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.

Metaduomuo	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 (Įstaigos vadovui ar jo įgaliotam 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/`	*Dublin Core* 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: *Organizacija* – programinę įrangą sukūrusios organizacijos pavadinimas; *Programa* – programinės įrangos pavadinimas; *Versija* – konkreti programinės įrangos versija; *tekstas* – papildoma informacija, nurodanti operacinės sistemos versiją, įdiegtus komponentus, kita.
Riboto pasirinkimo tekstas	(angl. *closed choice*) Tekstinis laukas, kuriame leidžiama nurodyti tik apibrėžtą aibę reikšmių.
Tekstas skirtingomis kalbomis	(angl. *language atlernative*) 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 „*x-default*“ standartinei teksto reikšmei nurodyti.
Kalbos kodas	(angl. *locale*) 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**
			Sudarytojui	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 schemos 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>Dokumento sudarytojas (-ai)
             </pdfaProperty:description>
              </rdf:li>
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>recipients</pdfaProperty:name>
                <pdfaProperty:valueType>seq Entity</pdfaProperty:valueType>
                <pdfaProperty:category>external</pdfaProperty:category>
                <pdfaProperty:description>Dokumento 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>Dokumento 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 dokumento registracija (-os)
             kopijoje</pdfaProperty:description>
              </rdf:li>
              <rdf:li rdf:parseType="Resource">
                <pdfaProperty:name>originalReceptions</pdfaProperty:name>
                <pdfaProperty:valueType>seq Registration</pdfaProperty:valueType>
```

```
            <pdfaProperty:category>external</pdfaProperty:category>
            <pdfaProperty:description>Gauto originalaus dokumento registracija
          (-os) kopijoje</pdfaProperty:description>
           </rdf:li>
           <rdf:li rdf:parseType="Resource">
            <pdfaProperty:name>originalReceivers</pdfaProperty:name>
            <pdfaProperty:valueType>seq Entity</pdfaProperty:valueType>
            <pdfaProperty:category>external</pdfaProperty:category>
            <pdfaProperty:description>Originalaus dokumento gavėjas (-ai)
          kopijoje</pdfaProperty:description>
           </rdf:li>
           <!-- Dokumento registravimo metaduomenys (nurodomi PDF parašo 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 schemos 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 ŽYMOS 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	Dokumento laiko žymos žodyno formato versija. Jeigu laukas nurodytas, reikšmė turi būti „0“.
Prop_Build	Žodynas (dictionary)	Ne	Žodynas, kuriame pateikiama programinės įrangos, naudotos dokumento laiko žymai įtraukti, techninė informacija.

Žodyno lauko raktas	Tipas[1]	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. *digest*)		
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. *signature*)		
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.

CAdES elementai, aprašomi ASN.1 koduote	Privalomas	Skaičius	Aprašas
CertificateChoices ::= CHOICE {		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. *trusted services list*, *TSL*).
certificate Certificate,	Privalomas	1	X509 sertifikatas.
extendedCertificate [0] IMPLICIT ExtendedCertificate,	Draudžiamas	0	
v1AttrCert [1] IMPLICIT AttributeCertificateV1,	Draudžiamas	0	
v2AttrCert [2] IMPLICIT AttributeCertificateV2,	Draudžiamas	0	
......other [3] IMPLICIT OtherCertificateFormat	Draudžiamas	0	
}			
crls [1] IMPLICIT RevocationInfoChoices OPTIONAL	Draudžiamas	0	
„*signerInfos*“ tipo elementas:			
signerInfos ::= SET OF	Taip	1	CAdES elektroniniame paraše turi būti tik vieno asmens parašo informacija.
SignerInfo ::= SEQUENCE {	Taip	1	
version CMSVersion,	Taip	1	Sintaksės versijos numeris. Reikšmė turi būti „1“ arba „3“ ir parenkama, kaip nurodyta RFC 5652 (11 priedo 22 punktas) 5.3 skyriuje.
sid SignerIdentifier ::= CHOICE {	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. *distinguished name*) 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			
Atribute ::= 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. *document time-stamp*), 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
„*unsignedAttrs*“ tipo elementas:			
`unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL`	Ne	0-1	Nepasirašomi CAdES elektroninio parašo atributai.
`UnsignedAttributes ::= SET SIZE (1..MAX) OF`			
`Atribute ::= SEQUENCE {`	Taip	1-N[1]	
`attrType OBJECT IDENTIFIER,`	Taip	1	
`-- attrType id-aa-signatureTimeStampToken`	Ne	0-1	Parašo laiko žyma, kuri atitinka RFC 3161 (11 priedo 16 punktas) reikalavimus.
`-- attrType id-aa-ets-certificateRefs`	Draudžiamas	0	Nuorodos į sertifikatus.
`-- attrType id-aa-ets-revocationRefs`	Draudžiamas	0	Nuorodos į atšaukimo duomenis.
`-- attrType id-aa-ets-certValues`	Draudžiamas	0	Sertifikatų reikšmės.
`-- attrType id-aa-ets-revocationValues`	Draudžiamas	0	Atšaukimo duomenys.
`-- attrType id-aa-ets-escTimeStamp`	Draudžiamas	0	CAdES-C formato elektroninio parašo laiko žyma.
`-- attrType id-aa-ets-certCRLTimestamp`	Draudžiamas	0	Nuorodų į sertifikatus ir atšaukimo duomenis laiko žyma.
`-- attrType id-aa-ets-archiveTimestampV2`	Draudžiamas	0	Archyvinė laiko žyma.
`-- attrType id-aa-ets-archiveTimestampV3`	Draudžiamas	0	Archyvinė laiko žyma.
`-- attrType id-aa-ets-longTermValidation`	Draudžiamas	0	Duomenų egzistavimo iki tam tikro laiko įrodymo atributas.
`-- attrType id-aa-ets-attrCertificateRefs`	Draudžiamas	0	Nuorodos į atributinius sertifikatus.
`-- attrType id-aa-ets-attrRevocationRefs`	Draudžiamas	0	Nuorodos į atributinių sertifikatų atšaukimo duomenis.
`-- attrType id-countersignature`	Draudžiamas	0	
`attrValues SET OF AttributeValue`	Taip	1	
`},`			
`}`			
`}`			

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 identifikatoriue „*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 naudojmas kitiems tikslams, nei nurodyti elektroninio parašo paskirtį, aprašytą PDF parašo žodymo lauke „***Reason***“.

TRUMPALAIKIŲ IR ILGALAIKIŲ PDF ELEKTRONINIŲ PARAŠŲ SCHEMOS

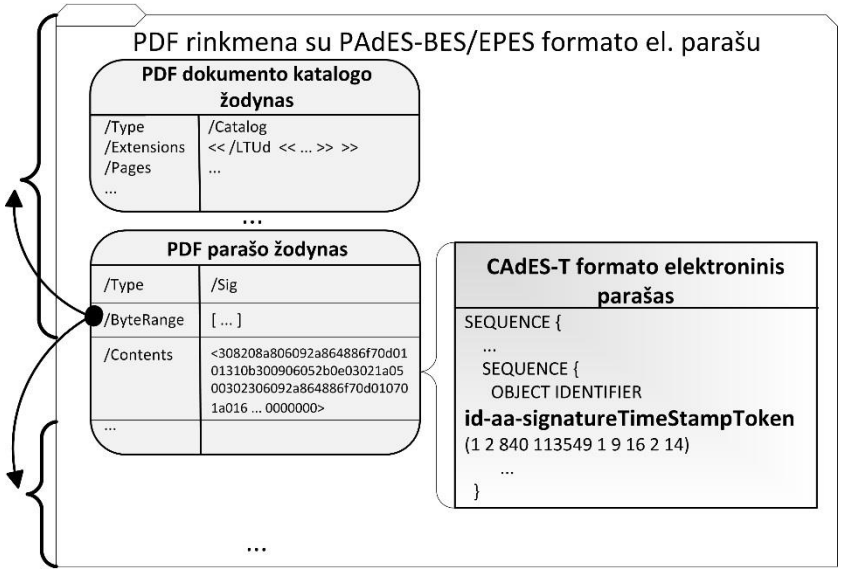
I SKYRIUS
TRUMPALAIKIS PDF ELEKTRONINIS PARAŠAS SU ELEKTRONINIO PARAŠO LAIKO ŽYMA

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 įtrauktų 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.



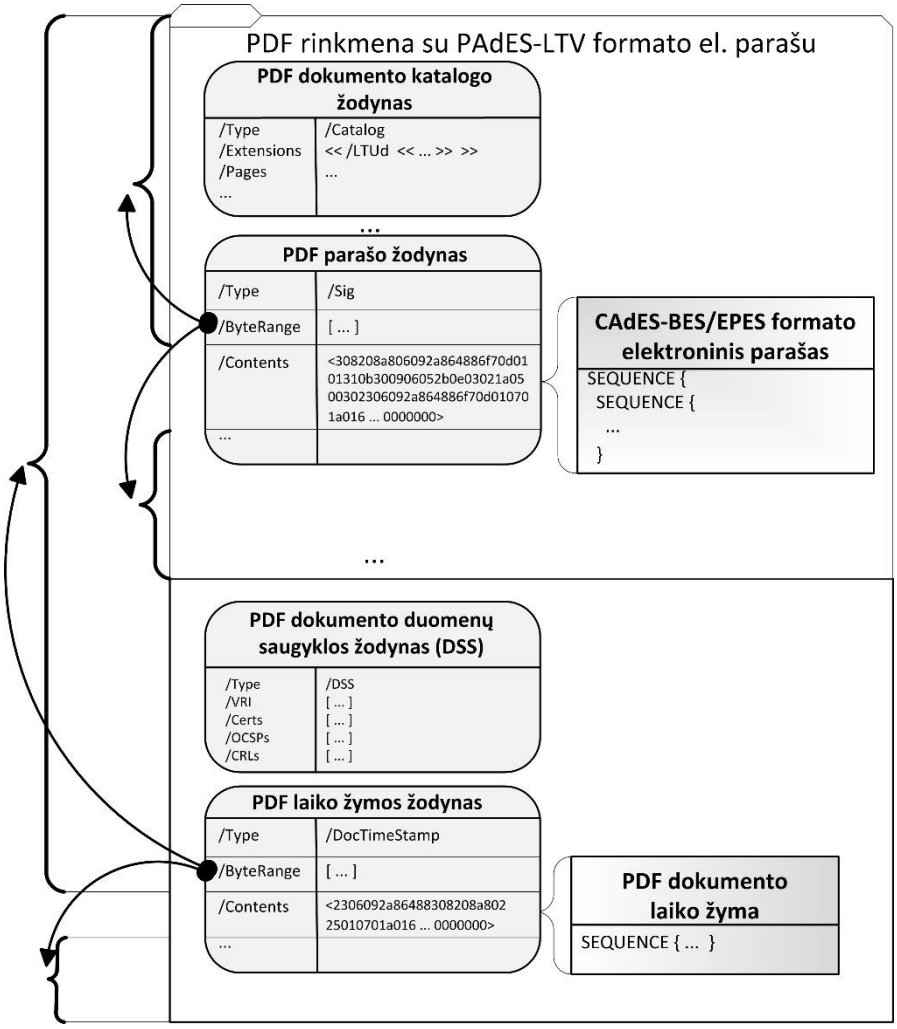
II SKYRIUS
TRUMPALAIKIS PDF ELEKTRONINIS PARAŠAS SU PDF DOKUMENTO LAIKO ŽYMA

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

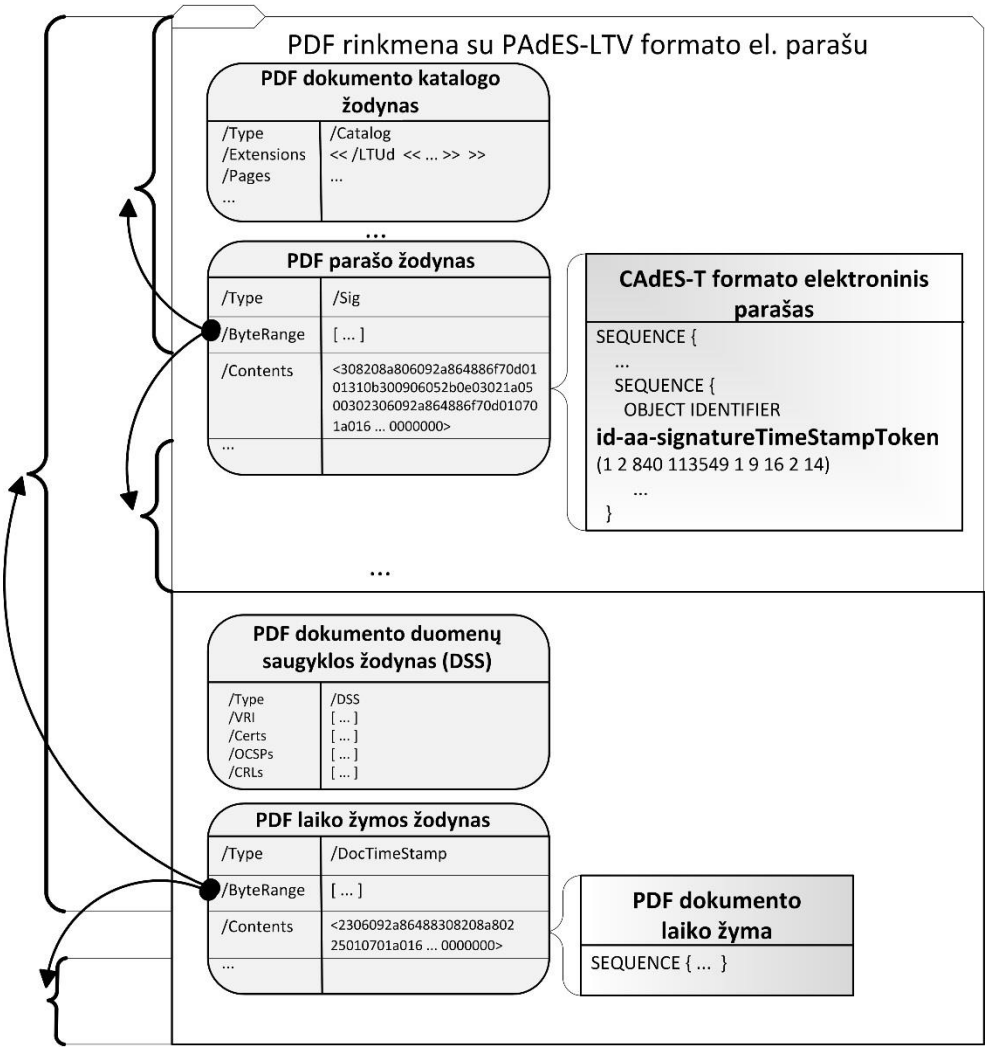
3. Ilgalaikis PDF elektroninis parašas su elektroninio parašo laiko žyma – tai PAdES-LTV formato elektroninis parašas, kuris atitinka visus šiuos reikalavimus:

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 ŽYMOS

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

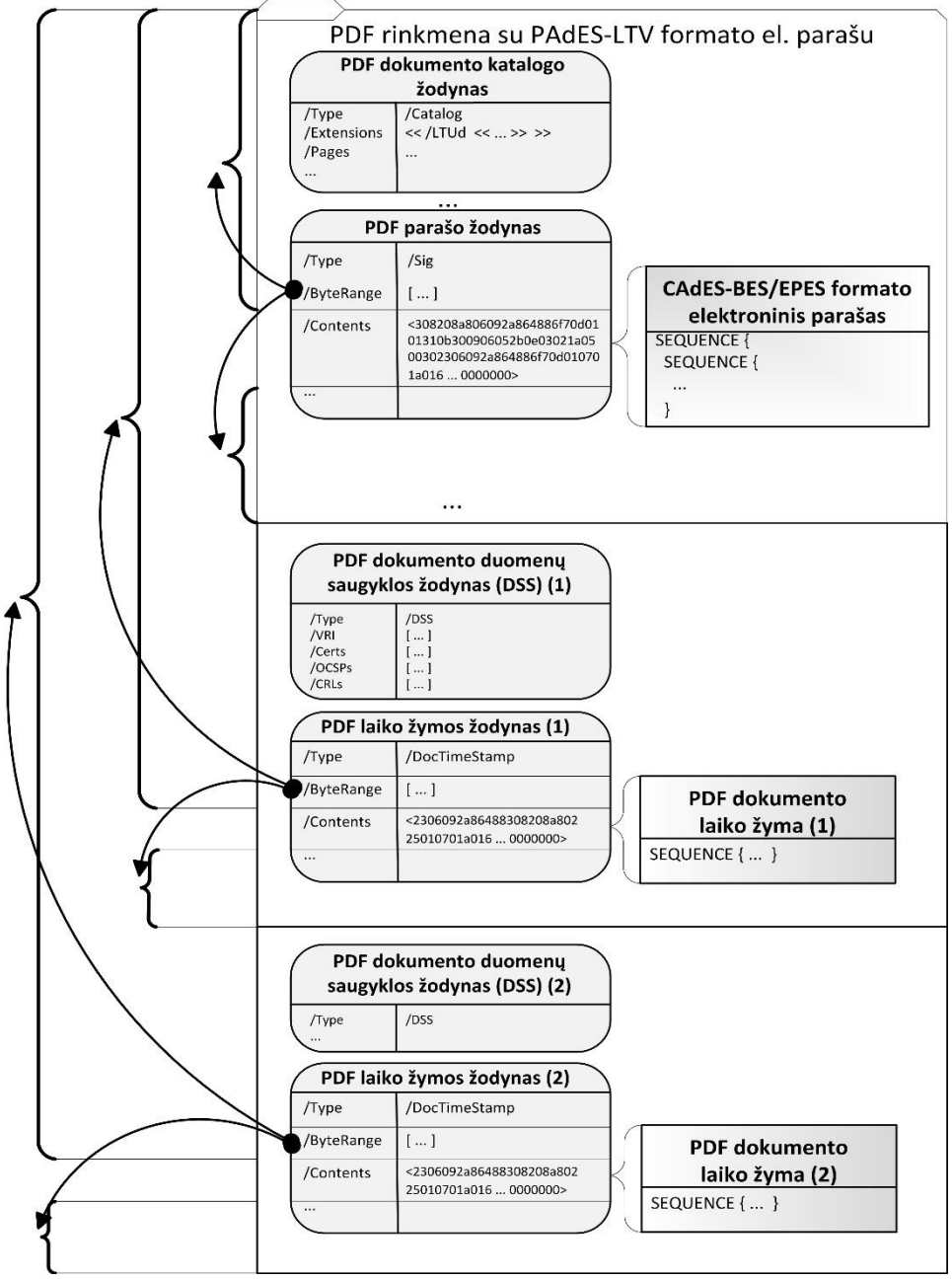
4.1. PDF parašo žodyno „***Contents***“ lauke saugomas CAdES-BES arba CAdES-EPES formato elektroninis parašas, kuriame nėra nepasirašomo parašo laiko žymos atributo „*signature-time-stamp*“ (objekto identifikatorius *„id-aa-signatureTimeStampToken*“; CAdES standarto 6.1.1 skyrius);

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 sudarusio asmens pareigos (metaduomuo LTUd_Role)	1 priedo III dalis;	Privalomas, kai pasirašantis asmuo yra įstaigos vadovas arjo 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 taikomosioms parašo formavimo sistemoms“.

2. LST ETSI TS 101 733 V2.2.1:2013 „Elektroniniai parašai ir infrastruktūros (EPI). Patobulintieji CMS elektroniniai parašai (CAdES)“.

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 formatas. 2 dalis. ISO 32000-1 (PDF/A-2) naudojimas (tapatus ISO 19005-2:2011)“.

14. LST ISO 32000-1:2009 „Dokumentų tvarkyba. PDF formatas. 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 išteklių 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.