyti 7 priede.
„signedAttrs“ tipo elementas:			
<code>signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL</code>	Taip	1	Pasirašomi CAdES formato skaitmeninio parašo atributai.
<code>SignedAttributes ::= SET SIZE (1..MAX) OF</code>			
<code>Attribute ::= SEQUENCE {</code>	Taip	3-N ¹	
<code>attrType OBJECT IDENTIFIER,</code>			
<code>-- attrType: id-contentType</code>	Taip	1	Pasirašomo turinio tipas. Turi būti nurodyta reikšmė „id-data“ (RFC 5652 4 skyrius).
<code>-- attrType: id-messageDigest</code>	Taip	1	Pasirašomų duomenų santrauka.
<code>-- attrType: id-aa-ets-signingCertificateV2</code>	Taip	1	Pasirašančiojo asmens sertifikato nuoroda. Naudojamas kai santraukos sudarymo algoritmas nėra SHA1.
<code>-- attrType id-aa-signingCertificate</code>	Draudžiamas	0	Pasirašančiojo asmens sertifikato nuoroda. Naudojamas kai santraukos sudarymo algoritmas yra SHA1.
<code>-- attrType id-aa-ets-otherSigCert</code>	Draudžiamas	0	Pasirašančiojo asmens sertifikato nuoroda.
<code>-- attrType id-signingTime</code>	Draudžiamas	0	Deklaruojamas pasirašymo laikas.
<code>-- attrType id-aa-ets-sigPolicyId</code>	Ne	0-1	Išreikštinės parašo taisyklės.
<code>-- attrType id-aa-ets-commitmentType</code>	Ne ²	0-1	Elektroninio parašo ar elektroninio spaudo paskirtis.
<code>-- attrType id-aa-ets-signerLocation</code>	Draudžiamas	0	Pasirašymo vieta.
<code>-- attrType id-aa-ets-signerAttr</code>	Draudžiamas	0	Pasirašančiojo asmens atributai (rolės).
<code>-- attrType id-aa-ets-signerAttrV2</code>	Draudžiamas	0	Pasirašančiojo asmens atributai (rolės).
<code>-- attrType id-aa-ets-contentTimestamp</code>	Ne	0-1	Pasirašomų duomenų elektroninė laiko žyma (sukuriama prieš pasirašymą). Šio atributo naudojimas yra nerekomenduojamas. Šiam tikslui rekomenduojama naudoti dokumento laiko žymą (angl. <i>document time-stamp</i>).
<code>-- attrType id-aa-contentReference</code>	Draudžiamas	0	Nuoroda į pasirašytus duomenis (skaitmeninį parašą).
<code>-- attrType id-aa-contentIdentifier</code>	Draudžiamas	0	Pasirašytų duomenų (skaitmeninio parašo) identifikatorius.
<code>-- attrType id-aa-contentHint</code>	Draudžiamas	0	Pasirašomo turinio formatas.
<code>-- attrType id-aa-ets-mimeType</code>	Draudžiamas	0	Pasirašomo turinio MIME tipas.
<code>attrValues SET OF AttributeValue</code>	Taip	1	

CAdES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
} ,			
signatureAlgorithm SignatureAlgorithmIdentifier,	Taip	1	Pasirašymo algoritmas. Pasirašymo algoritmai nurodyti 7 priede.
signature SignatureValue ::= OCTET STRING,	Taip	1	
„unsignedAttrs“ tipo elementas:			
unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL	Ne	0-1	Nepasirašomi CAdES formato skaitmeninio parašo atributai.
UnsignedAttributes ::= SET SIZE (1..MAX) OF			
Attribute ::= SEQUENCE {	Taip	1-N ¹	
attrType OBJECT IDENTIFIER,	Taip	1	
-- attrType id-aa-signatureTimeStampToken	Ne	0-1	Parašo laiko žyma, kuri atitinka RFC 3161 (Specifikacijos 12 priedo 20 punktas) reikalavimus.
-- attrType id-aa-ets-certificateRefs	Draudžiamas	0	Nuorodos į sertifikatus.
-- attrType id-aa-ets-revocationRefs	Draudžiamas	0	Nuorodos į atšaukimo duomenis.
-- attrType id-aa-ets-certValues	Draudžiamas	0	Sertifikatų reikšmės.
-- attrType id-aa-ets-revocationValues	Draudžiamas	0	Atšaukimo duomenys.
-- attrType id-aa-ets-escTimeStamp	Draudžiamas	0	CAdES-C formato skaitmeninio parašo elektroninė laiko žyma.
-- attrType id-aa-ets-certCRLTimeStamp	Draudžiamas	0	Nuorodų į sertifikatus ir atšaukimo duomenis laiko žyma.
-- attrType id-aa-ets-archiveTimeStampV2	Draudžiamas	0	Archyvinė laiko žyma.
-- attrType id-aa-ets-archiveTimeStampV3	Draudžiamas	0	Archyvinė laiko žyma.
-- attrType id-aa-ets-longTermValidation	Draudžiamas	0	Duomenų egzistavimo iki tam tikro laiko įrodymo atributas.
-- attrType id-aa-ets-attrCertificateRefs	Draudžiamas	0	Nuorodos į atributinius sertifikatus.
-- attrType id-aa-ets-attrRevocationRefs	Draudžiamas	0	Nuorodos į atributinių sertifikatų atšaukimo duomenis.
-- attrType id-aa-ets-sigPolicyStore	Draudžiamas	0	Parašo taisyklių saugykla.
-- attrType id-countersignature	Draudžiamas	0	
attrValues SET OF AttributeValue	Taip	1	
} ,			
}			
}			

Pastabos:

1. Neišvardyti CAdES formato skaitmeninio parašo pasirašomi ar nepasirašomi atributai draudžiami.

2. Draudžiamas, jeigu nėra parašo taisyklių identifikatoriaus atributo „signature-policy-identifier“ (objekto identifikatorius „id-aa-ets-sigPolicyId“; CAdES standarto 5.2.9.1 skyrius).

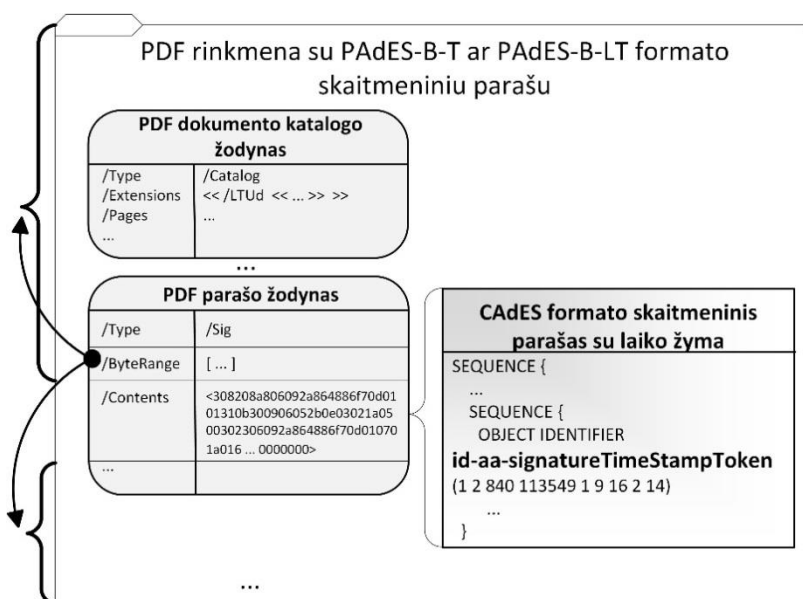
TRUMPALAIKIŲ IR ILGALAIKIŲ PDF ELEKTRONINIŲ PARAŠŲ SCHEMAS

I SKYRIUS TRUMPALAIKIS PAdES PARAŠAS SU PARAŠO LAIKO ŽYMA

1. Trumpalaikis PAdES parašas su parašo laiko žyma – tai PAdES-B-T arba PAdES-B-LT formato skaitmeninis parašas, kuris atitinka visus šiuos reikalavimus:

1.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES formato skaitmeninis parašas, kuriame yra nepasirašomas parašo laiko žymos atributas „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 5.3 skyrius);

1.2. PDF rinkmenoje nėra PDF dokumento laiko žymos, patvirtinančios PAdES parašo egzistavimą iki joje nurodyto laiko. PDF rinkmenoje gali būti anksčiau už PAdES parašą įtrauktų PDF dokumento laiko žymų, kurios nepatvirtina PAdES parašo egzistavimo iki jose nurodyto laiko.



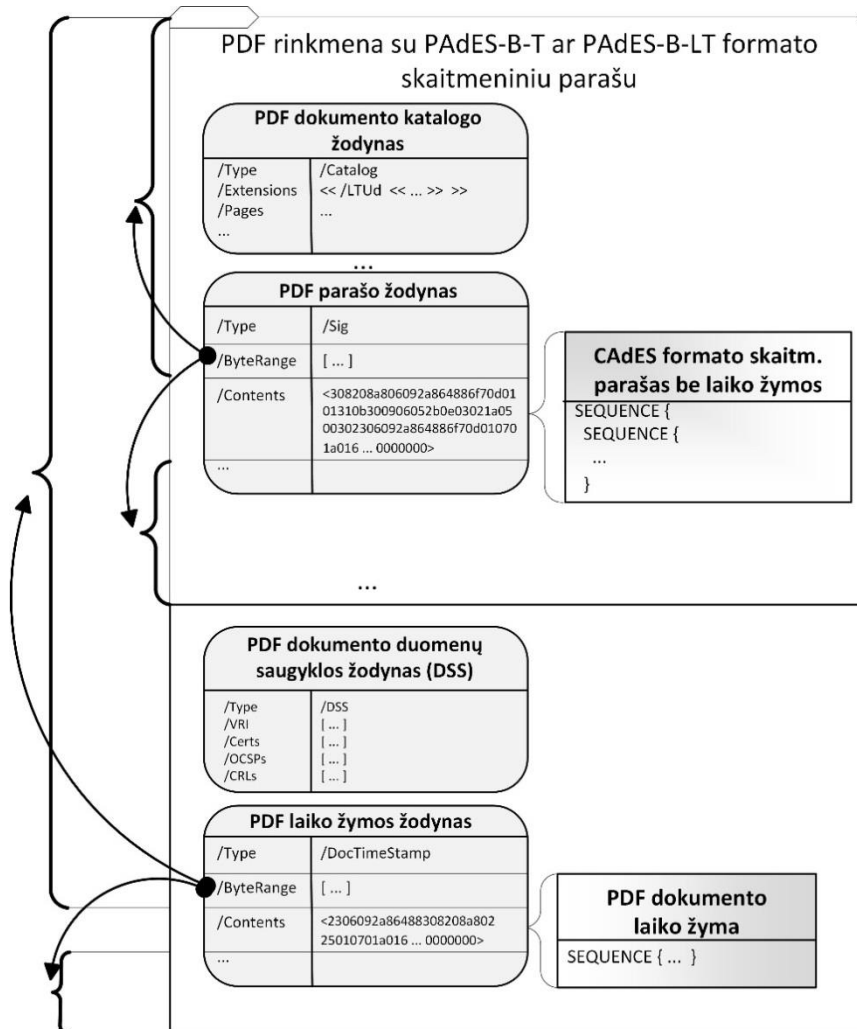
II SKYRIUS

TRUMPALAIKIS PAdES PARAŠAS SU PDF DOKUMENTO LAIKO ŽYMA

2. Trumpalaikis PAdES parašas su PDF dokumento laiko žyma – tai PAdES-B-T arba PAdES-B-LT formato skaitmeninis parašas, kuris atitinka visus šiuos reikalavimus:

2.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES formato skaitmeninis parašas, kuriame nėra nepasirašomo parašo laiko žymos atributo „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 5.3 skyrius);

2.2. PDF rinkmenoje yra viena PDF dokumento laiko žyma, patvirtinanti PAdES parašo egzistavimą iki joje nurodyto laiko. PDF rinkmenoje gali būti kitų anksčiau už PAdES parašą įtrauktų PDF dokumento laiko žymų, kurios nepatvirtina PAdES parašo egzistavimo iki joje nurodyto laiko.



III SKYRIUS

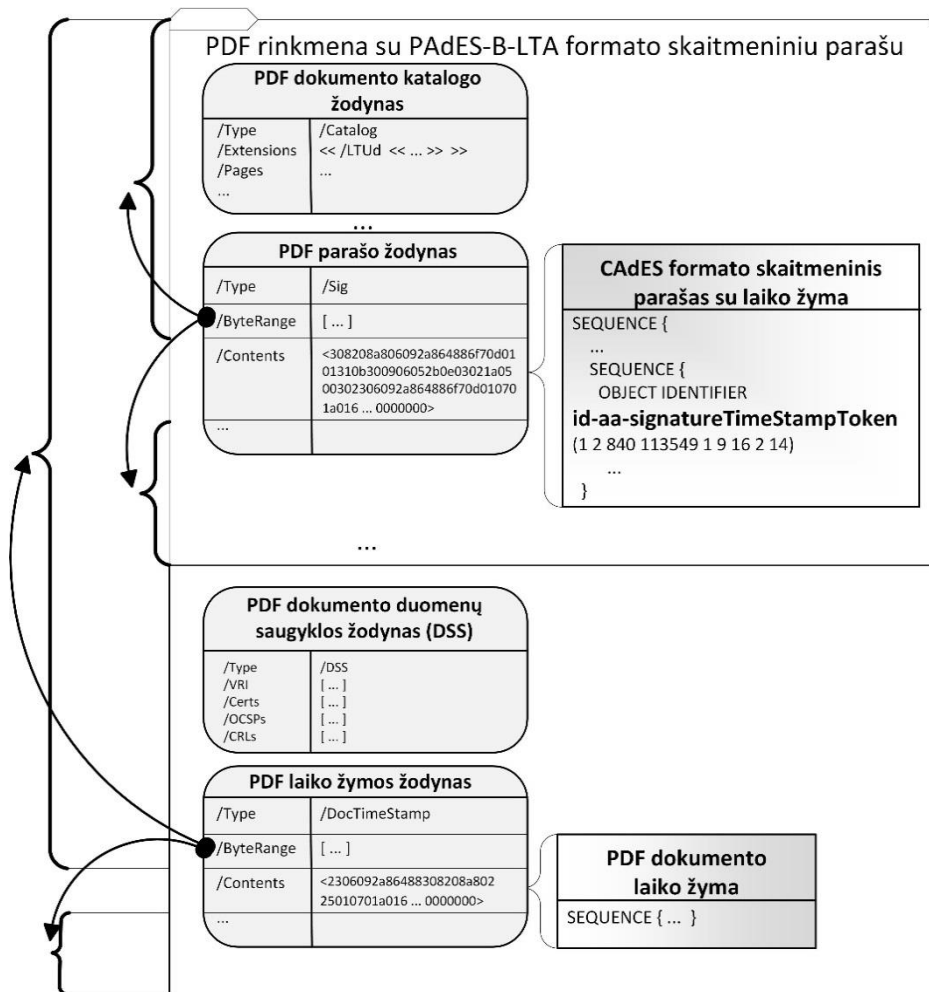
ILGALAIKIS PADES PARAŠAS SU PARAŠO LAIKO ŽYMA

3. Ilgalaikis PAdES parašas su parašo laiko žyma – tai PAdES-B-LTA formato skaitmeninis parašas, kuris atitinka visus šiuos reikalavimus:

3.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES formato skaitmeninis parašas, kuriame yra nepasirašomas parašo laiko žymos atributas „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 5.3 skyrius);

3.2. PDF rinkmenoje yra parašo galiojimą patvirtinantys duomenys, kurie yra įtraukti po parašo laiko žymos sukūrimo;

3.3. PDF rinkmenoje yra bent viena PDF dokumento laiko žyma, patvirtinanti parašo galiojimą patvirtinančių duomenų (ir PAdES parašo) egzistavimą iki joje nurodyto laiko.



IV SKYRIUS

ILGALAIKIS PADES PARAŠAS BE PARAŠO LAIKO ŽYMAS

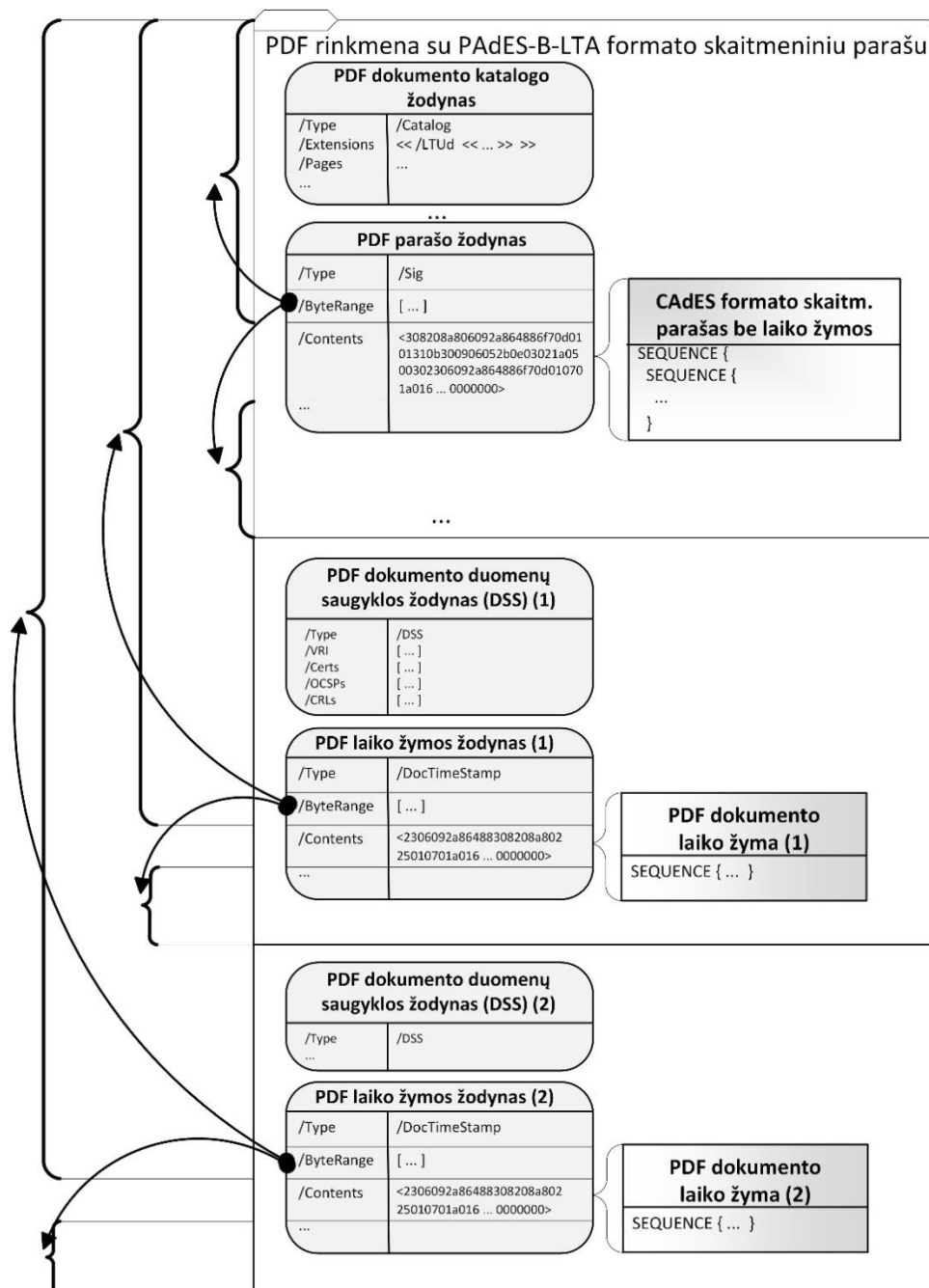
4. Ilgalaikis PAdES parašas be parašo laiko žymos – tai PAdES-B-LTA formato skaitmeninis parašas, kuris atitinka visus šiuos reikalavimus:

4.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES formato skaitmeninis parašas, kuriame nėra nepasirašomo parašo laiko žymos atributo „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 5.3 skyrius);

4.2. PDF rinkmenoje yra PDF dokumento laiko žyma (pirmoji), patvirtinanti PAdES parašo egzistavimą iki joje nurodyto laiko;

4.3. PDF rinkmenoje yra parašo galiojimą patvirtinantys duomenys, kurie yra įtraukti po pirmosios PDF dokumento laiko žymos sukūrimo;

4.4. PDF rinkmenoje yra bent viena PDF dokumento laiko žyma (antroji), patvirtinanti parašo galiojimą patvirtinančių duomenų (ir PAdES parašo) egzistavimą iki joje nurodyto laiko.



**SPECIFIKACIJOS REIKALAVIMŲ, SKIRTINGAI TAIKOMŲ A IR B LYGMENS ELEKTRONINIAMS
DOKUMENTAMS, SUVESTINĖ**

Metaduomenys	Aprašas Specifikacijoje	A lygmens dokumentas	B lygmens dokumentas
Atitikties A arba B reikalavimų lygmeniui deklaravimas	1 priedas;	Deklaravimas privalomas.	Deklaravimas neprivalomas.
Dokumento sudarymo metaduomenys	36.3 punktas; 1 priedo I dalis;	Metaduomenys privalomi.	Metaduomenys neprivalomi. Jei yra įtraukti, turi atitikti Specifikacijoje keliamus reikalavimus.
Dokumento registravimo metaduomenys	1 priedo II dalis;	Metaduomenys privalomi dokumento registravimo metu.	Metaduomenys neprivalomi. Jei yra įtraukti, turi atitikti Specifikacijoje keliamus reikalavimus.
Specifikacijoje apibrėžtų metaduomenų XMP schema	36.2 punktas; 2 priedas;	Schema privaloma.	Schema neprivaloma, jeigu rinkmenoje nėra metaduomenų, apibrėžtų LTUd vardų zonoje.
Elektroninį parašą sudariusio asmens pareigos (metaduomuo LTUd_Role)	1 priedo III dalis;	Privalomas, kai pasirašantis asmuo atstovauja viešą juridinį asmenį.	Metaduomuo neprivalomas. Jei yra įtrauktas, turi atitikti Specifikacijoje keliamus reikalavimus.
Elektroninį parašą sudariusio asmens pastaba (metaduomuo LTUd_SignerNotes)	1 priedo III dalis;	Privalomas pagal pobūdį.	Metaduomuo neprivalomas. Jei yra įtrauktas, turi atitikti Specifikacijoje keliamus reikalavimus.
Plėtinio „LTUd“ aprašas PDF katalogo plėtinių žodyne	15 punktas;	Plėtinio aprašas privalomas.	Plėtinio aprašas neprivalomas, jei nėra LTUd_Role ir (ar) LTUd_SignerNotes metaduomenų.

ELEKTRONINIO DOKUMENTO TURINIO RINKMENŲ FORMATAI

Nr.	Kriterijus	Aprašymas
1.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>Automatinio projektavimo rinkmenos (DWG) formatas</i> dwg application/acad, application/x-acad, image/x-dwg, application/dwg https://www.opendesign.com/files/guestdownloads/OpenDesign_Specification_for_dwg_files.pdf (Specifikacijos 12 priedo 17 punktas) Nėra
2.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>WEB puslapių dizaino rinkmenos (DWF) formatas</i> dwf application/dwf, application/x-dwf, drawing/x-dwf, image/vnd.dwf, image/x-dwf https://en.wikipedia.org/wiki/Design_Web_Format (Specifikacijos 12 priedo 1 punktas) Nėra
3.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>Brėžinių apskaitos rinkmenos (DXF) formatas</i> dxf image/vnd.dxf http://images.autodesk.com/adsk/files/autocad_2012_pdf_dxf-reference_enu.pdf Nėra
4.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis standartas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>Žymėtosios atvaizdų rinkmenos (TIFF) formatas</i> tif, tiff image/tif, image/tiff, image/tiff-fx LST ISO 12234-2:2008 (Specifikacijos 12 priedo 13 punktas) Nėra
5.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis standartas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>Fotografinių vaizdų saugojimo (JPEG) formatas</i> jpg, jpeg, jfif image/jpeg LST ISO/IEC 10918-1: 2008 (Specifikacijos 12 priedo 16 punktas) Nėra

Nr.	Kriterijus	Aprašymas
	rinkmenomis:	
6.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>MrSID (Multi-Resolution Seamless Image Database)</i> – sukurtas „Lizardtech“ suspaustų vilnelių (wavelet) formatas sid image/x-mrsid, image/x.mrsid, image/x-mrsid-image https://en.wikipedia.org/wiki/MrSID Nėra
7.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>ESRI atviras erdvinių vektorinių duomenų formatas, naudojantis SHP, SHX ir DBF failus</i> shp application/octet-stream http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf Tik kartu su SHX ir DBF formatų rinkmenomis
8.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>ESRI atviras erdvinių vektorinių duomenų formatas, naudojantis SHP, SHX ir DBF failus</i> shx application/octet-stream http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf Tik kartu su SHP ir DBF formatų rinkmenomis
9.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	<i>ESRI atviras erdvinių vektorinių duomenų formatas, naudojantis SHP, SHX ir DBF failus</i> dbf application/dbase, application/x-dbase, application/dbf, application/x-dbf http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf Tik kartu su SHP ir SHX formatų rinkmenomis
10.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo: Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	Rastrinių duomenų geografinio orientavimo parametrų ASCII byla tfw text/plain http://www.cartograph.com/help/8_4/Content/MapSolutions/MapSA/WorldFiles_Ref.htm , https://en.wikipedia.org/wiki/World_file , http://desktop.arcgis.com/en/arcmap/10.3/manage-data/raster-and-images/world-files-for-raster-datasets.htm Tik kartu su TIF formato rinkmena
11.	Formato pavadinimas: Rinkmenos plėtinys: MIME tipo žymuo:	<i>Rastrinių duomenų geografinio orientavimo parametrų ASCII byla</i> sdw text/plain

Nr.	Kriterijus	Aprašymas
	Formatą aprašantis dokumentas: Sąsaja su kitomis pridedamomis rinkmenomis:	http://www.cartograph.com/help/8_4/Content/MapSolutions/MapSA/WorldFiles_Ref.htm , https://en.wikipedia.org/wiki/World_file , http://desktop.arcgis.com/en/arcmap/10.3/manage-data/raster-and-images/world-files-for-raster-datasets.htm Tik kartu su SID format rinkmena

STANDARTŲ IR KITŲ DOKUMENTŲ SĄRAŠAS

1. Design Web Format, https://en.wikipedia.org/wiki/Design_Web_Format.
2. DXF Format, http://images.autodesk.com/adsk/files/autocad_2012_pdf_dxf-reference_enu.pdf, 2011.
3. ESRI Shapefile Technical Description, <http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf>, 1998.
4. Europos parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB, 2014.
5. LST EN 319 102-1 V1.1.1:2016 „Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation“.
6. LST EN 319 122-1 V1.1.1:2016 „Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures“.
7. LST EN 319 142-1 V1.1.1:2016 „Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures“.
8. LST EN 319 412-2 V2.1.1:2016 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“.
9. LST EN 319 412-3 V1.1.1:2016 „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons“.
10. LST EN 319 422 V1.1.1:2016 „Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles“.
11. LST ETSI TS 119 101 V1.1.1: 2016 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation“.
12. LST ETSI TS 119 312 V1.1.1:2016 "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"
13. LST ISO 12234-2:2008 „Elektroninis nejudamojo vaizdo vizualizavimas. Keičiamoji atmintinė. 2 dalis. TIFF/EP vaizdo duomenų formatas (tapatus ISO 12234-2:2001)“.
14. LST ISO 19005-3:2017 „Dokumentų tvarkyba. Ilgalaikio saugojimo elektroninio dokumento rinkmenos formatas. 3 dalis. ISO 32000-1 (PDF/A-3) naudojimas su pridėtinėmis rinkmenomis (tapatus ISO 19005-3:2012)“.
15. LST ISO 32000-1:2009 „Dokumentų tvarkyba. PDF formatas. 1 dalis. PDF 1.7 (tapatus ISO 32000-1:2008)“.
16. LST ISO/IEC 10918-1:2009 „Informacijos technologija. Nejudamųjų tolydžiojo atspalvio vaizdų skaitmeninė spūda ir kodavimas. 1 dalis. Reikalavimai ir gairės (tapatus ISO/IEC 10918-1:1994)“.
17. Open Design Specification for .dwg files Version 5.3., https://www.opendesign.com/files/guestdownloads/OpenDesign_Specification_for_.dwg_files.pdf, 1998-2013.
18. RFC 5758 „Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA“, <http://www.ietf.org/rfc/rfc5758.txt>, 2010.
19. RFC 3066 „Tags for the Identification of Languages“, <http://www.ietf.org/rfc/rfc3066.txt>, 2001.
20. RFC 3161 „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)“, <http://www.ietf.org/rfc/rfc3161.txt>, 2001.
21. RFC 3447 „Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1“, <http://www.ietf.org/rfc/rfc3447.txt>, 2003.
22. RFC 3986 „Uniform Resource Identifier (URI): Generic Syntax“, <http://www.ietf.org/rfc/rfc3986.txt>, 2005.
23. RFC 4055 „Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“, <http://www.ietf.org/rfc/rfc4055.txt>, 2005.
24. RFC 5280 „Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile“, <http://www.ietf.org/rfc/rfc5280.txt>, 2008.
25. RFC 5652 „Cryptographic Message Syntax (CMS)“, <http://www.ietf.org/rfc/rfc5652.txt>, 2009.
26. RFC 6960 „X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP“, <http://www.ietf.org/rfc/rfc6960.txt>, 2013.
27. W3C Recommendation „Extensible Markup Language (XML) 1.0 (Fifth Edition)“, <http://www.w3.org/TR/2008/REC-xml-20081126/>, 2008.
28. W3C Recommendation „RDF/XML Syntax Specification (Revised)“, <http://www.w3.org/TR/2004/REC-rdf-syntax-grammar-20040210/>, 2004.
29. World files, http://www.cartograph.com/help/8_4/Content/MapSolutions/MapSA/WorldFiles_Ref.htm, https://en.wikipedia.org/wiki/World_file, <http://desktop.arcgis.com/en/arcmap/10.3/manage-data/raster-and-images/world-files-for-raster-datasets.htm>, MrSID (Multi-Resolution Seamless Image Database), <https://en.wikipedia.org/wiki/MrSID>.

30. XMP Specification, Adobe Systems Incorporated, https://en.wikipedia.org/wiki/Extensible_Metadata_Platform, 2005.