

**GYVENTOJŲ RENGIAMŲ
OFICIALIŲ ELEKTRONINIŲ DOKUMENTŲ
KVALIFIKUOTO ELEKTRONINIO PARAŠO
TAISYKLĖS**

2009 m. sausio 26 d.

Vilnius

2008

PROJEKTAS

PATVIRTINTA

Gyventojų registro tarnybos direktorės

2009 _____ d. įsakymu Nr. _____

**GYVENTOJŲ RENGIAMŲ
OFICIALIŲ ELEKTRONINIŲ DOKUMENTŲ
KVALIFIKUOTO ELEKTRONINIO PARAŠO
TAISYKLĖS**

I. BENDROSIOS NUOSTATOS

1. Šios taisyklės (toliau vadinama Parašo taisyklės) nustato Gyventojų registro tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau - Gyventojų registro tarnyba) sistemoje gyventojų rengiamų oficialių elektroninių dokumentų kvalifikuoto elektroninio parašo sudarymo ir tikrinimo tvarką, dalyvių vaidmenis ir įsipareigojimus, nurodo techninius standartus ir veiksmus, kurie turi būti atliekami kuriant ir tikrinant oficialių elektroninių dokumentų kvalifikuotą elektroninį parašą.

2. Gyventojai, naudodami instrumentinę priemonę SIGNA arba kitas tinkamas instrumentines priemones, rengia, pasirašo ir teikia oficialius elektroninius dokumentus viešojo administravimo institucijoms, kurie priimami, patikrinami, parengiami ilgalaikiam saugojimui bei išsaugojami viešojo administravimo institucijos Informacinėje sistemoje.

3. Parašo taisyklės parengtos vadovaujantis Lietuvos Respublikos Elektroninio parašo įstatymu (Žin., 2000, Nr. 61-1827), poįstatyminiais 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:

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 14169:2004 „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 101 733 v1.5.1: „Electronics Signatures formats“;
 - 3.10. ETSI TS 101 903 v1.3.2: „XML Advanced Electronics Signatures (XAdES)“;
 - 3.11. ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“;
 - 3.12. ETSI TS 101 456 v1.2.1: „Policy requirements for certification authorities issuing qualified certificates“;
 - 3.13. ETSI TS 102 231: v2.1.1 „Requirements for Trust Service Provider status information“.
4. Parašo taisyklėse naudojamose pagrindinės sąvokos:

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

El. parašo sistema – Elektroninio parašo formavimo taikomoji sistema SIGNA arba kita instrumentinė priemonė, deklaruojanti standarto CWA 14170:2004 reikalavimų atitikimą.

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

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

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

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

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

Kvalifikuotas sertifikatas - sertifikatas, kurį sudarė sertifikavimo paslaugų teikėjas, atitinkantis 2002 m. gruodžio 31 d. LR Vyriausybės nutarimu Nr. 2108 nustatytus „Reikalavimus kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams“ ir įregistruotas šiame

nutarime nustatyta „Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarka“ arba Europos Sąjungos šalies sertifikavimo paslaugų teikėjas, kuriam suteiktas kvalifikuoto sertifikavimo paslaugų teikėjo statusas sutinkamai su Europos Sąjungos šalies teisės aktais. Šiame sertifikate yra tokie duomenys:

- užrašas, kad tai yra kvalifikuotas sertifikatas;
- sertifikavimo paslaugų teikėjo ir jo buveinės šalies identifikatoriai;
- pasirašančio asmens vardas ir pavardė arba slapyvardis;
- pasirašančio asmens specialūs atributai, jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus;
- parašo tikrinimo duomenys, atitinkantys pasirašančio asmens turimus parašo formavimo duomenis;
- sertifikato galiojimo pradžios ir pabaigos terminai;
- sertifikato identifikatorius, suteiktas sertifikavimo paslaugų teikėjo;
- sertifikavimo paslaugų teikėjo saugus elektroninis parašas;
- sertifikato naudojimo paskirties apribojimai, jei tai nustatyta;
- leistina operacijų piniginė vertė, kada sertifikatas gali būti naudojamas, jei tai nustatyta.

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

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

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

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

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

Parašo pirminis tikrinimas iki sertifikato atšaukimo laikotarpio pabaigos – elektroninio parašo pirminio tikrinimo etapas, atliekamas nedelsiant gavus pasirašytą elektroninį dokumentą ir susidedantis iš elektroninio parašo formato bei pasirašyto elektroninio dokumento

autentiškumo tikrinimo, laiko žymos suformavimo ir kvalifikuoto sertifikato galiojimo pirmojo tikrinimo.

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

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

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

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

- pasirašančiam asmeniui ar kitiems teisės aktų numatytiems asmenims kreiptis į kvalifikuotus sertifikatus sudarantį sertifikavimo paslaugų teikėją dėl kvalifikuoto sertifikato galiojimo atšaukimo arba sustabdymo, pradedant kreipimosi momentu;
- kvalifikuotus sertifikatus sudarančiam sertifikavimo paslaugų teikėjui išnagrinėti kreipimąsi ir priimti sprendimą dėl kvalifikuoto sertifikato galiojimo atšaukimo arba sustabdymo;
- kvalifikuotus sertifikatus sudarančiam sertifikavimo paslaugų teikėjui paskelbti duomenis apie kvalifikuoto sertifikato galiojimo atšaukimą arba sustabdymą.

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

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

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

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

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

Kitos šiose taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos elektroninio parašo įstatyme (Žin., 2000, Nr. 61-1827, Žin., 2002, Nr. 64-2572, toliau – Elektroninio parašo įstatymas), Lietuvos Respublikos asmens tapatybės kortelės įstatyme (Žin., 2001, Nr.97-3417; 2008, Nr.76-3007, toliau – Asmens tapatybės kortelės įstatymas), Reikalavimuose kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, Reikalavimuose elektroninio parašo įrangai, Kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkoje ir Elektroninio parašo priežiūros reglamente, patvirtintuose Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimu Nr. 2108 (Žin., 2003, Nr. 2-47), Gyventojų registro tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos direktoriaus tvirtinamose Sertifikato taisyklėse.

5. Parašo taisyklėse naudojamos santrumpos:

ASN	Abstrakti sintaksinė notacija („ <i>Abstract Syntax Notation</i> “)
CRL	Sertifikatų atšaukimo sąrašas („ <i>Certificate Revocation List</i> “)
CWA	Bendras seminaro sutarimas („ <i>Common Workshop Agreement</i> “)
EAL	Įvertinimo užtikrinimo lygis („ <i>Evaluation Assurance Level</i> “)
ESI	Elektroniniai parašai ir infrastruktūros („ <i>Electronic Signatures and Infrastructures</i> “)
ETSI	Europos telekomunikacijų standartų institutas („ <i>European Telecommunications Standards Institute</i> “)
ID	Identifikatorius
OCSP	Operatyvus sertifikato statuso protokolas („ <i>On-line Certificate Status Protocol</i> “)

OID	Objekto identifikatorius
OS	Operacinė sistema
TR	Techninė ataskaita („ <i>Technical Report</i> “)
TS	Techninė specifikacija („ <i>Technical Specification</i> “)
XAdES	XML saugūs elektroniniai parašai („ <i>XML Advanced Electronic Signatures</i> “)
XAdES-A	XML saugūs elektroniniai parašai – archyviniai („ <i>XML Advanced Electronic Signatures-Archive</i> “)
XAdES-BES	XML saugūs elektroniniai parašai – baziniai („ <i>XML Advanced Electronic Signatures-Basic Electronic Signature</i> “)
XAdES-EPES	XML saugūs elektroniniai parašai pagal parašo taisykles („ <i>XML Advanced Electronic Signatures-Explicit Policy Electronic Signature</i> “)
XAdES-C	XML saugūs elektroniniai parašai su pilnomis tikrumo duomenų nuorodomis („ <i>XML Advanced Electronic Signatures-with Complete validation data references</i> “)
XAdES-T	XML saugūs elektroniniai parašai su laiko žyma („ <i>XML Advanced Electronic Signatures-with Time</i> “)
XAdES-X	XML saugūs elektroniniai parašai su tikrumo nuorodomis ir laiko žyma („ <i>XML Advanced Electronic Signatures-eXtended signature with Time</i> “)
XAdES-X-L	XML saugūs elektroniniai parašai ilgalaikiam saugojimui XML Advanced Electronic Signatures-eXtended Long signature with Time
XML	Išplečiama žymėjimo kalba („ <i>eXtensible Markup Language</i> “)
XMLDSIG	XML skaitmeninis parašas („ <i>XML Digital SIGNature</i> “)

II. PARAŠO TAISYKLIŲ APIMTIS

6. Parašo taisyklės taikomos gyventojų oficialių elektroninių dokumentų pasirašymui kvalifikuotu elektroniniu parašu, naudojant stacionarią elektroninio parašo formavimo infrastruktūrą, o taip pat oficialių elektroninių dokumentų elektroninio parašo tikrinimui, panaudojant elektroninio parašo taikomąją sistemą SIGNA arba kitas tinkamas instrumentines priemones, įskaitant lokalų interaktyvų oficialių elektroninių dokumentų parengimą bei tikrinimą.

7. Parašo taisyklės taikomos:

7.1. gyventojams, disponuojantiems kvalifikuotu sertifikatu, saugia parašo formavimo įranga ir pasirašantiems oficialius elektroninius dokumentus kvalifikuotu elektroniniu parašu;

7.2. viešojo administravimo institucijų darbuotojams, atsakingiems už oficialių elektroninių dokumentų kvalifikuoto elektroninio parašo tikrinimą ir parengimą ilgalaikiam saugojimui;

7.3. pagalbinių sertifikavimo paslaugų teikėjų darbuotojams, atsakingiems už pagalbinių paslaugų, susijusių su oficialių elektroninių dokumentų kvalifikuoto elektroninio parašo sudarymu, tikrinimu ir parengimu ilgalaikiam saugojimui.

8. Gyventojų registro tarnyba gali pakeisti Parašo taisykles be išankstinio derinimo, iš anksto paskelbiant apie taisyklių pakeitimą ne vėliau, kaip 30 dienų iki pakeistų taisyklių įsigaliojimo datos.

9. Gyventojų registro tarnyba įsipareigoja išsaugoti visas ankstesnes šių parašo taisyklių versijas ir, esant paklausimui, pateikti jas besidominčioms šalims.

10. Oficialių elektroninių dokumentų kvalifikuoto elektroninio parašo sudarymo ir tikrinimo taisyklių taikoma versija konkrečiam elektroniniam dokumentui nustatoma pagal to elektroninio dokumento elektroninio parašo pirmojo tikrinimo etapo laiko žymoje nurodytą datą.

11. Aktuali šių taisyklių redakcija skelbiama Gyventojų registro tarnybos portalo viešojoje srityje.

III. OFICIALIŲ ELEKTRONINIŲ DOKUMENTŲ KVALIFIKUOTŲ ELEKTRONINIŲ PARAŠŲ KŪRIMAS

12. Oficialių elektroninių dokumentų kvalifikuotų elektroninių parašų kūrimas apima visas susijusias šalis: gyventojus, Gyventojų registro tarnybą bei kitas viešojo administravimo įstaigas, pagalbinių sertifikavimo paslaugų teikėjus.

13. Pasirašymo objektas yra duomenys, sudarantys docx, xlsx, pptx, odt, ods ar odp formato bylą. Pasirašomi (skaičiuojama santrauka) originalūs oficialių elektroninių dokumentų formato

duomenys, o ne šių duomenų perkoduotas variantas. Vienu kvalifikuotu elektroniniu parašu gali būti pasirašomi vienas arba daugiau duomenų objektų.

14. Oficialių elektroninių dokumentų pasirašymui kvalifikuotu elektroniniu parašu gyventojas, kreipdamasis į bet kurio Europos Sąjungos kvalifikuotus sertifikatus sudarančio sertifikavimo paslaugų teikėjo registravimo tarnybą, turi įsigyti elektroninio parašo kvalifikuotą sertifikatą bei saugią parašo formavimo įrangą stacionariame įrenginyje.

15. Oficialių elektroninių dokumentų kvalifikuotų elektroninių parašų kūrimas apima el. parašo taikomosios sistemos, pasižyminčios saugia docx, xlsx, pptx, odt, ods ar odp formatų duomenų vizualizacijos galimybe ir veikiančios lokaliaje gyventojų aplinkoje, panaudojimą.

16. Oficialių elektroninių dokumentų pasirašymo saugia parašo formavimo įranga variantai

16.1. Pasirašymas stacionaria saugia parašo formavimo įranga

16.1.1. Stacionari saugi parašo formavimo įranga, esanti pasirašančiojo asmens disponuojamo kompiuterio išoriniu įrenginiu ir naudojama oficialių elektroninių dokumentų pasirašymui, turi atitikti standarto CWA 14169:2004 „Secure Signature-Creation Devices „EAL 4+““ reikalavimus.

16.1.2. Pasirašymas stacionaria saugia parašo formavimo įranga gali būti atliekamas bet kurioje saugioje el. parašo taikomojoje sistemoje, veikiančioje lokaliaje gyventojų aplinkoje.

16.1.3. Konkrečią leistiną stacionarią saugaus parašo formavimo įrangą nustato konkreti el. parašo taikomoji sistema.

17. Oficialių elektroninių dokumentų pasirašymo priemonės:

17.1. El. parašo sistema, veikianti lokaliaje gyventojų aplinkoje:

17.1.1. Gyventojas, su elektroninio parašo taikomąja sistema parengęs oficialų elektroninį dokumentą, gali inicijuoti pasirašymo procesą, priklausomai nuo disponuojamos saugios parašo formavimo įrangos, pasirinkęs stacionarią parašo formavimo infrastruktūrą.

17.1.2. Naudojant el. parašo taikomąją sistemą arba gyventojų pasirinkimu pasitelkus sistemine pasirašomų duomenų vizualizavimo komponentę, gyventojas turi saugiai vizualizuoti pasirašomus oficialaus elektroninio dokumento duomenis.

17.1.3. Kiekvienas oficialus elektroninis dokumentas pasirašomas individualiai, išreiškiant pasirašančio asmens ketinimą patvirtinti pasirašomus duomenis. El. parašo taikomoji sistema suformuoja XAdES EPES formato parašo elementą. Pasirašytas oficialus elektroninis dokumentas, atsižvelgiant į apribojimus, pateiktus Parašo taisyklių VI skyriuje „Oficialaus elektroninio dokumento konteinerio formatas“, yra išsaugomas konteineryje.

17.1.4. Pasirašytam oficialiam elektroniniam dokumentui naudojama el. parašo taikomoji sistema turi suteikti privalomus GGeDOC grupės dokumento metaduomenis. Šiais metaduomenimis turi būti papildomas konteineris.

17.1.5. El. parašo taikomoji sistema, veikianti lokaliaje gyventojų aplinkoje, turi atitikti standarto CWA 14170:2004 reikalavimus saugioms el. parašo formavimo taikomosioms sistemoms.

IV. ELEKTRONINIO PARAŠO TIKRINIMAS IR PARENGIMAS ILGALAIKIAM SAUGOJIMUI

18. Elektroninio parašo tikrinimas

18.1. Oficialių elektroninių dokumentų kvalifikuoto elektroninio parašo tikrinimą atlieka Gyventojų registro tarnyba arba kita viešojo administravimo institucija. Tikrinimo objektas yra gyventojų oficialaus elektroninio dokumento konteineryje, parengtame pagal Parašo taisyklių VI skyriuje „Oficialaus elektroninio dokumento konteinerio formatas“ nustatytus reikalavimus, pateiktas pasirašytas oficialus elektroninis dokumentas.

18.2. Siekiant maksimaliai supaprastinti gyventojų pasirašymo procesą, bet tuo pat metu siekiant kiek galima greičiau gauti sertifikavimo paslaugų teikėjų patvirtintą laiko momentą, iki kurio gyventojų parašas buvo sukurtas, Gyventojų registro tarnyba arba kita viešojo administravimo institucija įsipareigoja (jeigu nėra tinklo ar aptarnaujančių sistemų sutrikimų) inicijuoti gauto pasirašyto oficialaus elektroninio dokumento patikrinimo procesą ir gauti sertifikavimo paslaugų teikėjų patvirtintą laiko momentą ne vėliau kaip per 1 valandą nuo oficialaus elektroninio dokumento gavimo momento, užfiksuoto Gyventojų registro tarnybos arba kitos viešojo administravimo institucijos informacinėje sistemoje.

18.3. Kvalifikuoto elektroninio parašo tikrinimas yra tęstinis procesas, apimantis tiek betarpiškai patį elektroninio parašo tikrinimą, tiek parengimą ilgalaikiam saugojimui su galimybe bet kuriuo vėlesniu laiko momentu patikrinti kvalifikuoto elektroninio parašo galiojimą, nesikreipiant į viešųjų raktų infrastruktūrą. Per visą kvalifikuoto elektroninio parašo gyvavimo ciklą kvalifikuoto elektroninio parašo tikrinimas apima šiuos nuoseklius etapus:

18.3.1. elektroninio dokumento konteinerio tikrinimas;

18.3.2. elektroninio parašo pirminis tikrinimas;

18.3.3. elektroninio parašo vėlesni tikrinimai.

18.4. Oficialaus elektroninio dokumento konteinerio tikrinimas

18.4.1. Oficialaus elektroninio dokumento konteinerio tikrinimo paskirtis – nustatyti gyventojų pateiktus aiškiai klaidingus konteinerius ir apie tai informuoti oficialius elektrinius

dokumentus pateikusius gyventojus. Radus klaidų, gauto oficialaus elektroninio dokumento apdorojimas nutraukiamas.

18.4.2. Oficialaus elektroninio dokumento konteinerio tikrinimas vykdomas sutinkamai su reikalavimais, nustatytais Parašo taisyklių VI skyriuje „Oficialaus elektroninio dokumento konteinerio formatas“.

18.5. Elektroninio parašo pirminis tikrinimas

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

18.5.2. Elektroninio parašo pirminis tikrinimas susideda iš dviejų etapų:

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

18.5.2.2. elektroninio parašo pirminio tikrinimo, pasibaigus sertifikato galiojimo atšaukimo laikotarpiui.

18.5.3. Pagal standarto CWA 14171:2004: „General guidelines for electronic signature verification“ nuostatas nėra galimybių iškart patikimai įsitikinti, ar elektroninis parašas yra sukurtas remiantis galiojančiu sertifikatu, nesulaukus sertifikato galiojimo atšaukimo laikotarpio pabaigos. Sertifikato galiojimo tikrinimas gali būti baigtas tik praėjus pasirašančio asmens kvalifikuoto sertifikato taisyklėse arba sertifikavimo veiklos nuostatuose nurodytam sertifikato galiojimo atšaukimo laikotarpiui nuo laiko žymoje nurodyto laiko, iki kurio buvo sudarytas elektroninio dokumento kvalifikuotas elektroninis parašas. Todėl elektroninio parašo pirminio tikrinimo iki sertifikato galiojimo atšaukimo laikotarpio pabaigos metu yra atliekamas pirmasis sertifikato galiojimo patikrinimas, o pasibaigus sertifikato galiojimo atšaukimo laikotarpiui, atliekamas antrasis sertifikato galiojimo patikrinimas, užbaigiantis sertifikato galiojimo tikrinimo procedūrą.

18.5.4. Elektroninio parašo pirminio tikrinimo eigoje gyventojų 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.

18.5.5. Elektroninio parašo pirminis tikrinimas iki sertifikato galiojimo atšaukimo laikotarpio pabaigos

18.5.5.1. Elektroninio parašo pirminis tikrinimas iki sertifikato galiojimo atšaukimo laikotarpio pabaigos apima elektroninio parašo formato patikrinimą, laiko žymos suformavimą ir sertifikato galiojimo pirmąjį patikrinimą.

18.5.5.2. Elektroninio parašo neatidėliotino pirminio patikrinimo paskirtis yra nustatyti tinkamu konteinerio formatu pateikto pasirašyto oficialaus elektroninio dokumento autentiškumą ir

autentiškam oficialiam elektroniniam dokumentui uždėti kvalifikuotų laiko žymų paslaugų teikėjo, atitinkančio standarto ETSI TS 102 023 v1.2.1 „Policy requirements for time-stamping authorities“ reikalavimus, sudarytą laiko žymą.

18.5.5.3. Laiko žymos suformavimu gyventojų pateiktas elektroninio dokumento konteineryje XAdES-EPES formato parašas papildomas iki XAdES-T formato parašo. Ši laiko žyma nustato laiką, iki kurio yra suformuotas gyventojų oficialaus 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 kelio sertifikatų iki patikimo sertifikato, esančio patikimų sertifikatų saugykloje, galiojimą.

18.5.5.4. Suformavus laiko žymą, atliekamas pasirašančiojo asmens kvalifikuoto sertifikato, įskaitant visus sertifikavimo kelio sertifikatus, galiojimo pirmasis patikrinimas. Jeigu patikrinimo metu nustatoma, kad pasirašančiojo asmens sertifikatas negaliojantis, elektroninio dokumento tolesnis tikrinimas nutraukiamas ir apie klaidą pranešama gyventojui.

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

18.5.6. Elektroninio parašo pirminis tikrinimas pasibaigus sertifikato galiojimo atšaukimo laikotarpiui

18.5.6.1. Elektroninio parašo pirminis tikrinimas pasibaigus sertifikato galiojimo atšaukimo laikotarpiui yra skirtas įsitikinti, ar tikrai pasirašantis asmuo pasirašė oficialų 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 kelio sertifikatų atšaukimą anksčiau negu parašo pirmojo tikrinimo etape nurodyta laiko žymos data.

18.5.6.2. 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 gyventojas.

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

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

18.5.7. Elektroninio parašo parengimas ilgalaikiam saugojimui

18.5.7.1. 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 elektroniniam parašui, tokiu būdu suformuojant XAdES-X pirmo tipo formato elektroninį parašą, ir sertifikatų bei jų atšaukimo duomenų surinkimo ir išsaugojimo pagal XAdES-C formato paraše esančias nuorodas, tuo pačiu suformuojant XAdES-X-L formato elektroninį parašą.

19. Elektroninio parašo vėlesni tikrinimai

19.1. Elektroninio parašo vėlesni tikrinimai apima tiek elektroninio parašo duomenų papildymą, užtikrinantį ilgalaikį elektroninio parašo galiojimą ir galiojimo įrodomumą, tiek ir patį elektroninio parašo galiojimo patikrinimą oficialaus elektroninio dokumento saugojimo laikotarpyje.

19.2. Elektroninio parašo vėlesnio tikrinimo duomenų papildymas susideda iš archyvinės laiko žymos uždėjimo XAdES-X-L elektroninio parašo formatui, tokiu būdu suformuojant XAdES-A elektroninio parašo formatą. Archyvinė laiko žyma gali būti dedama pakartotinai XAdES-A formato parašui. Poreikis papildyti XAdES-X-L formato parašą naujomis laiko žymomis ir pratęsti elektroninio parašo galiojimą ir galiojimo įrodomumą atsiranda tuomet, kad baigiasi panaudoto laiko žymos tarnybos sertifikato galiojimo laikas arba panaudoti kriptografiniai metodai tampa nebeatikimais.

V. ELEKTRONINIO PARAŠO TIKRUMO TAISYKLĖS

20. Elektroninio parašo tikrumo taisyklės formalizuotu būdu aprašo reikalavimus elektroninio parašo kūrimui ir tikrinimui, išdėstyti III ir IV skyriuose.

21. Sertifikavimo kelio sudarymo ir tikrinimo taisyklės

21.1. Kvalifikuoti sertifikatai turi būti sudaryti Europos Sąjungos šalių kvalifikuotų sertifikavimo paslaugų teikėjų, įregistruotų ir paskelbtų atitinkamos šalies elektroninio parašo priežiūros institucijoje sutinkamai su 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 Gyventojų registro

tarnybos ar gyventojų oficialius elektroninius dokumentus priimančios viešojo administravimo institucijos (toliau - Dokumentų gavėjas) laikomi patikimi.

21.2. Kvalifikuoti sertifikatai Dokumentų gavėjo yra laikomi patikimi, jei juos išdavęs kvalifikuotų sertifikatų paslaugų teikėjas yra įregistruotas atitinkamos šalies elektroninio parašo priežiūros institucijoje ir paskelbtas tos institucijos interneto svetainėje.

21.3. Patikimus kvalifikuotų sertifikatų paslaugų teikėjus ir jų sertifikatus Dokumentų gavėjas skelbia portale. Oficialūs elektroniniai dokumentai, kurių parašai patvirtinti sertifikatais, neįtrauktas į Dokumentų gavėjo patikimų sertifikavimo paslaugų teikėjų sertifikatų sąrašą, nėra priimami.

21.4. Duomenis apie kvalifikuotų sertifikatų paslaugų teikėjus Dokumentų gavėjas kaupia pagal Europos Sąjungos šalių elektroninio parašo priežiūros institucijų pateikiamą informaciją arba remiantis patikimų sertifikavimo paslaugų teikėjų statuso informacija sutinkamai su standarto „ETSI TS 102 231: v2.1.1 „Requirements for Trust Service Provider status information“.

21.5. Sertifikavimo kelias susideda iš vieno elemento – pasirašančio asmens kvalifikuoto sertifikato, kurį patvirtinęs kvalifikuotų sertifikavimo paslaugų teikėjo sertifikatas įtrauktas į patikimų sertifikatų saugyklą.

22. Kvalifikuotų sertifikatų atšaukimo būsenos nustatymo taisyklės

22.1. Kvalifikuoto sertifikato būsenos tikrinimas apima du etapus:

22.1.1. kvalifikuoto sertifikato būsenos pirmasis patikrinimas;

22.1.2. kvalifikuoto sertifikato būsenos antrasis patikrinimas.

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

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

22.4. Kvalifikuoto sertifikato atšaukimo būsenos nustatymo taisyklės formuluojamos atliktų parašo formavimo ir tikrinimo veiksmų laiko momentų atžvilgiu:

22.4.1. pasirašantis asmuo elektroninio dokumento kvalifikuotą elektroninį parašą sukuria laiko momentu t_1 ;

22.4.2. Dokumentų gavėjas priima pateiktą pasirašytą oficialų elektroninį dokumentą, atlieka konteinerio, metaduomenų bei parašo formato patikrinimą ir uždeda laiko žymą laiko momentu t_2 .

22.4.3. Dokumentų gavėjas atlieka kvalifikuoto sertifikato galiojimo pirmąjį patikrinimą po laiko momento t_2 .

22.5. 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, ir $t < t_2$, tai laikoma, kad parašas yra patvirtintas negaliojančiu kvalifikuotu sertifikatu, pats parašas yra negaliojantis ir apie tai yra pranešama gyventojui.

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

22.7. Jeigu pirmojo patikrinimo metu nėra duomenų apie kvalifikuoto sertifikato atšaukimą arba sustabdymą, išvadų dėl kvalifikuoto sertifikato galiojimo ar negaliojimo daryti negalima ir yra tęsiamas parašo pirminio tikrinimo procesas.

22.8. Parašo taisyklės nustato, kad kvalifikuoto sertifikato atšaukimo laikotarpiu laikomas pasirašančio asmens kvalifikuoto sertifikato taisyklėse arba sertifikavimo veiklos nuostatuose nurodytas sertifikatų atšaukimo laikotarpis c , jeigu toks nurodytas. Kvalifikuoto sertifikato taisyklėse nesant nurodytam kvalifikuoto sertifikatų atšaukimo laikotarpiui, laikoma, kad kvalifikuotų sertifikatų galiojimo atšaukimo laikotarpis yra lygus nuliui.

22.9. Kvalifikuoto sertifikato galiojimo antrasis patikrinimas turi būti atliktas laiko momentu $t_4 > t_3$, kai $t_3 = t_2 + c$ yra laiko momentas, kuriuo baigiasi kvalifikuoto sertifikato galiojimo atšaukimo laikotarpis, skaičiuojant nuo kvalifikuoto elektroninio parašo pirmosios laiko žymos uždėjimo. OCSP protokolas pateikia įrodymus, kad kvalifikuoto sertifikato galiojimo antrasis patikrinimas tikrai atliktas pasibaigus kvalifikuoto sertifikato galiojimo atšaukimo laikotarpiui.

22.10. Jeigu laiko 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.

22.11. Jeigu laiko 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 $t < t_2$, tai kvalifikuotas elektroninis parašas, patvirtintas tokiu kvalifikuotu sertifikatu yra negaliojantis. Kvalifikuoto sertifikato galiojimo tikrinimo laiką, kvalifikuoto sertifikato galiojimo statusą tikrinimo metu ir, kvalifikuoto sertifikato negaliojimo atveju, kreipimosi atšaukti kvalifikuotą sertifikatą laiką pateikia OCSP protokolo tinklinė paslauga.

23. Laiko žymos naudojimo taisyklės

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

23.2. Laiko žymos galiojimą patvirtinančio sertifikavimo kelio galiojimo patikrinimui taikomos tokios pat taisyklės, kaip ir pasirašančio asmens kvalifikuoto sertifikato galiojimo patikrinimui.

23.3. Oficialaus elektroninio dokumento kvalifikuoto elektroninio parašo laiko žymą Dokumentų gavėjas pirmą kartą uždeda elektroninio parašo pirminio tikrinimo pradžioje, suformuojant XAdES-T formato elektroninį parašą. Antrą kartą laiko žyma yra uždinama suformavus XAdES-C formato parašą, kuriame išsaugomos nuorodos į pasirašančio asmens sertifikavimo kelio galiojimo informaciją, ir tokiu būdu sudarant XAdES-X formato parašą.

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

23.4.1. jei baigiasi laiko žymą patvirtinusio sertifikato galiojimo laikas;

23.4.2. jei yra atšauktas laiko žymą patvirtinusio sertifikato galiojimas;

23.4.3. jei paraše panaudoti kriptografijos metodai tapo nebeapatikimi.

24. Pasirašančio asmens pateikiami kvalifikuoto elektroninio parašo tikrumo duomenys

24.1. Gyventojų pateikto oficialaus elektroninio dokumento kvalifikuoto elektroninio parašo formatas yra XAdES (XML Advanced Electronic Signatures, ETSI TS 101 903 V1.3.2) standarte apibrėžtas XAdES-EPES formato elektroninis parašas, nurodantis Parašo taisyklių taikymą.

24.2. Dokumentų gavėjas 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).

24.3. Dokumentų gavėjas priima tik tokius XAdES-EPES formato elektroninius parašus, į kuriuos yra įtrauktas kvalifikuotas sertifikatas, bei tenkinami kiti reikalavimai, nurodyti punkte 28.1.

25. Tikrinančio asmens surenkami kvalifikuoto elektroninio parašo tikrumo duomenys

25.1. Dokumentų gavėjas užtikrina gyventojų pateikto oficialaus elektroninio dokumento kvalifikuoto parašo ilgalaikį saugojimą. Tuo tikslu Dokumentų gavėjas surenka ir išsaugo ilgalaikiam saugojimui skirtuose XAdES-X-L ir XAdES-A formato parašuose parašo tikrumo duomenis, įgalinančius patikrinti parašo galiojimą nepriklausomai nuo viešųjų raktų (sertifikatų) infrastruktūros pagal standarto ETSI TS 101 903 v1.3.2 „XML Advanced Electronic Signatures (XAdES)“ reikalavimus:

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

25.3. Parašo nuorodų į sertifikavimo kelią ir sertifikavimo kelio sertifikatų atšaukimą elementai: CompleteCertificateRefs ir CompleteRevocationRefs (XAdES-C formato parašas), OCSP protokolo 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;

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

25.5. Parašo sertifikavimo kelio sertifikatų reikšmių ir sertifikavimo kelio sertifikatų atšaukimo reikšmių elementai: CertificateValues ir RevocationValues (XAdES-X-L formato parašas), saugantys XAdES-X formato paraše pateiktą nuorodų duomenis ir įrodantys pasirašančio asmens kvalifikuoto sertifikato, panaudoto gyventojų kvalifikuoto elektroninio parašo sukūrimui, galiojimo statusą;

25.6. Parašo laiko žymos elementas: ArchiveTimeStamp (XAdES-A formato parašas), įrodantis XAdES-A formato parašo integralumą ir galiojimą šios laiko žymos sertifikato galiojimo laikotarpiu.

VI. OFICIALAUS ELEKTRONINIO DOKUMENTO KONTEINERIO FORMATAS

26. Gyventojų kuriamas oficialaus elektroninio dokumento konteinerio formatas

26.1. Gyventojų sukurtas oficialaus elektroninio dokumento konteinerio formatas turi tenkinti žemiau išdėstytus reikalavimus.

26.2. Sukuriama konteinerio byla turi atitikti tokius reikalavimus:

26.2.1. Konteineris turi būti viena rinkmena su praplėtimu „adoc“.

26.2.2. Konteinerio formatas turi būti ZIP.

26.2.3. Konteinerio šaknyje turi būti viena ir tik viena rinkmena – elektroninio dokumento turinio pagrindinė rinkmena.

26.2.4. Konteinerio šaknyje gali būti vienas/keli katalogai laisvai pasirinktais pavadinimais (bet nesutampančiais su „META-INF“ ir „metadata“), kurių viduje gali būti katalogų hierarchinė struktūra, kurios gylis neviršija 3, bei gali būti elektroninio dokumento turinio priedų rinkmenos bei pridedami elektroniniai dokumentai.

26.2.5. Konteinerio šaknyje turi būti katalogas pavadinimu „metadata“, kurio viduje bus metaduomenų rinkmenos.

26.2.6. Konteinerio šaknyje turi būti katalogas pavadinimu „META-INF“:

26.2.6.1. Katalogo „META-INF“ viduje privalo būti elektroninių parašų rinkmenos. Kaip kiekvienos elektroninio parašo rinkmenos pavadinimo dalis turi būti žodis „signatures“. Elektroninių parašų rinkmenos gali būti grupuojamos į katalogus arba katalogų hierarchiją su laisvai pasirinktais pavadinimais. Rekomenduojama turėti vieną katalogą pavadinimu „signatures“.

26.2.6.2. Katalogo „META-INF“ viduje turi būti konteinerio dalių tipų aprašo rinkmena pavadinimu „manifest.xml“, rengiama pagal ODF standarto reikalavimus.

26.2.6.3. Katalogo „META-INF“ viduje turi būti konteinerio dalių tarpusavio ryšių rinkmena pavadinimu „relations.xml“.

27. Dokumentų gavėjo priimamas oficialaus elektroninio dokumento konteinerio formatas

27.1. Dokumentų gavėjas priiminės pasirašytus oficialius elektroninius dokumentus, išsaugotus oficialaus elektroninio dokumento konteineryje, kuris turi atitikti šiame skyriuje išdėstytus reikalavimus.

27.2. Priimamo oficialaus elektroninio dokumento konteineris turi tenkinti tokius reikalavimus:

27.2.1. ar elektroniniame dokumente yra viena ir tik viena pagrindinė dokumento turinio rinkmena;

27.2.2. ar vienareikšmiškai identifikuojamos dokumento turinio dalys, t.y., ar yra sąryšiais neidentifikuojamų turinio dalių; ar pagrindinė dokumento turinio rinkmena nėra kaž kurios kitos dalies priedas ar pridedamas dokumentas; ar priedas nėra kurios nors dalies pridedamas dokumentas; ar pridedamas dokumentas nėra kurios nors dalies priedas;

27.2.3. ar pridedamų dokumentų rinkmenos (jeigu jos yra) sąryšio tipu „Priedamo dokumento rinkmena“ siejamos tik su pagrindine turinio rinkmena;

27.2.4. ar pagrindinė dokumento turinio rinkmena ir visos dokumento priedų rinkmenos (jeigu jos yra) pagal sąryšio tipą „Elektroninio dokumento turinio priedo (priedų) rinkmena“ sudaro tvarkingą hierarchinę struktūrą, kurios viršuje yra pagrindinė dokumento turinio rinkmena, t.y., ar hierarchija vienintelė (apima visas priedų rinkmenas), ar nėra ciklą ir nuorodų į tą pačią rinkmeną;

27.2.5. ar visos elektroninio dokumento turinį sudarančios rinkmenos aprašytos konteinerio dalių tipų apraše, t.y., ar yra turinio rinkmenų, neįtrauktų į šį aprašą;

27.2.6. ar dokumento priedų ir pridedamų dokumentų rinkmenos atitinka turinio tipų reikalavimus, t.y., ar yra turinio rinkmenų, neatitinkančių turinio tipų reikalavimų;

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

28. Elektroninio parašo formatas

28.1. Oficialaus elektroninio dokumento parašo elementas turi tenkinti tokius reikalavimus:

28.1.1. Oficialaus elektroninio dokumento parašas yra elemente <Signature>.

28.1.2. Parašo elementas <Signature> atitinka XAdES formato EPES tipo parašą. XAdES formatą aprašanti XML schema pasiekama adresu: <http://uri.etsi.org/01903/v1.3.2>

28.1.3. Parašo elementas <Signature> neturi jokių aukštesniems XAdES 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>.
```

28.1.4. XAdES EPES formato paraše gali būti tokie pasirašomi atributai:

- naudojamas sertifikatas (SigningCertificate), privalomas, tikrinimo metu yra tikrinama, ar šis elementas nurodo sertifikatą esantį elemente <KeyInfo>,
- pasirašymo taisyklės (SignaturePolicyIdentifier), tikrinimo metu yra tikrinama ar elementas yra toks:

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

- pasirašymo laikas (SigningTime), neprivalomas, tikrinimo metu ignoruojamas,
- dokumento formatas (DataObjectFormat), neprivalomas, tikrinimo metu ignoruojamas,
- įsipareigojimo tipas (CommitmentTypeIndication), neprivalomas, tikrinimo metu yra tikrinama ar toks elementas yra ir, jeigu yra, tai ar įsipareigojimo tipas yra ProofOfOrigin,
- pasirašančiojo rolė (SignerRole), neprivalomas, tikrinimo metu ignoruojamas,
- pasirašymo vieta (SignatureProductionPlace), neprivalomas, tikrinimo metu ignoruojamas.

28.1.5. Visi kiti parašo atributai tikrinimo metu yra ignoruojami.

28.1.6. Parašo elemente <SignedInfo> turi būti bent dvi nuorodos (elementai <Reference>):

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

28.1.7. Parašo elemente <KeyInfo> turi būti elementas <X509Data>, kuriame yra pasirašančiojo asmens sertifikatas (elementas <X509Certificate>).

28.1.8. Elemente <Object> turi būti elementas <QualifyingProperties>, taip pat gali būti toks elementas, kuriam egzistuoja nuoroda elemente <SignedInfo> rodanti į jį (t.y., pasirašyti duomenys).

28.1.9. Paraše naudojami algoritmai (transformavimo, kodavimo BASE64, kanonizavimo, santraukų sudarymo, pasirašymo) turi būti standartiniai, kad automatinėmis priemonėmis būtų įmanomas parašo patikrinimas. Jokie specifiniai algoritmai yra neleistini.

28.1.10. Visada turi būti pasirašomas pats oficialus elektroninis dokumentas, o ne jo koduotė (BASE64 ar kokia kita), net jeigu pačiame konteineryje yra saugomas ne pats elektroninis dokumentas, o jo koduotė.

29. Metaduomenų formatas

29.1. Oficialaus elektroninio dokumento metaduomenys turi tenkinti tokius reikalavimus:

29.1.1. ar oficialiame elektroniniame dokumente yra visi privalomi metaduomenys, apibrėžti reikalavimuose GGeDOC grupės oficialių elektroninių dokumentų specifikacijoms.

29.1.2. ar metaduomenys apibrėžti tik vieną kartą, išskyrus metaduomenis, kurie gali būti apibrėžti kelis kartus.

29.1.3. ar visi metaduomenys, kurie privalo būti pasirašyti pagal GGeDOC grupės oficialių elektroninių dokumentų specifikacijos reikalavimus, yra pasirašyti.

30. Leistini parašo sudarymo algoritmai

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

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

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

30.1.1.1. Kodavimas (angl. „Encoding“):

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

30.1.1.2. 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>

30.1.1.3. 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>

30.1.1.4. Transformavimas (angl. „Transform“):

- XPath - ID: <http://www.w3.org/TR/1999/REC-xpath-19991116>
- base64 - ID: <http://www.w3.org/2000/09/xmlsig#base64>