VALSTYBINIO SOCIALINIO DRAUDIMO FONDO VALDYBOS
PRIE SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS DIREKTORIAUS
Į S A K Y M A S

DĖL ELEKTRONINIŲ PRANEŠIMŲ KVALIFIKUOTO ELEKTRONINIO PARAŠO TAISYKLIŲ PATVIRTINIMO

2007 m. gruodžio 20 d. Nr. V-666
Vilnius

1. T v i r t i n u pridedamas Elektroninių pranešimų kvalifikuoto elektroninio parašo taisykles.

2. N u s t a t a u, kad šio įsakymo 1 punktas įsigalioja nuo 2008 m. sausio 1 d.

3. Į p a r e i g o j u:

3.1. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos (toliau vadinama – Fondo valdyba) Teisės skyrių šį įsakymą paskelbti leidinyje „Valstybės žinios“;

3.2. Fondo valdybos Komunikacijos skyrių paskelbti šį įsakymą Fondo valdybos interneto svetainėje;

3.3. Fondo valdybos Dokumentų tvarkymo skyrių šio įsakymo elektroninius nuorašus išsiųsti Fondo valdybos direktoriaus pavaduotojams, Fondo valdybos skyriams, Fondo valdybos Vidaus audito tarnybai, Fondo valdybos teritoriniams skyriams, kitoms Valstybinio socialinio draudimo fondo įstaigoms, susijusioms su Valstybinio socialinio draudimo fondo administravimu, bei įsakymo nuorašą išsiųsti Lietuvos Respublikos socialinės apsaugos ir darbo ministerijai.

4. P a v e d u Fondo valdybos direktoriaus pavaduotojui Mindaugui Strumskiui šio įsakymo vykdymo kontrolę.

DIREKTORIUS MINDAUGAS MIKAILA

PATVIRTINTA
Valstybinio socialinio draudimo fondo
valdybos prie Socialinės apsaugos ir darbo
ministerijos direktoriaus
2007 m. gruodžio 20 d. įsakymu Nr. V-666

ELEKTRONINIŲ PRANEŠIMŲ KVALIFIKUOTO ELEKTRONINIO PARAŠO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Šios Elektroninių pranešimų kvalifikuoto elektroninio parašo taisyklės (toliau vadinama Taisyklės) nustato Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos (toliau vadinama Fondo valdyba) elektroninių pranešimų kvalifikuoto elektroninio parašo sudarymo ir tikrinimo tvarką, asmenų, dalyvaujančių pasirašymo procese, teises ir pareigas, nurodo techninius standartus ir veiksmus, kurie turi būti atliekami kuriant ir tikrinant elektroninių pranešimų kvalifikuotą elektroninį parašą.

2. Draudėjai, naudodami jiems tinkamas instrumentines priemones, rengia, pasirašo ir per Elektroninę draudėjų aptarnavimo sistemą (toliau vadinama EDAS) teikia Fondo valdybos informacinei sistemai pasirašytus elektroninius pranešimus, kurie priimami, patikrinami, parengiami ilgalaikiam saugojimui bei išsaugomi.

3. Taisyklėmis turi vadovautis:

3.1. draudėjų vadovai arba jų įgalioti asmenys, disponuojantys kvalifikuotu sertifikatu ir pasirašantys elektroninius pranešimus kvalifikuotu elektroniniu parašu;

3.2. Fondo valdybos darbuotojai, atsakingi už elektroninių pranešimų kvalifikuoto elektroninio parašo tikrinimą ir parengimą ilgalaikiam saugojimui.

4. Taisyklių aktuali redakcija, taikoma konkrečiam elektroniniam pranešimui, nustatoma pagal to elektroninio pranešimo elektroninio parašo pirmojo tikrinimo etapo laiko žymoje nurodytą datą.

5. Aktuali šių Taisyklių redakcija skelbiama draudėjų portalo (http://draudejai.sodra.lt) viešojoje srityje.

6. Taisyklės parengtos vadovaujantis Lietuvos Respublikos elektroninio parašo įstatymu (Žin., 2000, Nr. 61-1827) bei kitais teisės aktais, Europos Sąjungos elektroninio parašo standartizavimo iniciatyvos dokumentais bei minimaliais techninių standartų reikalavimais, apibrėžiančiais pakankamas sąlygas, kurioms esant elektroninis parašas tenkina kvalifikuotam elektroniniam parašui keliamus reikalavimus, apibrėžtus standartuose:

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

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

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

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

6.5. RFC 3125 – Electronics Signature Policies;

6.6. CWA 14168 „Secure Signature-Creation Devices „EAL 4“;

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

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

6.9. ETSI TS 101 733 v1.5.1: „Electronics Signatures formats“;

6.10. ETSI TS 101 903 v1.3.2: „XML Advanced Electronics Signatures (XAdES)“;

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

6.12. ETSI TS 101 861 V1.2.1 „Time stamping profile“;

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

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

7. Taisyklėse vartojamos pagrindinės sąvokos:

Archyvinė laiko žyma – laiko žyma, suteikiama XAdES-X-L formato parašui ir papildanti jį iki XAdES-A formato parašo.

Draudėjas – juridinis asmuo, jo filialai ir atstovybės, taip pat fizinis asmuo, kurie įstatymų nustatyta tvarka privalo mokėti valstybinio socialinio draudimo įmokas.

Draudėjo vadovas – fizinis asmuo, kuris mokesčių mokėtojų registre nurodytas kaip juridinio asmens vadovas, arba draudėjas fizinis asmuo.

Draudėjų portalas – interneto svetainė, pasiekiama adresu http://draudejai.sodra.lt per naršykles *Microsoft Internet Explorer 5.5, Opera 7, Mozilla Firefox 1.4* ar šių naršyklių aukštesnes versijas. Draudėjų portalas yra EDAS sudedamoji dalis, atliekanti EDAS grafinės vartotojo sąsajos funkcijas.

FFData formatas – XML struktūroje aprašyti elektroninio pranešimo duomenys. Kiekvieno elektroninio pranešimo tipo ir versijos XML duomenų struktūra patvirtinama Fondo valdybos direktoriaus įsakymu.

El. parašo TkS – Elektroninio parašo formavimo taikomoji sistema, deklaruojanti standarto CWA 14170:2004 reikalavimų atitiktį.

Elektroninis pranešimas – Draudėjo elektroniniu būdu Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinei sistemai teritoriniams skyriams privalomai teikiama informacija apie apdraustuosius asmenis, pasirašyta kvalifikuotu elektroniniu parašu.

Elektroninio pranešimo konteineris (toliau vadinama – Konteineris) – byla, kurioje XML struktūroje aprašomi pasirašytas elektroninis pranešimas, elektroninio pranešimo elektroninis parašas ir elektroninio pranešimo metaduomenys. Elektroninio pranešimo konteinerio formatas detaliai aprašytas Taisyklių V skyriuje.

Galiojantis kvalifikuotas sertifikatas – kvalifikuotas sertifikatas, kurio galiojimo laikotarpį sudaro laiko intervalas, tenkinantis visus šiuos 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 nurodytam sertifikato atšaukimo laikotarpiui.

Kvalifikuotas sertifikatas – sertifikatas, kurį sudarė sertifikavimo paslaugų teikėjas, atitinkantis 2002 m. gruodžio 31 d. LR Vyriausybės nutarimu Nr. 2108 (Žin., 2003, Nr. 2-47) nustatytus „Reikalavimus kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams“ ir įregistruotas šiame nutarime nustatyta tvarka, arba Europos Sąjungos šalies sertifikavimo paslaugų teikėjas, kuriam suteiktas kvalifikuoto sertifikavimo paslaugų teikėjo statusas remiantis 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 žymų tarnyba (angl. „Time Stamp 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 standarte ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“ nustatytus reikalavimus

Laiko žyma (angl. „time stamp“) – duomenų egzistavimo iki nurodyto laiko momento įrodymas laiko žymos tarnybos pasirašytų saugiu elektroniniu parašu duomenų forma. Atitinkanti reikalavimus, išdėstytus standarte ETSI TS 101 861 V1.2.1 „Time stamping profile“.

Lizdinė laiko žyma – laiko žyma, suteikiama XAdES-A formato parašui ir išplečianti XAdES-A formato parašą.

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

Naudotojo programinė įranga – programinė įranga, leidžianti rengti elektroninius pranešimus atjungtame nuo interneto kompiuteryje (pvz., gamintojo ABBYY sukurta ir Fondo valdybos nemokamai platinama elektroninių pranešimų rengimo programinė įranga eFormFiller).

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

Pasirašantis asmuo – veiksnus fizinis asmuo, kuris turi parašo formavimo įrangą ir, veikdamas savo valia ir savo arba kito asmens, kuriam jis atstovauja, vardu, sukuria elektroninį parašą.

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 pranešimą ir susidedantis iš elektroninio parašo formato bei pasirašyto elektroninio pranešimo 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 duomenų išsaugojimo XAdES-C formato paraše, laiko žymos šiam formatui uždėjimo ir sertifikavimo kelio bei atšaukimo duomenų išsaugojimo XAdES-X-L formato elektroniniame paraše.

Saugus elektroninis parašas – taip, kaip apibrėžta Lietuvos Respublikos elektroninio parašo įstatyme.

Saugi parašo formavimo įranga – elektroninio parašo formavimo įranga, kuri atitinka visus šiuos 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;

– tenkina standarto LST CWA 14168 „Saugi parašo formavimo įranga „EAL 4“ arba aukštesnius įvertinimo užtikrinimo lygio reikalavimus.

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

Sertifikato galiojimo antrasis tikrinimas – elektroninio pranešimo 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 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;

– kvalifikuotus sertifikatus sudarančiam sertifikavimo paslaugų teikėjui išnagrinėti kreipimąsi ir priimti sprendimą dėl kvalifikuoto sertifikato galiojimo atšaukimo;

– kvalifikuotus sertifikatus sudarančiam sertifikavimo paslaugų teikėjui paskelbti duomenis apie kvalifikuoto sertifikato galiojimo atšaukimą.

Sertifikato galiojimo atšaukimo laikotarpis nurodytas asmens kvalifikuoto sertifikato taisyklėse. Kvalifikuoto sertifikato taisyklėse nesant nurodyto kvalifikuoto sertifikatų atšaukimo laikotarpio, laikoma, kad kvalifikuotų sertifikatų galiojimo atšaukimo laikotarpis yra lygus nuliui.

Sertifikavimo kelias – sertifikatų grandinė, susidedanti iš pasirašančio asmens kvalifikuoto sertifikato, patvirtinto kvalifikuotų sertifikavimo paslaugų teikėjo sertifikatu.

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

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

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

Jeigu neapibrėžta kitaip, tekste vartojama sąvoka „Parašas“ reiškia „Kvalifikuotas elektroninis parašas“, o sąvoka „Sertifikatas“ reiškia „Kvalifikuotas sertifikatas“.

8. Taisyklėse vartojamos santrumpos:

ASN – Abstrakti sintaksinė notacija (angl. *„Abstract Syntax Notation“*);

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

CWA – Bendras seminaro sutarimas (angl. *„Common Workshop Agreement“*);

EAL – Įvertinimo užtikrinimo lygis (angl. *„Evaluation Assurance Level“*);

ESI – Elektroniniai parašai ir infrastruktūros (angl. *„Electronic Signatures and Infrastructures“*);

ETSI – Europos telekomunikacijų standartų institutas (angl. *„European Telecommunications Standards Institute“*);

ID – Identifikatorius;

MAC – Pranešimo autentifikavimo kodas (angl. *„Message Authentication Code“*);

MS – MicroSoft;

OCSP – Operatyvus sertifikato būklės protokolas (angl. *„On-line Certificate Status Protocol“*);

OID – Objekto identifikatorius;

OS – Operacinė sistema;

SD – Socialinis draudimas;

TR – Techninė ataskaita (angl. *„Technical Report“*);

TS – Techninė specifikacija (angl. *„Technical Specification“*);

TkS – Taikomoji sistema;

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 reiklavimai elektroninio parašo aprašymui XML struktūroje (angl. *„XML Digital Signatures (xmldsig)“*).

II. ELEKTRONINIŲ PRANEŠIMŲ KVALIFIKUOTŲ ELEKTRONINIŲ PARAŠŲ KŪRIMAS

9. Elektroninių pranešimų kvalifikuotų elektroninių parašų formavimo procese dalyvauja draudėjai ir Fondo valdyba.

10. Pasirašymo objektas yra FFData formato XML duomenys, sudarantys vieną bylą, kaip yra nurodyta šių taisyklių 26 p.

11. Asmuo, įgaliotas pasirašyti elektroninius pranešimus, kvalifikuotą elektroninį sertifikatą įsigyja pagal 17 p. nuostatas.

12. Elektroninių pranešimų kvalifikuotų elektroninių parašų kūrimas apima el. parašo TkS, pasižyminčios saugia FFData formato duomenų vizualizacijos galimybe, panaudojimą.

13. Elektroninių pranešimų pasirašymo saugi parašo formavimo įranga:

13.1. Saugi parašo formavimo įranga, esanti pasirašančiojo asmens disponuojamo kompiuterio išoriniu įrenginiu arba mobiliojo telefono sudėtine dalimi ir naudojama elektroninių pranešimų pasirašymui, turi atitikti standarto CWA 14168:2004 „Secure Signature Creation Devices „EAL 4“ arba aukštesnio įvertinimo užtikrinimo lygio reikalavimus;

13.2. Pasirašymas saugia parašo formavimo įranga pagal draudėjo pasirinkimą gali būti atliekamas bet kurioje saugioje el. parašo TkS;

13.3. Pasirašant mobiliąja saugia parašo formavimo įranga pasirašymo proceso saugumui užtikrinti saugi el. parašo TkS turi vizualizuoti jos sudarytą pasirašomą santrauką arba jos MAC trumpinį ir prieš pasirašymą ta pati santrauka arba jos trumpinys turi būti vizualizuojami draudėjo įgalioto pasirašančiojo asmens disponuojamame mobiliajame telefone, turinčiame mobiliąją saugią parašo formavimo įrangą;

13.4. Konkrečią galimą saugaus parašo formavimo įrangą nustato konkreti el. parašo TkS.

14. Elektroninių pranešimų pasirašymo priemonės:

14.1. Draudėjas, parengęs elektroninį pranešimą, gali inicijuoti pasirašymo procesą. Priklausomai nuo disponuojamos saugios parašo formavimo įrangos draudėjas pasirenka stacionarią ar mobiliąją parašo formavimo infrastruktūrą;

14.2. Naudojama el. parašo TkS turi saugiai vizualizuoti pasirašomus elektroninio pranešimo duomenis, atvaizduojant juos atitinkamoje elektroninio pranešimo formoje;

14.3. Kiekvienas elektroninis pranešimas pasirašomas individualiai, išreiškiant pasirašančiojo asmens valią patvirtinti pasirašomus duomenis. El. parašo TkS suformuoja XAdES EPES formato parašo elementą. Pasirašytas elektroninis pranešimas išsaugomas konteineryje atsižvelgiant į apribojimus, pateiktus Taisyklių V skyriuje „Elektroninio pranešimo konteinerio formatas“;

14.4. El. parašo TkS turi atitikti standarto CWA 14170:2004 reikalavimus saugioms elektroninio parašo formavimo taikomosioms sistemoms.

III. ELEKTRONINIO PARAŠO TIKRINIMO IR PARENGIMO ILGALAIKIAM SAUGOJIMUI PROCESO APRAŠYMAS

15. Elektroninio parašo tikrinimas:

15.1. Elektroninių pranešimų kvalifikuoto elektroninio parašo tikrinimą atlieka Fondo valdyba. Tikrinimo objektas yra draudėjo elektroninio pranešimo konteineryje, parengtame pagal Taisyklių V skyriuje nustatytus reikalavimus, pateiktas pasirašytas elektroninis pranešimas;

15.2. Per 1 valandą nuo elektroninio pranešimo gavimo momento, užfiksuoto draudėjų portale, Fondo valdyba inicijuoja jo tikrinimo procesą ir gauna laiko žymos tarnybos suformuotą laiko žymą, nurodančią laiko momentą, iki kurio draudėjo parašas buvo sukurtas;

15.3. Elektroninio parašo tikrinimas apima šiuos nuoseklius etapus:

15.3.1. elektroninio pranešimo konteinerio tikrinimas;

15.3.2. elektroninio parašo pirminis tikrinimas;

15.3.3. elektroninio parašo vėlesni tikrinimai.

15.4. Elektroninio pranešimo konteinerio tikrinimas:

15.4.1. Elektroninio pranešimo konteinerio tikrinimo paskirtis – nustatyti, ar elektroninio pranešimo konteinerio struktūra atitinka Taisyklių V skyriuje „Elektroninio pranešimo konteinerio formatas“ nustatytus reikalavimus. Radus klaidų, gauto elektroninio pranešimo apdorojimas nutraukiamas.

15.5. Elektroninio parašo pirminis tikrinimas:

15.5.1. Elektroninio parašo pirminis tikrinimas susideda iš dviejų etapų:

15.5.1.1. elektroninio parašo pirminio tikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos;

15.5.1.2. elektroninio parašo pirminio tikrinimo pasibaigus sertifikato galiojimo atšaukimo laikotarpiui.

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

15.5.3. Elektroninio parašo pirminis tikrinimas iki sertifikato galiojimo atšaukimo laikotarpio pabaigos:

15.5.3.1. Elektroninio parašo pirminio tikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos metu:

15.5.3.1.1. Patikrinamas pateikto elektroninio pranešimo elektroninio parašo formatas ir nustatomas elektroninio pranešimo autentiškumas;

15.5.3.1.2. Elektroniniam pranešimui suformuojama laiko žyma. Po laiko žymos suformavimo draudėjo pateiktas elektroninio pranešimo konteineryje XAdES-EPES formato parašas tampa papildytas iki XAdES-T formato parašo;

15.5.3.1.3. Atliekamas pasirašančiojo asmens kvalifikuoto sertifikato, įskaitant visus sertifikavimo kelio sertifikatus, galiojimo pirmasis patikrinimas. Jeigu patikrinimo metu nustatoma, kad pasirašančio asmens sertifikatas negaliojantis, elektroninio pranešimo tolesnis tikrinimas nutraukiamas ir apie klaidą pranešama draudėjui. Sertifikatų galiojimui tikrinti naudojamas OCSP protokolas sertifikatų būklės tikrinimui realiame laike, o nesant OCSP paslaugos, sertifikatų būklei nustatyti naudojama CRL informacija.

15.5.4. Elektroninio parašo pirminis tikrinimas pasibaigus sertifikato galiojimo atšaukimo laikotarpiui:

15.5.4.1. Elektroninio parašo pirminis tikrinimas pasibaigus sertifikato galiojimo atšaukimo laikotarpiui yra skirtas įsitikinti, ar tikrai pasirašantis asmuo pasirašė elektroninį pranešimą jo kvalifikuoto sertifikato galiojimo laikotarpiu, t. y. ar per leistiną sertifikato galiojimo atšaukimo laikotarpį nėra gauta naujų duomenų apie pasirašančiojo asmens sertifikato ir sertifikavimo kelio sertifikatų atšaukimą anksčiau negu elektroninio parašo pirmojo tikrinimo etape nurodyta laiko žymos data;

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

15.5.4.3. Sertifikato galiojimo antrojo patikrinimo metu tikrintų sertifikavimo kelio sertifikatų ir jų patikrinimo būklės nuorodos ir nurodomų duomenų santraukos yra išsaugomos suformuojant XAdES-C formato parašą. Taip pat atliekamas laiko žymos tarnybos sertifikato ir jos sertifikavimo kelio sertifikatų galiojimo patikrinimas;

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

15.5.4.5. Po elektroninio parašo pirminio patikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos elektroninis pranešimas perduodamas apdorojimui, nelaukiant sertifikato galiojimo patikrinimo rezultatų. Elektroninio parašo pirminio tikrinimo pasibaigus sertifikato galiojimo atšaukimo laikotarpiui metu nustačius sertifikatą esant negaliojantį, elektroninio pranešimo duomenys yra atšaukiami iš duomenų bazės, o pats elektroninis pranešimas Fondo valdybos dokumentų valdymo sistemoje pažymimas kaip negaliojantis.

15.5.5. Elektroninio parašo parengimas ilgalaikiam saugojimui:

15.5.5.1. Elektroninio parašo parengimas ilgalaikiam saugojimui susideda iš laiko žymos uždėjimo XAdES-C formato elektroniniam parašui, tokiu būdu suformuojant XAdES-X pirmo tipo formato elektroninį parašą, ir sertifikatų bei jų atšaukimo duomenų surinkimo ir išsaugojimo pagal iš XAdES-C formato paraše esančias nuorodas, kartu suformuojant XAdES-X-L formato elektroninį parašą.

16. Elektroninio parašo vėlesni tikrinimai:

16.1. Elektroninio parašo vėlesni tikrinimai apima:

16.1.1. elektroninio parašo duomenų papildymą, užtikrinantį ilgalaikį elektroninio parašo galiojimą ir galiojimo įrodomumą;

16.1.2. elektroninio parašo galiojimo patikrinimą per elektroninio pranešimo saugojimo laikotarpį.

16.2. Elektroninio parašo vėlesnio tikrinimo metu yra suformuojama archyvinė laiko žyma XAdES-X-L elektroninio parašo formatui. Tokiu būdu suformuojant XAdES-A elektroninio parašo formatą. XAdES-A formato parašui periodiškai turės būti formuojama

archyvinė laiko žyma. Poreikis tai daryti ir pratęsti elektroninio parašo galiojimą ir galiojimo įrodomumą atsiranda 19.4 p. nurodytais atvejais.

IV. ELEKTRONINIO PARAŠO TIKRUMO NUSTATYMO TVARKA

17. Sertifikavimo kelio sudarymas ir tikrinimas:

17.1. Kvalifikuoti sertifikatai turi būti sudaryti Europos Sąjungos šalių kvalifikuotų sertifikavimo paslaugų teikėjų, įregistruotų ir paskelbtų atitinkamos šalies elektroninio parašo priežiūros institucijoje remiantis elektroninių parašų direktyva „Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures“ ir nacionaliniais elektroninių parašų teisės aktais, bei Fondo valdybos laikomi patikimi;

17.2. Kvalifikuoti sertifikatai Fondo valdybos yra laikomi patikimi, jei juos išdavęs kvalifikuotų sertifikatų paslaugų teikėjas yra įregistruotas atitinkamos šalies elektroninio parašo priežiūros institucijoje ir paskelbtas tos institucijos interneto svetainėje, ir įtrauktas į Fondo valdybos patikimų sertifikavimo paslaugų teikėjų sertifikatų sąrašą;

17.3. Patikimus kvalifikuotų sertifikatų paslaugų teikėjus ir jų sertifikatus Fondo valdyba skelbia draudėjų portale. Elektroniniai pranešimai, kurių elektroniniai parašai patvirtinti sertifikatais, neįtrauktais į Fondo valdybos patikimų sertifikavimo paslaugų teikėjų sertifikatų sąrašą, nepriimami;

17.4. Duomenis apie kvalifikuotų sertifikatų paslaugų teikėjus Fondo valdyba kaupia pagal Europos Sąjungos šalių elektroninio parašo priežiūros institucijų pateikiamą informaciją arba remiantis patikimų sertifikavimo paslaugų teikėjų būklės informacija (vadovaujantis standartu „ETSI TS 102 231: v2.1.1 „Requirements for Trust Service Provider status information“).

18. Kvalifikuotų sertifikatų atšaukimo būsenos nustatymas:

18.1. Kvalifikuoto sertifikato būsenos tikrinimas apima du etapus:

18.1.1. kvalifikuoto sertifikato būsenos pirmasis patikrinimas;

18.1.2. kvalifikuoto sertifikato būsenos antrasis patikrinimas.

18.2. Kvalifikuoto sertifikato būsenos pirmasis patikrinimas atliekamas elektroninio parašo pirminio tikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos metu siekiant nustatyti, ar sertifikatas nėra atšauktas. Jeigu nustatoma, kad kvalifikuoto sertifikato galiojimas yra atšauktas, tai laikoma, kad parašas yra patvirtintas negaliojančiu kvalifikuotu sertifikatu, ir pats parašas yra negaliojantis;

18.3. Kvalifikuoto sertifikato vienareikšmiškas galiojimas arba atšaukimas yra nustatomas tik atlikus kvalifikuoto sertifikato būsenos antrąjį patikrinimą, kuris atliekamas elektroninio parašo pirminio tikrinimo pasibaigus sertifikato galiojimo atšaukimo laikotarpiui metu:

18.3.1. Jeigu patikrinimo metu informacijos apie kvalifikuoto sertifikato galiojimo atšaukimą nėra, tai laikoma, kad kvalifikuotas sertifikatas yra vienareikšmiškai galiojantis ir juo pagrįstas kvalifikuotas elektroninis parašas yra galiojantis;

18.3.2. Jeigu patikrinimo metu kvalifikuoto sertifikato galiojimo atšaukimas yra paskelbtas, o pasirašiusio asmens ar kitų teisės aktų numatytų asmenų kreipimosi atšaukti kvalifikuotą sertifikatą laiko momentas vėlesnis negu laiko žymoje, kuri suformuota elektroninio parašo pirminio tikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos metu, nurodytam laikui, tai kvalifikuotas elektroninis parašas, patvirtintas tokiu kvalifikuotu sertifikatu, laikomas galiojančiu;

18.3.3. Jeigu patikrinimo metu kvalifikuoto sertifikato galiojimo atšaukimas yra paskelbtas ir pasirašiusio asmens ar kitų teisės aktų numatytų asmenų kreipimosi atšaukti kvalifikuotą sertifikatą laiko momentas ankstesnis arba lygus laiko žymoje, kuri suformuota elektroninio parašo pirminio tikrinimo iki sertifikato galiojimo atšaukimo laikotarpio

pabaigos metu, nurodytas laikas, tai kvalifikuotas elektroninis parašas, patvirtintas tokiu kvalifikuotu sertifikatu, laikomas negaliojančiu.

18.4. Nustačius, kad elektroninis parašas yra negaliojantis, apie tai yra pranešama draudėjui.

19. Laiko žymos naudojimas:

19.1. Kvalifikuoto elektroninio parašo laiko žymą gali suformuoti tik patikimos laiko žymos tarnybos, atitinkančios standarto ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“ reikalavimus;

19.2. Laiko žymos galiojimą patvirtinantis sertifikatas yra įtraukiamas į patikimų sertifikatų sąrašą taip pat, kaip ir pasirašančio asmens kvalifikuoto sertifikato galiojimą patvirtinantis sertifikatas;

19.3. Elektroninio pranešimo kvalifikuoto elektroninio parašo laiko žymą Fondo valdyba pirmą kartą suformuoja elektroninio parašo pirminio tikrinimo pradžioje, suformuojant XAdES-T formato elektroninį parašą. Antrą kartą laiko žyma yra suformuojama suformavus XAdES-C formato elektroninį parašą, kuriame išsaugomos nuorodos į pasirašančio asmens sertifikavimo kelio galiojimo informaciją, ir tokiu būdu sudarant XAdES-X formato elektroninį parašą;

19.4. Archyvinė laiko žyma, sudarant XAdES-A formato elektroninį parašą, ir vėlesnės lizdinės laiko žymos suformuojamos šiais atvejais:

19.4.1. jei baigiasi laiko žymą patvirtinusio sertifikato galiojimo laikas;

19.4.2. jei yra atšauktas laiko žymą patvirtinusio sertifikato galiojimas;

19.4.3. jei elektroniniame paraše panaudoti kriptografijos metodai tapo nebepatikimi.

20. Elektroninio parašo pateikimas:

20.1. Fondo valdybos informacinė sistema priima tik XAdES standarte apibrėžtą elektroninio 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);

20.2. Fondo valdybos informacinė sistema priima tik tokius XAdES-EPES formato elektroninius parašus, į kuriuos yra įtrauktas kvalifkuotas sertifikatas, bei tenkinami kiti reikalavimai, nurodyti 24 p.

21. Elektroninio parašo tikrinimas:

21.1. Fondo valdyba užtikrina draudėjo pateiko elektroninio pranešimo kvalifikuoto elektroninio parašo ilgalaikį saugojimą. Tuo tikslu Fondo valdyba surenka ir išsaugo ilgalaikiam saugojimui skirtuose XAdES-X-L ir XAdES-A formato elektroniniuose parašuose parašo tikrumo duomenis, įgalinančius patikrinti parašo galiojimą nesikreipiant į viešųjų raktų infrastruktūrą:

21.1.1. Parašo laiko žymos elementas <SignatureTimeStamp>, įrodantis, kad draudėjo kvalifikuotas parašas yra sukurtas iki šioje laiko žymoje nurodyto laiko, yra sukuriamas formuojant XAdES-T formato parašą;

21.1.2. Parašo nuorodų į sertifikavimo kelią ir sertifikavimo kelio sertifikatų atšaukimą elementai <CompleteCertificateRefs> ir <CompleteRevocationRefs>, OCSP protokolo naudojimo atveju įrodantys, kad sertifikavimo kelio galiojimo patikrinimas yra atliktas pasibaigus kvalifikuoto sertifikato galiojimo atšaukimo laikotarpiui ir išsaugotos nuorodos į sertifikavimo kelio tikrinimo duomenis bei tų duomenų santraukos, yra sukuriami formuojant XAdES-C formato parašą;

21.1.3. Parašo laiko žymos elementas <SigAndRefsTimeStamp>, įrodantis XAdES-C formato parašo integralumą ir egzistavimą iki šioje laiko žymoje nurodyto laiko, yra sukuriamas formuojant XAdES-X formato parašą;

21.1.4. Parašo sertifikavimo kelio sertifikatų reikšmių ir sertifikavimo kelio sertifikatų atšaukimo reikšmių elementai <CertificateValues> ir <RevocationValues>, saugantys XAdES-X formato paraše pateiktų nuorodų duomenis ir įrodantys pasirašančio asmens

kvalifikuoto sertifikato, panaudoto kvalifikuoto elektroninio parašo sukūrimui, galiojimo būklę, yra sukuriami formuojant XAdES-X-L formato parašą;

21.1.5. Parašo laiko žymos elementas <ArchiveTimeStamp>, įrodantis XAdES-A formato parašo integralumą ir galojimą šios laiko žymos sertifikato galiojimo laikotarpiu, yra sukuriamas formuojant XAdES-A formato parašą.

V. ELEKTRONINIO PRANEŠIMO KONTEINERIO FORMATAS

22. Fondo valdybos informacinės sistemos priimamas elektroninio parašo konteinerio formatas:

22.1. Fondo valdybos informacinė sistema priims pasirašytus elektroninius pranešimus, tik išsaugotus elektroninio pranešimo konteinerio byloje, kuri atitiks tokius reikalavimus:

22.1.1. Konteinerio byla turi būti parengta XML formatu;

22.1.2. Konteineryje turi būti ir elektroninis parašas, ir pasirašomas elektroninis pranešimas, ir elektroninio pranešimo metaduomenys;

22.1.3. Konteineryje turi būti tik vienas parašo elementas <Signature> ir tik vienas metaduomenų elementas <LeadDocument>.

22.1.4. Konteineris gali būti trijų tipų:

22.1.4.1. „Enveloped“, tai toks konteineris, kurio pagrindą sudaro pasirašomas dokumentas (pasirašomų duomenų elementas <FFData>). Pasirašomame dokumente (pasirašomų duomenų elemente <FFData>) yra parašas (parašo elementas <Signature>), o parašo elemente <Signature> yra metaduomenys (metaduomenų elementas <LeadDocument>). Bendra „Enveloped“ tipo konteinerio struktūra būtų tokia:

```
<FFData>
...
 <Signature>
 ...
      <LeadDocument>
      ...
      <LeadDocument>
 </Signature>
</FFData>;
```

22.1.4.2. „Enveloping“, tai toks konteineris, kurio pagrindą sudaro parašas (parašo elementas <Signature>), kurio viduje yra ir pasirašomas dokumentas (pasirašomų duomenų elementas <FFData>) ir metaduomenys (metaduomenų elementas <LeadDocument>). Bendra „Enveloping“ tipo konteinerio struktūra būtų tokia:

```
<Signature>
...
 <FFData>
 ...
 </FFData>
 <LeadDocument>
 ...
 <LeadDocument>
</Signature> ;
```

22.1.4.3. „Detached“, tai toks konteineris, kurio pagrindą sudaro specialus konteinerio elementas. Specialiame konteinerio elemente yra ir pasirašomas dokumentas (pasirašomų duomenų elementas <FFData>), ir parašas (parašo elementas <Signature>), ir metaduomenys (metaduomenų elementas <LeadDocument>). Bendra „Detached“ tipo konteinerio struktūra būtų tokia:

```
<EDocument>
 <FFData>
```

```
...
</FFData>
<Signature>
...
</Signature>
<LeadDocument>
...
<LeadDocument>
</EDocument>.
```

22.1.5. Pasirašomų duomenų elementas <FFData> turi atitikti konkretaus eletroninio pranešimo duomenų struktūros apraše išdėstytus reikalavimus, kaip tai yra nurodyta šių taisyklių 26 p.;

22.1.6. Elektroninio parašo elementas <Signature> turi atitikti Fondo valdybos informacinės sistemos priimamą elektroninio parašo formatą (XAdES EPES formatą), kaip tai yra nurodyta šių taisyklių 24 p.;

22.1.7. Metaduomenų elementas <LeadDocument> turi atitikti Fondo valdybos informacinės sistemos priimamų metaduomenų formatą, kaip tai yra nurodyta šių taisyklių 25 p.

23. Draudėjų portale kuriamas elektroninio parašo konteinerio formatas:

23.1. Draudėjų portale sukurto elektroninio pranešimo konteinerio formatas atitinka tokius reikalavimus:

23.2. Konteineris yra „Enveloped“ tipo, kaip tai yra nurodyta šių taisyklių 21.1.4.1. p.;

23.3. Parašo elementas <Signature> atitinka Fondo valdybos informacinės sistemos priimamą parašo formatą, kaip tai yra nurodyta šių taisyklių 24 p.;

23.4. Metaduomenų elementas <LeadDocument> atitinka Fondo valdybos informacinės sistemos priimamų metaduomenų formatą, kaip tai yra nurodyta šių taisyklių 25 p.

23.4.1. Pasirašomų duomenų elementas <FFData> atitinka konkretaus eletroninio pranešimo duomenų struktūros aprašuose išdėstytus reikalavimus, kaip tai yra nurodyta šių taisyklių 26 p.

24. Elektroninio parašo formatas:

24.1. Elektroninio pranešimo parašas turi būti elemente <Signature>;

24.2. Elektroninio pranešimo parašo elementas <Signature> turi tenkinti tokius reikalavimus:

24.2.1. Parašo elementas <Signature> turi atitikti XAdES EPES formato parašą. XAdES standarto parašo formatą aprašanti XML schema pateikta 28.2 p. (byla XAdES_Schema.xsd);

24.2.2. Parašo elementas <Signature> negali turėti jokių aukštesniems XAdES standarto parašo formatams (XAdES-T, XAdES-C, XAdES-X, XAdES-X-L, XAdES-A) naudojamų elementų. Tokie elementai yra:

```
<AllDataObjectsTimeStamp>, <IndividualDataObjectsTimeStamp>,
<CounterSignature>, <SignatureTimeStamp>, <CompleteCertificateRefs>,
<CompleteRevocationRefs>, <AttributeCertificateRefs>,
<AttributeRevocationRefs>, <SigAndRefsTimeStamp>, <RefsOnlyTimeStamp>,
<CertificateValues>, <RevocationValues>, <ArchiveTimeStamp>.
```

24.2.3. XAdES EPES formato paraše privalo būti tokie pasirašomi atributai:

24.2.3.1. naudojamo sertifikato elementas <SigningCertificate>. Tikrinimo metu patikrinama, ar šis elementas nurodo sertifikatą, esantį elemente <KeyInfo>;

24.2.3.2. parašo taisyklių elementas <SignaturePolicyIdentifier>. Tikrinimo metu patikrinama, ar elementas atitinka šią struktūrą:

```
<SignaturePolicyIdentifier> <SignaturePolicyImplied/>
<SignaturePolicyIdentifier/>.
```

24.2.4. XAdES EPES formato paraše gali būti tokie neprivalomi pasirašomi atributai:

24.2.4.1. pasirašymo laiko elementas <SigningTime>. Patikrinimo metu ignoruojamas;

24.2.4.2. dokumento formato elementas <DataObjectFormat>. Patikrinimo metu ignoruojamas;

24.2.4.3. įsipareigojimo tipo elementas <CommitmentTypeIndication>. Patikrinimo metu yra tikrinama, ar toks elementas yra ir jeigu yra, tai papildomai patikrinama, ar įsipareigojimo tipo reikšmė yra ProofOfOrigin;

24.2.4.4. pasirašančiojo rolės elementas <SignerRole>. Patikrinimo metu ignoruojamas;

24.2.4.5. pasirašymo vietos elementas <SignatureProductionPlace>. Patikrinimo metu ignoruojamas;

24.2.4.6. visi kiti papildomai įvesti leistini parašo atributai tikrinimo metu yra ignoruojami.

24.2.5. Parašo elemente <SignedInfo> turi būti du elementai <Reference>:

a) į pasirašytus duomenis (elementą, kuriame pasirašyti duomenys yra saugomi); b) į pasirašytus atributus (elementą <SignedProperties>).

24.2.6. Parašo elemente <KeyInfo> privalo būti elementas <X509Data>, kuriame yra pasirašančiojo asmens sertifikato elementas <X509Certificate>;

24.2.7. Elementuose <Object> turi būti elementas <QualifyingProperties>, taip pat gali būti metaduomenų elementas <LeadDocument>, arba toks elementas, kuriam egzistuoja nuoroda elemente <SignedInfo>, rodanti į jį (t. y. pasirašyti duomenys);

24.2.8. Paraše turi būti naudojami tik tokie transformavimo, kodavimo, kanonizavimo, santraukų sudarymo, pasirašymo algoritmai, kokie apibrėžti 27 p.;

24.2.9. Elektroniniu parašu turi būti pasirašomas pats elektroninis pranešimas, o ne jo koduotė (pvz., BASE64 ar kokia kita), net jeigu pačiame konteineryje yra saugomas ne pats elektroninis pranešimas, o jo koduotė.

25. Metaduomenų formatas:

25.1. Elektroninio pranešimo metaduomenų elementas <LeadDocument> turi tenkinti tokius reikalavimus:

25.1.1. Elektroninio pranešimo metaduomenys turi būti pateikiami konteinerio byloje elemente <LeadDocument>;

25.1.2. Elementas <LeadDocument> turi atitikti Fondo valdybos informacinės sistemos metaduomenų XML schemos aprašymą, pateiktą 28.1 p. (byla Sodra_Metadata_Schema_v0.2.xsd);

25.1.3. Metaduomenų elemente <LeadDocument> privalo būti tokie elementai:

25.1.3.1. pateikiamo dokumento registravimo data, XML standartinis Date tipo elementas <DocumentDate>;

25.1.3.2. pateikiamo dokumento registravimo numerio elementas <DocumentNumber>;

25.1.3.3. parašo dokumente sukūrimo taikomosios sistemos identifikatoriaus elementas <InfrastructureId>.

26. Pasirašomo elektroninio pranešimo formatas:

26.1. Pasirašomo elektroninio pranešimo formatas turi tenkinti tokius reikalavimus:

26.1.1. Pasirašomas elektroninis pranešimas turi būti FFData formato;

26.1.2. Pasirašomas elektroninis pranešimas turi atitikti konkretaus tipo ir versijos eletroninio pranešimo duomenų struktūros apraše, kuris kartu su konkretaus tipo ir versijos socialinio draudimo pranešimo formos pildymo taisyklėmis patvirtintas Fondo valdybos direktoriaus įsakymu, išdėstytus reikalavimus.

27. Leistini parašo sudarymo algoritmai:

27.1. Elektroninių pranešimų kvalifikuotų parašų formavimui gali būti naudojami tik šie algoritmai:

27.1.1. Santraukos sudarymas (angl. „Digest“):

- SHA1 – ID: http://www.w3.org/2000/09/xmldsig#sha1.

27.1.1.1. Kodavimas (angl. „Encoding“):

- base64 – ID: http://www.w3.org/2000/09/xmldsig#base64.

27.1.1.2. Pasirašymas (angl. „Signature“):

- DSAwithSHA1 (DSS) – ID: http://www.w3.org/2000/09/xmldsig#dsa-sha1;
- RSAwithSHA1 – ID: http://www.w3.org/2000/09/xmldsig#rsa-sha1.

27.1.1.3. Kanonizavimas (angl. „Canonicalization“):

- Canonical XML (omits comments) – ID: http://www.w3.org/TR/2001/REC-xml-c14n-20010315;
- Canonical XML with Comments – ID: http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments;

27.1.1.4. Transformavimas (angl. „Transform“):

- Enveloped Signature – ID: http://www..w3.org/2000/09/xmldsig#enveloped-signature;
- XPath – ID: http://www.w3.org/TR/1999/REC-xpath-19991116;
- base64 – ID: http://www.w3.org/2000/09/xmldsig#base64.

28. XML schemos:

28.1. Dokumento metaduomenų elemento XML schema:

Bylos Sodra_Metadata_Schema_v0.2.xsd turinys:

```
<?xml version=„1.0“ encoding=„UTF-8“?>
<xsd:schema xmlns:xsd=„http://www.w3.org/2001/XMLSchema“
xmlns=„http://draudejai.sodra.lt/tech/Sodra_Metadata_Schema_v0.2.xsd“
targetNamespace=„http://draudejai.sodra.lt/tech/Sodra_Metadata_Schema_v0.2.
xsd“
elementFormDefault=„qualified“ version=„0.2“>
<!-- -->
<!-- Metadata definition -->
<!-- -->
<!-- Start LeadDocument -->
     <xsd:element name=„LeadDocument“ type=„LeadDocumentType“/>
     <xsd:complexType name=„LeadDocumentType“ mixed=„false“>
          <xsd:all>
          <xsd:element name=„DocumentDate“ type=„xsd:date“ minOccurs=„0“/>
          <xsd:element name=„DocumentNumber“ type=„xsd:string“
          minOccurs=„0“/>
          <xsd:element name=„InfrastructureId“ type=„xsd:string“/>
</xsd:all>
<xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>
<!-- End LeadDocument -->
<!-- -->
</xsd:schema>
```

28.2. XAdES formatą aprašanti XML schema:

Bylos XAdES_Schema.xsd turinys:

```
<?xml version=„1.0“ encoding=„UTF-8“?>
<xsd:schema targetNamespace=„http://uri.etsi.org/01903/v1.3.2#“
xmlns:xsd=„http://www.w3.org/2001/XMLSchema“
xmlns=„http://uri.etsi.org/01903/v1.3.2#“
xmlns:ds=„http://www.w3.org/2000/09/xmldsig#“
elementFormDefault=„qualified“>
 <xsd:import namespace=„http://www.w3.org/2000/09/xmldsig#“
 schemaLocation=„http://www.w3.org/TR/2002/REC-xmldsig-core-
20020212/xmldsig-core-schema.xsd“/>

<!-- Start auxiliary types definitions: AnyType, ObjectIdentifierType,
EncapsulatedPKIDataType and containers for time-stamp tokens -->

<!-- Start AnyType -->

 <xsd:element name=„Any“ type=„AnyType“/>
 <xsd:complexType name=„AnyType“ mixed=„true“>
```

```
          <xsd:sequence minOccurs=„0“ maxOccurs=„unbounded“>
             <xsd:any namespace=„##any“ processContents=„lax“/>
          </xsd:sequence>
          <xsd:anyAttribute namespace=„##any“/>
 </xsd:complexType>

<!-- End AnyType -->

<!-- Start ObjectIdentifierType-->

 <xsd:element name=„ObjectIdentifier“ type=„ObjectIdentifierType“/>
 <xsd:complexType name=„ObjectIdentifierType“>
          <xsd:sequence>
             <xsd:element name=„Identifier“ type=„IdentifierType“/>
             <xsd:element name=„Description“ type=„xsd:string“
            minOccurs=„0“/>
             <xsd:element name=„DocumentationReferences“
                  type=„DocumentationReferencesType“ minOccurs=„0“/>
          </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name=„IdentifierType“>
 <xsd:simpleContent>
 <xsd:extension base=„xsd:anyURI“>
 <xsd:attribute name=„Qualifier“ type=„QualifierType“ use=„optional“/>
 </xsd:extension>
 </xsd:simpleContent>
 </xsd:complexType>
 <xsd:simpleType name=„QualifierType“>
 <xsd:restriction base=„xsd:string“>
 <xsd:enumeration value=„OIDAsURI“/>
 <xsd:enumeration value=„OIDAsURN“/>
 </xsd:restriction>
 </xsd:simpleType>
 <xsd:complexType name=„DocumentationReferencesType“>
 <xsd:sequence maxOccurs=„unbounded“>
 <xsd:element name=„DocumentationReference“ type=„xsd:anyURI“/>
 </xsd:sequence>
 </xsd:complexType>

<!-- End ObjectIdentifierType-->

<!-- Start EncapsulatedPKIDataType-->

 <xsd:element name=„EncapsulatedPKIData“ type=„EncapsulatedPKIDataType“/>
 <xsd:complexType name=„EncapsulatedPKIDataType“>
 <xsd:simpleContent>
 <xsd:extension base=„xsd:base64Binary“>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
 <xsd:attribute name=„Encoding“ type=„xsd:anyURI“ use=„optional“/>
 </xsd:extension>
 </xsd:simpleContent>
 </xsd:complexType>

<!-- End EncapsulatedPKIDataType -->

 <!-- Start time-stamp containers types -->

 <!-- Start GenericTimeStampType -->

 <xsd:element name=„Include“ type=„IncludeType“/>
 <xsd:complexType name=„IncludeType“>
 <xsd:attribute name=„URI“ type=„xsd:anyURI“ use=„required“/>
 <xsd:attribute name=„referencedData“ type=„xsd:boolean“ use=„optional“/>
```

```
</xsd:complexType>
<xsd:element name=„ReferenceInfo“ type=„ReferenceInfoType“/>
<xsd:complexType name=„ReferenceInfoType“>
<xsd:sequence>
<xsd:element ref=„ds:DigestMethod“/>
<xsd:element ref=„ds:DigestValue“/>
</xsd:sequence>
<xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
<xsd:attribute name=„URI“ type=„xsd:anyURI“ use=„optional“/>
</xsd:complexType>

<xsd:complexType name=„GenericTimeStampType“ abstract=„true“>
<xsd:sequence>
<xsd:choice minOccurs=„0“>
<xsd:element ref=„Include“ maxOccurs=„unbounded“/>
<xsd:element ref=„ReferenceInfo“ maxOccurs=„unbounded“/>
</xsd:choice>
<xsd:element ref=„ds:CanonicalizationMethod“ minOccurs=„0“/>
<xsd:choice maxOccurs=„unbounded“>
<xsd:element name=„EncapsulatedTimeStamp“
type=„EncapsulatedPKIDataType“/>
<xsd:element name=„XMLTimeStamp“ type=„AnyType“/>
</xsd:choice>
</xsd:sequence>
<xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End GenericTimeStampType -->

<!-- Start XAdESTimeStampType -->

<xsd:element name=„XAdESTimeStamp“ type=„XAdESTimeStampType“/>
<xsd:complexType name=„XAdESTimeStampType“>
<xsd:complexContent>
<xsd:restriction base=„GenericTimeStampType“>
<xsd:sequence>
<xsd:element ref=„Include“ maxOccurs=„unbounded“/>
<xsd:element ref=„ds:CanonicalizationMethod“ minOccurs=„0“/>
<xsd:choice maxOccurs=„unbounded“>
<xsd:element name=„EncapsulatedTimeStamp“
type=„EncapsulatedPKIDataType“/>
<xsd:element name=„XMLTimeStamp“ type=„AnyType“/>
</xsd:choice>
</xsd:sequence>
<xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:restriction>
</xsd:complexContent>
</xsd:complexType>

<!-- End XAdESTimeStampType -->

<!-- Start OtherTimeStampType -->

<xsd:element name=„OtherTimeStamp“ type=„OtherTimeStampType“/>
<xsd:complexType name=„OtherTimeStampType“>
<xsd:complexContent>
<xsd:restriction base=„GenericTimeStampType“>
<xsd:sequence>
<xsd:element ref=„ReferenceInfo“ maxOccurs=„unbounded“/>
<xsd:element ref=„ds:CanonicalizationMethod“ minOccurs=„0“/>
<xsd:choice>
<xsd:element name=„EncapsulatedTimeStamp“
type=„EncapsulatedPKIDataType“/>
```

```
 <xsd:element name=„XMLTimeStamp“ type=„AnyType“/>
 </xsd:choice>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
 </xsd:restriction>
 </xsd:complexContent>
 </xsd:complexType>

 <!-- End OtherTimeStampType -->

 <!-- End time-stamp containers types -->

<!-- End auxiliary types definitions-->

<!-- Start container types -->

<!-- Start QualifyingProperties -->

 <xsd:element name=„QualifyingProperties“ type=„QualifyingPropertiesType“/>

 <xsd:complexType name=„QualifyingPropertiesType“>
 <xsd:sequence>
 <xsd:element name=„SignedProperties“ type=„SignedPropertiesType“
 minOccurs=„0“/>
 <xsd:element name=„UnsignedProperties“ type=„UnsignedPropertiesType“
 minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„Target“ type=„xsd:anyURI“ use=„required“/>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
 </xsd:complexType>

<!-- End QualifyingProperties -->

<!-- Start SignedProperties-->

 <xsd:element name=„SignedProperties“ type=„SignedPropertiesType“/>

 <xsd:complexType name=„SignedPropertiesType“>
 <xsd:sequence>
 <xsd:element name=„SignedSignatureProperties“
 type=„SignedSignaturePropertiesType“/>
 <xsd:element name=„SignedDataObjectProperties“
 type=„SignedDataObjectPropertiesType“ minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
 </xsd:complexType>

<!-- End SignedProperties-->

<!-- Start UnsignedProperties-->

<xsd:element name=„UnsignedProperties“ type=„UnsignedPropertiesType“ />

 <xsd:complexType name=„UnsignedPropertiesType“>
 <xsd:sequence>
 <xsd:element name=„UnsignedSignatureProperties“
 type=„UnsignedSignaturePropertiesType“ minOccurs=„0“/>
 <xsd:element name=„UnsignedDataObjectProperties“
 type=„UnsignedDataObjectPropertiesType“ minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
 </xsd:complexType>
```

```
<!-- End UnsignedProperties-->

<!-- Start SignedSignatureProperties-->

<xsd:element name=„SignedSignatureProperties“
 type=„SignedSignaturePropertiesType“ />

<xsd:complexType name=„SignedSignaturePropertiesType“>
 <xsd:sequence>
 <xsd:element name=„SigningTime“ type=„xsd:dateTime“ minOccurs=„0“/>
 <xsd:element name=„SigningCertificate“ type=„CertIDListType“
 minOccurs=„0“/>
 <xsd:element name=„SignaturePolicyIdentifier“
 type=„SignaturePolicyIdentifierType“ minOccurs=„0“/>
 <xsd:element name=„SignatureProductionPlace“
 type=„SignatureProductionPlaceType“
 minOccurs=„0“/>
 <xsd:element name=„SignerRole“ type=„SignerRoleType“ minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End SignedSignatureProperties-->

<!-- Start SignedDataObjectProperties-->

<xsd:element name=„SignedDataObjectProperties“
 type=„SignedDataObjectPropertiesType“/>

<xsd:complexType name=„SignedDataObjectPropertiesType“>
 <xsd:sequence>
 <xsd:element name=„DataObjectFormat“ type=„DataObjectFormatType“
 minOccurs=„0“ maxOccurs=„unbounded“/>
 <xsd:element name=„CommitmentTypeIndication“
 type=„CommitmentTypeIndicationType“ minOccurs=„0“
 maxOccurs=„unbounded“/>
 <xsd:element name=„AllDataObjectsTimeStamp“ type=„XAdESTimeStampType“
 minOccurs=„0“ maxOccurs=„unbounded“/>
 <xsd:element name=„IndividualDataObjectsTimeStamp“
 type=„XAdESTimeStampType“
 minOccurs=„0“ maxOccurs=„unbounded“/>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End SignedDataObjectProperties-->


<!-- Start UnsignedSignatureProperties-->

<xsd:element name=„UnsignedSignatureProperties“
 type=„UnsignedSignaturePropertiesType“/>

<xsd:complexType name=„UnsignedSignaturePropertiesType“>
 <xsd:choice maxOccurs=„unbounded“>
 <xsd:element name=„CounterSignature“ type=„CounterSignatureType“/>
 <xsd:element name=„SignatureTimeStamp“ type=„XAdESTimeStampType“/>
 <xsd:element name=„CompleteCertificateRefs“
 type=„CompleteCertificateRefsType“/>
 <xsd:element name=„CompleteRevocationRefs“
 type=„CompleteRevocationRefsType“/>
 <xsd:element name=„AttributeCertificateRefs“
 type=„CompleteCertificateRefsType“/>
```

```
 <xsd:element name=„AttributeRevocationRefs“
 type=„CompleteRevocationRefsType“/>
 <xsd:element name=„SigAndRefsTimeStamp“ type=„XAdESTimeStampType“/>
 <xsd:element name=„RefsOnlyTimeStamp“ type=„XAdESTimeStampType“/>
 <xsd:element name=„CertificateValues“
 type=„CertificateValuesType“/>
 <xsd:element name=„RevocationValues“ type=„RevocationValuesType“/>
 <xsd:element name=„AttrAuthoritiesCertValues“
 type=„CertificateValuesType“/>
 <xsd:element name=„AttributeRevocationValues“
 type=„RevocationValuesType“/>
 <xsd:element name=„ArchiveTimeStamp“ type=„XAdESTimeStampType“/>
 <xsd:any namespace=„##other“ />
 </xsd:choice>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End UnsignedSignatureProperties-->

<!-- Start UnsignedDataObjectProperties-->

<xsd:element name=„UnsignedDataObjectProperties“
 type=„UnsignedDataObjectPropertiesType“ />

<xsd:complexType name=„UnsignedDataObjectPropertiesType“>
 <xsd:sequence>
 <xsd:element name=„UnsignedDataObjectProperty“ type=„AnyType“
 minOccurs=„0“ maxOccurs=„unbounded“/>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End UnsignedDataObjectProperties-->

<!-- Start QualifyingPropertiesReference-->

<xsd:element name=„QualifyingPropertiesReference“
 type=„QualifyingPropertiesReferenceType“/>

<xsd:complexType name=„QualifyingPropertiesReferenceType“>
 <xsd:attribute name=„URI“ type=„xsd:anyURI“ use=„required“/>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End QualifyingPropertiesReference-->

<!-- End container types -->


<!-- Start SigningTime element -->
 <xsd:element name=„SigningTime“ type=„xsd:dateTime“/>

<!-- End SigningTime element -->

<!-- Start SigningCertificate -->
 <xsd:element name=„SigningCertificate“ type=„CertIDListType“/>
 <xsd:complexType name=„CertIDListType“>
 <xsd:sequence>
 <xsd:element name=„Cert“ type=„CertIDType“ maxOccurs=„unbounded“/>
 </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name=„CertIDType“>
 <xsd:sequence>
```

```
 <xsd:element name=„CertDigest“ type=„DigestAlgAndValueType“/>
 <xsd:element name=„IssuerSerial“ type=„ds:X509IssuerSerialType“/>
 </xsd:sequence>
 <xsd:attribute name=„URI“ type=„xsd:anyURI“ use=„optional“/>
 </xsd:complexType>
 <xsd:complexType name=„DigestAlgAndValueType“>
 <xsd:sequence>
 <xsd:element ref=„ds:DigestMethod“/>
 <xsd:element ref=„ds:DigestValue“/>
 </xsd:sequence>
 </xsd:complexType>

<!-- End SigningCertificate -->

<!-- Start SignaturePolicyIdentifier -->

 <xsd:element name=„SignaturePolicyIdentifier“
 type=„SignaturePolicyIdentifierType“/>
 <xsd:complexType name=„SignaturePolicyIdentifierType“>
 <xsd:choice>
 <xsd:element name=„SignaturePolicyId“ type=„SignaturePolicyIdType“/>
 <xsd:element name=„SignaturePolicyImplied“/>
 </xsd:choice>
 </xsd:complexType>
 <xsd:complexType name=„SignaturePolicyIdType“>
 <xsd:sequence>
 <xsd:element name=„SigPolicyId“ type=„ObjectIdentifierType“/>
 <xsd:element ref=„ds:Transforms“ minOccurs=„0“/>
 <xsd:element name=„SigPolicyHash“ type=„DigestAlgAndValueType“/>
 <xsd:element name=„SigPolicyQualifiers“
 type=„SigPolicyQualifiersListType“ minOccurs=„0“/>
 </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name=„SigPolicyQualifiersListType“>
 <xsd:sequence>
 <xsd:element name=„SigPolicyQualifier“ type=„AnyType“
 maxOccurs=„unbounded“/>
 </xsd:sequence>
 </xsd:complexType>
 <xsd:element name=„SPURI“ type=„xsd:anyURI“/>
 <xsd:element name=„SPUserNotice“ type=„SPUserNoticeType“/>
 <xsd:complexType name=„SPUserNoticeType“>
 <xsd:sequence>
 <xsd:element name=„NoticeRef“ type=„NoticeReferenceType“
 minOccurs=„0“/>
 <xsd:element name=„ExplicitText“ type=„xsd:string“ minOccurs=„0“/>
 </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name=„NoticeReferenceType“>
 <xsd:sequence>
 <xsd:element name=„Organization“ type=„xsd:string“/>
 <xsd:element name=„NoticeNumbers“ type=„IntegerListType“/>
 </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name=„IntegerListType“>
 <xsd:sequence>
 <xsd:element name=„int“ type=„xsd:integer“ minOccurs=„0“
 maxOccurs=„unbounded“/>
 </xsd:sequence>
 </xsd:complexType>

<!-- End SignaturePolicyIdentifier -->
```

```
<!-- Start CounterSignature -->
 <xsd:element name=„CounterSignature“ type=„CounterSignatureType“/>
 <xsd:complexType name=„CounterSignatureType“>
 <xsd:sequence>
 <xsd:element ref=„ds:Signature“/>
 </xsd:sequence>
 </xsd:complexType>

<!-- End CounterSignature -->

<!-- Start DataObjectFormat -->

 <xsd:element name=„DataObjectFormat“ type=„DataObjectFormatType“/>
 <xsd:complexType name=„DataObjectFormatType“>
 <xsd:sequence>
 <xsd:element name=„Description“ type=„xsd:string“ minOccurs=„0“/>
 <xsd:element name=„ObjectIdentifier“ type=„ObjectIdentifierType“
 minOccurs=„0“/>
 <xsd:element name=„MimeType“ type=„xsd:string“ minOccurs=„0“/>
 <xsd:element name=„Encoding“ type=„xsd:anyURI“ minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„ObjectReference“ type=„xsd:anyURI“ use=„required“/>
 </xsd:complexType>

<!-- End DataObjectFormat -->

<!-- Start CommitmentTypeIndication -->

 <xsd:element name=„CommitmentTypeIndication“
type=„CommitmentTypeIndicationType“/>
 <xsd:complexType name=„CommitmentTypeIndicationType“>
 <xsd:sequence>
 <xsd:element name=„CommitmentTypeId“ type=„ObjectIdentifierType“/>
 <xsd:choice>
 <xsd:element name=„ObjectReference“ type=„xsd:anyURI“
 maxOccurs=„unbounded“/>
 <xsd:element name=„AllSignedDataObjects“/>
 </xsd:choice>
 <xsd:element name=„CommitmentTypeQualifiers“
 type=„CommitmentTypeQualifiersListType“ minOccurs=„0“/>
 </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name=„CommitmentTypeQualifiersListType“>
 <xsd:sequence>
 <xsd:element name=„CommitmentTypeQualifier“ type=„AnyType“
 minOccurs=„0“ maxOccurs=„unbounded“/>
 </xsd:sequence>
 </xsd:complexType>

<!-- End CommitmentTypeIndication -->

<!-- Start SignatureProductionPlace -->

 <xsd:element name=„SignatureProductionPlace“
 type=„SignatureProductionPlaceType“/>
 <xsd:complexType name=„SignatureProductionPlaceType“>
 <xsd:sequence>
 <xsd:element name=„City“ type=„xsd:string“ minOccurs=„0“/>
 <xsd:element name=„StateOrProvince“ type=„xsd:string“ minOccurs=„0“/>
 <xsd:element name=„PostalCode“ type=„xsd:string“ minOccurs=„0“/>
 <xsd:element name=„CountryName“ type=„xsd:string“ minOccurs=„0“/>
 </xsd:sequence>
```

```
 </xsd:complexType>

<!-- End SignatureProductionPlace -->

<!-- Start SignerRole -->

<xsd:element name=„SignerRole“ type=„SignerRoleType“/>
<xsd:complexType name=„SignerRoleType“>
 <xsd:sequence>
 <xsd:element name=„ClaimedRoles“ type=„ClaimedRolesListType“
 minOccurs=„0“/>
 <xsd:element name=„CertifiedRoles“ type=„CertifiedRolesListType“
 minOccurs=„0“/>
 </xsd:sequence>
</xsd:complexType>

<xsd:complexType name=„ClaimedRolesListType“>
 <xsd:sequence>
 <xsd:element name=„ClaimedRole“ type=„AnyType“ maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>

<xsd:complexType name=„CertifiedRolesListType“>
 <xsd:sequence>
 <xsd:element name=„CertifiedRole“ type=„EncapsulatedPKIDataType“
 maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>

<!-- End SignerRole -->


 <xsd:element name=„AllDataObjectsTimeStamp“ type=„XAdESTimeStampType“/>

 <xsd:element name=„IndividualDataObjectsTimeStamp“
 type=„XAdESTimeStampType“/>

 <xsd:element name=„SignatureTimeStamp“ type=„XAdESTimeStampType“/>

<!-- Start CompleteCertificateRefs -->

<xsd:element name=„CompleteCertificateRefs“
type=„CompleteCertificateRefsType“/>

<xsd:complexType name=„CompleteCertificateRefsType“>
 <xsd:sequence>
 <xsd:element name=„CertRefs“ type=„CertIDListType“ />
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End CompleteCertificateRefs -->


<!-- Start CompleteRevocationRefs-->

<xsd:element name=„CompleteRevocationRefs“
type=„CompleteRevocationRefsType“/>

<xsd:complexType name=„CompleteRevocationRefsType“>
 <xsd:sequence>
 <xsd:element name=„CRLRefs“ type=„CRLRefsType“ minOccurs=„0“/>
 <xsd:element name=„OCSPRefs“ type=„OCSPRefsType“ minOccurs=„0“/>
```

```
 <xsd:element name=„OtherRefs“ type=„OtherCertStatusRefsType“
 minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<xsd:complexType name=„CRLRefsType“>
 <xsd:sequence>
 <xsd:element name=„CRLRef“ type=„CRLRefType“ maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>

<xsd:complexType name=„CRLRefType“>
 <xsd:sequence>
 <xsd:element name=„DigestAlgAndValue“ type=„DigestAlgAndValueType“/>
 <xsd:element name=„CRLIdentifier“ type=„CRLIdentifierType“
 minOccurs=„0“/>
 </xsd:sequence>
</xsd:complexType>

<xsd:complexType name=„CRLIdentifierType“>
 <xsd:sequence>
 <xsd:element name=„Issuer“ type=„xsd:string“/>
 <xsd:element name=„IssueTime“ type=„xsd:dateTime“ />
 <xsd:element name=„Number“ type=„xsd:integer“ minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„URI“ type=„xsd:anyURI“ use=„optional“/>
</xsd:complexType>

<xsd:complexType name=„OCSPRefsType“>
 <xsd:sequence>
 <xsd:element name=„OCSPRef“ type=„OCSPRefType“ maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>

<xsd:complexType name=„OCSPRefType“>
 <xsd:sequence>
 <xsd:element name=„OCSPIdentifier“ type=„OCSPIdentifierType“/>
 <xsd:element name=„DigestAlgAndValue“ type=„DigestAlgAndValueType“
 minOccurs=„0“/>
 </xsd:sequence>
</xsd:complexType>

 <xsd:complexType name=„ResponderIDType“>
 <xsd:choice>
 <xsd:element name=„ByName“ type=„xsd:string“/>
 <xsd:element name=„ByKey“ type=„xsd:base64Binary“/>
 </xsd:choice>
 </xsd:complexType>

<xsd:complexType name=„OCSPIdentifierType“>
 <xsd:sequence>
 <xsd:element name=„ResponderID“ type=„ResponderIDType“/>
 <xsd:element name=„ProducedAt“ type=„xsd:dateTime“/>
 </xsd:sequence>
 <xsd:attribute name=„URI“ type=„xsd:anyURI“ use=„optional“/>
</xsd:complexType>

<xsd:complexType name=„OtherCertStatusRefsType“>
 <xsd:sequence>
 <xsd:element name=„OtherRef“ type=„AnyType“ maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>
```

```
<!-- End CompleteRevocationRefs-->


<xsd:element name=„AttributeCertificateRefs“
 type=„CompleteCertificateRefsType“/>

<xsd:element name=„AttributeRevocationRefs“
 type=„CompleteRevocationRefsType“/>
<xsd:element name=„SigAndRefsTimeStamp“ type=„XAdESTimeStampType“/>

<xsd:element name=„RefsOnlyTimeStamp“ type=„XAdESTimeStampType“/>

<!-- Start CertificateValues -->

<xsd:element name=„CertificateValues“ type=„CertificateValuesType“/>

<xsd:complexType name=„CertificateValuesType“>
 <xsd:choice minOccurs=„0“ maxOccurs=„unbounded“>
 <xsd:element name=„EncapsulatedX509Certificate“
 type=„EncapsulatedPKIDataType“/>
 <xsd:element name=„OtherCertificate“ type=„AnyType“/>
 </xsd:choice>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<!-- End CertificateValues -->

<!-- Start RevocationValues-->

<xsd:element name=„RevocationValues“ type=„RevocationValuesType“/>

<xsd:complexType name=„RevocationValuesType“>
 <xsd:sequence>
 <xsd:element name=„CRLValues“ type=„CRLValuesType“ minOccurs=„0“/>
 <xsd:element name=„OCSPValues“ type=„OCSPValuesType“ minOccurs=„0“/>
 <xsd:element name=„OtherValues“ type=„OtherCertStatusValuesType“
minOccurs=„0“/>
 </xsd:sequence>
 <xsd:attribute name=„Id“ type=„xsd:ID“ use=„optional“/>
</xsd:complexType>

<xsd:complexType name=„CRLValuesType“>
 <xsd:sequence>
 <xsd:element name=„EncapsulatedCRLValue“ type=„EncapsulatedPKIDataType“
 maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>

<xsd:complexType name=„OCSPValuesType“>
 <xsd:sequence>
 <xsd:element name=„EncapsulatedOCSPValue“
 type=„EncapsulatedPKIDataType“ maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>
<xsd:complexType name=„OtherCertStatusValuesType“>
 <xsd:sequence>
 <xsd:element name=„OtherValue“ type=„AnyType“ maxOccurs=„unbounded“/>
 </xsd:sequence>
</xsd:complexType>

<!-- End RevocationValues-->
```

```
<xsd:element name=„AttrAuthoritiesCertValues“
type=„CertificateValuesType“/>

<xsd:element name=„AttributeRevocationValues“ type=„RevocationValuesType“/>

<xsd:element name=„ArchiveTimeStamp“ type=„XAdESTimeStampType“/>

</xsd:schema>
```