



LIETUVOS VYRIAUSIASIS ARCHYVARAS

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

2014 m. rugpjūčio d. Nr. V-
Vilnius

Vadovaudamasis Lietuvos Respublikos dokumentų ir archyvų įstatymo 5 straipsnio 3 dalies 6 punktu:

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

2. N u s t a t a u, kad:

2.1. Valstybės ir savivaldybių institucijų, įstaigų ir įmonių, valstybės įgaliotų asmenų (toliau – įstaigos) pagal šio įsakymo 1 punkte patvirtintą specifikaciją (toliau – Specifikacija) rengiami elektroniniai dokumentai turi atitikti Specifikacijoje apibrėžtus A lygmens dokumento reikalavimus.

2.2. Nevalstybinių organizacijų ir privačių juridinių ar fizinių asmenų (toliau – asmenys) pagal Specifikaciją rengiami dokumentai, kurių rengimą nustato teisės norminiai aktai, turi atitikti Specifikacijoje apibrėžtus A arba B lygmens dokumento reikalavimus.

2.3. Jei įstaiga gauna elektroninius dokumentus, atitinkančius Specifikacijoje apibrėžtus B lygmens dokumento reikalavimus, šie elektroniniai dokumentai Specifikacijoje aprašytu būdu papildomi trūkstamais metaduomenimis, kad gautas elektroninis dokumentas atitiktų Specifikacijoje apibrėžtus A lygmens dokumento reikalavimus.

2.4. Elektroninius dokumentus, atitinkančius Specifikacijoje apibrėžtus B lygmens dokumento reikalavimus, teikiantys asmenys dokumentus priimančios įstaigos nurodytu būdu turi pateikti trūkstamus metaduomenis.

Lietuvos vyriausiasis archyvaras

Ramojus Kraujelis

ELEKTRONINIO DOKUMENTO PDF-LT-V1.0 SPECIFIKACIJA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Elektroninio dokumento specifikacija PDF-LT-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 14 punkte) rašytiniams elektroniniams dokumentams, kurių turinys, metaduomenys ir elektroniniai 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 (toliau – Elektroninių dokumentų specifikacijų reikalavimų aprašas). Šios Specifikacijos keliamiems reikalavimams formuluoti panaudoti PDF/A-2, PAdES, PAdES bazinio profilio standartai ir kiti Specifikacijos 11 priede nurodyti dokumentai.

Specifikaciją atitinkantis dokumentas yra realizuojamas PDF/A-2 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“.

4. Specifikacijoje vartojamos sąvokos ir santrumpos:

CAdES – kriptografinių pranešimų sintakse (CMS) sudaryto (suformuoto) elektroninio parašo formatai, kuriuos aprašo standartas LST ETSI TS 101 733 V2.2.1:2013 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintieji CMS elektroniniai parašai (CAdES)“ (Specifikacijos 11 priedo 2 punktas; toliau – CAdES standartas).

CAdES-A – archyvinis elektroninio parašo formatas, aprašytas vadovaujantis CAdES standartu.

CAdES-BES – bazinis elektroninio parašo formatas, aprašytas vadovaujantis CAdES standartu.

CAdES-C – elektroninio parašo su nuorodomis į parašo galiojimą patvirtinančius duomenis formatas, aprašytas vadovaujantis CAdES standartu.

CAdES-EPES – pagal elektroninio parašo taisyklės sukurto elektroninio parašo formatas, aprašytas vadovaujantis CAdES standartu.

CAdES-LT – ilgalaikio galiojimo elektroninio parašo formatas, aprašytas vadovaujantis CAdES standartu.

CAdES-T – elektroninio parašo su laiko žyma formatas, aprašytas vadovaujantis CAdES standartu.

CAdES-X – elektroninio parašo su nuorodomis į parašo galiojimą patvirtinančius duomenis ir jų egzistavimą patvirtinančia laiko žyma formatas, aprašytas vadovaujantis CAdES standartu.

CAdES-X Long – elektroninio parašo su parašo galiojimą patvirtinančiais duomenimis formatas, aprašytas vadovaujantis CAdES standartu.

CMS elektroninio parašo formatas – elektroninio parašo formatas, atitinkantis RFC 5652 rekomendacijas (Specifikacijos 11 priedo 22 punktas).

CRL – sertifikatų, kurių galiojimas nutrauktas ar sustabdytas, sąrašas, atitinkantis RFC 5280 rekomendacijas (Specifikacijos 11 priedo 21 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 PDF elektroninių parašų, kuriais iki papildymo rinkmena galėjo būti pasirašyta, vientisumo.

OCSP paslauga – sertifikatų galiojimo patikrinimo paslauga, atitinkanti RFC 6960 rekomendacijas (Specifikacijos 11 priedo 15 punktas).

PAdES – elektroninio parašo PDF rinkmenoje formatai, kuriuos aprašo PDF elektroninio parašo standartų grupė (toliau – PAdES standartas). Šios standartų grupės apžvalga aprašyta pirmoje šios standartų grupės dalyje – standarte LST ETSI TS 102 778-1 V1.1.1:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo profiliai. 1 dalis. PAdES apžvalga. PAdES struktūros dokumentas“ (Specifikacijos 11 priedo 6 punktas).

PAdES-Basic – CMS elektroninio parašo formato pagrindu parengtas elektroninio parašo formatas, aprašytas vadovaujantis PAdES standarto 2 dalimi (Specifikacijos 11 priedo 7 punktas).

PAdES bazinis profilis – PDF elektroninių parašų profilis, atitinkantis standartą LST ETSI TS 103 172 V2.2.2:2013 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo (PAdES) bazinis profilis“ (Specifikacijos 11 priedo 12 punktas).

PAdES-BES – CAdES-BES arba CAdES-T elektroninio parašo formato pagrindu parengtas elektroninio parašo formatas, aprašytas vadovaujantis PAdES standarto 3 dalimi (Specifikacijos 11 priedo 8 punktas).

PAdES-EPES – pagal elektroninio parašo taisykles sukurtas elektroninio parašo formatas, kurio pagrindas yra CAdES-EPES arba CAdES-T elektroninio parašo formato pagrindu parengtas elektroninio parašo formatas, aprašytas vadovaujantis PAdES standarto 3 dalimi (Specifikacijos 11 priedo 8 punktas).

PAdES-LTV – ilgalaikio elektroninio parašo formatas, aprašytas vadovaujantis PAdES standarto 4 dalimi (Specifikacijos 11 priedo 9 punktas).

PAdES-XML – XAdES elektroninio parašo formato pagrindu parengtas elektroninio parašo formatas, aprašytas vadovaujantis PAdES standarto 5 dalimi (*angl. PAdES for XML content*) (Specifikacijos 11 priedo 10 punktas).

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

Patikimas sertifikatų centras – sertifikavimo paslaugų teikėjas, sudarantis kvalifikuotus sertifikatus arba kuriuo PDF elektroninio parašo tikrintojas pasitiki.

PDF – (angl. *portable document format*) kompiuterių rinkmenos formatas, aprašytas standartu LST ISO 32000-1:2009 „Dokumentų tvarkyba. PDF formatas. 1 dalis. PDF 1.7 (tapatus ISO 32000-1:2008)“ (Specifikacijos 11 priedo 14 punktas; toliau – PDF-1.7 standartas).

PDF/A-2 formatas – PDF-1.7 standarto pagrindu sukurtas ilgalaikio saugojimo paskirties rinkmenos formatas, aprašytas standartu LST ISO 19005-2:2011 „Dokumentų tvarkyba. Ilgalaikio saugojimo elektroninio dokumento rinkmenos formatas. 2 dalis. ISO 32000-1 (PDF/A-2) naudojimas (tapatus ISO 19005-2:2011)“ (Specifikacijos 11 priedo 13 punktas; toliau – PDF/A-2 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 laiko žyma, kurios santrauka skaičiuojama nuo visos PDF formato rinkmenos (išskyrus pačią laiko žymą). PDF dokumento laiko žyma patvirtina, kad visi objektai, įtraukti į PDF formato rinkmeną prieš sudarant PDF dokumento laiko žymą, egzistavo iki 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 4 dalies 3.1 skyrius). PDF dokumento laiko žymos žodynas yra PDF parašo žodynas, kuriam yra taikomi papildomi reikalavimai, nurodyti PAdES standarto 4 dalies A.2 priede.

PDF elektroninis parašas – elektroninis parašas ar duomenų vientisumą ir autentiškumą užtikrinantys duomenys, saugomi PDF parašo žodyne.

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 laukas – (angl. *signature form field*) PDF žodynas, kurio laukuose saugoma PDF elektroninio 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 elektroninio parašo duomenys ar duomenų vientisumą ir autentiškumą užtikrinantys 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 apibūdinančios schemos URI santrumpa.

Saugi elektroninio parašo formavimo sistema – programinė ir techninė įranga, susidedanti iš parašo formavimo įrangos, atitinkančios Reikalavimų elektroninio parašo įrangai, patvirtintų Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108, III skyriuje nustatytus reikalavimus, ir iš elektroninio parašo formavimo taikomosios sistemos, atitinkančios standarto LST CWA 14170:2005 (Specifikacijos 11 priedo 1 punktas) arba ekvivalentius reikalavimus saugioms elektroninio parašo formavimo taikomosios sistemoms.

URI – universalusis išteklių identifikatorius (angl. *uniform resource identifier*), kurio sandara atitinka RFC 3986 rekomendacijas (Specifikacijos 11 priedo 19 punktas), šioje Specifikacijoje naudojamas kaip XML arba XMP elementus, atributus ir jų reikšmių tipus apibūdinančios schemos identifikatorius.

XAdES – elektroninio parašo aprašymo XML struktūra standartas LST ETSI TS 101 903 V1.4.2:2011 „Patobulintieji XML elektroniniai parašai (XAdES)“ (Specifikacijos 11 priedo 5 punktas; toliau – XAdES standartas).

XML – (angl. *extensible markup language*) Pasaulinio tinklo konsorciumo (angl. *The World Wide Web Consortium, W3C*) rekomenduojama bendrosios paskirties duomenų struktūrų ir jų turinio aprašomoji kalba (Specifikacijos 11 priedo 25 punktas).

XMP – (angl. *extensible metadata platform*) Adobe Systems korporacijos rekomenduojama plečiama metaduomenų kūrimo, nuskaitymo ir keitimosi jais platforma, aprašyta viešai paskelbta XMP specifikacija (Specifikacijos 11 priedo 24 punktas; toliau – XMP specifikacija), kuri yra sudėtinė PDF-1.7 ir PDF/A-2 standartų dalis.

Kitos Specifikacijoje vartojamos sąvokos atitinka Lietuvos Respublikos dokumentų ir archyvų įstatyme, Lietuvos Respublikos elektroninio parašo įstatyme, Laiko žymos formavimo paslaugų teikimo tvarkos apraše, patvirtintame Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. balandžio 19 d. įsakymu Nr. 1V-407 „Dėl Laiko žymos formavimo paslaugų teikimo tvarkos aprašo patvirtinimo“, Elektroninių dokumentų specifikacijų reikalavimų apraše, patvirtintame Lietuvos vyriausiojo archyvaro 2014 m. rugpjūčio 29 d. įsakymu Nr. VE(1.3 E)-41 „Dėl Elektroninių dokumentų specifikacijų reikalavimų aprašo patvirtinimo“, ir kituose Lietuvos vyriausiojo archyvaro išleistuose teisės aktuose, kuriuose nustatomi dokumentų rengimo, tvarkymo, apskaitos, saugojimo bendrieji reikalavimai, vartojamas sąvokas.

II SKYRIUS

ELEKTRONINIO DOKUMENTO STRUKTŪRA

5. Elektroninio dokumento loginę struktūrą sudaro šios dalys:

- 5.1. turinys, susidedantis iš vieno privalomo pagrindinio dokumento ir neprivalomų priedų (loginių);
- 5.2. metaduomenys (tik nekeičiami);
- 5.3. vienas arba keli PAdES formato, kurio pagrindas yra CAdES elektroninio parašo formatas, elektroniniai parašai.

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

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

7.1. PDF puslapių medyje yra atvaizduotas visas turinys (pagrindinis dokumentas ir visi priedai). Turinio atvaizdavimo dalimi taip pat laikomi naudotojo darbui su PDF puslapių medžio struktūra palengvinti skirti dokumento struktūros, straipsnių, vardų, veiksmyų objektai ir kiti su puslapiais susiję objektai;

7.2. metaduomenų šaltiniuose, susietuose su PDF dokumento katalogo ar PDF parašų žodynais, ir Specifikacijoje nustatytuose PDF parašo žodyno laukuose yra atvaizduoti elektroninio dokumento metaduomenys;

7.3. PDF parašų žodynuose (išskyrus žodyno laukus, kuriais aprašomi metaduomenys ir susieti metaduomenų šaltiniai) yra atvaizduoti elektroniniai parašai arba duomenys, užtikrinantys kitų elektroninio dokumento duomenų vientisumą ir autentiškumą.

8. Elektroninio dokumento rinkmena, joje saugomas turinys ir metaduomenys turi atitikti Specifikacijoje keliamus reikalavimus, įskaitant PDF/A-2 standarto reikalavimus. PDF elektroniniai parašai turi atitikti Specifikacijoje keliamus reikalavimus, įskaitant PAdES ir PAdES bazinio profilio standartų reikalavimus.

9. Šią Specifikaciją atitinkančiame elektroniniame dokumente negali būti:

9.1. priedamųjų rinkmenų – PDF įdėtinės rinkmenos aprašo žodyne (angl. *file specification dictionary*) laukas „**EF**“ (PDF-1.7 standarto 7.11.3 skyrius) bei PDF dokumento vardų žodyne (angl. *name dictionary*) laukas „**EmbeddedFiles**“ (PDF-1.7 standarto 7.7.4 skyrius) yra draudžiami;

9.2. keičiamų metaduomenų;

9.3. lygiagrečiuoju pasirašymo būdu sudarytų elektroninių parašų.

10. Ši Specifikacija draudžia elektroniniame dokumente naudoti XML architektūros formas (XFA formas – PDF/A-2 standarto 6.4.2 skyrius).

III SKYRIUS ELEKTRONINIO DOKUMENTO PAKUOTĖ

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

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

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

11.3. rinkmena atitinka vieno pasirinkto suderinamumo su PDF/A-2 standartu lygio (PDF/A-2a, PDF/A-2b, PDF/A-2u) keliamus rinkmenos struktūros reikalavimus;

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

12. 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.

13. Kai naudojami šioje Specifikacijoje apibrėžti 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).

IV SKYRIUS TURINYS

14. Elektroninio dokumento turinį sudaro vienas privalomas pagrindinis dokumentas ir vienas ar keli loginiai priedai, kurie nėra privalomi. Elektroniniame dokumente negali būti pridedamų savarankiškų elektroninių dokumentų.

15. Elektroninio dokumento turinys turi būti išsaugotas PDF/A-2 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) bei kitų gamintojų programinė įranga.

16. Visas elektroninio dokumento turinys turi būti atvaizduotas viename PDF puslapių medžio žodyne, kuris nurodytas PDF dokumento katalogo lauke „**Pages**“.

17. Elektroninio dokumento turinyje turi būti tik statinio vaizdo informacija. Kintančio vaizdo, garso ir trimatės grafikos objektai yra draudžiami (PDF/A-2 standarto 6.3.1 skyrius).

18. Elektroninio dokumento turinys turi būti pasirašytas bent vienu elektroniniu parašu, kurio paskirtis nurodyta šios Specifikacijos 38 punkte.

19. Draudžiama šalinti ar keisti pasirašyto elektroninio dokumento turinio objektus ir turinį pildyti naujais objektais (pvz., inkrementinio keitimo būdu), išskyrus atvejus, nurodytus Specifikacijos 71 punkte.

V SKYRIUS METADUOMENYS

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

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

22. Metaduomenys skirstomi į šias grupes:

22.1. 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 71 punkte;

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

22.3. elektroninių parašų metaduomenys – kiekvieno PDF elektroninio parašo formavimo metu sukuriama metaduomenys.

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

24. Dokumento sudarymo metaduomenys turi būti fiksuojami XMP specifikaciją ir PDF/A-2 standarto 6.6.2 skyriaus reikalavimus atitinkančiu formatu PDF metaduomenų šaltinyje, susietame su PDF dokumento katalogo žodynu.

25. Dokumento registravimo metaduomenys turi būti fiksuojami XMP specifikaciją ir PDF/A-2 standarto 6.6.2 skyriaus reikalavimus atitinkančiu formatu PDF metaduomenų šaltinyje, susietame su PDF elektroniniu parašu.

26. Elektroninių parašų metaduomenys fiksuojami PDF parašo žodyno laukuose. Elektroninių parašų metaduomenys ir jų reikšmių tipai apibrėžti Specifikacijos 1 priedo 3 skyriuje.

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

27.1. PDF/A standarto versiją ir suderinamumo su standartu lygį identifikuojančius metaduomenis, aprašytus vadovaujantis PDF/A-2 standarto 6.6.4 skyriuje nustatytais reikalavimais;

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

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

28. Sudarant PDF elektroninį parašą, PDF parašo žodyne turi būti užpildyti privalomieji elektroninio parašo metaduomenų laukai (Specifikacijos 1 priedo 3 skyrius). Su PDF elektroniniu parašu gali būti siejami dokumento registravimo metaduomenys (Specifikacijos 1 priedo 2 skyrius), kurie metaduomenų šaltinio pavidalu nurodomi PDF parašo žodyno lauke „**Metadata**“.

29. Elektroniniame dokumente gali būti kitų PDF-1.7 ir PDF/A-2 standartuose bei XMP specifikacijoje apibrėžtų neprivalomų metaduomenų, kai jų įtraukimo būdas nepažeidžia šios Specifikacijos reikalavimų.

30. Elektroninis dokumentas, atsižvelgiant į jo gyvavimo ciklą, gali turėti ir kitų (papildomų) metaduomenų, kurie nėra apibrėžti šioje Specifikacijoje ir jos 29 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-2 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.

31. 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-2 standarto 6.6.3 skyriuje pateiktą PDF žodyno laukų ir XMP metaduomenų atitikčių lentelę.

32. 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.

33. Elektroninio dokumento metaduomenys privalo būti pasirašyti PDF elektroniniu parašu.

34. Pasirašyto elektroninio dokumento metaduomenis draudžiama šalinti, keisti ar pildyti (pvz., inkrementinio keitimo būdu), išskyrus šios Specifikacijos 71 punkte nurodytus atvejus.

VI SKYRIUS ELEKTRONINIAI PARAŠAI

35. Elektroninis dokumentas pasirašomas PAdES formato elektroniniu parašu, kuriuo pasirašomi visi PDF rinkmenoje esantys duomenys, išskyrus paties elektroninio parašo reikšmę (PAdES standarto 1 dalis, 4.1 skyrius; PDF/A-2 standarto B priedas).

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

37. Elektroniniame dokumente galimi šie PDF elektroniniai parašai:

37.1. kvalifikuoti elektroniniai parašai (turintys tą pačią teisinę galią kaip ir pasirašytieji ranka);

37.2. patikimo sertifikatų centro išduotu sertifikatu patvirtinti duomenys, užtikrinantys apsaugomų duomenų autentiškumą ir vientisumą.

38. Elektroninių dokumentų pasirašymo ir tvirtinimo, suderinimo bei kopijos tikrumo patvirtinimo paskirties elektroniniai parašai turi būti sudaryti naudojant saugią elektroninio parašo formavimo sistemą ir galiojantį kvalifikuotą sertifikatą, atitinkantį standartą LST ETSI TS 101 862 V1.3.3:2007 „Kvalifikuoto sertifikato profilis“ (Specifikacijos 11 priedo 4 punktas).

39. Elektroniniame dokumente galimi tik PAdES-BES, PAdES-EPES arba PAdES-LTV formato PDF elektroniniai parašai. PAdES standarto 2 ir 5 dalyse aprašyti elektroninių parašų formatai PAdES-Basic ir PAdES-XML yra draudžiami. Visi PAdES-LTV formato parašai turi būti sukurti PAdES-BES arba PAdES-EPES formatų pagrindu. Atsižvelgiant į tai, kad PAdES standartas yra universalus ir numato alternatyvas, Specifikacijoje sukonkretinamas PAdES parašų elementų naudojimas konkrečiau taikymo atveju.

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

40.1. ji turi būti sudaroma vadovaujantis PAdES standarto 6 dalies (Specifikacijos 11 priedo 11 punktas) 5 skyriaus reikalavimais;

40.2. negali uždengti dokumento turinį atvaizduojančios informacijos;

40.3. elektroniniame dokumente konkrečiau PDF elektroninio parašo buvimas gali būti atvaizduotas ne daugiau nei 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).

41. Elektroninis dokumentas gali būti papildytas PDF elektroniniais parašais, modifikuojant PDF rinkmeną inkrementinio keitimo būdu, kaip tai aprašyta PAdES standarto 1 dalies 4.4 skyriuje ir PDF-1.7 standarto 7.5.6 skyriuje.

42. Visi PDF elektroniniai 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*) parašai draudžiami.

43. Jeigu sudarant PDF elektroninį 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.

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

45. PDF parašo žodyno „**Contents**“ lauke saugomi PDF elektroninio parašo duomenys turi būti CAdES-BES, CAdES-EPES arba CAdES-T formato. CAdES-C, CAdES-X, CAdES-X Long, CAdES-A ir CAdES-LT formato parašai yra draudžiami.

46. PDF parašo žodyno „**Contents**“ lauke saugomų PDF elektroninio parašo duomenų struktūra, elementų privalomumo ir reikšmių pildymo reikalavimai nurodyti šios Specifikacijos 8 priede, algoritmai elektroniniams parašams formuoti pateikti Specifikacijos 7 priede.

47. PDF parašo žodyno „**Contents**“ lauke saugomų PDF elektroninio parašo duomenų atributai turi būti užkoduoti naudojant DER koduotę.

48. Tam, kad būtų galima automatinėmis priemonėmis patikrinti PDF elektroninį 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 laiko žymos.

49. Parašo galiojimą patvirtinantys duomenys turi būti išsaugoti PDF dokumento duomenų saugyklos žodyne (angl. *document security store dictionary*, *DSS*), kaip aprašyta PAdES standarto 4 dalyje. Konkretaus parašo galiojimą patvirtinantys duomenys papildomai gali būti nurodyti ir PDF parašo tikrinimo duomenų žodyne (angl. *Signature VRI (validation-related information) dictionary*, *VRI*). PDF dokumento duomenų saugyklos ir parašo tikrinimo duomenų žodynai aprašyti PAdES standarto 4 dalies A.1 priede.

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

50.1. parašo laiko žyma, saugoma CAdES-T formato elektroninio parašo nepasirašomame laiko žymos atribute „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 6.1.1 skyrius), patvirtinanti PDF elektroninio parašo, į kurį yra įtraukta, egzistavimą iki parašo laiko žymoje nurodyto laiko;

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

51. Visos laiko žymos turi atitikti standartą LST ETSI TS 101 861 V1.3.1:2007 „Laiko žymėjimo profilis“. Laiko žymos turi būti gaunamos HTTP arba HTTPS protokolu pagal RFC 3161 rekomendacijas (Specifikacijos 11 priedo 16 punktas).

52. CRL sąrašai turi atitikti RFC 5280 rekomendacijas (Specifikacijos 11 priedo 21 punktas) ir turi būti gaunami HTTP arba HTTPS protokolu.

53. OCSP paslaugų atsakymai turi atitikti RFC 6960 rekomendacijas (Specifikacijos 11 priedo 15 punktas) ir turi būti gaunami HTTP arba HTTPS protokolu.

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

55. Elektroniniame dokumente galimi einamieji, trumpalaikiai ir ilgalaikiai PDF elektroniniai parašai.

56. Einamasis PDF elektroninis parašas yra PAdES-BES ar PAdES-EPES formato elektroninis parašas be parašo laiko žymos, esantis PDF formato rinkmenoje, kurioje nėra nė vienos PDF dokumento laiko žymos, patvirtinančios PDF elektroninio parašo egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko. Einamasis PDF elektroninis parašas turi atitikti PAdES bazinio profilio standartą (Specifikacijos 11 priedo 12 punktą) apibrėžtą B-Level (bazinio lygio) atitikties lygmenį.

57. Trumpalaikiai PDF elektroniniai parašai gali būti dviejų tipų:

57.1. PAdES-BES arba PAdES-EPES formato elektroninis parašas su elektroninio parašo laiko žyma, esantis PDF formato rinkmenoje, kurioje nėra nė vienos PDF dokumento laiko žymos, patvirtinančios PDF elektroninio parašo egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko (Specifikacijos 9 priedo 1 punktą);

57.2. PAdES-LTV formato elektroninis parašas be elektroninio parašo laiko žymos, esantis PDF formato rinkmenoje, kurioje yra viena PDF dokumento laiko žyma, patvirtinanti PDF elektroninio parašo egzistavimą iki PDF dokumento laiko žymoje nurodyto laiko (Specifikacijos 9 priedo 2 punktą).

58. Ilgalaikiai PDF elektroniniai parašai gali būti dviejų tipų:

58.1. PAdES-LTV formato elektroninis parašas su elektroninio 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 punktą);

58.2. PAdES-LTV formato elektroninis parašas be elektroninio 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 PDF elektroninio 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 punktą).

VII SKYRIUS

ELEKTRONINIO DOKUMENTO TIKRINIMAS

59. Elektroninio dokumento tikrinimo metu turi būti patikrinta, kad elektroninis dokumentas atitinka visus šioje Specifikacijoje nustatytus elektroninio dokumento pakuotės, struktūros, metaduomenų ir elektroninių parašų reikalavimus, atsižvelgiant į reikalavimų lygmenį.

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.

60. PDF rinkmenos atitiktis PDF/A-2 standarto reikalavimams (šios Specifikacijos 8, 11, 15 punktai) patikra neturi apsiriboti vien tik šios Specifikacijos 27.1 punkte nurodytų metaduomenų egzistavimo patikra.

61. Visi PDF elektroniniai parašai turi būti tikrinami vadovaujantis Reikalavimų elektroninio parašo tikrinimo procedūrai aprašu, patvirtintu Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. balandžio 19 d. įsakymu Nr. 1V-409, ir laikantis PAdES standarte apibrėžtų reikalavimų.

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

63. 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 laiko žymose, atžvilgiu. Jeigu tokių laiko žymų nėra, tai parašo galiojimą patvirtinantys duomenys tikrinami einamojo laiko atžvilgiu.

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

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

65.1. sertifikatų galiojimą patvirtinantys duomenys yra surinkti PDF elektroninio parašo ar laiko žymos tikrinimo metu;

65.2. sertifikatų galiojimą patvirtinantys duomenys yra įtraukti į dokumentą ne anksčiau, nei buvo įtraukta anksčiausia iš laiko žymų, patvirtinančių PDF elektroninio parašo egzistavimą iki jose nurodyto laiko (laiko žymos tikrinimo atveju – ne anksčiau, nei buvo įtraukta pati tikrinamoji laiko žyma).

66. Kiekvienas PDF elektroninis parašas tikrinamas neatsižvelgiant į kitų elektroninio dokumento PDF elektroninių parašų galiojimą.

VIII SKYRIUS

SPECIFIKACIJOS REIKALAVIMŲ LYGMENYS

67. Pagal šią Specifikaciją sudarytas elektroninis dokumentas turi būti rengiamas pagal Specifikacijos 3 punkte apibrėžtus A arba B reikalavimų lygmenis.

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

68. 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.

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

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

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

71.1. elektroninio dokumento papildymas nauju PDF elektroniniu parašu kartu su registravimo metaduomenimis arba be jų (Specifikacijos 41 punktas);

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

71.3. elektroninio dokumento papildymas nauja PDF dokumento laiko žyma;

71.4. turinio papildymas PDF elektroninių parašų buvimo atvaizdavimo informacija (Specifikacijos 40 punktas);

71.5. PDF dokumento katalogo plėtinių žodyno papildymas PDF žodyno laukų prefiksu „LTUd“ (Specifikacijos 13 punktas);

71.6. B lygmens elektroninio dokumento PDF dokumento katalogo žodyno metaduomenų šaltinio papildymas XMP metaduomenų plėtinio schema (Specifikacijos 27.2 punktas);

71.7. B lygmens elektroninio dokumento PDF dokumento katalogo žodyno metaduomenų šaltinio papildymas dokumento sudarymo ir kitais metaduomenimis (Specifikacijos 27.3, 29, 30 punktai);

71.8. dokumento sudarymo metaduomenyse `xmp:Identifier` reikšmių rinkinio papildymas nauja dokumento atitikties reikalavimų lygmeniui deklaracijos reikšme (Specifikacijos 1 priedo 1 skyrius).

72. 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-2 standarto 6.6.6. skyriumi ir XMP specifikacija (Specifikacijos 11 priedo 24 punktas).

IX SKYRIUS BAIGIAMOSIOS NUOSTATOS

73. Dokumentų, kuriais remiantis parengta Specifikacija, sąrašas pateikiamas šios Specifikacijos 11 priede.

74. Pagal šią Specifikaciją sudaryti elektroniniai dokumentai valdomi vadovaujantis Elektroninių dokumentų valdymo taisyklėse nustatytais reikalavimais ir išsaugomi visą nustatytą jų saugojimo laiką.

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-LT-V1.0“.
Dokumento atitikties reikalavimų lygmeniui deklaracija	xmp:Identifier	Teksto reikšmių rinkinys	Taip	Atitiktis deklaruojama rinkinyje įdėjus reikšmę, kuria nurodomas lygmuo 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.

Metaduomuo	XMP vardas ¹	Tipas ²	Privalomas A lygmens dokumentui	Aprašas
Dokumento pavadinimas	dc:title	Tekstas skirtingomis kalbomis	Taip	Privaloma užpildyti reikšmę su atributo xml:lang reikšme „x-default“.
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 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 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. Viename PDF parašo 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. Viename PDF parašo 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. Viename PDF parašo žodyno metaduomenų šaltinyje gali būti nurodytas ne daugiau kaip vienas metaduomuo.

III SKYRIUS ELEKTRONINIŲ PARAŠŲ METADUOMENYS

Elektroninių parašų metaduomenys nurodomi kiekvieno PDF elektroninio parašo žodyno laukuose.

Metaduomuo	PDF parašo žodyno lauko raktas (vardas)	Tipas ⁵	Privalomas A lygmens dokumentui	Privalomas B lygmens dokumentui	Aprašas
Elektroninio parašo paskirtis	Reason	Tekstas (text string)	Taip	Taip	Elektroninio parašo paskirtis žyminčios reikšmės: pasirašymo – „signature“;

Metaduomuo	PDF parašo žodyno lauko raktas (vardas)	Tipas ⁵	Privalomas A lygmens dokumentui	Privalomas B lygmens dokumentui	Aprašas
					• tvirtinimo – „confirmation“; • suderinimo – „conciliation“; • vizavimo – „visa“; • sudaryto dokumento registravimo – „registration“; • gauto dokumento registravimo – „registration-of-incoming-documents“; • supažindinimo – „acknowledgement“; • rezoliucijos įrašymo – „resolution“; • žymos apie užduoties įvykdymą – „end-of-execution“; • archyvinio patvirtinimo – „notarisation“; • kopijos tikrumo patvirtinimo – „copy-certification“; • autentiškumo (vientisumo) patvirtinimo – „authenticity“. Šio lauko reikšmė privalo būti nurodyta be kabučių mažosiomis raidėmis. Jei reikšmė nesutampa su nė viena iš čia išvardytųjų, laikoma, kad parašo paskirtis – pasirašymas (t.y. atitinka reikšmę „signature“).
Elektroninį parašą sudariusio asmens vardas ir pavardė	Name	Tekstas (text string)	Taip, jei šių duomenų nėra sertifikate	Taip, jei šių duomenų nėra sertifikate	Jeigu 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.

Metadomuo	PDF parašo žodyno lauko raktas (vardas)	Tipas ⁵	Privalomas A lygmens dokumentui	Privalomas B lygmens dokumentui	Aprašas
Elektroninį parašą sudariusio asmens pareigos	LTud_Role	Tekstas (text string)	Taip (Istaigos vadovui ar jo įgaliojam asmeniui)	Ne	
Elektroninio parašo sudarymo data (deklaruojama)	M	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)“ (11 priedo 26 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
Asmuo	Šių pastabų 3 punkte aprašyta metaduomenų plėtinio struktūra.
Registracija	Šių pastabų 4 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: <i>Organizacija</i> – programinę įrangą sukūrusios organizacijos pavadinimas; <i>Programa</i> – programinės įrangos pavadinimas; <i>Versija</i> – konkreti programinės įrangos versija; <i>tekstas</i> – 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 IETF RFC 3066 rekomendacijas atitinkanti kalbos kodo reikšmė arba reikšmė „ <i>x-default</i> “ standartinei teksto reikšmei nurodyti.
Kalbos kodas	(angl. <i>locale</i>) Tekstinis laukas, kuriame nurodyta IETF RFC 3066 rekomendacijas 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
			Sudarytoji	Adresatui	Gavėjui	
Požymis: fizinis (taip) ar juridinis (ne) asmuo	LTUdEnt:individual	Loginis	Taip	Ne	Taip	

Laukas	XMP vardas	Tipas	Privalomas (nurodžius asmenį)			Pastabos
			Sudarytojui	Adresatui	Gavėjui	
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.
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. Teksto ir datos duomenų tipai, skirti PDF žodyno reikšmėms fiksuoti, apibrėžti PDF-1.7 standarto 7.9.2 ir 7.9.4 skyriuose.

6. 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 elektroninio parašo sudarymo data (PDF parašo žodyno lauko „*M*“ reikšmė) (kai dokumentas nėra registruojamas).

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

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

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 aprašas -->
  <pdfaExtension:schemas>
    <rdf:Bag>
      <rdf:li rdf:parseType="Resource">
        <pdfaSchema:schema>PDF-LT-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-LT-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>Dokumentu 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>originalRegistrations</pdfaProperty:name>
              <pdfaProperty:valueType>seq Registration</pdfaProperty:valueType>
              <pdfaProperty:category>external</pdfaProperty:category>
              <pdfaProperty:description>Originalaus dokumentu 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 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>
    </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 (2) ir suderinamumo lygis (A, B ar U) -->

    <rdf:Description rdf:about = ""
      xmlns:pdfaid = "http://www.aiim.org/pdfa/ns/id/">
      <pdfaid:part>2</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 -->

    <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:Bag>
      </xmp:Identifier>
    </rdf:Description>

    <!-- PDF-LT-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/"
      <LTUd:standardVersion>PDF-LT-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>
</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: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 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 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"?>

```

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	PDF elektroninio parašo tikrinimo valdiklio vardas. PDF elektroniniam parašui tikrinti gali būti naudojamas ir kitas, nei nurodytas, valdiklis, jeigu jis palaiko „ SubFilter “ lauke nurodytą elektroninio 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 elektroninis parašas.
Cert	Masyvas arba baitų seka (array or byte string)	Draudžiamas	Pasirašyti naudoto sertifikato ir jo kelio sertifikatai turi būti nurodyti CAdES formato elektroniniame paraše.
ByteRange	Masyvas (array)	Taip	Nurodo pasirašytų baitų intervalus. Turi nurodyti visą PDF rinkmeną, išskyrus šio parašo žodyno „ Contents “ lauką.
Reference	Masyvas (array)	Draudžiamas	Parašų nuorodų žodynai.
Changes	Masyvas (array)	Ne	Pakeitimai atlikti po paskutinio PDF elektroninio parašo sukūrimo. Jeigu nurodytas, tai visos trys masyvo reikšmės turi būti „0“.
Name	Tekstas (text string)	Taip, jei parašą sudariusio asmens vardo ir pavardės nėra sertifikate	Metaduomens „Elektroninį parašą sudariusio asmens vardas ir pavardė“ reikšmė (1 priedo 3 skyrius).
M	Data (date)	Taip	Metaduomens „Elektroninio parašo sudarymo data (deklaruojama)“ reikšmė (1 priedo 3 skyrius).
Location	Tekstas (text string)	Ne	Pasirašymo vieta.
Reason	Tekstas (text string)	Taip	Metaduomens „Elektroninio parašo paskirtis“ reikšmė (1 priedo 3 skyrius).
ContactInfo	Tekstas (text string)	Ne	Pasirašančiojo asmens ryšio duomenys.
R	Skaičius (integer)	Draudžiamas	PDF elektroninio parašo tikrinimo valdiklio versija.

Žodyno lauko raktas	Tipas ¹	Privalomumas	Aprašas
V	Skaičius (integer)	Ne	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 PDF elektroninio parašo sudarymo momento. Draudžiama lauką nurodyti, jeigu reikšmė nežinoma.
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).
Metadata	Duomenų šaltinis (stream)	Ne	XMP paketas, kuriame užfiksuoti dokumento registravimo metaduomenys (1 priedo 2 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 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	Laiko žyma, atitinkanti RFC3161 reikalavimus. 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	Dokumentu 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.

Žodyno lauko raktas	Tipas¹	Privalomumas	Aprašas
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.

PDF ELEKTRONINIUOSE PARAŠUOSE NAUDOJAMI ALGORITMAI

PDF elektroniniuose parašuose gali būti naudojami tik šie algoritmai:

Algoritmas	Identifikatorius	Identifikatorių aprašantis dokumentas
Santraukos sudarymas (angl. <i>digest</i>)		
SHA1 ¹	id-sha1	RFC 3279 (11 priedo 17 punktas)
SHA256	id-sha256	RFC 4055 (11 priedo 20 punktas)
SHA384	id-sha384	RFC 4055
SHA512	id-sha512	RFC 4055
Pasirašymas (angl. <i>signature</i>)		
RSAwithSHA1 ¹	sha1WithRSAEncryption	RFC 3447 (11 priedo 18 punktas)
RSAwithSHA256	sha256WithRSAEncryption	RFC 3447
RSAwithSHA384	sha384WithRSAEncryption	RFC 3447
RSAwithSHA512	sha512WithRSAEncryption	RFC 3447
DSAwithSHA1 (DSS) ¹	id-dsa-with-sha1	RFC 3279
DSAwithSHA256	id-dsa-with-sha256	RFC 5758 (11 priedo 23 punktas)
ECDSAwithSHA1 ¹	ecdsa-with-SHA-1	RFC 3279
ECDSAwithSHA256	ecdsa-with-SHA256	RFC 5758
ECDSAwithSHA384	ecdsa-with-SHA384	RFC 5758
ECDSAwithSHA512	ecdsa-with-SHA512	RFC 5758

Pastaba. ¹ Algoritmas nerekomenduojamas sudarant PDF elektroninius parašus ir laiko žymas. Algoritmas privalo būti palaikomas tikrinant PDF elektroninius parašus ir juos patvirtinti naudotus setifikatus, laiko žymas bei parašo galiojimą patvirtinančius duomenis.

CADES FORMATO ELEKTRONINIO PARAŠO STRUKTŪRA

Šis priedas aprašo PAdES-BES, PAdES-EPES ir PAdES-LTV formato PDF parašo žodyno lauke „**Contents**“ saugomo CAdES formato elektroninio 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 (11 priedo 22 punktas) 5.1 skyriuje.
digestAlgorithms DigestAlgorithmIdentifiers ::= SET OF	Taip	1	
DigestAlgorithmIdentifier,	Taip	1-N	Leistini 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 elektroninio parašo išorėje.
}			
certificates [0] IMPLICIT CertificateSet OPTIONAL ::= SET OF	Taip	1	Privalo būti pasirašančiojo asmens X509 v3 sertifikatas.

CAAdES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
<pre>CertificateChoices ::= CHOICE {</pre>		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>).
<pre>certificate Certificate,</pre>	Privalomas	1	X509 sertifikatas.
<pre>extendedCertificate [0] IMPLICIT ExtendedCertificate,</pre>	Draudžiamas	0	
<pre>v1AttrCert [1] IMPLICIT AttributeCertificateV1,</pre>	Draudžiamas	0	
<pre>v2AttrCert [2] IMPLICIT AttributeCertificateV2,</pre>	Draudžiamas	0	
<pre>.....other [3] IMPLICIT OtherCertificateFormat</pre>	Draudžiamas	0	
<pre>}</pre>			
<pre>crls [1] IMPLICIT RevocationInfoChoices OPTIONAL</pre>	Draudžiamas	0	
„signerInfos“ tipo elementas:			
<pre>signerInfos ::= SET OF</pre>	Taip	1	CAAdES elektroniniame paraše turi būti tik vieno asmens parašo informacija.
<pre>SignerInfo ::= SEQUENCE {</pre>	Taip	1	
<pre>version CMSVersion,</pre>	Taip	1	Sintaksės versijos numeris. Reikšmė turi būti „1“ arba „3“ ir parenkama, kaip nurodyta RFC 5652 (11 priedo 22 punktas) 5.3 skyriuje.
<pre>sid SignerIdentifier ::= CHOICE {</pre>	Taip	1	Pasirašančiojo asmens sertifikato identifikatorius.

CAdES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
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 RFC5652 5.3 skyriuje.
},			
digestAlgorithm DigestAlgorithmIdentifier,	Taip	1	Leistini santraukos sudarymo algoritmai nurodyti 7 priede.
„signedAttrs“ tipo elementas:			
signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL	Taip	1	Pasirašomi CAdES elektroninio parašo atributai.
SignedAttributes ::= SET SIZE (1..MAX) OF			
Attribute ::= SEQUENCE {	Taip	3-N ¹	
attrType OBJECT IDENTIFIER,			
-- attrType: id-contentType	Taip	1	Pasirašomo turinio tipas. Turi būti nurodyta reikšmė „id-data“ (pagal RFC5652 4 skyrių).
-- attrType: id-messageDigest	Taip	1	Pasirašomų duomenų santrauka.
-- attrType: id-aa-ets-signingCertificateV2	Ne ²	0-1	Pasirašančiojo asmens sertifikato nuoroda. Privalomas naudojant kitą nei SHA1 santraukos sudarymo algoritmą.

CAdES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
-- attrType id-aa-signingCertificate	Ne ²	0-1	Pasirašančiojo asmens sertifikato nuoroda. Privalomas naudojant SHA1 santraukos sudarymo algoritmą.
-- attrType id-aa-ets-otherSigCert	Draudžiamas	0	Pasirašančio asmens sertifikato nuoroda.
-- attrType id-signingTime	Draudžiamas	0	Deklaruojamas pasirašymo laikas.
-- attrType id-aa-ets-sigPolicyId	Ne ³	0-1	Išreikštinės elektroninio parašo taisyklės.
-- attrType id-aa-ets-commitmentType	Ne ⁴	0-1	Įsipareigojimo tipas ⁵ .
-- attrType id-aa-ets-signerLocation	Draudžiamas	0	Pasirašymo vieta.
-- attrType id-aa-ets-signerAttr	Draudžiamas	0	Pasirašančiojo asmens atributai (rolės).
-- attrType id-aa-ets-contentTimestamp	Ne	0-1	Pasirašomų duomenų laiko žyma (sukuriama prieš pasirašymą). Šio atributo naudojimas yra nerekomenduojamas. Šiam tikslui rekomenduojama naudoti dokumento laiko žymą (angl. <i>document time-stamp</i>), kaip aprašyta PAdES standarto 4 dalyje.
-- attrType id-aa-contentReference	Draudžiamas	0	Nuoroda į pasirašytus duomenis (parašą).
-- attrType id-aa-contentIdentifier	Draudžiamas	0	Pasirašytų duomenų (parašo) identifikatorius.
-- attrType id-aa-contentHint	Draudžiamas	0	Pasirašomo turinio formatas.
-- attrType id-aa-ets-mimeType	Draudžiamas	0	Pasirašomo turinio MIME tipas.
attrValues SET OF AttributeValue	Taip	1	
},			
signatureAlgorithm SignatureAlgorithmIdentifier,	Taip	1	Pasirašymo algoritmas. Leistini pasirašymo algoritmai nurodyti 7 priede.
signature SignatureValue ::= OCTET STRING,	Taip	1	

CADES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
„ <i>unsignedAttrs</i> “ tipo elementas:			
<code>unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL</code>	Ne	0-1	Nepasirašomi CAdES elektroninio parašo atributai.
<code>UnsignedAttributes ::= SET SIZE (1..MAX) OF</code>			
<code>Attribute ::= SEQUENCE {</code>	Taip	1-N ¹	
<code>attrType OBJECT IDENTIFIER,</code>	Taip	1	
<code>-- attrType id-aa-signatureTimeStampToken</code>	Ne	0-1	Parašo laiko žyma, kuri atitinka RFC 3161 (11 priedo 16 punktas) reikalavimus.
<code>-- attrType id-aa-ets-certificateRefs</code>	Draudžiamas	0	Nuorodos į sertifikatus.
<code>-- attrType id-aa-ets-revocationRefs</code>	Draudžiamas	0	Nuorodos į atšaukimo duomenis.
<code>-- attrType id-aa-ets-certValues</code>	Draudžiamas	0	Sertifikatų reikšmės.
<code>-- attrType id-aa-ets-revocationValues</code>	Draudžiamas	0	Atšaukimo duomenys.
<code>-- attrType id-aa-ets-escTimeStamp</code>	Draudžiamas	0	CAdES-C formato elektroninio parašo laiko žyma.
<code>-- attrType id-aa-ets-certCRLTimestamp</code>	Draudžiamas	0	Nuorodų į sertifikatus ir atšaukimo duomenis laiko žyma.
<code>-- attrType id-aa-ets-archiveTimestampV2</code>	Draudžiamas	0	Archyvinė laiko žyma.
<code>-- attrType id-aa-ets-archiveTimestampV3</code>	Draudžiamas	0	Archyvinė laiko žyma.
<code>-- attrType id-aa-ets-longTermValidation</code>	Draudžiamas	0	Duomenų egzistavimo iki tam tikro laiko įrodymo atributas.
<code>-- attrType id-aa-ets-attrCertificateRefs</code>	Draudžiamas	0	Nuorodos į atributinius sertifikatus.
<code>-- attrType id-aa-ets-attrRevocationRefs</code>	Draudžiamas	0	Nuorodos į atributinių sertifikatų atšaukimo duomenis.
<code>-- attrType id-countersignature</code>	Draudžiamas	0	
<code>attrValues SET OF AttributeValue</code>	Taip	1	
<code>},</code>			
<code>}</code>			
<code>}</code>			

Pastabos:

1. Neišvardyti CAdES pasirašomi ar nepasirašomi atributai nedraudžiami, tačiau PDF elektroninių parašų tikrinimo metu jie turi būti ignoruojami.

2. Privaloma nurodyti vieną pasirašančiojo asmens sertifikato nuorodos atributą („*signing-certificate-v2*“ (objekto identifikatorius „*id-aa-ets-signingCertificateV2*“; CAdES standarto 5.7.3.2 skyrius) arba „*signing-certificate*“ (objekto identifikatorius „*id-aa-signingCertificate*“; CAdES standarto 5.7.3.1 skyrius). Abu atributus kartu naudoti draudžiama.

3. Privalomas PAdES-EPES formato elektroniniam parašui.
 4. Draudžiamas, jeigu nėra parašo taisyklių identifikatoriaus atributo „*signature-policy-identifier*“ (objekto identifikatorius „*id-aa-ets-sigPolicyId*“; CAdES standarto 5.8.1 skyrius) atributo. Leistinas, jeigu yra parašo taisyklių identifikatoriaus atributas „*signature-policy-identifier*“.
 5. Įsipareigojimo tipas gali būti naudojamas kitiems tikslams, nei nurodyti elektroninio parašo paskirtį, aprašytą PDF parašo žodymo lauke „***Reason***“.
-

TRUMPALAIKIŲ IR ILGALAIKIŲ PDF ELEKTRONINIŲ PARAŠŲ SCHEMAS

I SKYRIUS

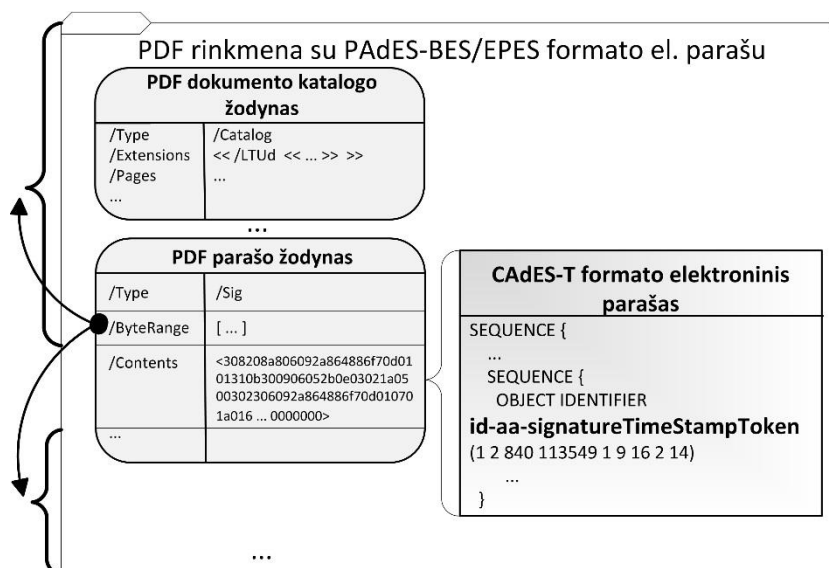
TRUMPALAIKIS PDF ELEKTRONINIS PARAŠAS SU ELEKTRONINIO PARAŠO LAIKO ŽYMA

1. Trumpalaikis PDF elektroninis parašas su elektroninio parašo laiko žyma – tai PAdES-BES arba PAdES-EPES formato elektroninis parašas, kuris atitinka visus šiuos reikalavimus:

1.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES-T formato elektroninis parašas, kuriame yra nepasirašomas parašo laiko žymos atributas „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 6.1.1 skyrius);

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

1.3. Trumpalaikis PDF elektroninis parašas turi atitikti PAdES bazinio profilio standarte (11 priedo 12 punktas) apibrėžtą T-Level (patikimo parašo egzistavimo laiko) atitikties lygmenį.



II SKYRIUS

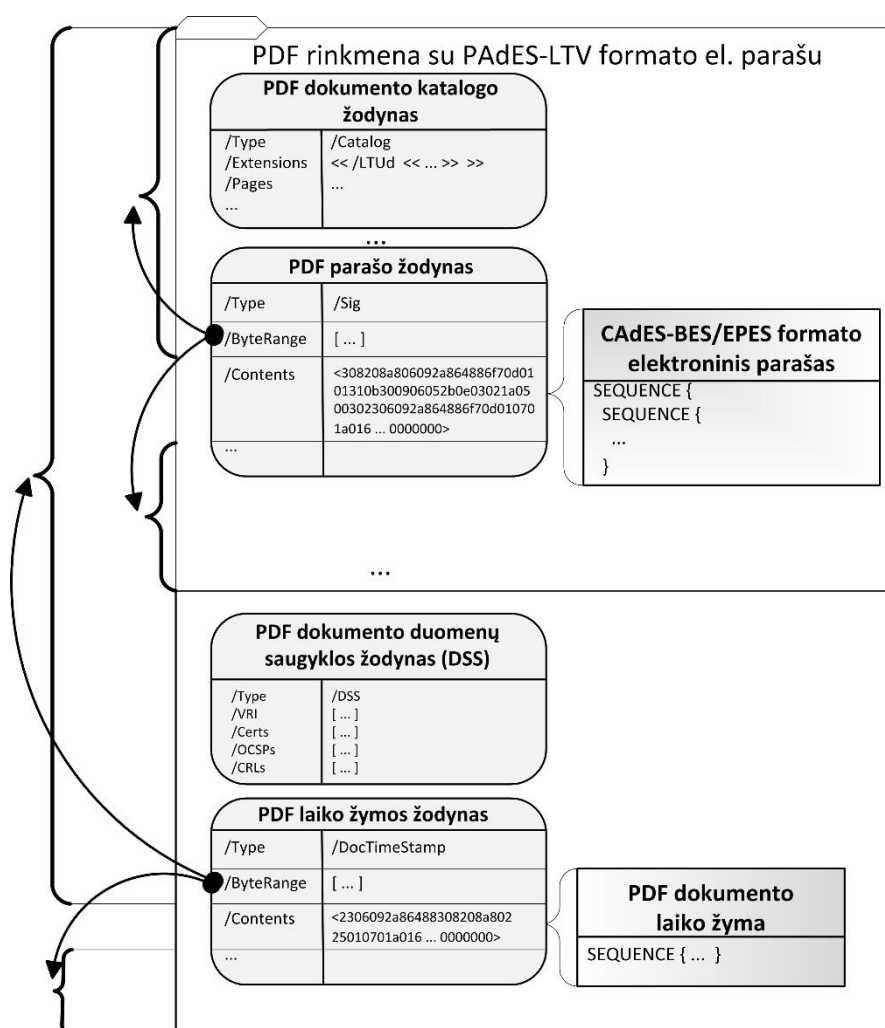
TRUMPALAIKIS PDF ELEKTRONINIS PARAŠAS SU PDF DOKUMENTO LAIKO ŽYMA

2. Trumpalaikis PDF elektroninis parašas su PDF dokumento laiko žyma – tai PAdES-LTV formato elektroninis parašas, kuris atitinka visus šiuos reikalavimus:

2.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES-BES arba CAdES-EPES formato elektroninis parašas, kuriame nėra nepasirašomo parašo laiko žymos atributo „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 6.1.1 skyrius);

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

2.3. Trumpalaikis PDF elektroninis parašas turi atitikti PAdES bazinio profilio standarte (11 priedo 12 punktas) apibrėžtą T-Level (patikimo parašo egzistavimo laiko) atitikties lygmenį.



III SKYRIUS

ILGALAIKIS PDF ELEKTRONINIS PARAŠAS SU ELEKTRONINIO PARAŠO LAIKO ŽYMA

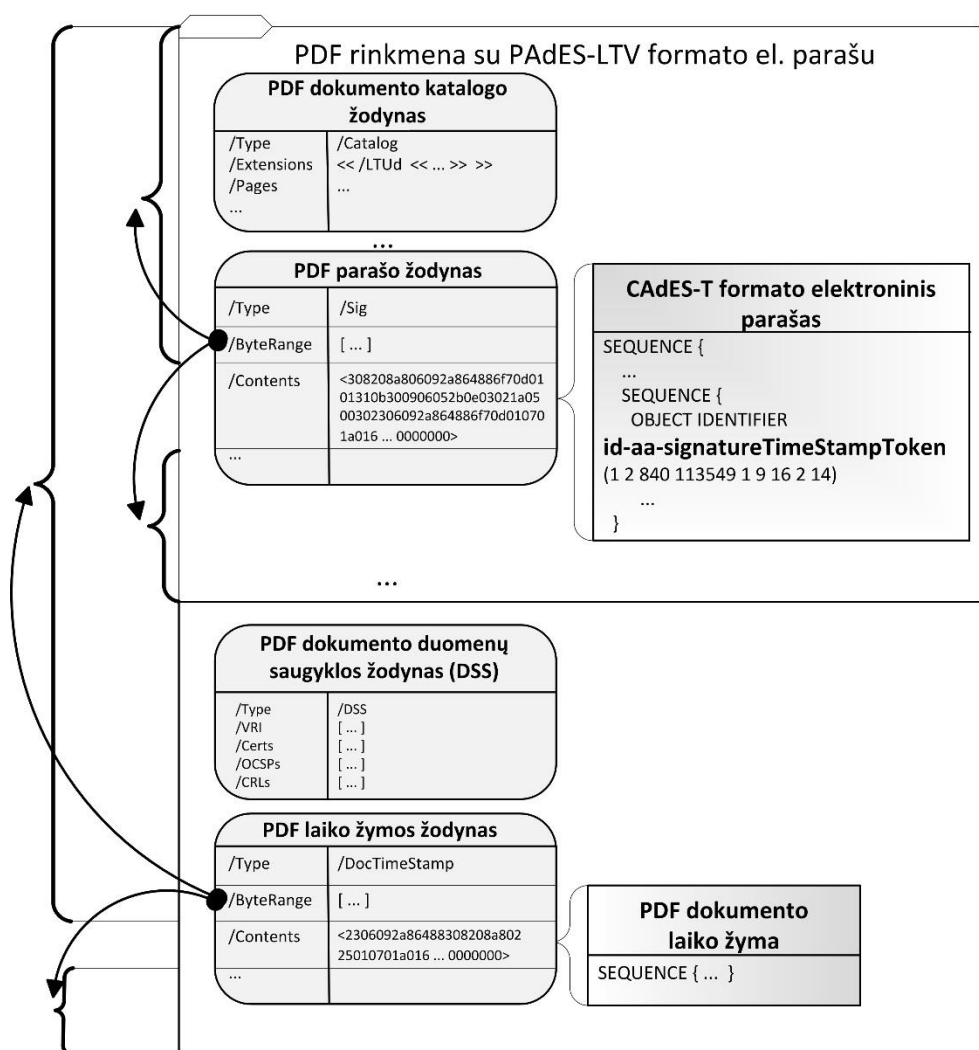
3. Ilgalaikis PDF elektroninis parašas su elektroninio parašo laiko žyma – tai PAdES-LTV formato elektroninis parašas, kuris atitinka visus šiuos reikalavimus:

3.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES-T formato elektroninis parašas, kuriame yra nepasirašomas parašo laiko žymos atributas „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 6.1.1 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 PDF elektroninio parašo) egzistavimą iki joje nurodyto laiko;

3.4. Ilgalaikis PDF elektroninis parašas turi atitikti PAdES bazinio profilio standarte (11 priedo 12 punktas) apibrėžtą LTA-Level (ilgalaikio su archyvine laiko žyma) atitikties lygmenį.



IV SKYRIUS

ILGALAIKIS ELEKTRONINIS PARAŠAS BE ELEKTRONINIO PARAŠO LAIKO ŽYMO

4. Ilgalaikis elektroninis parašas be elektroninio parašo laiko žymos – tai PAdES-LTV formato elektroninis parašas, kuris atitinka visus šiuos reikalavimus:

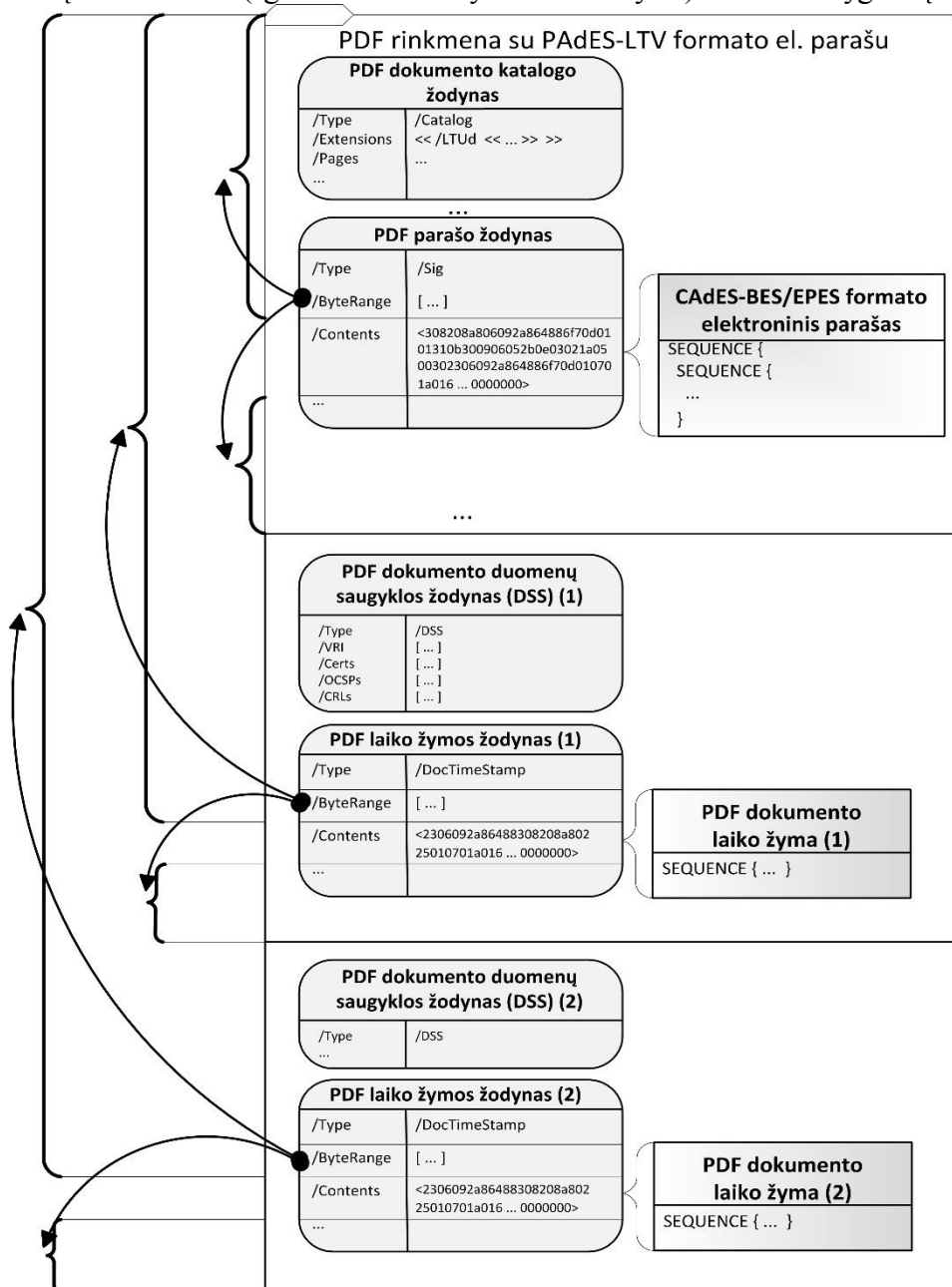
4.1. PDF parašo žodyno „**Contents**“ lauke saugomas CAdES-BES arba CAdES-EPES formato elektroninis parašas, kuriame nėra nepasirašomo parašo laiko žymos atributo „*signature-time-stamp*“ (objekto identifikatorius „*id-aa-signatureTimeStampToken*“; CAdES standarto 6.1.1 skyrius);

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

4.5. Ilgalaikis PDF elektroninis parašas turi atitikti PAdES bazinio profilio standarte (1 priedo 1 punktas) apibrėžtą LTA-Level (ilgalaikio su archyvine laiko žyma) atitikties lygmenį.



**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	27.3 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	27.2 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 yra įstaigos vadovas ar jo įgaliotas asmuo.	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	13 punktas;	Plėtinio aprašas privalomas.	Plėtinio aprašas neprivalomas, jei nėra LTUd_Role ir (ar) LTUd_SignerNotes metaduomenų.

STANDARTŲ IR KITŲ DOKUMENTŲ SĄRAŠAS

1. LST CWA 14170:2005 „Saugumo reikalavimai, keliami taikomosios parašo formavimo sistemoms“.
2. LST ETSI TS 101 733 V2.2.1:2013 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintieji CMS elektroniniai parašai (CAAdES)“.
3. LST ETSI TS 101 861 V1.3.1:2007 „Laiko žymėjimo profilis“.
4. LST ETSI TS 101 862 V1.3.3:2007 „Kvalifikuoto sertifikato profilis“.
5. LST ETSI TS 101 903 V1.4.2:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintieji XML elektroniniai parašai (XAdES)“.
6. LST ETSI TS 102 778-1 V1.1.1:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo profiliai. 1 dalis. PAdES apžvalga. PAdES struktūros dokumentas“.
7. LST ETSI TS 102 778-2 V1.2.1:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo profiliai. 2 dalis. PAdES pagrindai. Profilis pagal ISO 32000-1“.
8. LST ETSI TS 102 778-3 V1.2.1:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo profiliai. 3 dalis. PAdES išplėtimas. PAdES-BES ir PAdES-EPES profiliai“.
9. LST ETSI TS 102 778-4 V1.1.2:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo profiliai. 4 dalis. PAdES ilgalaikiškumas. PAdES-LTV profilis“.
10. LST ETSI TS 102 778-5 V1.1.2:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo profiliai. 5 dalis. PAdES, skirtas XML kalbos turiniui. XAdES parašų profiliai“.
11. LST ETSI TS 102 778-6 V1.1.1:2011 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo profiliai. 6 dalis. Elektroninių parašų regimasis atvaizdavimas“.
12. LST ETSI TS 103 172 V2.2.2:2013 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintojo PDF elektroninio parašo (PAdES) bazinis profilis“.
13. LST ISO 19005-2:2011 „Dokumentų tvarkyba. Ilgalaikio saugojimo elektroninio dokumento rinkmenos formatai. 2 dalis. ISO 32000-1 (PDF/A-2) naudojimas (tapatus ISO 19005-2:2011)“.
14. LST ISO 32000-1:2009 „Dokumentų tvarkyba. PDF formatai. 1 dalis. PDF 1.7 (tapatus ISO 32000-1:2008)“.

15. RFC 6960 „X.509 viešojo rakto infrastruktūra internete: Sertifikatų galiojimo patikros protokolas OCSP“ (angl. „X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP“), <http://www.ietf.org/rfc/rfc6960.txt>, 2013.
 16. RFC 3161 „X.509 viešojo rakto infrastruktūra internete: Laiko žymų protokolas (TSP)“ (angl. „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)“), <http://www.ietf.org/rfc/rfc3161.txt>, 2001.
 17. RFC 3279 „Algoritmai ir identifikatoriai, skirti naudoti X.509 viešojo rakto infrastruktūros internete sertifikatų ir atšauktų sertifikatų sąrašų (CRL) profilyje“ (angl. „Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“), <http://www.ietf.org/rfc/rfc3279.txt>, 2002.
 18. RFC 3447 „Viešojo rakto kriptografijos standartai (PKCS). Nr. 1: RSA kriptografijos specifikacijų versija 2.1“ (angl. „Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1“), <http://www.ietf.org/rfc/rfc3447.txt>, 2003.
 19. RFC 3986 „Universalusis išteklų identifikatorius (URI): Bendroji sintaksė“ (angl. „Uniform Resource Identifier (URI): Generic Syntax“), <http://www.ietf.org/rfc/rfc3986.txt>, 2005.
 20. RFC 4055 „Papildomi RSA kriptografijos algoritmai ir identifikatoriai, skirti naudoti X.509 viešojo rakto infrastruktūros internete sertifikatų ir atšauktų sertifikatų sąrašų (CRL) profilyje“ (angl. „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.
 21. RFC 5280 „X.509 viešojo rakto infrastruktūra internete: Sertifikatų ir atšauktų sertifikatų sąrašų (CRL) profilis“ (angl. „Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile“), <http://www.ietf.org/rfc/rfc5280.txt>, 2008.
 22. RFC 5652 „Kriptografinių pranešimų sintaksė (CMS)“ (angl. „Cryptographic Message Syntax (CMS)“), <http://www.ietf.org/rfc/rfc5652.txt>, 2009.
 23. RFC 5758 „X.509 viešojo rakto infrastruktūra internete: papildomi DSA ir ECDSA algoritmai ir identifikatoriai“ (angl. „Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA“), <http://www.ietf.org/rfc/rfc5758.txt>, 2010.
 24. XMP specifikacija, Adobe Systems Incorporated, http://www.aiim.org/documents/standards/pdf/xmp_specification.pdf, 2005.
 25. W3C rekomendacija „Plečiamoji žymėjimo kalba XML 1.0 (penktoji laida)“ (angl. “Extensible Markup Language (XML) 1.0 (Fifth Edition)”), <http://www.w3.org/TR/2008/REC-xml-20081126/>, 2008.
 26. W3C rekomendacija „RDF/XML sintaksės specifikacija (peržiūrėta)“, <http://www.w3.org/TR/2004/REC-rdf-syntax-grammar-20040210/>, 2004.
-

DETALŪS METADUOMENYS

Dokumento sudarytojas (-ai)	Lietuvos vyriausiojo archyvaro tarnyba 188697087, Algirdo g. 31, Vilnius
Dokumento pavadinimas (antraštė)	ISAKYMAS DĖL ELEKTRONINIO DOKUMENTO SPECIFIKACIJOS PDF-LT-V1.0 PATVIRTINIMO
Dokumento registracijos data ir numeris	2014-08-29 Nr. VE(1,3 E)-42
Dokumento registracijos data ir numeris	2014-08-29 Nr. 2014-11409
Dokumento gavimo data ir dokumento gavimo registracijos numeris	2014-08-29 Nr. 10857
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Ramojus Kraujelis, Lietuvos vyriausiasis archyvaras
Sertifikatas išduotas	RAMOJUS KRAUJELIS, Lietuvos vyriausiojo archyvaro tarnyba LT
Parašo sukūrimo data ir laikas	2014-08-29 14:16:21
Parašo formatas	XAdES-T
Laiko žymoje nurodytas laikas	2014-08-29 14:16:34
Informacija apie sertifikavimo paslaugų teikėją	Nacionalinis sertifikavimo centras (IssuingCA-B), Gyventojų registro tarnyba prie LR VRM - i.k. 188756767 LT
Sertifikato galiojimo laikas	2013-02-27 - 2016-02-27
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "VI Registru Centras RCSC (IssuingCA-A), VI Registru Centras - I.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema Avilys, Lietuvos vyriausiojo archyvaro tarnyba - į. k. 188697087 LT", sertifikatas galioja nuo 2014-07-10 iki 2015-07-10 "Gauto dokumento registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "SSC GDL NH CA, Skaitmeninio sertifikavimo centras LT" išduotą sertifikatą "TEISĖS AKTŲ REGISTRAS, Lietuvos Respublikos Seimo kanceliarija LT", sertifikatas galioja nuo 2013-12-31 iki 2014-12-31 "Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "SSC GDL NH CA, Skaitmeninio sertifikavimo centras LT" išduotą sertifikatą "TEISĖS AKTŲ REGISTRAS, Lietuvos Respublikos Seimo kanceliarija LT", sertifikatas galioja nuo 2013-12-31 iki 2014-12-31
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.0.13
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2014-08-30)
Paieškos nuoroda	https://www.e-tar.lt/portal/legalAct.html?documentId=ec0161902fbf11e4b487eaa-be28831e8
Papildomi metaduomenys	Nuorašą suformavo 2014-08-30 00:04:40 TAIS