VALSTYBINĖS MOKESČIŲ INSPEKCIJOS
PRIE LIETUVOS RESPUBLIKOS FINANSŲ MINISTERIJOS VIRŠININKO
Į S A K Y M A S

DĖL KOMPIUTERIO SKAITOMŲ ELEKTRONINIŲ DOKUMENTŲ KVALIFIKUOTO ELEKTRONINIO PARAŠO TAISYKLIŲ PATVIRTINIMO

2010 m. rugsėjo 2 d. Nr. VA-96
Vilnius

Vadovaudamasis Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos nuostatų, patvirtintų Lietuvos Respublikos finansų ministro 1997 m. liepos 29 d. įsakymu Nr. 110 „Dėl Valstybinės mokesčių inspekcijos prie Lietuvos Respublikos finansų ministerijos nuostatų patvirtinimo“ (Žin., 1997, Nr. 87-2212; 2004, Nr. 82-2966), 18.11 punktu ir atsižvelgdamas į Reikalavimus elektroninio parašo tikrinimo procedūrai, patvirtintus Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. sausio 29 d. įsakymu Nr. T-8 (Žin., 2003, Nr. 11-432),

t v i r t i n u pridedamas Kompiuterio skaitomų elektroninių dokumentų kvalifikuoto elektroninio parašo taisykles.

VIRŠININKAS MODESTAS KASELIAUSKAS

_____

PATVIRTINTA

Valstybinės mokesčių inspekcijos prie
Lietuvos Respublikos finansų
ministerijos viršininko
2010 m. rugsėjo 2 d. įsakymu Nr. VA-96

KOMPIUTERIO SKAITOMŲ ELEKTRONINIŲ DOKUMENTŲ KVALIFIKUOTO ELEKTRONINIO PARAŠO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Šios Kompiuterio skaitomų elektroninių dokumentų kvalifikuoto elektroninio parašo taisyklės (toliau – Parašo taisyklės) nustato mokesčių administratoriui elektroniniu būdu teikiamų mokesčių mokėtojų elektroninių deklaracijų, elektroninio parašo kvalifikuotų sertifikatų deklaracijų ir kitų dokumentų (toliau – elektroniniai dokumentai) kvalifikuoto elektroninio parašo sudarymo ir tikrinimo tvarką, pasirašančio asmens ir tikrinančio asmens įsipareigojimus, nurodo techninius standartus ir veiksmus, kurie turi būti atliekami kuriant ir tikrinant mokesčių mokėtojų elektroninių dokumentų kvalifikuotus elektroninius parašus.

2. Mokesčių mokėtojai, naudodami jiems tinkamas instrumentines priemones, per Valstybinės mokesčių inspekcijos Elektroninio deklaravimo informacinę sistemą (toliau – EDS) rengia, pasirašo ir/arba teikia elektronines deklaracijas, kitus kompiuterio skaitomus elektroninius dokumentus, kurie priimami, patikrinami, įskaitant ilgalaikio saugojimo parašo formato suformavimą, bei saugomi EDS duomenų bazėse.

3. Parašo taisyklės parengtos vadovaujantis Lietuvos Respublikos elektroninio parašo įstatymu (Žin., 2000, Nr. 61-1827), Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108 „Dėl Reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“ (Žin., 2003, Nr. 2-47), Elektroninių dokumentų valdymo taisyklėmis, patvirtintomis Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus 2006 m. sausio 11 d. įsakymu Nr. V-12 (Žin., 2006, Nr. 7-268), Reikalavimais elektroninio parašo tikrinimo procedūrai, patvirtintais Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. sausio 29 d. įsakymu Nr. T-8 (Žin., 2003, Nr. 11-432), Laiko žymos formavimo paslaugų teikimo tvarka, patvirtinta Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės direktoriaus 2003 m. sausio 29 d. įsakymu Nr. T-10 (Žin., 2003, Nr. 11-434), kitais teisės aktais bei Europos Sąjungos elektroninio parašo standartizavimo iniciatyvos dokumentais ir minimaliais techninių standartų reikalavimais, apibrėžiančiais pakankamas sąlygas, kurioms esant elektroninis parašas tenkina kvalifikuotam elektroniniam parašui keliamus reikalavimus, apibrėžtais tarptautiniuose standartuose:

3.1. ETSI TR 102 038 v1.1.1: „TS Security – Electronic Signatures and Infrastructures (ESI); XML format for signature policies“;

3.2. ETSI TR 102 272 v1.1.1: „Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies“;

3.3. ETSI TR 102 041 v1.1.1: „Signature policy report“;

3.4. ETSI TR 102 045 v1.1.1: „Signature Policy for Extended Business Model“;

3.5. RFC 3125 – „Electronics Signature Policies“;

3.6. CWA 14169:2009 „Secure Signature-Creation Devices „EAL 4+“;

3.7. CWA 14170:2004 „Security Requirements for Signature Creation Applications“;

3.8. CWA 14171:2004: „General guidelines for electronic signature verification“;

3.9. ETSI TS 101 903 v1.4.1: „XML Advanced Electronics Signatures (XAdES)“;

3.10. ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“;

3.11. ETSI TS 101 456 v1.2.1: „Policy requirements for certification authorities issuing qualified certificates“;

3.12. ETSI TS 102 231: v2.1.1 „Requirements for Trust Service Provider status information“.

4. Parašo taisyklėse naudojamos pagrindinės sąvokos ir santrumpos:

CRL – Sertifikatų atšaukimo sąrašas (angl. *Certificate Revocation List*);

EDS elektroninis dokumentas – mokesčių mokėtojo elektroniniu būdu teikiamas MDOC-V1.0 specifikacijos dokumentas, pasirašytas kvalifikuotu elektroniniu parašu, kurio turinį sudaro tik viena FFData formato pagrindinio dokumento rinkmena;

elektroninio dokumento pakuotė (toliau **– Pakuotė**) – rinkmena, kurioje pateikiamas pasirašyto elektroninio dokumento turinys, elektroninio dokumento elektroniniai parašai ir elektroninio dokumento metaduomenys;

elektroninio parašo kvalifikuoto sertifikato deklaracija (toliau – **Sertifikato deklaracija**) – MDOC-V1.0 specifikacijos elektroninis dokumentas, kurio turinį sudaro elektroninio parašo kvalifikuoto sertifikato deklaracijos pagrindinė rinkmena, pateikianti sertifikato turėtojo vardą ir pavardę, asmens kodą ir kitus duomenis, būtinus sertifikato susiejimui su asmeniu, XML formatu, ir vienas XSLT transformacijų (angl. *XSLT Transformations*) formato priedas, elektroninės deklaracijos elektroninis parašas ir elektroninės deklaracijos metaduomenys;

elektroninio parašo TPĮ – elektroninio parašo formavimo taikomoji programinė įranga, tenkinanti tarptautinio standarto CWA 14170:2004 „Security Requirements for Signature Creation Applications“ reikalavimus;

ID – Identifikatorius;

FFData formatas – XML struktūroje aprašyti kompiuterio skaitomi elektroninio dokumento ABBYY eFormFiller duomenys;

galiojantis kvalifikuotas sertifikatas – kvalifikuotas sertifikatas, kurio galiojimo laikotarpį sudaro laiko intervalas, atitinkantis visus toliau nurodytus reikalavimus:

1) sertifikato galiojimo laikotarpis yra apribotas sertifikato galiojimo pradžios ir pabaigos laiko momentais, nurodytais kvalifikuotame sertifikate;

2) sertifikato galiojimo laikotarpis yra apribotas kreipimosi dėl sertifikato galiojimo nutraukimo ar sustabdymo laiku, paskelbtu ne vėliau negu praėjus kvalifikuoto sertifikato taisyklėse nurodytam sertifikato paskelbimo negaliojančiu terminui;

GeDOC grupės elektroniniai dokumentai – valstybės ir savivaldybių institucijų, įstaigų ir įmonių, kitų subjektų, įgaliotų atlikti viešojo administravimo funkcijas, ir valstybės įgaliotų asmenų rengiami oficialieji elektroniniai dokumentai, įskaitant dokumentus, rengiamus kartu su nevalstybinėmis organizacijomis, privačiais juridiniais ar fiziniais asmenimis (pavyzdžiui, sutartis);

GGeDOC grupės elektroniniai dokumentai – valstybės ir savivaldybių institucijų, įstaigų ir įmonių, kitų subjektų, įgaliotų atlikti viešojo administravimo funkcijas, ir valstybės įgaliotų asmenų iš nevalstybinių organizacijų, privačių juridinių ir fizinių asmenų gaunami elektroniniai dokumentai;

kompiuterio skaitomas elektroninis dokumentas (toliau **– Elektroninis dokumentas**) – EDS elektroninis dokumentas arba elektroninio parašo kvalifikuoto sertifikato deklaracija;

kvalifikuotas sertifikatas – sertifikatas, kurį sudarė sertifikavimo paslaugų teikėjas, atitinkantis Reikalavimus kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, patvirtintus Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108, ir įregistruotas Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos, patvirtintos Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108, nustatyta tvarka, arba Europos Sąjungos valstybės sertifikavimo paslaugų teikėjas, turintis Europos Sąjungos valstybės narės teisės aktų suteiktą kvalifikuoto sertifikavimo paslaugų teikėjo statusą. Šiame sertifikate yra duomenys nurodyti Lietuvos

Respublikos elektroninio parašo įstatyme;

kvalifikuotas elektroninis parašas – saugus elektroninis parašas, sudarytas saugia parašo formavimo įranga ir patvirtintas galiojančiu kvalifikuotu sertifikatu;

laiko žymų tarnyba (angl. *Time Stamping Authorities*) – tarnyba, kuri teikia laiko žymas kaip įrodymus, kad tam tikri duomenys (pvz., elektroninis parašas) jau egzistavo iki žymoje užfiksuoto laiko. Laiko žymos tarnybų veiklos procedūros ir naudojama įranga turi atitikti tarptautiniame standarte ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“ nustatytus reikalavimus;

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 įvardytos elektroniniu parašu pasirašytame elektroniniame dokumente arba patvirtintos elektroninių dokumentų naudojimą reglamentuojančiuose teisės aktuose ir nurodytos XAdES-EPES formato elektroniniame paraše elementu <*SignaturePolicyIdentifier*>, kurio viduje yra elementas <*SignaturePolicyImplied*>;

OCSP – Operatyvus sertifikato statuso protokolas (angl. *On – line Certificate Status Protocol*);

pagalbinių sertifikavimo paslaugų teikėjas – sertifikavimo paslaugų teikėjas, teikiantis sertifikavimo paslaugas, susijusias su elektroninio parašo naudojimu, išskyrus pagrindines sertifikavimo paslaugas. Pagalbinių sertifikavimo paslaugų teikėjas gali tikrinti fiziniam ar juridiniam asmeniui adresuotų pasirašytų elektroninių dokumentų elektroninius parašus, vadovaudamasis tarp asmens, kuriam yra adresuoti pasirašyti elektroniniai dokumentai, ir sertifikavimo paslaugų teikėjo sudaryta sutartimi;

parašo pirminis tikrinimas – elektroninio parašo galiojimo tikrinimas ir parengimas ilgalaikiam saugojimui, taip suteikiant galimybę ateityje patikrinti elektroninio parašo galiojimą nesikreipiant į viešųjų raktų infrastruktūrą;

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 ir visų sekos sertifikatų atšaukimo laikotarpiui, skaičiuojant nuo elektroninio parašo laiko žymoje nurodyto laiko momento, ir susidedantis iš kvalifikuoto sertifikato galiojimo antrojo tikrinimo, nuorodų į sertifikavimo seką bei atšaukimo duomenų išsaugojimo XAdES-C formato paraše, laiko žymos šiam formatui uždėjimo ir sertifikavimo sekos bei šios sekos sertifikatų atšaukimo duomenų išsaugojimo XAdES-X-L formato elektroniniame paraše;

patikima laiko žymų tarnyba – laiko žymų tarnyba, atitinkanti tarptautinio standarto LST ETSI TS 102 023 v1.2.1:2007 keliamus reikalavimus ir įtraukta į patikimų sertifikavimo paslaugų teikėjų sąrašą, esantį tinklalapyje adresu *https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml,* arba laiko žymų tarnyba, kuria elektroninio parašo tikrintojas pasitiki;

patikimas sertifikatas – patikimo sertifikavimo centro sudarytas kvalifikuotas sertifikatas;

patikimas sertifikavimo centras – sertifikavimo paslaugų teikėjas, sudarantis kvalifikuotus sertifikatus ir įtrauktas į patikimų sertifikavimo paslaugų teikėjų sąrašą, *https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml*;

saugus elektroninis parašas – elektroninis parašas, pasižymintis saugaus elektroninio parašo savybėmis, kaip apibrėžta Lietuvos Respublikos elektroninio parašo įstatyme, ir yra sukurtas priemonėmis, tenkinančiomis standarto LST CWA 14170:2005 „Reikalavimai,

keliami parašo formavimo taikomosioms sistemoms“ reikalavimus;

saugi parašo formavimo įranga – elektroninio parašo formavimo įranga, kuri atitinka šiuos reikalavimus:

1) parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, praktiškai įmanoma gauti tik vienintelį kartą ir užtikrinamas jų slaptumas;

2) parašo formavimo duomenų, naudojamų elektroniniam parašui sukurti, atkurti praktiškai neįmanoma ir nuo elektroninio parašo klastočių apsaugo esamos technologijos;

3) parašo formavimo duomenis, naudojamus elektroniniam parašui sukurti, pasirašantis asmuo gali patikimai apsaugoti nuo kitų asmenų;

4) parašo formavimo įranga, kuriant elektroninį parašą, nekeičia pasirašomų duomenų;

5) tenkina standarto LST CWA 14169 „Saugi parašo formavimo įranga „EAL4+“ arba aukštesnius įvertinimo užtikrinimo lygio reikalavimus;

sertifikato galiojimo antrasis tikrinimas – elektroninio dokumento parašą patvirtinančio kvalifikuoto sertifikato ir sertifikatų sekos galiojimo tikrinimas, atliekamas pasibaigus kvalifikuoto sertifikato ir visų sekos sertifikatų paskelbimo negaliojančiais terminui, skaičiuojant nuo parašo laiko žymoje nurodyto laiko momento;

sertifikato galiojimo pirmasis tikrinimas – elektroninio dokumento parašą patvirtinančio kvalifikuoto sertifikato ir sertifikavimo sekos galiojimo tikrinimas, atliekamas nedelsiant, gavus pasirašytą elektroninį dokumentą ir suformavus gauto parašo laiko žymą;

sertifikato įspėjamasis laikotarpis – elektroninio dokumento parašą patvirtinančio kvalifikuoto sertifikato ir visų sertifikavimo sekos sertifikatų, įskaitant laiko žymų tarnybos sertifikavimo sekos sertifikatus, maksimalus sertifikato paskelbimo negaliojančiu laikotarpis;

sertifikato paskelbimo negaliojančiu terminas (angl. *grace period*) – laikotarpis, skirtas pasirašančiam asmeniui ar kitiems teisės aktų numatytiems asmenims kreiptis į kvalifikuotus sertifikatus sudarantį sertifikavimo paslaugų teikėją paskelbti duomenis apie kvalifikuoto sertifikato galiojimo nutraukimą arba sustabdymą. Terminas pradedamas skaičiuoti nuo kreipimosi momento ir apima laikotarpį, reikalingą kvalifikuotus sertifikatus sudarančiam sertifikavimo paslaugų teikėjui išnagrinėti kreipimąsi, priimti sprendimą ir paskelbti duomenis apie kvalifikuoto sertifikato galiojimo nutraukimą arba sustabdymą. Sertifikato galiojimo atšaukimo laikotarpis nurodytas asmens kvalifikuoto sertifikato taisyklėse. Kvalifikuoto sertifikato taisyklėse nesant nurodytam kvalifikuoto sertifikatų atšaukimo laikotarpiui, laikoma, kad kvalifikuotų sertifikatų galiojimo atšaukimo laikotarpis yra lygus nuliui;

sertifikatų seka – pasirašančiojo asmens parašą patvirtinančių sertifikatų rinkinys, susidedantis iš pasirašančiojo asmens sertifikato, jį sudariusio ir pasirašiusio paslaugų teikėjo sertifikato ir kitų (jei yra) tokiu būdu susijusių paslaugų teikėjų sertifikatų, pasibaigiantis patikimu arba šakniniu paslaugų teikėjo sertifikatu;

sertifikavimo paslaugų teikėjas – įmonė, juridinis asmuo, sudarantis sertifikatus arba teikiantis kitas paslaugas, susijusias su elektroniniu parašu;

šakninis sertifikatas – pats save patvirtinantis sertifikatas, kuris gali būti patikrintas jame nurodytu viešuoju raktu.

TPĮ – Taikomoji programinė įranga;

TSL – Europos Sąjungos patikimų sertifikavimo paslaugų teikėjų sąrašas;

Viešųjų raktų infrastruktūra (angl. *Public Key Infrastructure – PKI*) – techninės, programinės įrangos, žmonių ir procedūrų visuma, kuri naudojama saugoti, kurti, valdyti, suteikti, atnaujinti sertifikatus viešųjų raktų kriptografijos metodais;

XAdES – elektroninio parašo aprašymo XML struktūra standartas LST ETSI TS 101 903 V1.4.1:2009 „Patobulintieji XML elektroniniai parašai (XAdES)“ (toliau – XadES standartas);

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

XAdES-C – elektroninio parašo su visomis tikrumo duomenų nuorodomis formatas,

aprašytas vadovaujantis XAdES standartu;

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

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

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

XAdES-X-L – ilgalaikio saugojimo elektroninio parašo formatas, aprašytas vadovaujantis XAdES standartu;

XSLT – Plečiamos stilių lentelių kalbos transformacijos (angl. *Extensible Stylesheet Language Transformations*);

XML – pasaulinio tinklo konsorciumo (angl. *The Worl Wide Web Consortium, W3C*) rekomenduojama bendrosios paskirties duomenų struktūra ir jų turinio aprašomoji kalba (angl. *eXtensible Markup Language*);

XMLDSIG – pasaulinio tinklo konsorciumo (angl. *The Worl Wide Web Consortium, W3C*) rekomenduojamas elektroninio parašo aprašymas naudojant XML struktūrą.

II. KOMPIUTERIO SKAITOMŲ ELEKTRONINIŲ DOKUMENTŲ KVALIFIKUOTŲ ELEKTRONINIŲ PARAŠŲ KŪRIMAS

5. Elektroninių dokumentų kvalifikuotų elektroninių parašų kūrimas apima mokesčių mokėtojus, mokesčių administratorių ir sertifikavimo paslaugų teikėjus.

6. Pasirašymo objektas yra turinio duomenys, sudarantys pagrindinio dokumento vieną FFData formato rinkmeną arba vieną XML formato pagrindinę rinkmeną ir XSLT formato priedą, bei elektroninio dokumento metaduomenys. Pagrindinio dokumento ir jo metaduomenų duomenų objektai pasirašomi vienu elektroniniu parašu.

7. Elektroninių dokumentų pasirašymui kvalifikuotu elektroniniu parašu mokesčių mokėtojas, kreipdamasis į bet kurio Europos Sąjungos kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjo registravimo tarnybą, turi įsigyti elektroninio parašo kvalifikuotą sertifikatą bei saugią parašo formavimo įrangą stacionariame arba mobiliajame įrenginyje.

8. EDS elektroninių dokumentų kvalifikuotų elektroninių parašų kūrimas apima pasiekiamos per interneto naršyklę EDS elektroninio parašo TPĮ, arba mokesčių mokėtojų lokalių pasirašymo priemonių, integruotų su ABBYY eFormFiller, EDS elektroniniams dokumentams kurti panaudojimą.

REIKALAVIMAI SAUGIA PARAŠO FORMAVIMO ĮRANGA PASIRAŠOMIEMS ELEKTRONINIAMS DOKUMENTAMS

9. EDS elektroninis dokumentas turi būti kvalifikuotu elektroniniu parašu pasirašytas kompiuterio skaitomas elektroninis dokumentas, atitinkantis Elektroniniu parašu pasirašyto kompiuterio skaitomo elektroninio dokumento specifikacijos MDOC-V1.0, patvirtintos Lietuvos archyvų departamento prie Lietuvos Respublikos Vyriausybės generalinio direktoriaus 2010 m. rugpjūčio 25 d. įsakymu Nr. V-42 (Žin., 2010, Nr.102-5321; toliau – MDOC-V1.0 specifikacija) reikalavimus bei turintis pagrindinę FFData formato turinio rinkmeną ir neturintis priedų.

10. Sertifikato deklaracija turi būti kvalifikuotu elektroniniu parašu pasirašytas kompiuterio skaitomas elektroninis dokumentas, atitinkantis MDOC-V1.0 specifikacijos reikalavimus bei turintis pagrindinę XML formato turinio rinkmeną, taip pat turintis vieną XSLT transformacijų (angl. *XSLT Transformations*) formato priedą.

Elektroninių dokumentų pasirašymo saugia parašo formavimo įranga būdai

11. Elektroninių dokumentų pasirašymui kvalifikuotu elektroniniu parašu gali būti naudojama saugi stacionari arba mobili kvalifikuoto elektroninio parašo formavimo įranga.

Pasirašymas stacionaria saugia parašo formavimo įranga

12. Stacionari saugi parašo formavimo įranga, esanti pasirašančiojo asmens disponuojamo kompiuterio išoriniame įrenginyje ir naudojama elektroninių dokumentų pasirašymui, turi atitikti standarto CWA 14169:2009 „Secure Signature-Creation Devices „EAL 4+“ reikalavimus.

13. EDS elektroninių dokumentų pasirašymas stacionaria saugia parašo formavimo įranga pagal pasirašančio asmens pasirinkimą gali būti atliekamas EDS TPĮ arba bet kurioje kitoje saugioje elektroninio parašo TPĮ.

14. Sertifikatų deklaracijų pasirašymas stacionaria saugia parašo formavimo įranga gali būti atliekamas tik EDS TPĮ.

15. Konkrečiu atveju leistiną stacionarią saugaus parašo formavimo įrangą nustato atitinkama elektroninio parašo TPĮ.

Pasirašymas mobiliąja saugia parašo formavimo įranga

16. Mobilioji saugi parašo formavimo įranga, esanti pasirašančiojo asmens disponuojamame mobiliajame telefone ir naudojama elektroninių dokumentų pasirašymui, turi atitikti standarto CWA 14169:2009 „Secure Signature-Creation Devices „EAL 4+“ reikalavimus.

17. Pasirašant mobilia saugia parašo formavimo įranga, yra reikalingos pagalbinių sertifikavimo paslaugų teikėjo paslaugos sertifikatui, kuriuo patvirtinamas elektroninis parašas, pateikti, pasirašomų duomenų santraukai saugiai perduoti į mobiliąją saugią parašo formavimo įrangą ir santraukai, užšifruotai pasirašančiojo asmens privačiu raktu, priimti.

18. Pasirašymo proceso saugumui užtikrinti saugi elektroninio parašo TPĮ turi vizualizuoti jos sudarytą pasirašomą santrauką arba jos kodą ir prieš pasirašymą ta pati santrauka arba jos trumpinys turi būti vizualizuojami pasirašančiojo asmens disponuojamame mobiliajame telefone, turinčiame mobiliąją saugią parašo formavimo įrangą.

19. Mokesčių mokėtojų elektroninių dokumentų pasirašymas mobiliąja saugia parašo formavimo įranga pagal pasirašančiojo asmens pasirinkimą gali būti atliekamas EDS TPĮ ar bet kurioje kitoje saugioje elektroninio parašo TPĮ.

20. Sertifikatų deklaracijų pasirašymas mobiliąja saugia parašo formavimo įranga gali būti atliekamas tik EDS TPĮ.

21. Konkrečiu atveju leistiną mobilią saugaus parašo formavimo įrangą nustato atitinkama elektroninio parašo TPĮ.

Kompiuterio skaitomų elektroninių dokumentų sudarymo ir pasirašymo priemonės

22. Pasirašantis asmuo gali parengti, pasirašyti ir pateikti EDS elektroninį dokumentą panaudodamas pasiekiamą per naršyklę EDS elektroninio parašo TPĮ, lokalias pasirašymo priemones, integruotas su ABBYY eFormFiller arba kitas mokesčių mokėtojo pasirinktas priemones, tenkinančias šio poskyrio punktų reikalavimus.

23. EDS elektroninis dokumentas turi atitikti MDOC-V1.0 specifikacijos reikalavimus bei turėti pagrindinę FFData formato turinio rinkmeną ir neturėti priedų.

24. EDS elektroniniam dokumentui naudojama elektroninio parašo TPĮ turi suteikti privalomus GGeDOC grupės dokumento metaduomenis. Šių metaduomenų rinkmenomis turi būti papildoma pasirašyto elektroninio dokumento pakuotė.

25. Elektroninio parašo TPĮ turi tenkinti standarto CWA 14170:2004 reikalavimus

saugioms parašo formavimo taikomosioms sistemoms.

26. Elektroninio parašo TPĮ turi saugiai vizualizuoti pasirašomus kompiuterio skaitomų elektroninių dokumentų duomenis, atvaizduojant juos atitinkamoje dokumento formoje, naudojamo pasirašymui sertifikato duomenis bei elektroninio dokumento metaduomenis.

III. ELEKTRONINIO PARAŠO TIKRINIMAS IR PARENGIMAS ILGALAIKIAM SAUGOJIMUI

Elektroninio parašo tikrinimas

27. Kvalifikuoto elektroninio parašo tikrinimas per visą gyvavimo laiką apima elektroninio dokumento pakuotės tikrinimą, elektroninio parašo pirminį tikrinimą ir elektroninio parašo vėlesnius tikrinimus.

28. Elektroninių dokumentų kvalifikuoto elektroninio parašo tikrinimą atlieka mokesčių administratorius. Tikrinimo objektas yra pasirašytų elektroninių dokumentų elektroniniai parašai, esantys elektroninio dokumento pakuotėje, parengtoje pagal Parašo taisyklių V skyriuje „Kompiuterio skaitomo elektroninio dokumento pakuotės formatas“ nustatytus reikalavimus.

29. Elektroninio dokumento pakuotės tikrinimo paskirtis yra nustatyti aiškiai klaidingas pakuotes ir apie tai informuoti elektroninius dokumentus pateikusius mokesčių mokėtojus. Esant klaidų, pateikto elektroninio dokumento apdorojimas yra nutraukiamas, apie tai informuojamas juos pateikęs mokesčių mokėtojas.

30. Siekiant supaprastinti pasirašymo elektroniniu parašu procesą ir operatyviai gauti sertifikavimo paslaugų teikėjo patvirtintą laiko momentą, iki kurio pasirašančio asmens parašas buvo sukurtas, mokesčių administratorius inicijuoja pateikto pasirašyto elektroninio dokumento patikrinimo procesą ir gauna sertifikavimo paslaugų teikėjo patvirtintą laiko žymą ne vėliau kaip per 1 valandą nuo elektroninio dokumento pateikimo momento, užfiksuoto EDS. Esant EDS, tinklo ar aptarnaujančių sistemų sutrikimams, sertifikavimo paslaugų teikėjo laiko žymos gavimas gali būti inicijuojamas ir vėliau nei per 1 valandą nuo dokumento pateikimo momento, užfiksuoto EDS.

Elektroninio parašo pirminis tikrinimas

31. Elektroninio parašo pirminis tikrinimas apima patį elektroninio parašo tikrinimą ir elektroninio parašo parengimą ilgalaikiam saugojimui:

31.1. Elektroninio parašo pirminis tikrinimas susideda iš elektroninio parašo pirminio tikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos ir elektroninio parašo pirminio tikrinimo pasibaigus sertifikato galiojimo atšaukimo laikotarpiui.

31.2. Sertifikato galiojimo tikrinimas gali būti baigtas tik praėjus pasirašančio asmens kvalifikuoto sertifikato taisyklėse arba sertifikavimo veiklos nuostatuose nurodytam sertifikato galiojimo paskelbimo negaliojančiu laikotarpiui nuo laiko žymoje nurodyto laiko, iki kurio buvo sudarytas elektroninio dokumento kvalifikuotas elektroninis parašas.

31.3. Elektroninio parašo pirminio tikrinimo eigoje pasirašančio asmens pateiktas XAdES-EPES formato elektroninis parašas papildomas iki XAdES-X-L formato parašo, skirto ilgalaikiam saugojimui, pereinant XAdES-T, XAdES-C, XAdES-X, XAdES-X-L formatų parašo formavimo etapus.

Elektroninio parašo pirminis tikrinimas iki sertifikato galiojimo atšaukimo laikotarpio pabaigos

31.4. Elektroninio parašo pirminis tikrinimas iki sertifikato galiojimo atšaukimo laikotarpio pabaigos apima elektroninio parašo formato patikrinimą, laiko žymos

suformavimą ir sertifikato galiojimo pirmąjį patikrinimą.

31.5. Elektroninio parašo pirminio tikrinimo paskirtis yra nustatyti tinkamu pakuotės formatu pateikto pasirašyto elektroninio dokumento autentiškumą uždedant laiko žymų paslaugų teikėjo, atitinkančio standarto ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“ reikalavimus, sudarytą laiko žymą.

31.6. Laiko žymos suformavimu mokesčių mokėtojo pateiktas elektroninio dokumento pakuotėje XAdES-EPES formato parašas papildomas iki XAdES-T formato parašo. Ši laiko žyma nustato laiką, iki kurio yra suformuotas mokesčių mokėtojo elektroninio dokumento elektroninis parašas. Būtent šio laiko atžvilgiu yra tęsiamas elektroninio parašo pirminis tikrinimas pasibaigus sertifikato galiojimo atšaukimo laikotarpiui, nustatant pasirašančiojo asmens kvalifikuoto sertifikato galiojimą bei sertifikavimo sekos sertifikatų iki patikimo sertifikato, esančio patikimų sertifikatų saugykloje, galiojimą, arba iki šakninio sertifikato.

31.7. Suformavus laiko žymą, atliekamas pasirašančiojo asmens kvalifikuoto sertifikato, įskaitant visus sertifikavimo sekos sertifikatus, galiojimo pirmasis patikrinimas. Jeigu patikrinimo metu nustatoma, kad pasirašančio asmens sertifikatas negaliojantis, elektroninio dokumento tolesnis tikrinimas nutraukiamas.

31.8. Sertifikatų galiojimui tikrinti naudojamas OCSP protokolas sertifikatų statuso tikrinimui realiame laike, o nesant OCSP paslaugos, sertifikatų statusui nustatyti naudojama CRL informacija.

Elektroninio parašo pirminis tikrinimas pasibaigus sertifikato galiojimo atšaukimo laikotarpiui

31.9. Elektroninio parašo pirminis tikrinimas pasibaigus sertifikato galiojimo atšaukimo laikotarpiui, o tiksliau apibūdinant – pasibaigus sertifikato įspėjamajam laikotarpiui, yra skirtas įsitikinti, ar pasirašantis asmuo tikrai pasirašė elektroninį dokumentą jo kvalifikuoto sertifikato galiojimo laikotarpiu, tai yra, ar per leistiną sertifikato galiojimo atšaukimo laikotarpį nėra gauta naujų duomenų apie pasirašančiojo asmens sertifikato ir sertifikavimo sekos sertifikatų atšaukimą anksčiau negu parašo pirmojo tikrinimo etape nurodyta laiko žymos data.

31.10. Pasibaigus pasirašančiojo asmens sertifikato galiojimo atšaukimo laikotarpiui, atliekamas pasirašančiojo asmens kvalifikuoto sertifikato, įskaitant visus sertifikavimo sekos sertifikatus, galiojimo antrasis patikrinimas. Jei pasirašančiojo asmens sertifikato ar sertifikavimo sekos sertifikatų atšaukimas įvyko anksčiau negu parašo pirmojo tikrinimo etape nurodyta laiko žymos data, parašas laikomas negaliojančiu ir apie tai informuojamas pasirašantysis asmuo.

31.11. Sertifikato galiojimo antrojo patikrinimo metu tikrintų sertifikavimo sekos sertifikatų ir jų patikrinimo statuso nuorodos ir nurodomų duomenų santraukos yra išsaugomos elektroninio parašo formate suformuojant XAdES-C formato duomenis. Taip pat atliekamas laiko žymos tarnybos sertifikato ir jo sertifikavimo sekos sertifikatų galiojimo patikrinimas.

31.12. Elektroninio parašo pirminis tikrinimas suformavus XAdES-C formato duomenis tęsiamas sukaupiant ir papildant elektroninį parašą duomenimis, leidžiančiais patikrinti elektroninio parašo galiojimą, nesikreipiant į viešųjų raktų infrastruktūrą.

31.13. Po elektroninio parašo pirminio patikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos elektroninio dokumento apdorojimas tęsiamas, nelaukiant sertifikato galiojimo galutinio patikrinimo rezultatų. Elektroninio parašo pirminio tikrinimo metu nustačius sertifikatą esant negaliojantį, elektroninis dokumentas EDS pažymimas kaip negaliojantis.

31.14. Elektroninio parašo parengimas ilgalaikiam saugojimui yra elektroninio parašo pirminio tikrinimo proceso dalis ir apima duomenų apie sertifikatų galiojimą surinkimą ir išsaugojimą, siekiant elektroninio parašo vėlesnio tikrinimo metu užtikrinti elektroninio

parašo galiojimo įrodymus, nesikreipiant į sertifikavimo paslaugų teikėjus. Elektroninio parašo parengimas ilgalaikiam saugojimui susideda iš laiko žymos uždėjimo XAdES-C formato duomenims, tokiu būdu suformuojant XAdES-X pirmo tipo formato elektroninį parašą ir sertifikatų bei jų atšaukimo duomenų surinkimo ir išsaugojimo remiantis XAdES-C formato duomenyse esančiomis nuorodomis, tuo pačiu suformuojant XAdES-X-L formato elektroninį parašą.

Elektroninio parašo vėlesni tikrinimai

32. Elektroninio parašo vėlesni tikrinimai apima elektroninio parašo galiojimo tikrinimą elektroninio dokumento saugojimo laikotarpiu

IV. ELEKTRONINIO PARAŠO TIKRUMO NUSTATYMO TAISYKLĖS

Sertifikavimo sekos sudarymo ir tikrinimo taisyklės

33. Patikimais kvalifikuotais sertifikatais yra laikomi sertifikatai, sudaryti Europos Sąjungos šalių kvalifikuotų sertifikavimo paslaugų teikėjų, įregistruotų ir paskelbtų atitinkamos šalies elektroninio parašo priežiūros institucijoje pagal 1999 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvą 1999/93/EB dėl Bendrijos elektroninių parašų reguliavimo sistemos (OL 2000 L 013, p. 0012–0020) ir nacionalinius elektroninių parašų teisės aktus bei įtraukti į EDS patikimų sertifikavimo paslaugų teikėjų sertifikatų duomenų bazę.

34. Elektroniniai dokumentai, kurių parašai yra patvirtinti sertifikatais, neįtrauktais į Patikimų sertifikavimo paslaugų teikėjų sertifikatų duomenų bazę, nėra priimami.

35. Informacija apie Lietuvos Respublikos prižiūrimų ir/ar akredituotų Sertifikavimo paslaugų teikėjus skelbiama Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos interneto svetainėje adresu http://epp.ivpk.lt/lt/TSL/. Informacija apie Europos Sąjungos patikimus sertifikavimo paslaugų teikėjus, įskaitant laiko žymų paslaugų teikėjus, yra skelbiama adresu https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml.

36. EDS patikimų sertifikavimo paslaugų teikėjų sertifikatų duomenų bazė sudaroma pagal Europos Sąjungos patikimų sertifikavimo paslaugų teikėjų sąrašą TSL.

37. Sertifikato galiojimo patikrinimas apima visos sertifikatų sekos sertifikatų galiojimo patikrinimą:

37.1. Sertifikatų seka susideda iš vieno elemento – pasirašančio asmens kvalifikuotą sertifikatą patvirtinusio kvalifikuotų sertifikavimo paslaugų teikėjo sertifikato, įtraukto į patikimų sertifikatų saugyklą.

37.2. Sertifikavimo sekos sudaromos laiko žymų tarnybos sertifikatų, OCSP atsakymus patvirtinusių sertifikatų ir CRL sąrašus patvirtinusių sertifikatų galiojimo patikrinimui.

Kvalifikuotų sertifikatų galiojimo tikrinimo tvarka

38. Kvalifikuotas sertifikatas galioja sertifikate nurodytu galiojimo laikotarpiu, jeigu sertifikato galiojimas nėra atšauktas.

39. Kvalifikuotas sertifikatas, kuriuo yra patvirtintas tikrinamas elektroninis parašas, negalioja, jeigu kreipimosi atšaukti sertifikato galiojimą laikas yra ankstesnis už elektroninio parašo laiko žymoje nurodytą laiką.

40. Kvalifikuoto sertifikato galiojimo tikrinimas apima du etapus: kvalifikuoto sertifikato galiojimo pirmasis patikrinimas ir laiko žymos uždėjimas ir kvalifikuoto sertifikato galiojimo antrasis patikrinimas ir ilgalaikio saugojimo elektroninio parašo formato sudarymas:

40.1. Kvalifikuoto sertifikato galiojimo pirmasis patikrinimas turi būti atliekamas iš karto po kvalifikuoto elektroninio parašo laiko žymos uždėjimo, siekiant nustatyti, ar sertifikatas nėra atšauktas.

40.2. Kvalifikuoto sertifikato galiojimo pirmojo patikrinimo metu sertifikato galiojimo faktas negali būti patvirtintas. Kvalifikuoto sertifikato galiojimas, atšaukimas arba sustabdymas yra nustatomas kvalifikuoto sertifikato galiojimo antrojo patikrinimo metu, kuris yra atliekamas praėjus kvalifikuoto sertifikato galiojimo atšaukimo paskelbimo laikotarpiui bei sertifikato įspėjamajam laikotarpiui po kvalifikuoto elektroninio parašo laiko žymos uždėjimo.

40.3. Kvalifikuoto sertifikato galiojimo patikrinimo tvarka formuluojama atliktų parašo tikrinimo veiksmų laiko momentų atžvilgiu nepriklausomai nuo kvalifikuoto elektroninio parašo sudarymo faktinio laiko momento. Mokesčių administratorius atlieka pateiktos pasirašytos elektroninio dokumento pakuotės, metaduomenų bei parašo formato patikrinimą ir uždeda laiko žymą laiko momentu t_2. Mokesčių administratorius atlieka kvalifikuoto sertifikato galiojimo pirmąjį patikrinimą po laiko momento t_2. Jeigu pirmojo patikrinimo metu nustatoma, kad kvalifikuoto sertifikato galiojimas yra atšauktas arba sustabdytas ir kvalifikuoto sertifikato galiojimo atšaukimo laikas t, kuris yra prilyginamas kreipimosi į sertifikavimo paslaugų teikėją atšaukti arba sustabdyti kvalifikuoto sertifikato galiojimą laikui, yra mažesnis už t_2, t. y. $t < t_2$“ tai laikoma, kad parašas yra patvirtintas negaliojančiu kvalifikuotu sertifikatu, t. y. pats parašas yra negaliojantis.

40.4. Jeigu kvalifikuoto sertifikato galiojimo atšaukimo laikas t yra didesnis arba lygus t_2, t. y. t ? t_2, tai parašo pirminio tikrinimo procesas yra tęsiamas.

40.5. Jeigu pirmojo patikrinimo metu nėra duomenų apie kvalifikuoto sertifikato atšaukimą arba sustabdymą, yra tęsiamas parašo pirminio tikrinimo procesas.

40.6. Parašo taisyklės nustato, kad kvalifikuoto sertifikato atšaukimo laikotarpiu laikomas pasirašančio asmens kvalifikuoto sertifikato taisyklėse nurodytas sertifikato atšaukimo laikotarpis c. Kvalifikuoto sertifikato taisyklėse nesant nurodytam kvalifikuoto sertifikato atšaukimo laikotarpiui, laikoma, kad kvalifikuoto sertifikato galiojimo atšaukimo laikotarpis yra lygus nuliui.

40.7. Kvalifikuoto sertifikato galiojimo antrasis patikrinimas turi būti atliktas praėjus sertifikato paskelbimo negaliojančiu laikotarpiui ir sertifikato įspėjamajam laikotarpiui C, skaičiuojant nuo kvalifikuoto elektroninio parašo laiko žymos sukūrimo laiko t_2, t. y. kvalifikuoto sertifikato galiojimo antrasis patikrinimas turi būti atliktas laiko momentu $t_4 > t_3$, kur $t_3 = t_2 + C$. Tokiu būdu užtikrinama, kad kvalifikuoto sertifikato galiojimo antrojo patikrinimo metu bus gauta teisinga informacija apie sertifikatus, kurių atšaukimas įvyko prieš laiko žymos sukūrimą, o vėlesnis sertifikatų atšaukimas neįtakoja tikrinimo rezultatų. OCSP protokolas pateikia įrodymus, kad kvalifikuoto sertifikato galiojimo antrasis patikrinimas buvo atliktas tam tikru laiku, pagal kurį galima nustatyti, kad tikrinimas atliktas pasibaigus kvalifikuoto sertifikato galiojimo atšaukimo laikotarpiui.

40.8. Jeigu tikrinimo momentu t_4 nėra informacijos apie kvalifikuoto sertifikato galiojimo atšaukimą, tai laikoma, kad kvalifikuotas sertifikatas yra galiojantis ir juo pagrįstas kvalifikuotas elektroninis parašas yra galiojantis.

40.9. Jeigu tikrinimo momentu t_4 kvalifikuoto sertifikato galiojimo atšaukimas yra paskelbtas, tai kvalifikuoto elektroninio parašo, patvirtinto tokiu kvalifikuotu sertifikatu, galiojimas ar negaliojimas priklauso nuo kreipimosi atšaukti kvalifikuotą sertifikatą laiko t. Jeigu t yra daugiau arba lygu t_2, tai kvalifikuotas elektroninis parašas yra galiojantis. Jeigu kreipimosi atšaukti kvalifikuotą sertifikatą laiko momentas t yra ankstesnis negu elektroninio parašo laiko žymoje nurodytas laiko momentas t_2, t. y. jeigu $t < t_2$, tai kvalifikuotas elektroninis parašas, patvirtintas tokiu kvalifikuotu sertifikatu yra negaliojantis. Kvalifikuoto sertifikato galiojimo tikrinimo laiką, kvalifikuoto sertifikato galiojimo statusą tikrinimo metu ir kreipimosi atšaukti kvalifikuotą sertifikatą laiką kvalifikuoto sertifikato negaliojimo atveju pateikia OCSP protokolo tinklinė paslauga.

Laiko žymos naudojimo taisyklės

41. Kvalifikuoto elektroninio parašo laiko žymą gali uždėti tik patikimos laiko žymos tarnybos.

42. Laiko žymos galiojimą patvirtinančio sertifikavimo sekos galiojimo patikrinimui naudojamas laiko žymų tarnybos sertifikatas iš patikimų sertifikatų sąrašo.

43. Elektroninio dokumento kvalifikuoto elektroninio parašo laiko žymą mokesčių administratorius pirmą kartą uždeda elektroninio parašo pirminio tikrinimo pradžioje, suformuojant XAdES-T formato elektroninį parašą. Antrą kartą laiko žyma yra uždedama suformavus XAdES-C formato duomenis, kuriuose išsaugomos nuorodos į pasirašančio asmens sertifikavimo sekos galiojimo informaciją, ir tokiu būdu eigoje sudarant XAdES-X formato parašą.

Pasirašančio asmens pateikiami kvalifikuoto elektroninio parašo tikrumo duomenys

44. Mokesčių mokėtojo pateikto elektroninio dokumento kvalifikuoto elektroninio parašo formatas yra XAdES [ETSI TS 101 903] standarte apibrėžtas XAdES-EPES formato elektroninis parašas, nurodantis neišreikštinių Parašo taisyklių taikymą.

45. Mokesčių administratorius priima tik XAdES standarte apibrėžtą XAdES-EPES formato elektroninį parašą ir nepriima parašų, kuriuose yra naudojami elementai, skirti tik aukštesniems formatų tipams (XAdES-T, XAdES-C, XAdES-X, XAdES-X-L, XAdES-A).

46. Mokesčių administratorius priima tik tokius XAdES-EPES formato elektroninius parašus, į kuriuos yra įtrauktas kvalifikuotas sertifikatas bei tenkinami kiti reikalavimai, nurodyti Parašo taisyklių 50 p.

Tikrinančio asmens surenkami kvalifikuoto elektroninio parašo tikrumo duomenys

47. Mokesčių administratorius užtikrina mokesčių mokėtojo pateikto elektroninio dokumento kvalifikuoto elektroninio parašo ilgalaikį saugojimą. Mokesčių administratorius surenka ir išsaugo ilgalaikiam saugojimui skirtuose XAdES-X-L formato parašuose parašo tikrumo duomenis, įgalinančius patikrinti parašo galiojimą nepriklausomai nuo viešųjų raktų (sertifikatų) infrastruktūros pagal XAdES [ETSI TS 101 903] standarto reikalavimus:

47.1. Parašo laiko žymos elementas: SignatureTimeStamp (XAdES-T formato parašas), įrodantis, kad pasirašančio asmens kvalifikuotas parašas yra sukurtas iki šioje laiko žymoje nurodyto laiko;

47.2. Parašo nuorodų į sertifikavimo sekos sertifikatus ir jų atšaukimą elementai: CompleteCertificateRefs ir CompleteRevocationRefs (XAdES-C formato parašas), OCSP protokolo atveju įrodantys, kad sertifikavimo sekos galiojimo patikrinimas yra atliktas pasibaigus kvalifikuoto sertifikato negaliojimo paskelbimo laikotarpiui ir išsaugotos nuorodos į sertifikavimo sekos tikrinimo duomenis bei tų duomenų santraukos;

47.3. Parašo laiko žymos elementas: SigAndRefsTimeStamp (XAdES-X formato parašas), įrodantis XAdES-C formato parašo integralumą ir egzistavimą iki šioje laiko žymoje nurodyto laiko;

47.4. Parašo sertifikavimo sekos sertifikatų reikšmių ir sertifikavimo sekos sertifikatų atšaukimo reikšmių elementai: CertificateValues ir RevocationValues (XAdES-X-L formato parašas), saugantys XAdES-X-L formato paraše pateiktus duomenis ir įrodantys pasirašančio asmens kvalifikuoto sertifikato, panaudoto fizinio asmens kvalifikuoto elektroninio parašo sukūrimui, galiojimo statusą.

V. KOMPIUTERIO SKAITOMO ELEKTRONINIO DOKUMENTO PAKUOTĖS FORMATAS

Priimamo elektroninio dokumento pakuotės formatas

48. Priimamo elektroninio dokumento pakuotės rinkmena turi tenkinti MDOC-V1.0 specifikacijos reikalavimus pasirašytų kompiuterio skaitomų elektroninių dokumentų pakuotėms, esant tik FFData formato pagrindinės rinkmenos turiniui EDS elektroninių dokumentų ir XML formato pagrindinei rinkmenai ir XSLT formato priedui sertifikato deklaracijų atveju.

Elektroninio dokumento pakuotės formatas

49. Mokesčių mokėtojų EDS arba instaliuojamomis kompiuteryje lokaliomis pasirašymo priemonėmis, integruotomis su ABBYY eFormFiller, sukurto elektroninio dokumento pakuotės formatas turi tenkinti žemiau išdėstytus reikalavimus:

49.1. Pakuotė yra viena rinkmena su praplėtimu „mdoc“;

49.2. Pakuotės formatas yra ZIP;

49.3. Pakuotės šaknyje yra viena ir tik viena rinkmena – pagrindinio dokumento turinio FFData formato rinkmena mokesčių mokėtojo elektroninio dokumento atveju, arba XML formato pagrindinė rinkmena bei XSLT formato priedas sertifikato deklaracijos atveju;

49.4. Pakuotės šaknyje yra katalogas pavadinimu „metadata“, kurio viduje yra metaduomenų rinkmenos;

49.5. Pakuotės šaknyje yra katalogas pavadinimu „META-INF“:

49.5.1. Katalogo „META-INF“ viduje yra elektroninių parašų rinkmenos, grupuojamos į katalogą su pavadinimu „signatures“.

49.5.2. Katalogo „META-INF“ viduje yra pakuotės dalių tipų aprašo rinkmena pavadinimu „manifest.xml“, rengiama pagal ODF standarto reikalavimus.

49.5.3. Katalogo „META-INF“ viduje yra pakuotės dalių tarpusavio ryšių rinkmena pavadinimu „relations.xml“.

Elektroninio parašo formatas

50. Elektroninio dokumento parašo elementas turi tenkinti tokius reikalavimus:

50.1. Elektroninių parašų struktūra turi tenkinti reikalavimus, išdėstytus MDOC – V1.0 specifikacijos XAdES-EPES, XAdES-T ir XAdES-X-L formatams. Kitų formatų parašai neleistini;

50.2. Elektroninių parašų rinkmenose esantys parašo elementai (<*Signature*>) tikrinami pagal importuojamas XMLDSIG ir XAdES schemas;

50.3. Papildomai turi būti atliekamas MDOC–V1.0 specifikacijos elektroninių parašų elementų privalomumo bei apribojimų patikrinimas;

50.4. Gautas elektroninis dokumentas turi būti pasirašytas XAdES standarte aprašytu XAdES-EPES formato elektroniniu parašu elemente <Signature>;

50.5. Negalimi tokie elektroninio parašo atributai:

<AllDataObjectsTimeStamp>,
<IndividualDataObjectsTimeStamp>,
<CounterSignature>,
<SignatureTimeStamp>,
<CompleteCertificateRefs>,
<CompleteRevocationRefs>,
<AttributeCertificateRefs>,
<AttributeRevocationRefs>,
<SigAndRefsTimeStamp>,
<RefsOnlyTimeStamp>,
<CertificateValues>,

<RevocationValues>,

<ArchiveTimeStamp>.

50.6. Parašo elementas <Signature> neturi jokių aukštesniems XAdES formatams (XAdES-T, XAdES-C, XAdES-X, XAdES-X-L, XAdES-A) naudojamų elementų;

50.7. XAdES EPES formato paraše turi būti pasirašomas atributas – Parašo taisyklių identifikatorius (*SignaturePolicyIdentifier*), privalomas, tikrinimo metu yra tikrinama, ar elementas yra toks:

<SignaturePolicyIdentifier>

<SignaturePolicyImplied/>

</SignaturePolicyIdentifier>

50.8. Parašo elemente <SignedInfo> turi būti nuorodos kiekvienam pasirašomų duomenų objektui, įskaitant pasirašomus metaduomenis (elementai <Reference>):

a) į pasirašytus duomenis (elementą, kuriame pasirašyti duomenys yra saugomi);

b) į pasirašytus atributus (elementą <Object><QualifyingProperties><SignedProperties>).

50.9. Paraše naudojami algoritmai (transformavimo, kodavimo BASE64, kanonizavimo, santraukų sudarymo, pasirašymo) turi būti standartiniai, kad automatinėmis priemonėmis būtų įmanomas parašo patikrinimas;

50.10. Elektroninis dokumentas gali būti pasirašytas tik lygiagrečiuoju būdu, t. y. gaubiantis parašas (*„counter signature“*) yra neleistinas.

Metaduomenų formatas

51. Elektroninio dokumento metaduomenys turi tenkinti tokius reikalavimus:

51.1. elektroniniame dokumente yra visi MDOC-V1.0 specifikacijoje apibrėžti privalomi metaduomenys;

51.2. visi metaduomenys, kurie privalo būti pasirašyti pagal elektroninių dokumentų MDOC-v1.0 specifikacijos reikalavimus, turi būti pasirašyti;

51.3. sudaromų elektroninių dokumentų metaduomenys turi tenkinti MDOC-V1.0 specifikacijoje nurodytus GGeDOC grupės metaduomenų reikalavimus.

Leistini parašo sudarymo algoritmai

52. Elektroninių dokumentų kvalifikuotų parašų formavimui, patvirtinimui ir ilgalaikiam saugojimui gali būti naudojami šie algoritmai:

Algoritmas	Identifikatorius
Santraukos sudarymas (angl. „Digest“)	
SHA1	http://www.w3.org/2000/09/xmldsig#sha1
SHA256	http://www.w3.org/2001/04/xmlenc#sha256
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
RSAwithSHA256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Kanonizavimas (angl. „Canonicalization“)	
Canonical XML 1.0 (omits comments)	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Canonical XML 1.0 with Comments	http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
Transformavimas (angl. „Transform“)	

Algoritmas	Identifikatorius
XPath	http://www.w3.org/TR/1999/REC-xpath-19991116
Base64	http://www.w3.org/2000/09/xmldsig#base64