



LIETUVOS VYRIAUSIASIS ARCHYVARAS

ĮSAKYMAS

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

2014 m. rugpjūčio 29 d. Nr. VE(1.3 E)-42

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 taisyklės 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, apibūdinamas kaip lentelė, sudaryta iš PDF objektų porų – PDF žodyno laukų, nustatytu formatu aprašančių tų sudėtingų objektų atributus (PDF-1.7 standarto 7.3.7 skyrius).

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

Prefiksas – (angl. *prefix*) PDF žodyno lauko, XML arba XMP elemento, atributo ar reikšmių tipo vardo sudėtinė dalis, nurodoma vardo pradžioje, skirta vardo unikalumui užtikrinti ir

(ar) vienareikšmei vardo naudojimo sričiai nustatyti. Prefiksas taip pat naudojamas kaip XML arba XMP elementus, atributus ir jų reikšmių tipus apibrėžiančios schemos URI santrumpa.

Saugi elektroninio parašo formavimo sistema – programinė ir techninė įranga, 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 apibrėžiančios 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, veiksmų 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 priedamų 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 priedami 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 dvių rūšių laiko žymos:

50.1. parašo laiko žyma, saugoma CAdES-T formato elektroninio parašo nepasirašomame laiko žymos attribute „*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 punktas) 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 punktas);

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 punktas).

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 punktas);

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 punktas).

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 lygmenis.

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 prefiksiu „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 vadovaujamas 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.
