

**Techninė programinės įrangos SIGNA ir
elektroninio dokumento formato specifikacija**

Vilnius
2008

Turinys

1.	Bendrosios nuostatos	3
1.1.	Specifikacijos paskirtis ir apimtis.....	3
1.2.	Specifikacijos taikymas	3
1.2.1.	Taikymas dokumentams	3
1.2.2.	Taikymas programinėms priemonėms.....	3
1.3.	Sąvokos.....	4
1.4.	Specifikacijos struktūra	6
2.	Elektroninio dokumento konteineris	7
2.1.	Konteinerio modelio apžvalga.....	7
2.2.	Fizinis konteinerio dizainas	8
2.3.	Konteinerio dalių specifikacija.....	10
2.3.1.	Turinio tipai	10
2.3.2.	Ryšių dalys	11
2.3.3.	Pagrindiniai ir papildomi metaduomenys.....	13
3.	Elektroninio dokumento turinys	15
3.1.	Turinio rinkmenų struktūra.....	16
4.	Elektroniniai parašai	17
5.	Elektroninio dokumento tikrinimas	20
5.1.	Elektroninio dokumento turinio tikrinimas	20
5.2.	Specifikacijos formato tikrinimas.....	21
5.3.	Elektroninių parašų tikrinimas	22
5.4.	Nuorodos	23

1. Bendrosios nuostatos

1.1. Specifikacijos paskirtis ir apimtis

Dokumentas „Techninė programinės įrangos SIGNA ir elektroninio dokumento formato specifikacija“ (toliau - Specifikacija) yra skirtas apibrėžti gyventojų parengtų oficialių elektroninių dokumentų, skirtų pateikti viešojo administravimo institucijoms, formatą, tenkinantį Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus 2008 m. spalio 9 d. įsakymu Nr. V-119 „Dėl elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos reikalavimų aprašo patvirtinimo“ (Žin., 2008, Nr. 118-4488) (toliau – Reikalavimai specifikacijoms) nustatytus reikalavimus oficialių elektroninių dokumentų formatams, bei apibūdinti tokių dokumentų rengimo ir tikrinimo priemonę.

1.2. Specifikacijos taikymas

1.2.1. Taikymas dokumentams

Specifikacija apibrėžia gyventojų rengiamų GGeDOC grupės oficialių elektroninių dokumentų formatą: jų turinį, elektroninius parašus bei metaduomenis. Pasirašytą elektroninį dokumentą sudaro elektroninio dokumento turinys, susidedantis iš pagrindinio dokumento, priedų ir pridedamų dokumentų, elektroniniai parašai ir dokumento turinio bei elektroninių parašų metaduomenys, kurių keitimas keičia patį elektroninį dokumentą.

1.2.2. Taikymas programinėms priemonėms

Programinė įranga atitinka Lietuvos Respublikos Elektroninio parašo įstatymą (Žin., 2000, Nr. 61-1827) ir kitus teisės aktus, ES standartus, reglamentuojančius el. parašo naudojimą.

Programinė įranga yra suderinta su Lietuvos archyvų departamento Reikalavimais specifikacijoms „Dėl elektroniniu parašu pasirašyto elektroninio dokumento specifikacijos reikalavimų aprašo patvirtinimo“.

Specifikacija apibūdina programinę priemonę, skirtą sudaryti GGeDOC grupės oficialų elektroninį dokumentą bei patikrinti pasirašyto elektroninio dokumento autentiškumą. Programinė priemonė sukuria oficialius elektroninius dokumentus, pasirašytus XAdES-EPES formato kvalifikuotu elektroniniu parašu, turinčiu tokią pat juridinę galią kaip ir ranka pasirašytas parašas.

Programinė priemonė, tikrindama pasirašyto elektroninio dokumento autentiškumą, patikrina dokumento integralumą, kvalifikuoto elektroninio parašo autentiškumą bei sertifikato galiojimą.

Kvalifikuoto sertifikato, kuriuo patvirtinamas oficialus elektroninis dokumentas, galiojimas taip pat yra tikrinamas prieš pasirašant dokumentą: elektroninio parašo sukūrimo metu vykdoma pasirašančio asmens kvalifikuoto elektroninio parašo sertifikato kontrolė, apimanti sertifikato galiojimo patikrinimą pagal sertifikato duomenis. Nepatenkinus visų kontrolės reikalavimų programa neleidžia sukurti el. parašo.

Programinė įranga teikia anksčiau sukurtų el. dokumentų, pasirašytų el. parašu, peržiūros ir kontrolės funkcijas. Programinė priemonė, tikrindama pasirašyto elektroninio dokumento autentiškumą, patikrina dokumento integralumą, kvalifikuoto elektroninio parašo autentiškumą bei sertifikato galiojimą, taikant CRL ir/arba OCSP HTTP protokolu, patikrinimus.

Programinė įranga turi šias vartotojo sąsajos funkcijas:

- pasirinkti pasirašomo el. dokumento turinio failą;

- vizualizuoti el. dokumento turinį arba leisti vartotojui kitaip peržiūrėti el. dokumento turinio failus, dirbant programinės įrangos terpėje;
- įvesti ir koreguoti metaduomenis;
- pasirinkti kvalifikuoto el. parašo sertifikatą;
- pasirašyti el. dokumentą XAdES-EPES formato kvalifikuotu el. parašu, panaudojant stacionarų saugaus parašo formavimo įrenginį per operacinės sistemos pateikiamą API sąsają ir vizualizuojant sertifikato kontrolės bei parašo sukūrimo rezultatus;
- išsaugoti el. dokumentą, pasirašytą el. parašu;
- atidaryti anksčiau išsaugotą el. dokumentą, pasirašytą el. parašu, ir leisti peržiūrėti el. dokumento turinį, metaduomenis bei el. parašo informaciją;
- atlikti anksčiau išsaugoto el. dokumento, pasirašyto el. parašu, kontrolę ir vizualizuoti kontrolės rezultatus;
- nustatyti programinės įrangos konfigūracinius parametrus, leidžiant vartotojui pasirinkti sertifikatų kontrolę OCSP protokolu privalomą arba neprivalomą.

Programinė įranga tenkina šiuos nefunkcinius reikalavimus:

- programinė įranga realizuota klientinės taikomosios programinės įrangos, veikiančios Microsoft Windows 2000/XP/Vista operacinių sistemų terpėje, pavidalu;
- programinė įranga pateikiama diegimo paketo pavidalu, kuris yra tinkamas parsisiųsti internetu ir kurį gali įsidiegti kompiuterio naudotojas.

1.3. Sąvokos

Galiojantis kvalifikuotas sertifikatas – kvalifikuotas sertifikatas, kurio galiojimo laikotarpį sudaro laiko intervalas, tenkinantis visus žemiau pateiktus reikalavimus:

- sertifikato galiojimo laikotarpis yra apribotas sertifikato galiojimo pradžios ir pabaigos terminais, nurodytais kvalifikuotame sertifikate;

- sertifikato galiojimo laikotarpis yra apribotas sertifikato atšaukimo kreipimosi laiku, paskelbtu ne vėliau negu praėjus kvalifikuoto sertifikato taisyklėse arba sertifikavimo veiklos nuostatuose nurodytam sertifikato atšaukimo laikotarpiui;

- sertifikato galiojimo laikotarpis yra apribotas sertifikato sustabdymo kreipimosi laiku, paskelbtu ne vėliau negu praėjus kvalifikuoto sertifikato taisyklėse arba sertifikavimo veiklos nuostatuose nurodytam sertifikato galiojimo sustabdymo laikotarpiui.

Išreikštinės parašo taisyklės – elektroninio parašo sudarymo ir tikrinimo taisyklės, kurios yra įvardintos pasirašytame elektroniniame dokumente arba patvirtintos elektroninio dokumento naudojimą reglamentuojančiuose teisės aktuose bei XAdES-EPES formato paraše nurodytos elementu “SignaturePolicyIdentifier = SignaturePolicyIdentifier”.

Kvalifikuotas sertifikatas - sertifikatas, kurį sudarė sertifikavimo paslaugų teikėjas, atitinkantis 2002 m. gruodžio 31 d. LR Vyriausybės nutarimu Nr. 2108 nustatytus „Reikalavimus kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams“ ir įregistruotas šiame nutarime nustatyta „Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarka“ arba Europos Sąjungos šalies sertifikavimo paslaugų teikėjas, kuriam suteiktas kvalifikuoto sertifikavimo paslaugų teikėjo statusas sutinkamai su Europos Sąjungos šalies teisės aktais. Šiame sertifikate yra tokie duomenys:

- užrašas, kad tai yra kvalifikuotas sertifikatas;
- sertifikavimo paslaugų teikėjo ir jo buveinės šalies identifikatoriai;
- pasirašančio asmens vardas ir pavardė arba slapyvardis;
- pasirašančio asmens specialūs atributai, jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus;
- parašo tikrinimo duomenys, atitinkantys pasirašančio asmens turimus parašo formavimo duomenis;

- sertifikato galiojimo pradžios ir pabaigos terminai;
- sertifikato identifikatorius, suteiktas sertifikavimo paslaugų teikėjo;
- sertifikavimo paslaugų teikėjo saugus elektroninis parašas;
- sertifikato naudojimo paskirties apribojimai, jei tai nustatyta;
- leistina operacijų piniginė vertė, kada sertifikatas gali būti naudojamas, jei tai nustatyta.

Kvalifikuotas elektroninis parašas – saugus elektroninis parašas, sudarytas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu.

Laiko žyma (angl. „time stamp“) – duomenų egzistavimo iki nurodyto laiko momento įrodymas laiko žymos tarnybos pasirašytų saugiu elektroniniu parašu duomenų forma.

Metaduomenys – neatsiejama elektroninio dokumento dalis, kurioje gali būti pateikiama elektroninių dokumentų rengimo, registravimo, sisteminimo, priėjimo, saugojimo ir naikinimo procedūras aprašanti struktūrizuota kontekstinė informacija.

Neišreikštinės parašo taisyklės – elektroninio parašo sudarymo ir tikrinimo taisyklės, kurios yra įvardintos pasirašytame elektroniniame dokumente arba patvirtintos elektroninio dokumento naudojimą reglamentuojančiuose teisės aktuose bei XAdES-EPES formato paraše nurodytos elementu „SignaturePolicyIdentifier = SignaturePolicyImplied“.

Parašo pirminis tikrinimas – elektroninio parašo galiojimo tikrinimas ir parengimas ilgalaikiam saugojimui su galimybe patikrinti elektroninio parašo galiojimą nepriklausomai nuo viešųjų raktų infrastruktūros.

Parašo pirminis tikrinimas iki sertifikato atšaukimo laikotarpio pabaigos – elektroninio parašo pirminio tikrinimo etapas, atliekamas nedelsiant gavus pasirašytą elektroninį dokumentą ir susidedantis iš elektroninio parašo formato bei pasirašyto elektroninio dokumento autentiškumo tikrinimo, laiko žymos suformavimo ir kvalifikuoto sertifikato galiojimo pirmojo tikrinimo.

Parašo pirminis tikrinimas, pasibaigus sertifikato atšaukimo laikotarpiui – elektroninio parašo pirminio tikrinimo etapas, atliekamas pasibaigus kvalifikuoto sertifikato atšaukimo laikotarpiui, skaičiuojant nuo elektroninio parašo laiko žymoje nurodyto laiko momento, ir susidedantis iš kvalifikuoto sertifikato galiojimo antrojo tikrinimo, nuorodų į sertifikavimo kelią bei atšaukimo duomenis išsaugojimo XAdES-C formato paraše, laiko žymos šiam formatui uždėjimo ir sertifikavimo kelio bei atšaukimo duomenų išsaugojimo XAdES-X-L formato elektroniniame paraše.

Saugi parašo formavimo įranga – elektroninio parašo formavimo įranga, kuri atitinka visus žemiau nurodytus reikalavimus:

- parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, praktiškai įmanoma gauti tik vienintelį kartą, ir užtikrinamas jų slaptumas;
- parašo formavimo duomenų, naudojamų elektroniniam parašui sukurti, atkurti praktiškai neįmanoma, ir nuo elektroninio parašo klastočių apsaugo esamos technologijos;
- parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, pasirašantis asmuo gali patikimai apsaugoti nuo kitų asmenų;
- parašo formavimo įranga, kuriant elektroninį parašą, nekeičia pasirašomų duomenų ir netrukdo pasirašančiam asmeniui stebėti tuos duomenis prieš pasirašant;
- tenkina standarto CWA 14169:2004 „Secure Signature-Creation Devices „EAL 4+““ reikalavimus.

Sertifikato galiojimo atšaukimo laikotarpis (angl. „grace period“) – laikotarpis, skirtas:

- pasirašančiam asmeniui ar kitiems teisės aktų numatytiems asmenims kreiptis į kvalifikuotus sertifikatus sudarantį sertifikavimo paslaugų teikėją dėl kvalifikuoto sertifikato galiojimo atšaukimo arba sustabdymo, pradėdant kreipimosi momentu;
- kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjui išnagrinėti kreipimąsi ir priimti sprendimą dėl kvalifikuoto sertifikato galiojimo atšaukimo arba sustabdymo;

- kvalifikuotus sertifikatus sudarančiam sertifikavimo paslaugų teikėjui paskelbti duomenis apie kvalifikuoto sertifikato galiojimo atšaukimą arba sustabdymą.

Sertifikato galiojimo antrasis tikrinimas – elektroninio dokumento parašą patvirtinančio kvalifikuoto sertifikato ir sertifikavimo kelio galiojimo tikrinimas, atliekamas pasibaigus kvalifikuoto sertifikato atšaukimo laikotarpiui, skaičiuojant nuo parašo laiko žymoje nurodyto laiko momento.

Sertifikato galiojimo pirmasis tikrinimas – elektroninio dokumento parašą patvirtinančio kvalifikuoto sertifikato ir sertifikavimo kelio galiojimo tikrinimas, atliekamas nedelsiant, gavus pasirašytą dokumentą ir suformavus gauto parašo laiko žymą.

Sertifikavimo kelias – sertifikatų grandinė, susidedanti iš pasirašančio asmens kvalifikuoto sertifikato, patvirtinto kvalifikuotų sertifikavimo paslaugų teikėjo sertifikatu, ir nulinio arba daugiau sertifikavimo paslaugų teikėjų sertifikatų, pasirašytų kitų sertifikavimo paslaugų teikėjų.

Šaknis sertifikatas – sertifikatas, kuris nėra patvirtintas kitu sertifikatu, ir gali būti patikrintas tuo pačiu viešuoju raktu, nurodytu sertifikate. Šaknis sertifikatas yra pats save patvirtinantis sertifikatas.

Viešųjų raktų infrastruktūra – visuma, susiejanti asimetrinio šifravimo viešuosius raktus su asmenimis ar esybėmis, remiantis sertifikavimo paslaugų teikėjais.

XAdES – elektroninio parašo aprašymo XML struktūroje standartas, apibrėžtas ETSI TS 101 903 v1.3.2: „XML Advanced Electronics Signatures (XAdES)“;

XAdES-A – archyvinis elektroninio parašo formatas, aprašytas vadovaujantis XAdES standartu;

XAdES-BES – elektroninio parašo formatas, aprašytas vadovaujantis XAdES standartu;

XAdES-EPES – pagal parašo taisykles sukurtas elektroninio parašo formatas, aprašytas vadovaujantis XAdES standartu;

XAdES-C – elektroninio parašo formatas su pilnomis tikrumo duomenų nuorodomis, aprašytas vadovaujantis XAdES standartu;

XAdES-T – elektroninio parašo formatas su laiko žyma, aprašytas vadovaujantis XAdES standartu;

XAdES-X – elektroninio parašo formatas su tikrumo nuorodomis ir laiko žyma, aprašytas vadovaujantis XAdES standartu;

XAdES-X-L – elektroninio parašo formatas ilgalaikiam saugojimui, aprašytas vadovaujantis XAdES standartu;

XML – Organizacijos „W3C“ (The World Wide Web Consortium, <http://www.w3c.org>) rekomenduojama bendros paskirties duomenų struktūrų bei jų turinio aprašomoji kalba (angl. „*eXtensible Markup Language*“);

XMLDSIG – Organizacijos „IETF“ (The Internet Engineering Task Force, <http://www.ietf.org>) parengti reikalavimai elektroninio parašo aprašymui XML struktūroje (angl. „*XML Digital Signatures (xmldsig)*“).

Jeigu nepasakyta kitaip, žemiau tekste naudojama sąvoka „Parašas“ reiškia „Kvalifikuotas elektroninis parašas“, o sąvoka „Sertifikatas“ reiškia „Kvalifikuotas sertifikatas“.

Kitos specifikacijoje naudojamos sąvokos yra tokios pat, kaip Reikalavimuose specifikacijoms.

1.4. Specifikacijos struktūra

Specifikacija susideda iš penkių skyrių. Pirmame specifikacijos skyriuje pateikiama bendra informacija apie specifikaciją, įskaitant specifikacijos paskirtį, taikymą bei pagrindines sąvokas. Antras specifikacijos skyrius yra skirtas elektroninio dokumento konteinerio ir jo sudėtinių dalių bendrai apžvalgai bei metaduomenų detaliam specifikavimui. Trečias ir ketvirtas skyriai yra skiriami atitinkamai elektroninio dokumento turinio bei elektroninių parašų

specifikavimui. Penktas skyrius nustato elektroninio dokumento turinio, elektroninių parašų ir specifikacijos formato tikrinimo reikalavimus.

2. Elektroninio dokumento konteineris

Elektroninio dokumento samprata. Elektroninis dokumentas yra skaitmeninis rašytinio dokumento analogas. Kaip ir rašytinį dokumentą, elektroninį dokumentą sudaro šios būtinos dalys:

1. turinys – statinė tekstinė/vizualinė informacija, skirta skaityti žmogui,
2. elektroninis parašas – ranka dedamo parašo skaitmeninis analogas,
3. turinio ir parašo metaduomenys. Metaduomenys neformaliai apibrėžiami kaip „duomenys apie duomenis“. Čia turima omenyje duomenis apie turinį ir parašą, pvz.: dokumento pavadinimas, sudarymo data, ir pan.

Elektroniniam dokumentui būtinos savybės:

1. Integralumas (vientisumas ir nekeičiamumas) – elektroninis dokumentas susideda iš aukščiau išvardintų būtinų dalių (rinkinys iš mažiau dalių nėra elektroninis dokumentas), ir nė viena iš šių dalių per dokumento gyvavimo ciklą negali kisti. Jei bent viena iš šių dalių (kad ir metaduomenys) laikui bėgant pakinta, yra laikoma, kad elektroninis dokumentas nustojo gyvuoti (t.y., tai jau nebe elektroninis dokumentas arba nebe tas pats elektroninis dokumentas).
2. Autentiškumas – elektroninio dokumento tikrumo išsaugojimas elektroninio dokumento gyvavimo ciklo metu. Elektroninio dokumento autentiškumo tikrinimas susideda iš elektroninio parašo autentiškumo tikrinimo (bet kuriuo elektroninio dokumento gyvavimo ciklo metu turi būti įmanoma vienareikšmiškai nustatyti dokumentą pasirašiusį asmenį) ir elektroninio dokumento integralumo tikrinimo.

Elektroninio dokumento autentiškumo užtikrinimas. Remiantis aukščiau pateiktu elektroninio dokumento bei jo autentiškumo apibrėžimu, seka, kad jokia elektroninio dokumento dalis jo gyvavimo ciklo metu negali būti pakeista arba ištrinta. Todėl, siekiant užtikrinti dokumento autentiškumo patikrinimo galimybę, yra reikalaujama, kad egzistuotų bent vienas elektroninis parašas, kuriuo yra pasirašytos visos būtinos elektroninio dokumento dalys.

2.1. Konteinerio modelio apžvalga

Konteineris prisideda užtikrinant elektroninio dokumento vientisumą, t.y. visos būtinos elektroninio dokumento dalys turi būti sudėtos į vieną konteinerį. Tačiau vien tik konteineris negali užtikrinti, kad gyvavimo ciklo metu dokumentas neprarastų vientisumo savybės – techniškai galima bet kurią konteinerio dalį ištrinti. Tam, kad aptikti tokius vientisumo pažeidimus (taip pat ir nekeičiamumo pažeidimus), yra naudojamas elektroninis parašas, kuriuo pasirašomos visos elektroninio dokumento dalys. Jei nebūtų konteinerio, tikrinant elektrinius parašus būtų sunku (jei iš vis įmanoma) surasti visas sudėtines elektroninio dokumento dalis.

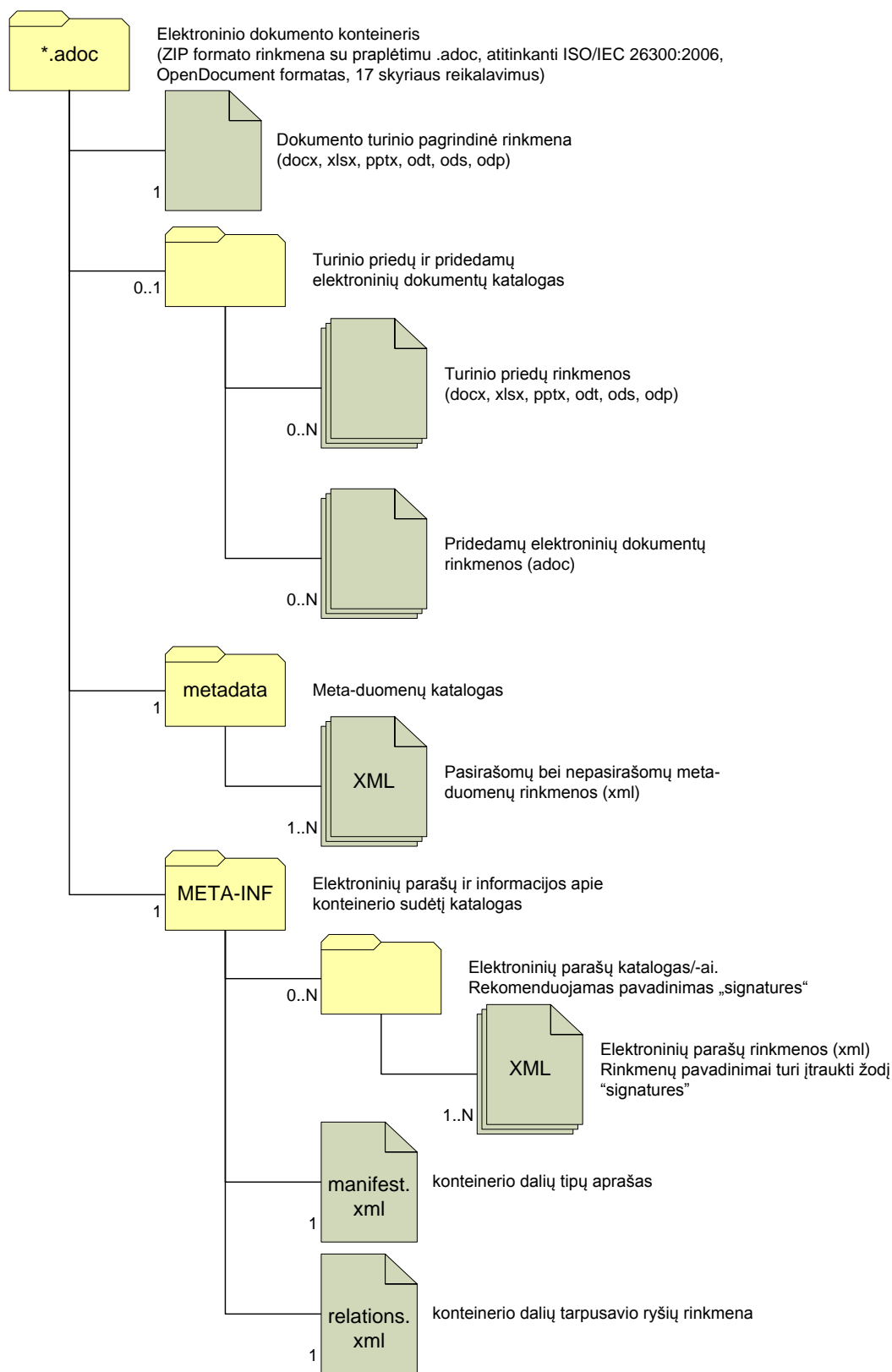
Konteineryje bus saugomos šios esybės:

1. Elektroninio dokumento turinio pagrindinė rinkmena.
2. Turinio priedai.
3. Turinio pridedami elektroniniai dokumentai.
4. Metaduomenys.
5. Elektroniniai parašai.
6. Konteinerio dalių tipų aprašas.
7. Konteinerio dalių tarpusavio ryšių aprašas.

2.2. Fizinis konteinerio dizainas

Reikalavimai fizinei konteinerio struktūrai:

1. Konteineris turi būti viena rinkmena su praplėtimu „adoc“.
2. Konteinerio formatas turi būti ZIP.
3. Konteinerio šaknyje turi būti viena ir tik viena rinkmena – elektroninio dokumento turinio pagrindinė rinkmena.
4. Konteinerio šaknyje gali būti vienas/keli katalogai laisvai pasirinktais pavadinimais (bet nesutampančiais su „META-INF“ ir „metadata“), kurių viduje gali būti katalogų hierarchinė struktūra, kurios gylis neviršija 3, bei gali būti elektroninio dokumento turinio priedų rinkmenos bei pridėdami elektroniniai dokumentai.
5. Konteinerio šaknyje turi būti katalogas pavadinimu „metadata“, kurio viduje bus metaduomenų rinkmenos.
6. Konteinerio šaknyje turi būti katalogas pavadinimu „META-INF“:
 - a. Katalogo „META-INF“ viduje privalo būti elektroninių parašų rinkmenos. Kaip kiekvienos elektroninio parašo rinkmenos pavadinimo dalis turi būti žodis „signatures“. Elektroninių parašų rinkmenos gali būti grupuojamos į katalogus arba katalogų hierarchiją su laisvai pasirinktais pavadinimais. Rekomenduojama turėti vieną katalogą pavadinimu „signatures“.
 - b. Katalogo „META-INF“ viduje turi būti konteinerio dalių tipų aprašo rinkmena pavadinimu „manifest.xml“, rengiama pagal ODF standarto reikalavimus.
 - c. Katalogo „META-INF“ viduje turi būti konteinerio dalių tarpusavio ryšių rinkmena pavadinimu „relations.xml“.



1 pav. Elektroninio dokumento fizinė konteinerio struktūra

2.3. Konteinerio dalių specifikacija

Elektroninį dokumentą gali sudaryti šios dokumento konteinerio dalys:

- pagrindinė dokumento turinio rinkmena;
- vienas ar daugiau priedų;
- vienas ar daugiau pridedamų elektroninių dokumentų;
- metaduomenys;
- elektroniniai parašai;
- konteinerio dalių tipų aprašas;
- konteinerio dalių tarpusavio ryšių rinkmena (sąryšių rinkmena).

2.3.1. Turinio tipai

Pagrindinė elektroninio dokumento turinio rinkmena bei jos priedai gali būti sudaryti iš lentelėje nurodytų atvirųjų formatų rinkmenų:

Rinkmenos formatas	Plėtinys	Rinkmenos turinio duomenų tipas
Microsoft Office Word 2007 dokumentas	docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Microsoft Office Excel 2007 dokumentas	xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
Microsoft Office PowerPoint 2007 pristatymo dokumentas	pptx	application/vnd.openxmlformats-officedocument.presentationml.presentation
Microsoft Office PowerPoint 2007 pristatymo pateikties dokumentas	ppsx	application/vnd.openxmlformats-officedocument.presentationml.slideshow
OpenOffice.org Writer dokumentas	odt	application/vnd.oasis.opendocument.text
OpenOffice.org Calc dokumentas	ods	application/vnd.oasis.opendocument.spreadsheet
OpenOffice.org Impress dokumentas	odp	application/vnd.oasis.opendocument.presentation

Reikalavimus atviriesiems Microsoft Office 2007 rinkmenų formatams apibrėžia tarptautinis standartas ISO/IEC DIS 29500 „Information technology. Office Open XML file formats“ (ECMA-376).

Reikalavimus OpenOffice.org rinkmenų formatams apibrėžia standartas LST ISO/IEC 26300:2007 „Informacijos technologija. Atvirasis biuro dokumentų formatas v 1.0 (tapatus ISO/IEC 26300:2006)“.

Pridedami elektroniniai dokumentai turi atitikti šiuos reikalavimus:

Elektroninio dokumento formatas	Plėtinys	Rinkmenos turinio duomenų tipas
Elektroninis dokumentas konteineryje, atitinkantis šios specifikacijos reikalavimus	adoc	application/vnd.lt.archyvai.adoc-2008

2.3.1.1. Turinio tipų aprašo rinkmena

Turinio tipų aprašo rinkmena yra konteinerio XML rinkmena, kurioje aprašyti elektroninį dokumentą sudarančių dalių (rinkmenų) turinio tipai. Elektroninio dokumento konteineryje privalo būti viena ir tik viena turinio tipų aprašo rinkmena.

Turinio tipų aprašo rinkmenos pavadinimas yra: `META-INF/manifest.xml`.

Šios XML rinkmenos struktūra turi atitikti ISO/IEC 26300:2006 (OpenDocument formato) 17.7 skyriaus preambulės bei 17.7.1 – 17.7.3 poskyrių reikalavimus. Elektroninio dokumento turinys nėra šifruojamas.

Rinkmeną sudaro šakninis `manifest` elementas, susidedantis iš vieno apibrėžtojo atributo, apibrėžiančio elemento vardų sritį ir daugybės `file-entry` elementų aprašančių konteinerio sudėtyje esančias rinkmenas ir jų turinio tipus.

Visos elektroninį dokumentą sudarančios rinkmenos turi būti nurodytos elektroninio dokumento konteinerio dalių turinio tipų aprašo rinkmenoje.

2.3.1.2. Konteinerio dalių turinio tipai

Turinio tipų apraše turi būti nurodyti šie elektroninio dokumento dalių rinkmenų turinio duomenų tipai:

Dokumento dalis	Rinkmenos turinio duomenų tipas
Konteineris (<i>full-path</i> ="/")	application/vnd.lt.archyvai.adoc-2008
Dokumento turinio rinkmenos	<i>pagal rinkmenos rūšį (žr. 2.3.1 "Turinio tipai")</i>
Sąryšių rinkmena	Application/vnd.lt.archyvai.adoc-2008#relations+xml
Metaduomenys	Application/vnd.lt.archyvai.adoc-2008#metadata+xml
Elektroniniai parašai	application/vnd.lt.archyvai.adoc-2008#signature+xml

2.3.2. Ryšių dalys

Elektroninio dokumento dalys (rinkmenos) yra tarpusavyje susijusios: dokumento turinio rinkmena gali turėti priedų ar pridedamų dokumentų, elektroninio dokumento turinio rinkmenos ir pasirašomi metaduomenys yra pasirašyti elektroniniais parašais. Elektroninio dokumento naudotojas turi žinoti, kur yra pagrindinė turinio rinkmena, kur konteineryje išsaugoti dokumento metaduomenys ir elektroniniai parašai, kaip tarpusavyje yra susijusios elektroninio dokumento turinio dalys.

Elektroninio dokumento konteineryje dalys tarpusavyje susiejamos *sąryšiais*, kurie nusako, kokios rūšies sąsają viena dokumento dalis turi su kita dokumento dalimi. Sąryšiai gali tarnauti kaip nuorodos, nusakančios dokumento dalies paskirtį. Sąryšiais taip pat galima logiškai apjungti dokumento dalis, nors jos ir neturi tarpusavio nuorodų.

Dokumento naudotojui pakanka peržvelgti sąryšių struktūrą, neanalizuojant kiekvienos dokumento dalies turinį, kad suprastų kur yra pagrindinė dokumento turinio rinkmena, kur metaduomenys, kur elektroniniai parašai, ir kaip dokumento dalys yra tarpusavyje susijusios. Sąryšiai atlieka dar vieną funkciją – jie aprašo loginę elektroninio dokumento dalių struktūrą, tokiu būdu ją atsiedami nuo fizinio dokumento dalių išdėstymo konteineryje. Elektroninį dokumentą kuriančiai programai nereikia dokumento turinio rinkmenos išsaugoti tik tam tikru, specifikacijoje nurodytu pavadinimu, ar ją išsaugoti tik tam tikrame, ir jokių būdu ne kitame konteinerio kataloge, kad rinkmeną surastų ir tinkamai panaudotų kita elektroninį dokumentą naudojanti programa.

Elektroninio dokumento dalių ryšius aprašo sąryšių rinkmena.

2.3.2.1. Sąryšių rinkmena

Sąryšių rinkmena yra konteinerio XML rinkmena pavadinimu „relations.xml“, aprašanti pagrindines elektroninio dokumento dalis ir elektroninio dokumento dalių tarpusavio sąryšius. Elektroninio dokumento konteineryje privalo būti viena ir tik viena sąryšių rinkmena.

Sąryšių rinkmenos duomenų tipas yra:

```
application/vnd.lt.archyvai.adoc-2008#relations+xml
```

Sąryšių rinkmenos pavadinimas yra: META-INF/relations.xml.

Sąryšiai XML rinkmenoje aprašomi `Relationship` elementais, įterptais `SourcePart` elementų viduje, kurie talpinami į šakninį `Relationships` elementą.

`Relationships` elementas yra šakninis sąryšių rinkmenos elementas, turintis vieną ar daugiau `SourcePart` elementų, kurie aprašo konteinerio ar konteinerio dalių sąryšius su kitomis dalimis.

Elektroninio dokumento sąryšių rinkmenoje turi būti:

- vienas `SourcePart` elementas, kuris aprašo konteinerio struktūrą nusakančius sąryšius;
- bent vienas `SourcePart` elementas, kurie aprašo dokumento dalių tarpusavio sąryšius.

`SourcePart` elementas aprašo konteinerio struktūrą nusakančius sąryšius arba dokumento dalies, susietos su kitomis dokumento dalimis, sąryšius. Elemento atributas `full-path` nurodo arba konteinerį, arba sąryšių turinčią dokumento dalį.

Atributo `full-path` reikšmė `"/` (`full-path="/`) identifikuoja konteinerį. Kitos atributo `full-path` reikšmės identifikuoja pilną kelią iki dokumento dalių. Elemento atributas `full-path` turi vienareikšmiškai nurodyti konteinerį arba dokumento dalį.

`Relationship` elementas aprašo konteinerio ar dokumento dalies, kurią apibrėžia `SourcePart` elementas, kuriame šis elementas yra patalpintas, sąryšio tipą su kita dokumento dalimi. Elemento atributas `full-path` nurodo dokumento dalį, su kuria konteineris ar dalis turi sąryšį, o atributas `type` apibrėžia sąryšio tipą. Neprivalomas elemento atributas `id` yra sąryšio identifikatorius.

2.3.2.2. Sąryšių tipai

Sąryšio tipą apibrėžia `SourcePart` elemento atributo `type` reikšmė. Ši specifikacija apibrėžia šiuos sąryšių tipus:

Sąryšio tipas	<code>SourcePart</code> elemento atributo <code>type</code> reikšmė
Pagrindinė elektroninio dokumento turinio rinkmena	http://www.archyvai.lt/adoc/2008/relationships/content/main
Elektroninio dokumento turinio priedo (priedų) rinkmena	http://www.archyvai.lt/adoc/2008/relationships/content/appendix
Pridedamo dokumento rinkmena	http://www.archyvai.lt/adoc/2008/relationships/content/attachment
Metaduomenų rinkmena	http://www.archyvai.lt/adoc/2008/relationships/metadata
Elektroninis parašas	http://www.archyvai.lt/adoc/2008/relationships/signature

2.3.3. Pagrindiniai ir papildomi metaduomenys

Elektroninio dokumento metaduomenys yra duomenys apie elektroninio dokumento formatą, sandarą, turinį, naudojimą ir pasirašymą. Metaduomenys skirstomi į:

- pasirašomus metaduomenis – tai tokie metaduomenys, kurių turinio po dokumento pasirašymo keisti nebegalima, ir privalo būti pasirašyti, jeigu jie yra;
- nepasirašomus metaduomenis – metaduomenis, kurių turinys elektroninio dokumento gyvavimo metu kinta, ir jie neturi būti pasirašyti; ir
- metaduomenis, kurie gali būti pasirašomi – tai metaduomenys, kuriais elektroninis dokumentas jo gyvavimo metu gali būti papildytas ir (jei reikia) elektroniniu parašu apsaugotas nuo pakeitimų.

Elektroninio dokumento metaduomenys aprašomi XML formatu, ir gali būti saugomi vienoje ar keliose XML rinkmenose. Pasirašomi ir nepasirašomi metaduomenys turi būti saugomi atskirose rinkmenose. Jeigu elektroninis dokumentas jo gyvavimo metu yra papildomas metaduomenimis, kurių dalį numatoma pasirašyti, kita dalį – ne, tokie metaduomenys turi būti saugomi atskirose rinkmenose.

Pasirašytos ir nepasirašytos metaduomenų rinkmenos nustatomos pagal elektroninio dokumento dalių tarpusavio sąryšius (žr. 2.3.2 Ryšių dalys).

Elektroninio dokumento metaduomenys. Elektroninio dokumento metaduomenys yra grupuojami į pasirašomus ir nepasirašomus metaduomenis. Sutinkamai su Reikalavimais specifikacijoms metaduomenų rinkiniai taip pat priklauso nuo elektroninio dokumento grupės: GGeDOC (GeDOC), BeDOC ir CeDOC.

Elektroninio dokumento metaduomenys:

Metaduomenys	XML elementas	Duomenų tipas	Privaloma grupėms			Pasirašomas
			GGeDOC	BeDOC	CeDOC	
PASIRAŠOMI METADUOMENYS						
Šaknis metaduomenų rinkmenos elementas:	Metadata	Elementas ⁷	Taip ¹⁰	Taip ¹⁰	Taip ¹⁰	Taip
Dokumentą ir jo sudarymą aprašantys metaduomenys						
El. dokumento turinį aprašantys metaduomenys:	document	Elementas ⁵	Taip ¹⁰	Taip ¹⁰	Ne ¹⁰	Taip ³
El. dokumento pavadinimas (antraštė)	title	Tekstinis	Taip	Taip	Taip ⁹	Taip ¹
Sudarytojai:	authors	Elementas ⁵	Taip ¹⁰	Taip ¹⁰	Taip ¹⁰	Taip
Sudarytojas:	author	Elementas ⁵	Taip ¹⁰	Taip ¹⁰	Taip ¹⁰	Taip
Sudarytojas (pavadinimas arba pavardė, vardas)	name	Tekstinis	Taip	Taip	Taip	Taip ¹
Sudarytojo kodas	code	Tekstinis	Taip	Taip	Ne	Taip ^{3,1}
Sudarytojo adresas	address	Tekstinis	Taip	Taip	Taip	Taip ¹
Dokumento sudarymas:	created	Elementas ⁵	Ne ¹⁰	Taip ¹⁰	Taip ¹⁰	Taip ³
Sudarymo data	date	Data ²	Ne	Taip	Taip	Taip ^{3,1}
Adresatai:	recipients	Elementas ⁵	Ne ¹⁰	Ne ¹⁰	Ne ¹⁰	Taip ³
Adresatas:	recipient	Elementas ⁵	Ne ¹⁰	Ne ¹⁰	Ne ¹⁰	Taip ^{3,1}
Adresatas (pavadinimas arba pavardė, vardas)	name	Tekstinis	Ne	Ne	Ne	Taip ^{3,1}
Adresato kodas	code	Tekstinis	Ne	Ne	Ne	Taip ^{3,1}
Adresato adresas	address	Tekstinis	Ne	Ne	Ne	Taip ^{3,1}

Metaduomenys	XML elementas	Duomenų tipas	Privaloma grupėms			Pasirašomas
			GGeDOC	BeDOC	CeDOC	
Dokumento registravimo metaduomenys						
Dokumento registravimas:	registered	Elementas ⁵	Taip ¹⁰	Ne ¹⁰	Ne ¹⁰	Taip ³
Registravimo data	date	Data ²	Taip	Taip ⁹	Taip ⁹	Taip ¹
Dokumento registracijos Nr.	number	Tekstinis	Taip	Taip ⁹	Taip ⁹	Taip ¹
Dokumentą užregistravęs darbuotojas	registrar	Darbuotojas ⁸	Ne	Ne	Ne	Taip ^{3,1}
Gauto dokumento registravimo metaduomenys						
Siuntėjas :	sender	Tekstinis	Ne ¹⁰	Ne ¹⁰	Ne ¹⁰	Taip ³
Siuntėjas (pavadinimas arba pavardė, vardas)	name	Tekstinis	Ne	Ne	Ne	Taip ^{3,1}
Siuntėjo kodas	code	Tekstinis	Ne	Ne	Ne	Taip ^{3,1}
Siuntėjo adresas	address	Tekstinis	Ne	Ne	Ne	Taip ^{3,1}
Gavėjas:	receiver	Tekstinis	Ne ^{6,10}	Ne ¹⁰	Ne ¹⁰	Taip ³
Gavėjo pavadinimas arba pavardė, vardas	name	Tekstinis	Taip ⁹	Taip ⁹	Taip ⁹	Taip ^{3,1}
Gavėjo kodas	code	Tekstinis	Taip ⁹	Taip ⁹	Ne	Taip ^{3,1}
Gavėjo adresas	address	Tekstinis	Taip ⁹	Taip ⁹	Taip ⁹	Taip ^{3,1}
Dokumento gavimas:	received	Elementas ⁵	Ne ^{6,10}	Ne ¹⁰	Ne ¹⁰	Taip ³
Gavimo data	date	Data ²	Taip ⁹	Taip ⁹	Taip ⁹	Taip ^{3,1}
Dokumento gavimo registracijos Nr.	number	Tekstinis	Taip ⁹	Taip ⁹	Taip ⁹	Taip ^{3,1}
Dokumentą užregistravęs darbuotojas	registrar	Darbuotojas ⁸	Ne	Ne	Ne	Taip ^{3,1}
Elektroninių parašų metaduomenys (metaduomenys turi būti pasirašyti tuo el. parašu, kurį papildo)						
El. parašų metaduomenys:	signatures	Elementas ⁵	Taip	Taip	Taip	Taip ¹
El. parašo metaduomenys:	signature	Elementas ⁵	Taip ¹⁰	Taip ¹⁰	Taip ¹⁰	Taip
El. parašo identifikacinis numeris	signatureID	Nuoroda (IRI)	Taip	Taip	Taip	Taip ¹
Pasirašymo data	signingTime	Data ir laikas ²	Taip	Taip	Taip	Taip ¹
El. parašo paskirtis (pasirašymas, tvirtinimas, vizavimas, suderinimas, registravimas, gauto dokumento registravimas, supažindinimas)	signingPurpose	Tekstinis (pasirenkamas)	Taip	Taip	Taip	Taip ¹
Pasirašantis asmuo	signer	Darbuotojas ⁸	Taip	Taip	Taip	Taip ¹
NEPASIRAŠOMI METADUOMENYS						
Šakninis metaduomenų rinkmenos elementas:	metadata	Elementas ⁷	Taip	Taip	Taip	Ne
Dokumento techniniai metaduomenys						
El. dokumento naudojimo metaduomenys:	use	Elementas ⁵	Taip	Taip	Taip	Ne
Techninė informacija:	technical_environment	Elementas ⁵	Taip	Taip	Taip	Ne
Elektroninio dokumento specifikacijos identifikatorius: ADOC-V1.0	standardVersion	Tekstinis	Taip	Taip	Taip	Ne
Elektroninio dokumento grupė: GGeDOC, BeDOC, CeDOC	documentCategory	Tekstinis (pasirenkamas)	Ne	Taip	Taip	Ne

Metaduomenys	XML elementas	Duomenų tipas	Privaloma grupėms			Pasirašomas
			GGeDOC	BeDOC	CeDOC	
Elektroninį dokumentą rengusios sistemos pavadinimas ir versija	generator	Tekstinis	Ne	Ne	Ne	Ne
Operacinės sistemos, kurioje buvo parengtas dokumentas, pavadinimas ir versija	os	Tekstinis	Ne	Ne	Ne	Ne
Dokumento dalių tarpusavio sąsajų informacija (žr. 2.3.2 Ryšių dalys)						Ne
Elektroninio dokumento dalių turinio tipų aprašas (žr. 2.3.2 Ryšių dalys)						Ne

Pastabos:

¹ Metaduomuo atskirai nėra pasirašomas, o tik kaip anksčiau nurodytų metaduomenų grupių, kurioms metaduomuo priklauso ir turi unikalų identifikatorių, sudėtinė dalis.

² Data arba data ir laikas, kaip tai apibrėžta XML formato W3C rekomendacijose.

³ Pasirašoma, jeigu duomenys pateikti.

⁴ Jei nėra metaduomens, laikoma, kad apribojimų nėra.

⁵ Elementas, kurį sudaro žemiau išvardinti grupę sudarantys metaduomenų elementai.

⁶ Metaduomuo nurodomas, jei tokie duomenys privalomi pagal dokumento pobūdį.

⁷ Elementas, kurį sudaro toliau išvardinti ir kitose dalyse aprašyti grupę sudarantys metaduomenų elementai.

⁸ Darbuotojo duomenų tipas:

Atsakingo asmens pavardė, vardas	individualName	Tekstinis	Taip	GB
Atsakingo asmens pareigos	positionName	Tekstinis	Taip	GB
Struktūrinis padalinys	structuralSubdivision	Tekstinis	Ne	GB

GB – metaduomenys gali būti pasirašomi.

⁹ Privalomas, jeigu yra elementą gaubiantis (tėvinis) elementas.

¹⁰ Elementui (jeigu nurodytas) privalomas atributas ID, kuriame įrašytas unikalus identifikatorius.

Metaduomenų XML rinkmenos. Elektroninio dokumento metaduomenų rinkmena susideda iš šakninio elemento *metadata* su nuoroda į vardų sritį, apibrėžiamą metaduomenų XML schema, kurio turinį gali sudaryti vienas ar keli aukščiau apibrėžtų metaduomenų elementų. Metaduomenų elementų tvarka rinkmenoje nėra svarbi.

Tikrinimas, ar elektroniniame dokumente yra visi privalomi metaduomenys, atliekamas pagal pridėdamą metaduomenų profilio XML rinkmeną. Metaduomenų elementų atitikimo metaduomenų profiliui tikrinimas atliekamas taip, tarsi visi tos pačios XML vardų srities metaduomenų elementai, esantys skirtingose metaduomenų rinkmenose, būtų vienoje metaduomenų rinkmenoje.

Elektroninio dokumento tarpusavio sąsajų informacijos ir elektroninio dokumento dalių turinio tipų aprašo struktūras apibrėžia atitinkamos šios specifikacijos dalys: 2.3.2 Ryšių dalys ir 2.3.1 Turinio tipai.

3. Elektroninio dokumento turinys

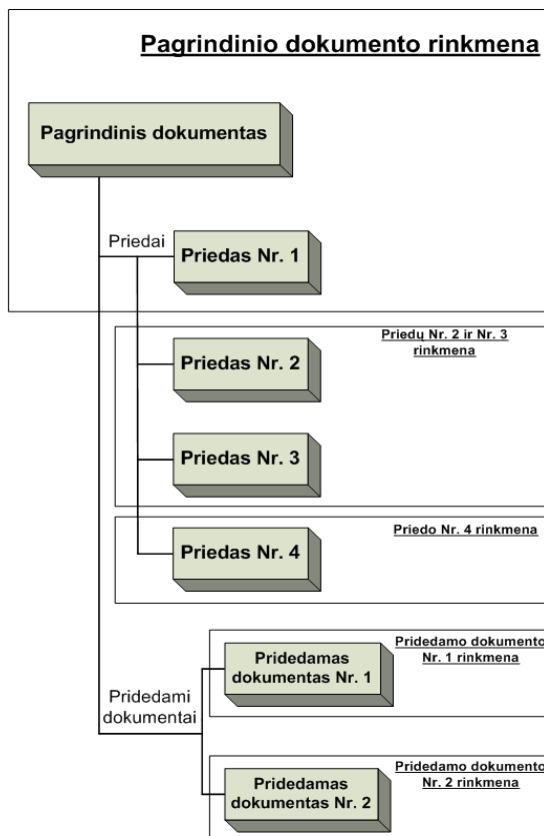
Elektroninio dokumento turinį gali sudaryti šios dalys:

- pagrindinis dokumentas – elektroninio dokumento turinio dalis, kurioje pateikiama pagrindinė elektroninio dokumento turinio informacija, arba lydraštis, kuriame fiksuojama informacija apie persiunčiamus elektroninius dokumentus;
- vienas ar daugiau dokumento priedų – elektroninio dokumento turinio dalis, kurioje pateikiama pagrindinį dokumentą papildanti elektroninio dokumento turinio informacija;
- vienas ar daugiau pridėdamų elektroninių dokumentų – savarankiški elektroniniai dokumentai, pridėdami prie pagrindinio dokumento kaip jo turinį papildanti,

paaškinanti ar pagrindinio dokumento turinyje pateiktus faktus pagrindžianti informacija, taip pat su lydraščiu siunčiami elektroniniai dokumentai.

3.1. Turinio rinkmenų struktūra

Turi būti viena ir tik viena pagrindinio dokumento rinkmena. Gali būti viena ar daugiau dokumento priedo rinkmenų. Pagrindinio dokumento ir dokumento priedų rinkmenos gali apimti vieną ar daugiau priedų, tačiau vienas priedas negali būti keliose rinkmenose. Priedai gali turėti kitų priedų, saugomų atskirose rinkmenose.



2 pav. Elektroninio dokumento turinio struktūros schema

Elektroninio dokumento turinį gali sudaryti vienas ar daugiau pridedamų dokumentų rinkmenų, kiekvieną iš jų turi sudaryti vienas ir tik vienas elektroninis dokumentas. Priedamo elektroninio dokumento turinį gali sudaryti kiti pridedami dokumentai. Bendras elektroninio dokumento rinkmenos dydis neturi viršyti 4 GB.

Elektroninio dokumento pagrindinio dokumento rinkmena saugoma šakniniame elektroninio dokumento kataloge. Dokumento priedų rinkmenos ir pridedami elektroniniai dokumentai saugomi dokumento priedų ir pridedamų elektroninių dokumentų kataloge (žr. 1 pav.).

Esant dideliame priedų ar pridedamų dokumentų skaičiui, priedų ir/ar pridedamų dokumentų katalogai gali būti sudaromi hierarchinės katalogų struktūros principu, kai žemesniuose hierarchinės katalogų struktūros lygmenyse gali būti vienas ar daugiau katalogų, sudarytų iš vienos ar daugiau priedų ar pridedamų dokumentų, priklausomai nuo katalogo, kuriame ši hierarchinė struktūra sukurta.

Apribojimai dokumento turinio rinkmenų ir katalogų struktūrai (sąlygoja konteineris):

- ilgiausios URI nuorodos į dokumento rinkmeną ilgis neturi viršyti 65535 simbolių;
- bendras dokumento priedų, pridedamų dokumentų ir hierarchinės struktūros katalogų skaičius neturi viršyti 65000.

4. Elektroniniai parašai

GGeDOC grupės oficialaus elektroninio dokumento turinys ir privalomai pasirašomi metaduomenys turi būti pasirašyti XAdES-EPES formato elektroniniu parašu. Vienas pasirašomų duomenų objektas gali būti pasirašytas keliais elektroniniais parašais, o taip pat keli pasirašomų duomenų objektai gali būti pasirašyti vienu elektroniniu parašu. Vienoje elektroninio parašo rinkmenoje gali būti tik vienas parašas.

Parašų galiojimui laikui bėgant užtikrinti naudojamos laiko žymos (angl. *time-stamp*), suformuojant elektroninio parašo formatą XAdES-T ir kitus aukštesnio lygio formatus: XAdES-C, XAdES-X, XAdES-X-L, orientuojantis į ilgalaikį oficialaus elektroninio dokumento saugojimą. Visoms laiko žymoms išsaugoti naudojamas tik neišreikštinis mechanizmas (angl. *implicit*), pagal XAdES standarto „7.1.4.3 The XAdESTimeStampType data type“ punktą. Už aukštesnio lygmens elektroninio parašo formato sukūrimą yra atsakinga GGeDOC grupės oficialų elektroninį dokumentą priimanti institucija.

Gyventojo sukuriamas GGeDOC grupės oficialus elektroninis dokumentas yra pasirašomas XAdES-EPES formato parašu neišreikštinių parašo taisyklių variantu.

XAdES-EPES formato parašo struktūra:

XML elementas	Privalomas	Skaičius	Pastaba
ds:Signature	Taip	1	Vienoje rinkmenoje gali būti tik vienas el. parašas
ds:SignedInfo	Taip	1	
ds:CanonicalizationMethod	Taip	1	
ds:SignatureMethod	Taip	1	
ds:Reference	Taip	2-N	Nuorodos gali būti tik į dokumento pakuotėje esančius objektus. Viena iš nuorodų turi rodyti į pasirašomus atributus (elementas <i>SignedProperties</i>) parašo rinkmenos viduje. Jeigu nuoroda rodo į toje pačioje parašo rinkmenoje esantį objektą, tai atributo ds:URI reikšmė turi būti sudaryta tik iš URI fragmento dalies (pvz., <i>URI</i> =“#SignPr“). Jeigu nuoroda rodo į objektą, nesantį toje pačioje parašo rinkmenoje, tai atributo ds:URI reikšmė turi būti sudaryta tik iš URI kelio iki rinkmenos (URI fragmentas negali būti naudojamas).
Ds:Transforms	Ne	0-N	

XML elementas	Privalomas	Skaičius	Pastaba
Ds:DigestMethod	Taip	1	
Ds:DigestValue	Taip	1	
ds:SignatureValue	Taip	1	
ds:KeyInfo	Taip	1	Privalo turėti elementą X509Data, kuriame būtų sertifikato elementas X509Certificate
ds:Object	Taip	1	
QualifyingProperties	Taip	1	
SignedProperties	Taip	1	
SignedSignatureProperties	Taip	1	
SigningTime	Taip	1	
SigningCertificate	Taip	1	Turi nurodyti sertifikatą, esantį elemente KeyInfo
SignaturePolicyIdentifier	Taip	1	
SignatureProductionPlace	Ne	0-1	
SignerRole	Ne	0-1	
SignedDataObjectProperties	Ne	0-1	
DataObjectFormat	Ne	0-1	
CommitmentTypeIndication	Taip	1	
AllDataObjectsTimeStamp	Neleistinas	0	
IndividualDataObjectsTimeStamp	Neleistinas	0	
UnsignedProperties	Taip	1	
UnsignedSignatureProperties	Taip	1	
CounterSignature	Neleistinas	0	

Elementų privalomumas apibrėžiamas taip:

Privalomas	Kurianti aplikacija	Apdorojanti aplikacija
Taip	Privalo sukurti šį elementą	Privalo apdoroti šį elementą
Ne	Gali sukurti šį elementą	Gali apdoroti šį elementą, jei jis yra
Neleistinas	Negali kurti šio elemento	Neapdoroja šio elemento ir grąžina klaidą

XAdES-T formato parašo struktūra:

XML elementas	Privalomas	Kiekis	Pastaba
ds:Signature	Taip	1	Vienoje rinkmenoje gali būti tik vienas parašas
ds:SignedInfo	Taip	1	
ds:CanonicalizationMethod	Taip	1	
ds:SignatureMethod	Taip	1	
ds:Reference	Taip	2-N	Nuorodos gali būti tik į dokumento konteineryje esančius objektus. Viena nuorodų turi rodyti į pasirašomus atributus (elementas SignedProperties) parašo rinkmenos viduje
ds:Transforms	Ne	0-N	

XML elementas	Privalomas	Kiekis	Pastaba
ds:DigestMethod	Taip	1	
ds:DigestValue	Taip	1	
ds:SignatureValue	Taip	1	
ds:KeyInfo	Taip	1	Privalo turėti elementą X509Data, kuriame būtų sertifikato elementas X509Certificate
ds:Object	Taip	1	
QualifyingProperties	Taip	1	
SignedProperties	Taip	1	
SignedSignatureProperties	Taip	1	
SigningTime	Ne	0-1	
SigningCertificate	Taip	1	Turi nurodyti sertifikatą, esantį elemente KeyInfo
SignaturePolicyIdentifier	Taip	1	
SignatureProductionPlace	Ne	0-1	
SignerRole	Ne	0-1	
SignedDataObjectProperties	Ne	0-1	
DataObjectFormat	Ne	0-1	
CommitmentTypeIndication	Ne	0-1	
AllDataObjectsTimeStamp	Neleistinas	0	
IndividualDataObjectsTimeStamp	Neleistinas	0	
UnsignedProperties	Taip	1	
UnsignedSignatureProperties	Taip	1	
CounterSignature	Neleistinas	0	
SignatureTimeStamp	Taip	1	Laiko žyma saugoma EncapsulatedTimeStamp elemente; XMLTimeStamp elementas neleistinas

XAdES-C formato parašo struktūra atitinka XAdES-T formato struktūrą, kurios UnsignedSignatureProperties elementas papildytas šiais elementais:

XML elementas	Privalomas	Kiekis	Pastaba
UnsignedSignatureProperties	Taip	1	
CompleteCertificateRefs	Taip	1	
CompleteRevocationRefs	Taip	1	Naudojami tik CRLRefs ir OCSPRefs elementai (OtherRefs neleistinas)
AttributeCertificateRefs	Neleistinas	0	
AttributeRevocationRefs	Neleistinas	0	

XAdES-X-L formato parašo struktūra atitinka XAdES-C formato struktūrą, kurios UnsignedSignatureProperties elementas papildytas šiais elementais:

XML elementas	Privalomas	Kiekis	Pastaba
UnsignedSignatureProperties	Taip	1	
SigAndRefsTimeStamp	Taip	1	Realizuotas remiantis nepaskirstytu variantu (XAdES standarto punktas „7.5.1.1 Not distributed case“)

XML elementas	Privalomas	Kiekis	Pastaba
RefsOnlyTimeStamp	Neleistinas	0	
CertificateValues	Taip	1	Sertifikatams saugoti naudojamasi EncapsulatedX509Certificate elementas; OtherCertificate elementas neleistinas
RevocationValues	Taip	1	Atšaukimo informacijai saugoti naudojami tik CRLValues ir OCSPValues elementai (OtherValues neleistinas)
AttrAuthoritiesCertValues	Neleistinas	0	
AttributeRevocationValues	Neleistinas	0	

Elektroninių parašų formavimui gali būti naudojami tik šie algoritmai:

Algoritmas	Identifikatorius
Santraukos sudarymas (angl. „Digest“)	
SHA1	http://www.w3.org/2000/09/xmldsig#sha1
Kodavimas (angl. „Encoding“)	
Base64	http://www.w3.org/2000/09/xmldsig#base64
Pasirašymas (angl. „Signature“)	
DSAwithSHA1 (DSS)	http://www.w3.org/2000/09/xmldsig#dsa-sha1
RSAwithSHA1	http://www.w3.org/2000/09/xmldsig#rsa-sha1
Kanonizavimas (angl. „Canonicalization“)	
Canonical XML (omits comments)	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Canonical XML with Comments	http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
Transformavimas (angl. „Transform“)	
XPath	http://www.w3.org/TR/1999/REC-xpath-19991116
Base64	http://www.w3.org/2000/09/xmldsig#base64

5. Elektroninio dokumento tikrinimas

Elektroninio dokumento tikrinimas vyksta trimis etapais:

- tikrinamas elektroninio dokumento turinys,
- tikrinamas specifikacijoje apibrėžto konteinerio formatas,
- tikrinami konteineryje esantys parašai.

5.1. Elektroninio dokumento turinio tikrinimas

Išsamus elektroninio dokumento turinio patikrinimas apima šiuos etapus:

1. Dokumento turinio dalių tarpusavio sąryšių patikrinimas:

- ar elektroniniame dokumente yra viena ir tik viena pagrindinė dokumento turinio rinkmena;
- ar vienareikšmiškai identifikuojamos dokumento turinio dalys, t.y., ar yra sąryšiais neidentifikuojamų turinio dalių; ar pagrindinė dokumento turinio rinkmena nėra kažkurios kitos dalies priedas ar pridedamas dokumentas; ar priedas nėra kurios

nors dalies pridedamas dokumentas; ar pridedamas dokumentas nėra kurios nors dalies priedas;

- ar pridedamų dokumentų rinkmenos (jeigu jos yra) sąryšio tipu „Priedamo dokumento rinkmena“ siejamos tik su pagrindine turinio rinkmena;
- ar pagrindinė dokumento turinio rinkmena ir visos dokumento priedų rinkmenos (jeigu jos yra) pagal sąryšio tipą „Elektroninio dokumento turinio priedo (priedų) rinkmena“ sudaro tvarkingą hierarchinę struktūrą, kurios viršuje yra pagrindinė dokumento turinio rinkmena, t.y., ar hierarchija vienintelė (apima visas priedų rinkmenas), ar nėra ciklų ir nuorodų į tą pačią rinkmeną.

2. Turinio tipų patikrinimas:

- ar visos elektroninio dokumento turinį sudarančios rinkmenos aprašytos konteinerio dalių tipų apraše, t.y., ar yra turinio rinkmenų, neįtrauktų į šį aprašą;
- ar dokumento priedų ir pridedamų dokumentų rinkmenos atitinka turinio tipų reikalavimus, t.y., ar yra turinio rinkmenų, neatitinkančių turinio tipų reikalavimų.

3. Turinio dalių naudojamumo patikrinimas:

- ar visos elektroninio dokumento turinį sudarančios rinkmenos atitinka deklaruojamą formatą, t.y., atidaromos atitinkama rinkmenos formatą realizuojančia programine įranga.

4. Metaduomenų patikrinimas:

- ar elektroniniame dokumente yra visi privalomi metaduomenys;
- ar metaduomenys apibrėžti tik vieną kartą, išskyrus metaduomenis, kurie gali būti apibrėžti kelis kartus (pvz., el. parašo metaduomenys);
- ar visi metaduomenys, kurie privalo būti pasirašyti, yra pasirašyti;
- ar visi el. parašų metaduomenys pasirašyti aprašomais el. parašais.

5.2. Specifikacijos formato tikrinimas

Konteinerio atitikimo formatui metu yra įsitikinama:

- 1) Ar konteinerio rinkmena yra ZIP archyvo rinkmena.
- 2) Ar ZIP archyvo rinkmenoje yra visos privalomos elektroninio dokumento dalys (turinio pagrindinio dokumento rinkmena, privalomos metaduomenų rinkmenos, bent viena parašų rinkmena, elektroninio dokumento konteinerio dalių turinio tipų aprašo rinkmena (`manifest.xml`), elektroninio dokumento dalių ryšių rinkmena (`relations.xml`)).
- 3) Ar elektroninio dokumento konteinerio dalių tipų aprašo rinkmena (`manifest.xml`) tenkina ODF 1.2 standarto reikalavimus:
 - ar tipų aprašo rinkmena yra META_INF direktorijoje,
 - ar tipų aprašo rinkmena nurodo visų elektroninio dokumento dalių (MIME) tipus išskyrus `manifest.xml`.
 - Ar visos elektroninio dokumento dalys tenkina rinkmenų tipų reikalavimus: pagrindinio turinio dokumento ir turinio priedų rinkmenos yra docx, xlsx, pptx, odt, ods ar odp tipų rinkmenos, savarankiškų pridedamų elektroninių dokumentų rinkmenos yra adoc tipo rinkmenos, metaduomenų, elektroninių parašų,

- elektroninio dokumento konteinerio dalių tipų aprašo ir elektroninio dokumento dalių tarpusavio ryšių rinkmenos yra xml tipo rinkmenos.
- 4) Ar elektroninio dokumento dalių tarpusavio ryšių rinkmena (`relations.xml`) tenkina specifikacijos reikalavimus:
 - ar yra visi konteinerio struktūrą nusakantys sąryšiai ir ar jie tenkina apibrėžtus reikalavimus,
 - ar visos sąryšių aprašuose sutinkamos elektroninio dokumento dalys yra korektiškos,
 - ar visos ryšių rinkmenoje nurodytos pasirašytos elektroninio dokumento dalys iš tikrųjų yra pasirašytos nurodytais parašais,
 - ar visos pasirašytos elektroninio dokumento dalys turi atitinkamus sąryšius ryšių rinkmenoje.
 - 5) Ar metaduomenų rinkmenos tenkina metaduomenų rinkmenoms keliamus reikalavimus, ar visi privalomai pasirašomi metaduomenys yra pasirašyti.
 - 6) Ar parašų rinkmenos tenkina ODF 1.2 standarto reikalavimus:
 - ar atitinka parašų rinkmenos XML schemą,
 - ar parašų rinkmena yra META_INF kataloge (arba jo vidiniame kataloge),
 - ar parašų rinkmenos pavadinime yra žodis “signatures”.
 - 7) Ar vienoje parašų rinkmenoje yra lygiai vienas parašas.
 - 8) Ar elektroninio dokumento turinio pagrindinė rinkmena yra konteinerio šakniniame kataloge.

5.3. Elektroninių parašų tikrinimas

Tikrinant elektroninį dokumentą, yra tikrinami visi elektroniniame dokumente esantys parašai. Kiekvienas parašas turi būti atskiroje rinkmenoje. Elektroniniame dokumente esančio elektroninio parašo tikrinimo metu yra įsitikinama:

- 1) Ar parašas atitinka XMLDSIG ir XAdES standartus.
- 2) Ar pasirašymui naudoti sertifikatai buvo išduoti patikimų sertifikavimo tarnybų.
- 3) Ar elektroniniame paraše yra pasirašymui naudotas sertifikatas (elemente `<KeyInfo>` turi būti elementas `<X509Data>`, kuriame yra pasirašiusio asmens sertifikatas (elementas `<X509Certificate>`)).
- 4) Ar elektroninis parašas tenkina elektroninio parašo formatą XAdES-EPES.
- 5) Ar elektroniniame paraše naudojami algoritmai (transformavimo, kodavimo BASE64, kanonizavimo, santraukų darymo, pasirašymo) yra palaikomi.
- 6) Ar elektroninis parašas tenkina kitus, šiame dokumente elektroniniam parašui apibrėžtus, reikalavimus.
- 7) Ar visos elektroninio dokumento turinio dalys yra pasirašytos kaip pilnos dvejetainės rinkmenos (pasirašyta visa, o ne dalis rinkmenos; nuorodose į turinio rinkmenas nėra naudojama transformacijų).

Naudojamų sertifikatų profiliai turi atitikti RFC 3280 „Internet X.509 Public Key Infrastructure: Certificate and CRL Profile“ ir RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“ standartus.

Sertifikatų atšaukimo informacija turi būti pasiekama naudojant OCSP paslaugą, teikiamą HTTP arba HTTPS protokolais, pagal RFC 2560 „X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP“ standartą.

Nesant OCSP paslaugos, turi būti naudojami sertifikatų atšaukimo sąrašai (CRL), atitinkantys RFC 3280 „Internet X.509 Public Key Infrastructure: Certificate and CRL Profile“ ir pasiekiami HTTP arba HTTPS protokolais.

Laiko žymos paslaugos turi būti pasiekiamos HTTP protokolu, pagal RFC 3161 „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)“ standartą.

5.4. Nuorodos

- | | |
|-------------|--|
| [CWA 14171] | CWA 14171 - General guidelines for electronic signature verification, 2004 |
| [ODF 1.2] | Open Document Format for Office Applications (v1.2 Part 3: Packages Pre-Draft6, 12 Sep 2007 |
| [RFC 2560] | RFC 2560 „X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP“ |
| [RFC 3161] | RFC 3161 „Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)“ |
| [RFC 3280] | RFC 3280 „Internet X.509 Public Key Infrastructure: Certificate and CRL Profile“ |
| [RFC 3739] | RFC 3739 „Internet X.509 Public Key Infrastructure: Qualified Certificates Profile“ |
| [XMLDSIG] | XML-Signature Syntax and Processing, W3C Recommendation 2002 |
| [XAdES] | ETSI TS 101 903 V1.3.2 (2006-03), XML Advanced Electronic Signatures (XAdES) |