Vilniaus universitetas
Matematikos ir informatikos fakultetas
Programų sistemų katedra

Valdas UNDZĖNAS
http://www.mif.vu.lt/~valund

# ELEKTRONINIO PARAŠO INFRASTRUKTŪRA IR ELEKTRONINĖ KOMERCIJA

Mokymo medžiaga

(atnaujinta 2008 m.)

VILNIUS – 2003

# TURINYS

1. ĮVADAS Į ELEKTRONINĮ PARAŠĄ IR JO INFRASTRUKTŪRĄ ..... 4
1.1. Įžanga ..... 4
1.2. Duomenų šifravimas ..... 5
1.3. Sertifikatai ..... 6
1.4. Sertifikatų centrai (CA) ..... 7
1.5. El. parašų kūrimas ir tikrinimas ..... 7
1.6. Laiko žymos ..... 8
1.7. El. parašo infrastruktūros reglamentavimas ..... 10
1.8. El. parašo infrastruktūros atitikties reikalavimams vertinimas ..... 11
2. ELEKTRONINIO PARAŠO ALGORITMAI ..... 13
2.1. SHA-1 algoritmas ..... 13
2.2. RSA algoritmas ..... 16
3. SERTIFIKATAI ..... 18
3.1. Sertifikato struktūra ir duomenys ..... 18
3.2. Sertifikato išplėtimai (extensions) ..... 20
3.3. Sertifikato papildymai pagal RFC 3739 standartą ..... 21
3.4. Sertifikato papildymai pagal ETSI TS 101 862 standartą ..... 22
3.5. Pavyzdys: Geteborgo universiteto CA sertifikatas [36] ..... 22
4. SERTIFIKATŲ CENTRAI (CA) ..... 24
4.1. CA funkcijos ir struktūra ..... 24
4.2. Reikalavimai kvalifikuotus sertifikatus sudarantiems CA ..... 25
5. SERTIFIKATO TAISYKLĖS IR CA SERTIFIKAVIMO VEIKLOS NUOSTATAI ..... 29
5.1. Bendrieji klausimai ..... 29
5.2. Pagrindinės sąvokos ..... 29
5.3. Santykis tarp sertifikato taisyklių ir sertifikavimo veiklos nuostatų ..... 32
5.4. Sertifikato taisyklių ir CA sertifikavimo veiklos nuostatų struktūra ..... 33
6. PATIKIMA SERTIFIKATŲ TVARKYMO SISTEMA ..... 36
6.1. Bendrosios nuostatos ..... 36
6.2. Saugumo reikalavimų lygiai ir reikalavimų grupės ..... 37
6.3. Bendrieji Sistemos saugumo reikalavimai ..... 37
6.4. Pagrindiniai Sistemos saugumo reikalavimai ..... 42
6.5. Papildomi Sistemos saugumo reikalavimai ..... 49
6.6. Kriptografinis modulis ..... 52
7. ELEKTRONINIO PARAŠO FORMATAI ..... 56
7.1. El. parašo elementai ir formatai ..... 56
7.2. Į archyvą dedamų dokumentų el. parašas ..... 60

8. PARAŠO TAISYKLĖS ..... 62
8.1. Įžanga ..... 62
8.2. Parašo taisyklių kontekstas ..... 63
8.3. Parašo taisyklių leidėjai ir naudotojai ..... 66
8.4. Reikalavimai parašo taisyklėms ..... 67
9. ELEKTRONINIO PARAŠO KŪRIMAS ..... 77
9.1. Parašo kūrimo funkcinis modelis ..... 77
9.2. Parašo kūrimo informacinis modelis ..... 79
9.3. Parašo formavimo taikomosios programos (SCA) sudėtis ..... 80
9.4. Bendrieji SCA saugumo reikalavimai ..... 84
9.5. Saugumo reikalavimai SCA komponentams ..... 86
9.6. Saugi parašo formavimo įranga (SSCD) ..... 89
10. LAIKO ŽYMA ..... 92
10.1. Laiko žymos samprata ..... 92
10.2. Laiko žymų teikėjų (TSA) veiksmai ..... 93
10.3. Laiko žymų prašytojų veiksmai ..... 93
10.4. Užklausų ir atsakymų formatai ..... 94
10.5. Pranešimų perdavimas ..... 99
10.6. Saugumo klausimai ..... 101
10.7. Reikalavimai laiko žymų prašytojų ir TSA įrangai ..... 102
10.8. Reikalavimai TSA ..... 104
10.9. Laiko žymos taisyklės ..... 108
11. ELEKTRONINIO PARAŠO TIKRINIMAS ..... 109
11.1. Bendrosios nuostatos ..... 109
11.2. Parašo tikrinimo procesas ..... 110
11.3. Parašo tikrinimo sistemos ..... 119
11.4. Parašo tikrinimo aplinkos ..... 123
11.5. Teisiniai aspektai ..... 126
12. PASLAUGŲ IR ĮRANGOS ATITIKTIES VERTINIMAS ..... 130
12.1. Sertifikatų centrų (CA) atitikties reikalavimams vertinimas ..... 130
12.2. El. parašo įrangos atitikties reikalavimams vertinimas ..... 137
SANTRUMPOS ..... 143
ŠALTINIAI ..... 144
PRIEDAI ..... 148
1 priedas. El. parašo kūrimo įrangos atitikties deklaracijos ..... 148
2 priedas. El. parašo tikrinimo įrangos atitikties deklaracijos ..... 150

# 1. ĮVADAS Į ELEKTRONINĮ PARAŠĄ IR JO INFRASTRUKTŪRĄ

Skyriuje trumpai apžvelgiamos elektroninio parašo (toliau – el. parašas) atsiradimo priežastys, pasirašymo ir el. parašo tikrinimo principai, būtina infrastruktūra.

## 1.1. Įžanga

Daugelyje veiklos sričių žmonės naudoja dokumentus. Teisiniai, banko, apskaitos, techniniai ir kitokie dokumentai yra tvirtinami atsakingojo asmens rašytiniu parašu ir/arba antspaudu. Tai istoriškai susidariusi praktika.

Šiandieną vis daugiau dokumentų tvarkoma kompiuteriais. Tai gali būti kompiuterinio pavidalo tekstas, garsas, vaizdas ar kitokie duomenys. Jau niekam nekyla abejonių dėl el. dokumentų patogumo. Esant išplėtotoms telekomunikacijoms, juos galima labai greitai ir daug kartų pigiau nei paprastu paštu perduoti bet kur esantiems vartotojams. Plėtojantiems verslą tarptautiniu mastu tai yra labai svarbu, o el. komercija be el. dokumentų yra praktiškai neįmanoma. El. dokumentams saugoti reikia daug mažiau vietos, jiems apdoroti reikia mažesnių sąnaudų, informacija pasiekiama daug kartų greičiau ir patogiau.

Tačiau problemos iškyla dėl informacijos patikimumo. Popierinio dokumento atveju atsakingasis asmuo patvirtina jį savo parašu ir/arba antspaudu. O kaip patvirtinti el. dokumentą? Kaip užtikrinti, kad informaciją pateikė konkretus asmuo ir kad el. dokumento turinys kelyje nuo siuntėjo iki gavėjo nebuvo pakeistas? Tam ir buvo sugalvotas el. parašas.

El. parašas garantuoja pasirašytų el. duomenų (el. dokumento) autentiškumą ir įgalina patikrinti pasirašiusio asmens tapatybę. Jis sudaro prielaidas patikimam, greitesniam, patogesniam asmenų bendravimui su įvairiomis institucijomis, padeda greičiau plėtoti verslą, suteikia aukštesnį finansinių operacijų saugumą, pagerina įvairių institucijų veiklą.

El. parašo diegimui įtakos turi ne vien finansiniai ištekliai ar technologiniai sprendimai, bet ir teisinė bazė bei visuomenės žinių lygis. Šiandieną Lietuvoje teisės aktų reikalavimus atitinkančio el. parašo teisinė galia yra tokia pati kaip ir ranka rašyto parašo rašytiniuose dokumentuose, ir leidžiama naudoti jį kaip įrodinėjimo priemonę teisme.

Šioje mokymo medžiagoje skaitytojai supažindinami su el. parašo technologija ir infrastruktūra jam naudoti. Pateikiama medžiaga turėtų padėti lengviau suprasti el. parašo teisės ir norminius aktus [46, 47, 48], diegimo darbų apimtis, naudojimo niuansus.

## 1.2. Duomenų šifravimas

El. parašai remiasi kriptologija – mokslu apie duomenų šifravimą [35]. Duomenų užšifravimas yra duomenų pavertimas nesuprantamais, kol jie nebus atšifruoti atitinkamu būdu.

Yra du duomenų šifravimo metodai: simetrinis ir asimetrinis.

***Simetrinio šifravimo metode*** sugeneruojamas vienas šifravimo raktas (labai didelis skaičius). Jį gauna du asmenys - duomenų siuntėjas ir gavėjas. Duomenims užšifruoti prieš siunčiant ir gautiems užšifruotiems duomenims atšifruoti yra naudojamas tas pats raktas. Metodas naudojamas duomenų konfidencialumui užtikrinti, t. y. kai norima apsisaugoti nuo duomenų atskleidimo tretiesiems asmenims. Simetrinio šifravimo metodo privalumas yra tas, kad duomenų užšifravimas ir atšifravimas vyksta greitai. Trūkumai: raktą žino du arba daugiau asmenų, todėl ginčo atveju sunku įrodyti, kuris asmuo neteisus; raktui perduoti asmenys turi susitikti betarpiškai arba naudoti kitokius saugius perdavimo būdus.

***Asimetrinio šifravimo metode*** generuojami du matematiškai tarpusavyje susiję raktai. Tikimybė sugeneruoti du kartus tokią pačią šifravimo raktų porą yra labai maža. Jei duomenys užšifruojami vienu raktu, tai juos atšifruoti įmanoma tik kitu tos poros raktu. Žinant vieną poros raktą praktiškai neįmanoma atskleisti kito rakto.

Šis metodas taip pat naudojamas duomenų konfidencialumui užtikrinti. Tačiau palyginus su simetrinio šifravimo metodu, duomenims užšifruoti ir atšifruoti reikia žymiai daugiau laiko.

El. parašo technologija dabartiniu metu yra pagrįsta asimetrinio šifravimo metodu, nes kol kas jis yra geriausiai ištyrinėtas, išplėtotas. Tai skaitmeninis metodas. Todėl dažnai vietoje termino “el. parašas” naudojamas “skaitmeninis parašas”.

El. parašo tikslams sugeneruotos šifravimo raktų poros vienas raktas atiduodamas tik vienam asmeniui. Šis raktas vadinamas privačiuoju raktu. Privatųjį raktą reikia laikyti ypač saugiai, pavyzdžiui, intelektualioje kortelėje (*smartcard*), nešiojamame kompiuteryje ar intelektualiajame diske (*smartdisk*).

Šis raktas turi būti pasiekiamas tik įvedus slaptažodį (pvz., PIN kodą) arba/ir asmens biometrinius duomenis: pirštų atspaudus, akių rainelės vaizdą, kt. Kitas raktas yra viešas, ir jį gali sužinoti kiekvienas norintis.

Priklausomai nuo reikalaujamo saugumo lygio, asimetrinio šifravimo metodo raktų ilgis gali būti įvairus: nuo 512 bitų iki 4096 bitų.

Asimetrinio šifravimo algoritmas dar yra vadinamas viešojo rakto algoritmu, o juo pagrįsto el. parašo infrastruktūra (teisinių, organizacinių, technologinių priemonių visuma) – viešojo rakto infrastruktūra (**PKI** – *Public Key Infrastructure*).

El. parašui naudojamas šifravimo raktų poras asmenims dažniausiai sugeneruoja patikimi paslaugų teikėjai, tačiau juos gali susigeneruoti ir patys asmenys.

## 1.3. Sertifikatai

El. parašu pasirašantis asmuo turi turėti sertifikatą. Sertifikatas – tai elektroninio pavidalo liudijimas, patvirtinantis, kad šifravimo raktų pora priklauso sertifikate nurodytam asmeniui. Sertifikatą galima būtų prilyginti piliečio pasui, tik jis yra skirtas saugiam asmenų bendravimui elektroninėje erdvėje. Sertifikatams sudaryti turi būti įsteigti patikimi sertifikatų centrai (**CA** – *Certificate Authorities*). Sertifikatui gauti asmenys privalo CA pateikti tapatybę patvirtinančius dokumentus ir kitą būtiną informaciją, įskaitant viešąjį raktą, jei asmuo raktų porą susigeneravo kitur, o ne tame CA. Sertifikatų mechanizmas yra būdas patikrinti, kad el. duomenis iš tikro pasirašė sertifikate įvardintas asmuo. Asmens sertifikato nuoroda – sertifikatą sudariusio CA identifikatorius, sertifikato serijinis numeris, sertifikato santrauka - visada įterpiama į el. parašą.

Skiriamos dvi sertifikatų rūšys:

- ♦ paprasti sertifikatai;
- ♦ kvalifikuoti sertifikatai (angl. *qualified certificate*). Tai išsamūs, aukštesnio lygio sertifikatai, kuriuos sudaro nustatytus reikalavimus atitinkantys CA.

Sertifikate turi būti šie duomenys:

- ♦ asmens vardas;
- ♦ viešasis raktas, atitinkantis asmens turimą privatųjį raktą;
- ♦ sertifikato galiojimo pradžios ir pabaigos terminai;
- ♦ sertifikatą sudariusio CA ir jo buveinės šalies identifikatoriai;

- sertifikato identifikatorius, kurį suteikia CA;
- sertifikato naudojimo paskirties apribojimai, jei tai nustatyta;
- CA el. parašas.

Sertifikatai turi būti patvirtinti juos sudariusio CA el. parašu. Todėl CA, kaip juridinis asmuo, savo ruožtu turi būti gavęs sertifikatą iš aukštesnio lygmens CA. Aukščiausiojo lygmens CA sertifikatą pasidaro pats, ir todėl toks CA dažniausiai vadinamas šakniniu (*root*) CA.

## 1.4. Sertifikatų centrai (CA)

CA pagrindinė funkcija yra sudaryti sertifikatus asmenims, norintiems savo veikloje naudoti el. parašą, ir teikti sertifikatų informaciją el. parašų tikrintojams bet kuriuo metu, kai tik gaunama užklausa. Šioms funkcijoms vykdyti CA turi turėti tokias tarnybas: klientų registravimo, sertifikatų sudarymo, sertifikatų duomenų teikimo, sertifikatų atšaukimo (galiojimo nutraukimo), atšauktų sertifikatų sąrašų (**CRL** – *Certificate Revocation List*) teikimo.

Asmens el. parašas yra galiojantis, jei jis buvo sukurtas asmens sertifikato galiojimo laikotarpiu. CRL sąrašai reikalingi tam, kad el. parašo tikrintojai galėtų įsitikinti, ar pasirašiusiam asmeniui išduotas sertifikatas dėl kokių nors priežasčių (pvz., pametus arba pavogus jo kortelę su privačiuoju raktu) nebuvo atšauktas anksčiau, nei sertifikate nurodytas galiojimo pabaigos terminas.

Sudarant sertifikatus jau turi būti sugeneruoti šifravimo raktai. Viešasis raktas dedamas į sertifikatą, o privatusis raktas įrašomas į saugią laikmeną, pvz., intelektualiąją kortelę, ir atiduodamas tik užsakiusiam asmeniui. Todėl CA sudėtyje gali būti ir parašo formavimo įrangos tarnyba raktų poroms generuoti ir privatiesiems raktams įrašyti į saugias laikmenas.

Raktų poras generuoti ir privačiuosius raktus rašyti į saugias laikmenas gali tuo besiverčiantys kiti paslaugų teikėjai (ne tik CA). Šiuo atveju asmuo, norėdamas gauti sertifikatą, turi pateikti CA savo viešąjį raktą.

Parašo formavimo įrangos parengimas (pvz., intelektualiosios kortelės) yra kritinis el. parašo saugumo klausimas.

## 1.5. El. parašų kūrimas ir tikrinimas

Kuriant el. parašą naudojami pasirašomi duomenys. Kadangi duomenų apimtis gali būti didelė ir įvairi, visų pirma sukuriama trumpa fiksuoto ilgio duomenų santrauka (angliškai ji vadinama įvairiai: *hash, message digest,*

*imprint*). Dažniausiai ji būna 128 arba 160 bitų ilgio, o ypatingo saugumo atvejais - 512 bitų. Skaitmeninis parašas – tai pasirašomų duomenų ir papildomos informacijos (pvz., pasirašiusio asmens sertifikato nuorodos, parašo taisyklių nuorodos, pasirašymo vietos, laiko, kt.) santrauka, užšifruota asmens privačiuoju raktu. Pasirašyti duomenys – tai duomenys plius el. parašas. Ateityje atkreipkime dėmesį į sąvokų „skaitmeninis parašas“ ir „elektroninis parašas“ naudojimą. Skaitmeninis parašas yra tik el. parašo viena iš dalių.

Duomenų santraukos algoritmo savybės yra tokios:

- iš santraukos neįmanoma atstatyti pačių duomenų;
- praktiškai neįmanoma rasti dviejų skirtingų duomenų, kurių santraukos būtų vienodos.

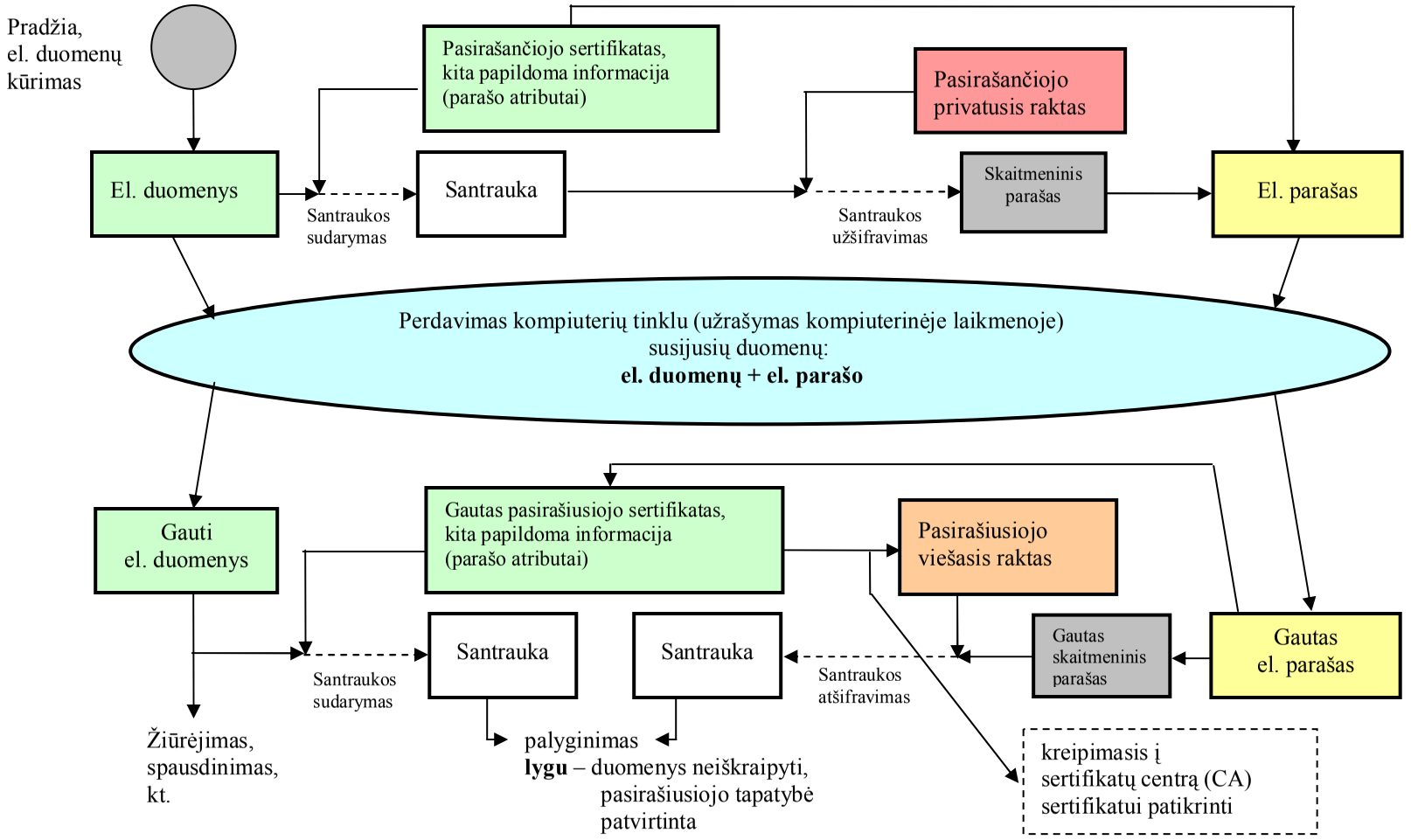
Pasirašytų duomenų gavėjas el. parašui tikrinti naudoja gautus duomenis, papildomą informaciją bei pasirašiusio asmens viešąjį raktą. Tam gavėjas taip pat sudaro gautų duomenų ir papildomos informacijos santrauką. Toliau, atšifruojant skaitmeninį parašą pasirašiusio asmens viešuoju raktu, atstatoma pasirašiusiojo sudaryta santrauka. Palyginus šias dvi santraukas, įsitikinama el. parašo tikrumu, t. y. ar duomenys nebuvo iškraipyti ir ar el. parašą sukūrė asmuo, turintis privatųjį raktą, kuris atitinka atšifravimui naudotą viešąjį raktą. Viešasis raktas yra pasirašiusiojo sertifikate, o šio asmens sertifikato nuoroda visada yra el. paraše šalia kitos informacijos. Galimybę pasitikrinti, ar pasirašytus duomenis ir sertifikato nuorodą iš tikro atsiuntė prisistatęs asmuo, suteikia sertifikatų sudarytojai - sertifikatų centrai (CA).

Tikrinant el. parašą taip pat svarbu įsitikinti, ar el. parašo kūrimo metu galiojo pasirašiusio asmens sertifikatas, ar nepažeisti sertifikate nustatyti apribojimai.

1.1 pav. parodyta el. parašo kūrimo ir tikrinimo schema.

## 1.6. Laiko žymos

Pasirašančiųjų asmenų sertifikatuose yra sertifikato galiojimo pradžios ir pabaigos terminai. Tačiau sertifikatas dėl įvairių priežasčių gali būti atšauktas anksčiau. Pavyzdžiui, asmeniui pametus kortelę su privačiuoju raktu, būtina nedelsiant kreiptis į CA dėl sertifikato atšaukimo (galiojimo nutraukimo anksčiau, nei sertifikate nurodytas pabaigos terminas).




1.1 pav. El. parašo kūrimo ir tikrinimo schema

Galioja tik tokie el. parašai, kuriuos asmenys sukūrė jų sertifikatų galiojimo laikotarpiu. Pasibaigus sertifikatų galiojimo terminui, pavyzdžiui, jau archyve esantiems el. dokumentams, būtina turėti galimybę patikrinti, ar asmenys el. dokumentus pasirašė atitinkamų sertifikatų galiojimo laikotarpiu. Todėl į el. parašus gali būti įterpiamos (dedamos) laiko žymos. Jos turėtų būti dedamos kaip galima greičiau po pasirašymo.

Kad tikrintojas galėtų įsitikinti, jog el. parašas buvo sukurtas pasirašiusio asmens sertifikato galiojimo laikotarpiu, reikalinga el. parašo laiko žyma ir sertifikato duomenys. Informacija apie atšauktus sertifikatus saugoma CA atšauktų sertifikatų sąraše (CRL). El. parašui laiko žyma turi būti dedama pasirašiusio asmens sertifikato galiojimo laikotarpiu. Priešingu atveju el. parašo laiko žyma neturės prasmės.

Laiko žymas kuria (deda) patikimos trečiosios šalys - laiko žymų tarnybos (**TSA** – *Time Stamping Authorities*). Asmenys, norintys gauti laiko žymą el. duomenims, turi nusiųsti į TSA užklausą su šių el. duomenų santrauka. Laiko žyma yra įrodymas, kad el. duomenys, pavyzdžiui, skaitmeninis parašas, jau egzistavo iki žymoje užfiksuoto laiko.

## 1.7. El. parašo infrastruktūros reglamentavimas

Europos Sąjungos valstybės yra parengusios nemažai el. parašo infrastruktūrą reglamentuojančių dokumentų. Kadangi yra keturi pagrindiniai el. parašo mechanizmo dalyviai – CA, pasirašantieji asmenys, parašo tikrintojai ir TSA – tai atitinkamai grupuosime reglamentuojančius dokumentus. 1.2 pav. schemiškai parodyti šio mechanizmo dalyviai, reikalavimai jų veiklai bei naudojamai įrangai.

CA veiklos ir naudotinos įrangos reikalavimai apibrėžti šaltiniuose [1, 4, 5, 8, 9, 24, 25].

El. parašo struktūra, pasirašymo įrangos, procedūrų ir aplinkos reikalavimai apibrėžti šaltiniuose [2, 11, 12].

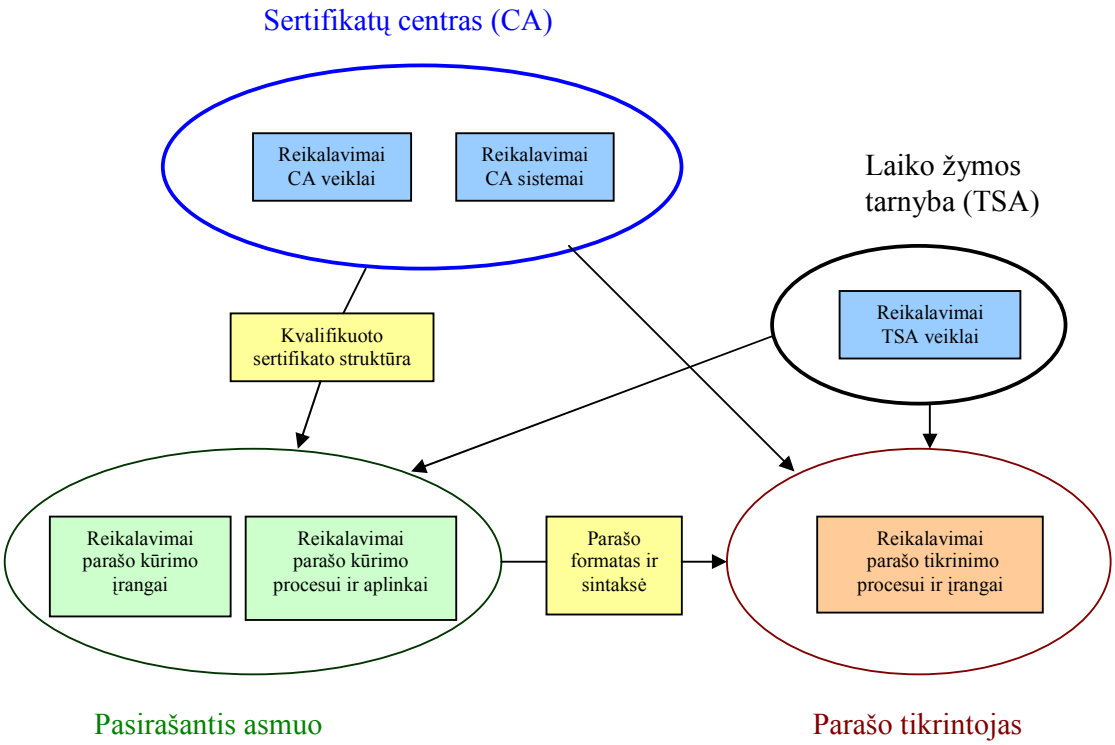
El. parašo tikrinimo procedūros ir aplinkos reikalavimai apibrėžti šaltinyje [13].

Laiko žymų tarnybų (TSA) veiklos ir įrangos reikalavimai yra šaltiniuose [3, 6, 29].

Šie reikalavimai smulkiau dėstomi kituose šios mokymo medžiagos skyriuose.

## 1.8. El. parašo infrastruktūros atitikties reikalavimams vertinimas

El. parašo infrastruktūros dalyvių atliekamos procedūros ir naudojama įranga turi atitikti nustatytus reikalavimus. CA teikiamų paslaugų, įrangos gamintojų išleidžiamų priemonių kokybę turi vertinti atitinkamos institucijos, prisilaikydamos apibrėžtų vertinimo procedūrų, taisyklių.




1.2 pav. El. parašo infrastruktūros elementų ir reikalavimų schema

EESSI (*Europen Electronic Signature Standardisation Initiative;* ši institucija, atlikus jai pavestus darbus, panaikinta 2004 m.) yra parengusi procedūrų ir įrangos atitikties nustatytiems reikalavimams vertinimo vadovus [14-18].

CA pasirengimo atlikti savo funkcijas lygiui įvertinti valstybės turi būti parengusios CA savanoriškos akreditacijos reikalavimus ir akreditavimo tvarką. Apie reikalavimus kvalifikuotus sertifikatus sudarantiems CA žiūr. [1, 15].

El. parašo įrangą leidžia gamintojai. Todėl visų pirma jie turėtų pasirūpinti išleidžiamos įrangos atitikties nustatytiems reikalavimams įvertinimu. Vartotojai - CA, TSA, el. parašų kūrėjai ir tikrintojai – turėtų

naudoti tik įrangą, turinčią patikimų kokybės kontrolės institucijų išduotą pažymėjimą-sertifikatą.

El. parašo priežiūros institucijos (tokią turime ir Lietuvoje, tai Informacinės visuomenės plėtros komitetas) turėtų akredituoti CA, tikrinti jų veiklą. Priežiūros institucijos jokia bendra veikla neturi būti susijusios su įrangos gamintojais ar paslaugų teikėjais.

# 2. ELEKTRONINIO PARAŠO ALGORITMAI

Skyriuje supažindinama su el. parašo technologijoje naudojamais duomenų santraukos gavimo SHA-1 (*Secure Hash Algorithm)* ir asimetrinio šifravimo RSA (*Rivest-Shamir-Adlemann*) algoritmais.

## 2.1. SHA-1 algoritmas

El. parašo kūrimo procese naudojami pasirašomi el. duomenys ir kita būtina informacija (pvz., pasirašančio asmens sertifikato nuoroda, kt.). Kadangi šio duomenų rinkinio apimtis gali būti didelė ir įvairi, visų pirma sukuriama trumpa fiksuoto ilgio santrauka (*hash*). Dažniausiai ji būna 128 ar 160 bitų ilgio, bet gali būti ir ilgesnė – iki 512 bitų. Skaitmeninis parašas – tai pasirašančio asmens privačiuoju raktu užšifruota santrauka.

El. parašo technologijoje naudojami įvairūs duomenų santraukos gavimo algoritmai: SHA-1 (*Secure Hash Algorithm*; duoda 160 bitų ilgio santrauką) [30], MD5 (*Message Digest algorithm 5*; 128 bitų santrauka; jau nerekomenduojamas algoritmas) [21], RIPEMD-160 (*Race Integrity Primitives Evaluation Message Digest 160*; 160 bitų santrauka), SHA-224, SHA-256, SHA-384, SHA-512, WHIRLPOOL.

Santraukos algoritmų pagrindinės savybės yra šios:

- ♦ iš santraukos neįmanoma atstatyti pačių duomenų;
- ♦ praktiškai neįmanoma rasti dviejų skirtingų duomenų, kurių santraukos būtų vienodos.

Šias savybes turintys algoritmai vadinami vienos krypties, kolizijoms atspariais santraukos algoritmais.

Šiandieną plačiausiai yra naudojamas SHA-1 algoritmas [30]. Jo paskirtis yra iš kompiuterinio pavidalo duomenų (dokumento), kurių ilgis mažesnis kaip $2^{64}$ bitai, padaryti 160 bitų ilgio santrauką. Panagrinėkime jo veikimą.

Algoritmo įeities duomenys (pvz., dokumentas) traktuojami kaip bitų seka, kurios ilgis L. Tuščio dokumento L=0. Dokumento ilgis visuomet dalinsis iš 8 (1 baitas = 8 bitai), jei jis nėra tuščias.

Pirmiausiai dokumentas yra pailginamas (*padding*). Šio veiksmo tikslas yra padaryti dokumento ilgį kartotinį skaičiui 512, t. y. $L_p=512*n$, $n>0$, bei užfiksuoti pradinį dokumento ilgį. Tam dokumentas papildomas tokiais bitais: vienu bitu lygiu 1, paskui 0 bitais, kurių kiekis priklauso nuo pradinio dokumento ilgio, ir dar 64 bitais, kuriuose įrašomas dokumento pradinis ilgis bitais.

Pavyzdžiui, turime 40 bitų ilgio dokumentą:

01100001 01100010 01100011 01100100 01100101 .

Jį papildę 1, gausime

01100001 01100010 01100011 01100100 01100101 1 .

0 (nulinių) bitų kiekis, kuriais dar reikia papildyti šį dokumentą, bus lygus 407.

Šio dokumento pradinio ilgio reikšmė 40 tam skirtuose 64 bituose užrašoma taip:

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00101000

Viso pailginto dokumento dvejetainis pavidalas bus toks:

01100001 01100010 01100011 01100100 01100101 10000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00101000

Šio dvejetainio kodo kompaktiškesnis užrašas šešioliktainiu pavidalu yra:

61 62 63 64 65 80 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 28

Bet kuriame pailgintame dokumente bus n blokų M, turinčių po 16 žodžių (1 žodis = 32 bitai), kur n>0, o $M_1$ - blokas dokumento pradžioje, $M_n$ – blokas dokumento gale (su pailginimo bitais).

SHA-1 algoritme naudojamos tokios operacijos:

- OR – loginė operacija ARBA (disjunkcija),
  AND – loginė operacija IR (konjunkcija),
  NOT – loginė operacija NE (neigimas, inversija),
  XOR – loginė operacija griežtasis ARBA (sudėtis moduliu 2).
  Šios operacijos atliekamos su atitinkamais žodžių bitais;
- **+** - sudėties operacija, kuri atliekama tik su teigiamais sveikaisiais skaičiais, kurie yra mažesni už $2^{32}$. Sudėties rezultato reikšmė visada yra mažesnė už $2^{32}$ (gautas perpildymo vienetas atmetamas);
- funkcija $S_n(X)$, kuri reiškia žodžio *X* ciklinį postūmį kairėn per n bitų, t. y. $S_n(X) = (X<<n)$ OR $(X>>(32-n))$ , kur X<<n reiškia X postūmį į kairę per n bitų, o X>>n - X postūmį į dešinę per n bitų.

Santraukai skaičiuoti naudojamos funkcijos $f_0$, $f_1$, ... , $f_{79}$. Kiekviena $f_t$ , 0<=t<=79, operuoja su trimis 32-bitų žodžiais B, C, D ir grąžina 32-bitų rezultatą. $f_t$ (B, C, D) apibrėžiamos taip:

$f_t$ (B, C, D) = (B AND C) OR ((NOT B) AND D) , kai 0<=t<=19,
$f_t$ (B, C, D) = B XOR C XOR D , kai 20<=t<=39,
$f_t$ (B, C, D) = (B AND C) OR (B AND D) OR (C AND D), kai 40<=t<=59,
$f_t$ (B, C, D) = B XOR C XOR D, kai 60<=t<=79.

SHA-1 algoritme naudojamos specialios konstantos, kurių šešioliktainis pavidalas:

$K_t$ = 5A 82 79 99 , kai 0<=t<=19,
$K_t$ = 6E D9 EB A1 , kai 20<=t<=39,
$K_t$ = 8F 1B BC DC , kai 40<=t<=59,
$K_t$ = CA 62 C1 D6 , kai 60<=t<=79.

Pailginto dokumento santraukos skaičiavimo procese naudojami du buferiai, kurie turi po 5 žodžius, bei vienas buferis, turintis 80 žodžių. Pirmojo buferio žodžiai vadinami A, B, C, D, E, antrojo - $H_0$, $H_1$, $H_2$, $H_3$, $H_4$, o trečiojo - $W_0$, $W_1$, ... , $W_{79}$. Taip pat reikalingas vieno žodžio dydžio laikinas buferis TEMP.

Skaičiuojant santrauką, kiekvienas duomenų blokas M apdorojamas atskirai. Kiekvieno bloko apdorojimas susideda iš 80 žingsnių.

Iš pradžių suteikiamos H pradinės reikšmės (toliau nurodytos jų šešioliktainės reikšmės):

$H_0$ = 67 45 23 01,
$H_1$ = EF CD AB 89,
$H_2$ = 98 BA DC FE,
$H_3$ = 10 32 54 76,
$H_4$ = C3 D2 E1 F0.

Blokai $M_1$, $M_2$, … $M_n$ iš eilės apdorojami taip:

a) daliname $M_1$ bloką į 16 žodžių $W_0$, $W_1$, ... , $W_{15}$ , kur $W_0$ yra kairysis;

b) for (t=16; t<=79; t++)

{ $W_t = S_1(W_{t-3}$ XOR $W_{t-8}$ XOR $W_{t-14}$ XOR $W_{t-16})$ }

Pastaba: šiame cikle t reikšmė keičiama nuo 16 iki 79 žingsniu 1.

$S_1$ – ciklinio postūmio kairėn per 1 bitą funkcija;

c) priskiriama A=$H_0$, B=$H_1$, C=$H_2$, D=$H_3$, E=$H_4$ ;

d) for (t=0; t<=79; t++)

{ TEMP=$S_5$(A)+$f_t$ (B,C,D)+E+$W_t$+$K_t$;
E=D; D=C; C=$S_{30}$(B); B=A; A=TEMP; }

Pastaba: šiame cikle t reikšmė keičiama nuo 0 iki 79 žingsniu 1.

$S_5$ ir $S_{30}$ – ciklinio postūmio kairėn per 5 ir 30 bitų funkcijos;

e) priskiriama $H_0=H_0+A$, $H_1=H_1+B$, $H_2=H_2+C$, $H_3=H_3+D$, $H_4=H_4+E$ ;

f) grįžtama į punktą a) likusiems, t. y. $M_2$, $M_3$, …, $M_n$ duomenų blokams apdoroti.

Apdorojus visus blokus, dokumento santrauka yra $H_0H_1H_2H_3H_4$. Šie penki žodžiai ir yra 160 bitų santrauka.

## 2.2. RSA algoritmas

RSA (Rivest, Shamir ir Adleman yra mokslininkai, sukūrę šį algoritmą) yra labiausiai paplitęs el. parašo srityje asimetrinio šifravimo algoritmas [23]. Šio algoritmo patikimumas pagrįstas didelių skaičių skaidymo į daugiklius sudėtingumu. Reikia labai daug laiko norint atspėti privatųjį raktą, kai žinomas tos poros viešasis raktas.

RSA šifravimo raktai veikia abiem kryptim, t. y. galima užšifruoti duomenis privačiuoju raktu, o atšifruoti viešuoju raktu, arba galima užšifruoti duomenis viešuoju raktu, o atšifruoti privačiuoju raktu. Tai tapo pagrindu el. parašui, kadangi parašo autorius yra vienintelis to privačiojo rakto savininkas.

Susipažinkime su RSA algoritmu. Aiškinant algoritmą naudojami tokie operacijų žymėjimai:

* - daugyba,

*mod* - sveikųjų skaičių dalyba, kurios rezultatas yra dalybos liekana.

1. Raktų generavimas:

a) imami du dideli atsitiktiniai pirminiai skaičiai p ir q (didesni už $10^{100}$). Šie du skaičiai savo dydžiu neturi skirtis labai žymiai, t. y.
$0{,}1 < |\log_2 p - \log_2 q| < 30$ , kur $\log_2$ – logaritmas pagrindu 2. Didelių atsitiktinių pirminių skaičių radimas yra nemaža problema. Plačiau apie šios problemos sprendimą galima rasti [31];

b) apskaičiuojamos sandaugos n=p*q ir s=(p-1)*(q-1). Reikalaujama, kad n reikšmei užrašyti būtų ne mažiau kaip 1020 bitų (n reikšmė būtų apie $10^{300}$ );

c) pasirenkamas skaičius e iš intervalo nuo 3 iki n-1 , kuris būtų tarpusavyje pirminis (neturintis bendro daliklio) su s. Skaičių pora (e, n) bus viešasis raktas. n vadinamas moduliu (*modulus*), o e – eksponente (*exponent*);

d) randamas toks skaičius d , kad sandaugą d*e padalinus iš s, gautųsi liekana lygi 1, t. y. (d*e) mod s = 1. Skaičių pora (d, n) bus privatusis raktas.

2. Duomenų pasirašymas (užšifravimas) ir parašo tikrinimas (atšifravimas):

a) apskaičiuojama pasirašomų el. parašu duomenų (dokumento) santrauka T pagal, pavyzdžiui, SHA-1 algoritmą;

b) skaičiaus T užšifravimui reikia apskaičiuoti $C = T^d \bmod n$. Atšifruojant skaičiuojama $T = C^e \bmod n$. Taigi, skaičiaus T užšifravimui reikia žinoti skaičių porą (d, n), o atšifravimui - skaičių porą (e, n). Pirmoji pora yra privatusis raktas, antroji pora – viešasis raktas.

3. Algoritmo iliustravimo pavyzdys:

a) tegul $p = 3$, $q = 11$ (abu pirminiai skaičiai).

b) raktų porai gauti apskaičiuojama

$n = p*q = 3*11 = 33$,

$s = (p-1)*(q-1) = (3-1)*(11-1) = 20$;

c) parenkamas skaičius e, tarpusavyje pirminis su s=20. Pavyzdžiui, e=7 (mūsų pavyzdyje galimos e reikšmės – 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31);

d) surandame tokį skaičių d, kad $(d*e) \bmod s = (d*7) \bmod 20 = 1$. Tai bus d=3.

Taigi, mūsų raktų pora: privatusis raktas $(d, n) = (3, 33)$,

viešasis raktas $(e, n) = (7, 33)$.

Tarkime, mums reikia užšifruoti skaičių x=14 (sakykime, tai gauta dokumento santraukos reikšmė). Leidžiama šifruoti skaičius nuo 1 iki n-1 (mūsų pavyzdyje n=33).

Užšifravimas vyksta taip:

a) pakeliame skaičių x=14 laipsniu d=3: $14^3 = 2744$;

b) daliname šį rezultatą iš n=33 ir sužinome dalybos liekaną:

$2744 \bmod 33 = 5$.

Taip gavome mūsų skaičiaus x=14 šifrą y=5.

Atšifravimas vyksta taip:

a) mūsų skaičiaus šifras y=5 keliamas laipsniu e=7: $5^7 = 78125$;

b) daliname šį rezultatą iš n=33 ir sužinome dalybos liekaną:

$78125 \bmod 33 = 14$.

Taip iš skaičiaus šifro y=5 atstatėme skaičių x=14.

# 3. SERTIFIKATAI

El. parašu pasirašiusio asmens tapatybę ir įgaliojimus galima patikrinti naudojant jo sertifikatą. Sertifikatas - tai asmens tapatybės dokumentas elektroninėje erdvėje. Ypač svarbi sertifikato funkcija yra jame įvardinto asmens susiejimas su tam asmeniui priklausančiais šifravimo raktais.

Sertifikatus sudaro patikimi sertifikatų centrai (CA). Jie privalo sertifikatų duomenis teikti visiems el. parašų tikrintojams bet kuriuo metu. El. paraše visada turi būti pasirašiusio asmens sertifikato nuoroda, t. y. sertifikatą sudariusio CA adresas, sertifikato serijinis numeris, sertifikato santrauka.

Šiame skyriuje aprašomi reikalavimai sertifikatams ir kokie duomenys turėtų būti juose.

## 3.1. Sertifikato struktūra ir duomenys

Sertifikato struktūrą visų pirma nustato IETF RFC 3280 standartas [24]. IETF RFC 3739 standarte [27] išdėstyti reikalavimai kvalifikuotiems sertifikatams, patikslinti reikalavimai kai kurių sertifikato laukų turiniui. ETSI TS 101 862 standartas [4] įveda papildomus laukus į sertifikatą, siekiant glaudesnio ryšio su Europos Sąjungos teisės aktais (el. parašo Direktyva 1999/93/EB).

Sertifikato struktūra, naudojant ASN.1 (*Abstract Syntax Notation One*) standarto žymėjimą, IETF RFC 3280 standarte pateikta taip:

```
Certificate ::= SEQUENCE {
    tbsCertificate          TBSCertificate,
    signatureAlgorithm      AlgorithmIdentifier,
    signatureValue          BIT STRING  }

TBSCertificate ::= SEQUENCE {
    version                 EXPLICIT Version DEFAULT v1,
    serialNumber            CertificateSerialNumber,
    signature               AlgorithmIdentifier,
    issuer                  Name,
    validity                Validity,
    subject                 Name,
    subjectPublicKeyInfo    SubjectPublicKeyInfo,
    issuerUniqueID          IMPLICIT UniqueIdentifier OPTIONAL,
        -- If present, version MUST be v2 or v3
    subjectUniqueID         IMPLICIT UniqueIdentifier OPTIONAL,
        -- If present, version MUST be v2 or v3
    extensions              EXPLICIT Extensions OPTIONAL
        -- If present, version MUST be v3      }
```

```
Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }
CertificateSerialNumber  ::=  INTEGER
Validity ::= SEQUENCE {
                    notBefore      Time,
                    notAfter       Time    }
Time ::= CHOICE {
                    utcTime          UTCTime,
                    generalTime    GeneralizedTime }
UniqueIdentifier  ::=  BIT STRING
SubjectPublicKeyInfo  ::=  SEQUENCE  {
                    algorithm              AlgorithmIdentifier,
                    subjectPublicKey     BIT STRING   }
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
  Extension  ::=  SEQUENCE  {
                    extnID        OBJECT IDENTIFIER,
                    critical      BOOLEAN DEFAULT FALSE,
                    extnValue     OCTET STRING  }
```

Matome, kad sertifikate turi būti tokie laukai:

1) sertifikato versijos numeris (*version*). Dabar naudojama v3 versija;

2) sertifikato serijinis numeris (*serialNumber*). Šį numerį suteikia CA;

3) algoritmo, kurį CA naudoja pasirašyti sertifikatams, identifikatorius (*signature*). Tai RSA su SHA-1 ar kitokio algoritmo identifikatorius. Jis turi būti toks pat, kaip ir 11 p. lauke (*signatureAlgorithm*);

4) CA, kuris sudarė ir pasirašė sertifikatą, pavadinimas (*issuer*). Nurodoma valstybė, kurioje yra CA, organizacija, organizacijos padalinio vardas ir kiti CA identifikuojantys duomenys;

5) sertifikato galiojimo laikas (*validity*). Nurodoma nuo kokios datos ir laiko, taip pat iki kokios datos ir laiko galioja sertifikatas;

6) asmuo, kuriam sudarytas sertifikatas (*subject*). Tai fizinio arba juridinio asmens vardas, kuriam priklauso sertifikate nurodytas viešasis raktas;

7) asmeniui priklausantis viešasis raktas *(subjectPublicKeyInfo*). Nurodomas algoritmo identifikatorius ir viešojo rakto reikšmė;

8) CA unikalus identifikatorius (*issuerUniqueID*). Nebūtinas laukas sertifikate;

9) asmens unikalus identifikatorius (*subjectUniqueID).* Nebūtinas laukas sertifikate;

10) sertifikato išplėtimai (*extensions*). Nebūtini laukai sertifikate. Juose nurodoma įvairi papildoma informacija;

11) algoritmo, kurį CA naudoja pasirašyti sertifikatams, identifikatorius (*signatureAlgorithm*). Tai RSA su SHA-1 ar kitokio algoritmo identifikatorius;

12) CA el. parašas (*signatureValue*). Šiame lauke užrašoma parašo reikšmė.

## 3.2. Sertifikato išplėtimai (*extensions*)

Toliau detalizuokime, kokia informacija gali būti sertifikato išplėtimų laukuose. Kiekvienas sertifikato išplėtimas turi turėti identifikatorių (pavadinimą). Jie gali būti pažymėti kaip „kritiniai"(nustatantys apribojimus) ir „nekritiniai"(paaiškinamieji). Išplėtimai skirstomi į standartinius ir internetinius-privačiuosius (asmens arba CA adresai, kt.). Standartiniai išplėtimai, kuriems pagal X.509 standartą yra duoti pavadinimai, yra šie:

1) CA raktą, naudojamą pasirašyti sertifikatams, identifikuojanti informacija (*AuthorityKeyIdentifier*). Šiame išplėtime gali būti:

- ♦ CA rakto identifikatorius;
- ♦ CA sertifikatą sudaręs kitas (aukštesnio lygmens) CA ;
- ♦ CA sertifikato serijinis numeris;

2) asmens, kuriam CA sudarė sertifikatą, rakto identifikatorius (*SubjectKeyIdentifier*). Šis išplėtimas naudojamas ypatingos paskirties raktų atvejais (pvz., kitam CA išduotas raktas, kurį jis naudos sudarytiems sertifikatams pasirašyti).

3) rakto naudojimo paskirtis (*KeyUsage*). Šiame lauke nurodomos rakto paskirtys, pvz., pasirašyti duomenims, pasirašyti sertifikatams, pasirašyti CRL sąrašams (jei raktas priklauso CA) ir/arba kitos. Kai kurių rakto paskirčių kombinacijos yra neleistinos;

4) privačiojo rakto naudojimo periodas (*PrivateKeyUsagePeriod*). Privačiojo rakto naudojimo periodas gali skirtis nuo sertifikato galiojimo periodo. Pvz., sudarant naują sertifikatą gali būti naudojami senieji raktai;

5) sertifikato taisyklių nuoroda (*CertificatePolicies*). Sertifikato taisyklių išplėtimo lauke nurodomi vienerių arba keleto sertifikato taisyklių (CP) identifikatoriai. Taip pat gali būti paaiškinimai, kur galima rasti tas taisykles, CA sertifikavimo veiklos nuostatus (CPS), kt. Plačiau apie sertifikato taisykles žiūr. 5 skyriuje SERTIFIKATO TAISYKLĖS ir kt.;

6) sertifikato taisyklių sąsajos (*PolicyMappings*). Šį išplėtimą gali turėti tik CA sertifikatai. Jame nurodomos viena arba kelios ekvivalentiškų sertifikato taisyklių poros. To reikia kryžminio sertifikavimo atvejais;

7) asmens papildomi duomenys (*SubjectAltName*). Šiame lauke užrašomi asmens el. pašto adresas, DNS vardas, IP adresas, URI identifikatorius;

8) CA papildomi duomenys (*IssuerAltName*). Šiame lauke užrašomi CA el. pašto adresas, DNS vardas, IP adresas, URI identifikatorius;

9) asmens atributai. Šis nekritinis laukas skirtas perteikti kai kurią asmenį identifikuojančią informaciją (pvz., tautybę);

10) baziniai apribojimai (*BasicConstraints*). Nurodoma, ar sertifikate nurodytas asmuo yra CA, ir koks gali būti sertifikatų sekos ilgis (sertifikatų seka – tai sertifikatų grandinė pradedant pasirašiusio asmens sertifikatu, jam sudariusio CA sertifikatas, aukštesnio lygmens CA, kuris sudarė sertifikatą žemesniam CA, sertifikatas, t.t. ir baigiant sertifikatu tokio CA, kuris sertifikatą sudarė pats sau). Jei šiame lauke yra reikšmė TRUE, tai sertifikatas priklauso CA. Eiliniams asmenims turi būti FALSE reikšmė, todėl šio išplėtimo lauko jų sertifikatuose nebūna;

11) vardų apribojimai (*NameConstraints*). Šis išplėtimas naudojamas tik CA sertifikatuose. Jame nurodomi leistini CA vardai ir jų ilgis sertifikatų sekoje. Apribojimai apibrėžiami leistinų arba draudžiamų medžio šakų terminais;

12) sertifikato taisyklių apribojimai. Šis laukas gali būti tik CA sertifikate;

13) parašo naudojimo paskirties papildomas laukas. Nurodomi sertifikato naudojimo tikslai, papildant arba vietoje lauko “rakto naudojimo paskirtis (*KeyUsage*)” (žiūr. 3 p.);

14) CRL sąrašų teikimo taškai. Nurodoma, kur galima gauti CRL informaciją;

15) draudžiamų sertifikato taisyklių išplėtimas (*inhibit Any-Policy*). Leidžiamas tik CA sertifikatuose;

16) naujausių CRL išplėtimas (*freshest CRL*). Jame nurodomi delta-CRL teikimo taškai.

## 3.3. Sertifikato papildymai pagal RFC 3739 standartą

RFC 3739 standartas [27] papildo RFC 3280 standartą [24] nuostatomis, privalomomis kvalifikuotiems sertifikatams.

Šiame standarte akcentuojama, kad sertifikato lauke, skirtame nurodyti CA, kuris sudarė ir pasirašė sertifikatą (*issuer*), turi būti atitinkami duomenys iš šio sąrašo: domeno komponentas, valstybės pavadinimas, valstijos ar provincijos pavadinimas, organizacijos pavadinimas, organizacijos padalinio pavadinimas, buvimo vietovės pavadinimas, serijinis numeris.

Asmeniui nurodyti skirtame lauke (*subject*) turi būti atitinkami duomenys iš šio sąrašo: domeno komponentas, valstybės pavadinimas, bendrasis vardas, pavardė, vardas, slapyvardis, serijinis numeris,

organizacijos pavadinimas, organizacijos padalinio pavadinimas, valstijos arba provincijos pavadinimas, buvimo vietovės pavadinimas.

Asmens atributams (*Subject Directory Attributes*) nurodyti skirtame sertifikato išplėtime (*extension*) rašomi reikalingi duomenys iš šio sąrašo: titulas, gimimo data, gimimo vieta, lytis, kurios valstybės pilietis yra, kurioje valstybėje gyvena.

Išplėtime sertifikato taisyklėms nurodyti (*Certificate Policies*) turi būti bent vienerių taisyklių identifikatorius, kurias įgyvendina CA. Jame turi būti visa taisyklių informacija, reikalinga sertifikato galiojimui patvirtinti.

Akcentuojamas sertifikato išplėtimas rakto naudojimo paskirčiai nurodyti (*key usage*).

Apibrėžiamas naujas išplėtimas asmens biometriniams duomenims nurodyti (*Biometric Information*). Jame turi būti nurodoma asmens biometrinės informacijos saugojimo vieta ir šios informacijos santrauka (*hash*).

Kvalifikuoto sertifikato statusą patvirtinantis išplėtimas (*Qualified Certificate Statements*) įvestas tam, kad aiškiai būtų išreikšta ši sertifikato savybė.

### 3.4. Sertifikato papildymai pagal ETSI TS 101 862 standartą

ETSI TS 101 862 standarte [4] nustatomi tikslesni ir įvedami papildomi reikalavimai kvalifikuotiems sertifikatams.

Sertifikato lauke, skirtame nurodyti sertifikatą sudariusiam ir pasirašiusiam CA (*issuer*), privalo būti valstybės pavadinimas, kurioje CA yra įsikūręs.

Sertifikato savybei, kad jis yra kvalifikuotas, nurodyti turi būti atskiras išplėtimas (*qCStatements extension*). Jame nurodomi tokie požymiai: sertifikatas yra kvalifikuotas; leistina operacijų (transakcijų) piniginė vertė; kiek laiko sertifikatas bus saugomas pasibaigus jo galiojimui; patvirtinimas, kad asmens privatusis raktas įrašytas į saugią laikmeną (SSCD).

### 3.5. Pavyzdys: Geteborgo universiteto CA sertifikatas [36]

| | | |
|---|---|---|
| **Version:** | | 3 (Ox2) |
| **Serial Number:** | | 12 (OxC) |
| **Signature Algorithm:** | | sha1WithRSAEncryption |
| **Issuer:** | | C=SE, O=Umea University, OU=SwUPKI-PCA, CN=SwUPKI_Policy CA |
| **Validity** | **Not Before:** | May 12 10:48:03 2005 GMT |
| | **Not After :** | May 11 10:48:03 2008 GMT |
| **Subject:** | | C=SE, O=Goteborgs universitet, CN=Goteborgs universitet CA |

**Subject Public Key Info:**
**Public Key Algorithm:** rsaEncryption
**RSA Public Key:** (2048 bit)
Modulus (2048 bit):
00:be:e5:21:fe:fd:cd:f3:00:bc:f0:16:50:79:51:f8:78:74:94:b5:74:d5:02:7c:d8:ae:60:ab:d6:ef:
dd:79:c2:da:ea:32:84:27:ec:fd:60:b8:3a:14:0f:86:68:30:98:43:f0:da:48:db:c1:b5:63:5e:9b:c7:
52:03:04:e8:c1:35:a7:9a:44:16:6a:5e:a3:51:33:09:43:a7:6c:40:bc:f0:d6:9a:c0:bc:56:eb:53:ef:
63:6b:c1:0a:98:fc:a8:d3:46:43:2e:45:5d:e6:82:90:f8:b7:d1:a2:2f:05:0e:af:b4:e5:34:10:45:55:
67:b3:75:bf:1c:f7:18:4c:e3:34:90:0e:d6:8c:0a:b0:29:10:4a:5a:8b:ec:31:42:e8:d3:99:44:4d:48:
5c:b7:52:9e:36:75:8d:26:fc:94:8a:21:87:15:95:83:d6:c0:4d:ac:8e:c8:c9:ad:86:23:31:8c:e1:24:
33:77:93:7f:71:0f:81:4a:08:35:b4:ea:a3:55:2a:c0:09:73:fe:43:50:54:d6:9e:2a:7e:0d:28:9d:5b:
41:f7:f5:40:20:2e:62:ab:d6:61:b7:ed:14:e4:b4:0c:7c:a9:7a:82:5e:5d:65:62:1b:c7:2d:c6:4a:db:
bc:2e:a8:08:db:ff:66:f5:cd:21:cd:3e:a3:6d:04:d9:5f
Exponent:
65537 (Ox10001)

**X509v3 extensions:**
**X509v3 Subject Key Identifier:**
87:D4:BD:14:DB:59:1C:B7:52:34:FE:AD:6F:47:4A:EE:93:79:FD:A9
**X509v3 Authority Key Identifier:**
**keyid:** 85:BC:EA:90:04:ED:9A:D1:47:26:46:94:5D:EA:09:31:C8:6D:31:CA
**DirName:** /C=SE/O=Umea University/OU=SwUPKI-PCA/CN=SwUPKI Policy CA
**serial:** 00
**X509v3 CRL Distribution Points:**
URI:http://crl1.swupki.org/crl_v2.crl
URI:http://crl2.swupki.org/crl_v2.crl
URI:http://crl3.swupki.org/crl_v2.crl
**X509v3 Certificate Policies:**
**Policy:** 1.2.752.43.2.1.1.1
**CPS:** http://www.swupki-pca.umu.se/CPS
User Notice:
Explicit Text: Limited Liability, see http://www.swupki.su.se/CP
**X509v3 Basic Constraints:**
CA: TRUE
**X509v3 Key Usage:** Certificate Sign, CRL Sign
**X509v3 Issuer Alternative Name**:
email: pca@swupki.su.se, URI:http://www.swupki.su.se
**Netscape Cert Type:** SSL CA, S/MIME CA, Object Signing CA

**Signature Algorithm:** sha1WithRSAEncryption
0d:16:b7:7a:63:61:b8:8c:d7:3d:67:6b:92:a8:4f:ce:9d:ca:42:97:c2:4d:73:21:eb:ac:a4:65:7c:74:
c5:2d:fd:48:42:9f:6b:44:68:b0:cd:aa:e1:1e:f9:1d:c0:ab:04:ef:c0:a5:8b:66:26:39:56:fe:1e:77:
93:aa:05:b1:30:52:4f:3f:12:58:04:3a:21:5f:d9:38:b4:a0:4b:a6:6a:c4:38:98:b2:90:49:c9:98:b5:
b9:ab:4b:0d:73:a5:33:fb:7e:4e:45:4f:0a:a3:a3:55:c9:cd:0e:a1:a9:fa:0b:86:73:99:d3:b7:77:d9:
d8:83:52:dd:8f:69:ef:f1:a5:cb:5b:92:b0:a1:c9:d0:5d:40:c3:c0:9b:e2:68:94:47:1c:9b:f0:c5:4e:
ec:53:8a:73:4b:c4:39:7c:10:81:46:c7:e3:c6:1a:01:23:05:d4:a1:9c:3c:d3:54:49:db:a6:88:ba:f0:
d3:c4:d3:54:10:a7:67:e0:34:b1:a0:d9:ca:d9:c7:76:61:cf:ab:9a:6c:8c:3f:27:7a:20:50:51:ad:8d:
93:77:1a:37:bf:27:1a:7b:6b:41:88:22:37:30:19:3f:3d:a9:11:96:25:53:98:63:52:13:e2:68:a4:52:
c0:a6:87:08:c1:93:a3:30:eb:d0:b2:3c:19:db:da:32

# 4. SERTIFIKATŲ CENTRAI (CA)

Kiekvienas el. parašu pasirašantis asmuo turi turėti sertifikatą. Sertifikatus sudaro ir vėliau jų duomenis el. parašų tikrintojams teikia sertifikatų centrai (**CA** – *Certificate Authority*). Kadangi sertifikatas yra asmens tapatybės dokumentas elektroninėje erdvėje, juos sudarančių CA patikimumas turi būti labai aukštas.

Skyriuje aprašomos CA funkcijos, struktūra ir pagrindiniai veiklos reikalavimai.

## 4.1. CA funkcijos ir struktūra

CA paskirtis yra sudaryti sertifikatus asmenims, norintiems savo veikloje naudoti el. parašą, ir sertifikatų duomenis teikti el. parašų tikrintojams. Pagrindinės jo funkcijos yra:

- registruoti asmenis, prašančius sudaryti sertifikatus, patikrinti dokumentus jų tapatybei nustatyti ir kitus pateikiamus dokumentus, kurių reikia sertifikatui sudaryti;
- sudaryti sertifikatus;
- tvarkyti sertifikatų duomenis;
- laiku sustabdyti arba atšaukti sertifikatų galiojimą, gavus atitinkamą prašymą;
- teikti atšauktų sertifikatų sąrašų (CRL) duomenis el. parašų tikrintojams.

Šioms funkcijoms vykdyti CA sudėtyje turi būti tokie tokie padaliniai:

♦ **registravimo tarnyba** (**RA –** *Registration Authority*). Ji iš asmenų priima būtinus duomenis sertifikatams sudaryti, patikrina juos ir perduoda sertifikatų sudarymo tarnybai. CA gali turėti kelias tokias tarnybas, pavyzdžiui, įvairiose vietovėse;

♦ **sertifikatų sudarymo tarnyba**. Ji iš RA gautų asmens duomenų ir viešojo rakto, gauto iš asmens kartu su jo duomenimis arba iš parašo formavimo įrangos tarnybos (papildomai tokia tarnyba gali būti CA), sudaro sertifikatą, pasirašo jį savo el. parašu ir atiduoda sertifikatų duomenų teikimo tarnybai;

♦ **sertifikatų duomenų teikimo tarnyba** (**katalogo tarnyba** - *directory service*). Sertifikatas atiduodamas jo savininkui ir užrašomas į sertifikatų duomenų bazę - katalogą. Iš pastarosios duomenų bazės pagal užklausas sertifikatų duomenys teikiami el. parašų tikrintojams;

♦ **sertifikatų atšaukimo tarnyba**. Šios tarnybos funkcijos yra nutraukti sertifikato galiojimą pačiam sertifikato savininkui paprašius,

teisėsaugos institucijų sprendimu, paprašius asmeniui, kuriam atstovauja sertifikato savininkas. Tai turi būti atliekama greitai, sugaištant ne daugiau nustatyto laiko. Informacija apie atšauktus sertifikatus kaupiama atšauktų sertifikatų sąraše (**CRL** – *Certificate Revocation List*), kuris periodiškai perduodamas CRL teikimo tarnybai;

- **CRL teikimo tarnyba**. Ji informaciją apie atšauktus sertifikatus laiko pas save ir operatyviai pagal užklausas teikia el. parašų tikrintojams. Tie el. parašai, kurie buvo sukurti sertifikato galiojimo laikotarpiu, išlieka galiojantys. El. parašas, sukurtas negaliojant sertifikatui, yra negaliojantis.

Sudarant sertifikatus, jau turi būti sugeneruoti šifravimo raktai. Viešasis raktas dedamas į sertifikatą, o privatusis raktas įrašomas į saugią laikmeną (pvz., į intelektualiąją kortelę) ir atiduodamas tik užsakiusiam asmeniui. Šifravimo raktų poroms generuoti ir parengti įrangai privatiesiems raktams saugoti ir naudoti (**SSCD** – *Secure Signature Creation Device*) CA papildomai gali turėti atitinkamą tarnybą – **parašo formavimo įrangos tarnybą**.

Raktų poras generuoti ir privačiuosius raktus rašyti į saugias laikmenas gali tuo besiverčiantys kiti paslaugų teikėjai (ne tik CA). Šiuo atveju asmuo, norėdamas gauti sertifikatą, pateikia CA ir savo viešąjį raktą.

CA veiklos procesai ir naudojama įranga turi atitikti ETSI TS 101 456, CWA 14167-1**,** CWA 14167-2 standartų reikalavimus [1, 5, 8, 9].

4.1 pav. parodyta CA struktūros schema.

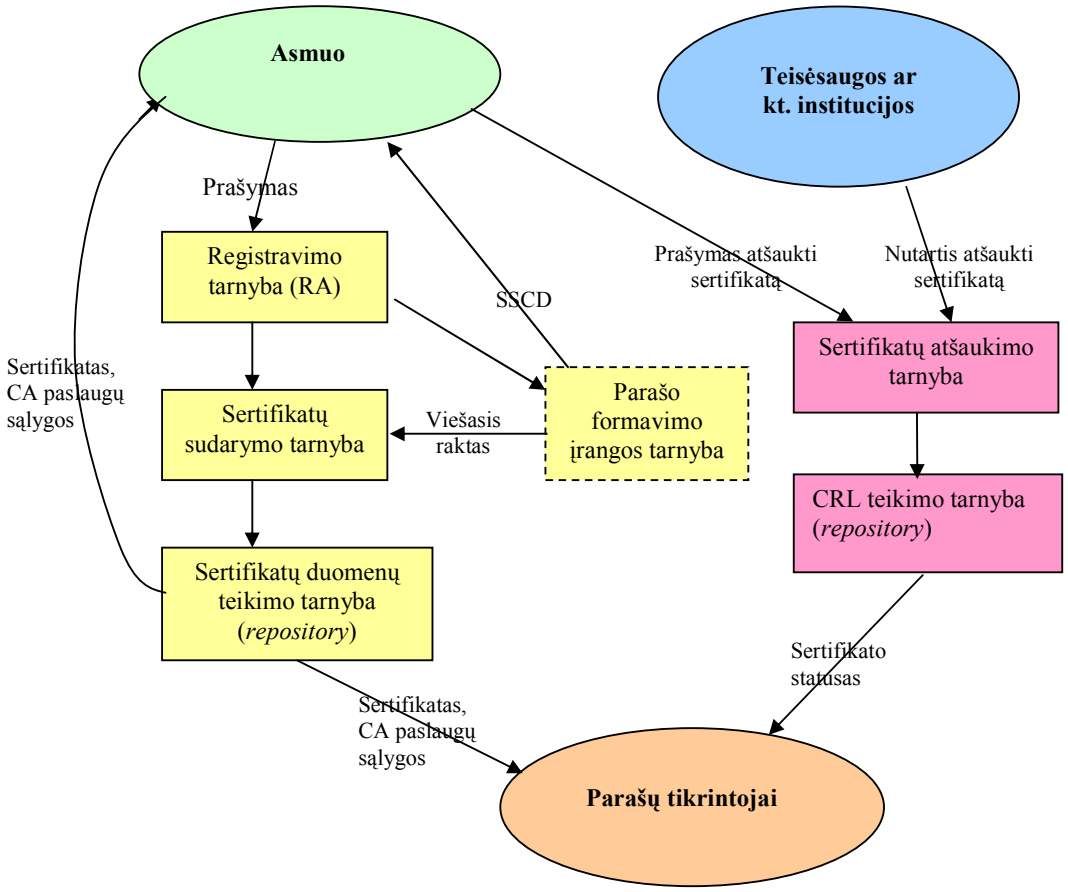
## 4.2. Reikalavimai kvalifikuotus sertifikatus sudarantiems CA

### 4.2.1. Bendrieji CA veiklos klausimai

CA, prieš pradėdamas veiklą, turi parengti savo veiklos nuostatus (**CPS** – *Certification Practice Statement*). CPS – tai pagrindinės CA veiklos taisyklės, kuriose detaliai atspindimi CA atliekami veiksmai, pradedant dokumentų priėmimu iš asmenų, sertifikatų sudarymu, ir baigiant sertifikatų duomenų teikimu el. parašų tikrintojams pagal jų užklausas. Registruodamasis el. parašo priežiūros institucijoje (Lietuvoje tokia institucija yra IVPK prie Vyriausybės), CA turi pateikti jai savo CPS. Pagal CPS ir kai kuriuos kitus dokumentus el. parašo priežiūros institucija priima sprendimą, ar CA yra pasirengęs tinkamai vykdyti sertifikavimo funkcijas, ir išduoda leidimą veiklai.

Kiekvienoje žmogaus veiklos srityje yra savi saugumo reikalavimai. Skirtingos el. parašo naudotojų grupės (valstybės institucijose, bankuose, teisėsaugoje, kt.) gali turėti savo reikalavimus, kad pasitikėtų CA

sudaromais sertifikatais. Sertifikatų sudarymo, tvarkymo ir naudojimo reikalavimai išdėstomi naudotojų grupės parengtose sertifikato taisyklėse (CP – *Certificate Policy*). Sertifikato taisyklės turi turėti identifikatorių ir būti laisvai prieinamos internetu.




4.1 pav. Sertifikatų centro (CA) struktūra

CP rengėju gali būti ir CA. Jei el. parašo naudotojų grupei šios CP yra priimtinos, jie gali naudotis to CA paslaugomis.

CA savo sertifikavimo veiklos nuostatuose (CPS) turi nurodyti identifikatorius tų sertifikato taisyklių (CP), kurias jis įgyvendina. Plačiau apie CP ir CPS žiūrėkite 5 skyriuje SERTIFIKATO TAISYKLĖS ir kt.

Toliau šiame skyriuje naudojama sąvoka:

abonentas – asmuo, atstovaujantis vienam arba daugiau asmenų, pasirašęs sutartį su CA dėl sertifikatų sudarymo ir tvarkymo.

### 4.2.2. Reikalavimai CA veiklai

***1) CA veiklos nuostatai***.

CA turi parengti savo veiklos nuostatus (CPS), kurie atitiktų pasirinktas sertifikato taisykles (CP) ir užtikrintų patikimą paslaugų teikimą, ir paskelbti internete paslaugų teikimo sąlygas;

***2) raktų tvarkymas***.

CA turi užtikrinti:

- kad raktai būtų kuriami kontroliuojamoje aplinkoje, naudojant saugią el. parašo įrangą (SSCD, žiūr. 9.6 skyrių) ir dalyvaujant bent dviems įgaliotiems darbuotojams. Raktai gali būti kuriami tiek paties CA reikmėms, tiek abonentams;
- CA privačiojo rakto konfidencialumą ir saugumą (kad šis raktas nebūtų pakeistas nežinant to CA saugumo pareigūnams);
- sertifikatuose esantiems CA parašams tikrinti skirto viešojo rakto saugumą (kad šis raktas nebūtų pakeistas nežinant to CA saugumo pareigūnams) ir autentiškumą bei šio rakto saugų teikimą el. parašo naudotojams;
- kad CA nelaikytų ir nekopijuotų abonentams parengtų privačiųjų raktų;
- kad CA privatusis raktas būtų naudojamas saugiai ir tik sertifikatams bei CRL sąrašams pasirašyti, o pasibaigus šio rakto galiojimo laikui, jis būtų sunaikinamas;
- saugų raktų porų kūrimą, kai juos savo abonentams teikia CA, ir privačiųjų raktų slaptumą;
- saugios parašo formavimo įrangos (SSCD), jei CA ją teikia savo abonentams, saugų rengimą;

***3) sertifikatų tvarkymas.***

CA turi užtikrinti:

- kad abonentai iki sutarties pasirašymo būtų tinkamai informuoti apie sertifikatų teikimo ir naudojimo sąlygas bei šių sąlygų laisvą teikimą el. priemonėmis;
- kad būtų tinkamai patikrinta asmens, kuriam sudaromas sertifikatas, tapatybė ir kiti jo duomenys;
- kad jau anksčiau užregistruoto asmens prašymas sudaryti naują arba atnaujinti senąjį sertifikatą pagal patikslintus asmens duomenis būtų išsamus ir sankcionuotas;
- sertifikatų sudarymo saugumą, padedantį išsaugoti jų autentiškumą;
- kad sertifikatų duomenys esant užklausai būtų teikiami abonentams ir el. parašų tikrintojams;

- savalaikį sertifikatų atšaukimą ar galiojimo sustabdymą remiantis prašymais asmenų, kurie turi teisę pateikti tokį prašymą, ir patikrinus jų tapatybę;

***4) valdymas ir veikla.***

CA turi užtikrinti, kad:

- jo organizacinė struktūra, administracinės ir valdymo procedūros būtų patikimos;
- jo informacija ir visa paslaugoms teikti reikalinga įranga būtų tinkamai apsaugota;
- personalas būtų reikiamos kvalifikacijos ir laikytųsi CA nustatytų taisyklių ir paslaugų teikimo tvarkos;
- būtų naudojama patikima sertifikatų tvarkymo sistema, apsaugota nuo modifikavimo (plačiau žiūr. 6 skyriuje PATIKIMA SERTIFIKATŲ TVARKYMO SISTEMA);
- tik įgalioti asmenys turėtų prieigą prie patikimos sertifikatų tvarkymo sistemos ir ji būtų naudojama teisingai su minimaliu sutrikimų pavojumi;
- fizinė prieiga prie kritinių paslaugos vietų (pvz., sertifikatų sudarymo ir pasirašymo) būtų kontroliuojama;
- nesėkmės atveju, įskaitant sertifikatams pasirašyti naudojamo CA privačiojo rakto kompromitaciją, paslaugų teikimas būtų kaip galima greičiau atstatytas;
- būtų minimizuota potenciali abonentų ir el. parašo tikrintojų žala CA nutraukus veiklą, ir su sudarytais sertifikatais susijusi informacija kaip įrodinėjimo priemonė būtų teikiama teismams bet kuriuo metu to prireikus;
- būtų laikomasi teisės aktų reikalavimų (pvz., Asmens duomenų teisinės apsaugos įstatymo, kt.);
- visa sutartyje su abonentu nurodyta informacija, susijusi su sertifikatais, būtų užrašoma ir saugoma nurodytą laiką, kad galima būtų ją panaudoti kaip įrodinėjimo priemonę teisme;
- būtų apdrausta CA civilinė atsakomybė. To reikia, kad CA galėtų padengti abonentų nuostolius savo klaidos arba nenumatytais atvejais;
- CA veikla būtų nutraukiama vadovaujantis įstatymais. Šiuo atveju turi būti nutraukiamas galiojimas visų CA sudarytų sertifikatų, o atšauktų sertifikatų sąrašas (CRL) perduotas kitam CA arba el. parašo priežiūros institucijai.

# 5. SERTIFIKATO TAISYKLĖS IR CA SERTIFIKAVIMO VEIKLOS NUOSTATAI

Kiekvienoje veiklos srityje yra savi saugumo reikalavimai. Todėl el. parašų naudotojai turi turėti galimybę įvertinti, kokiu laipsniu galima pasitikėti sertifikatų centrais (CA), jų sudarytais sertifikatais ir funkcijų atlikimo kokybe. Tam naudojamos sertifikato taisyklės (*Certificate Policy*) ir CA sertifikavimo veiklos nuostatai (*Certification Practice Statement*).

Sertifikato taisyklių rengėjas gali būti el. parašo naudotojų grupė (pvz., valstybės institucija, bankas, įmonė) arba CA. El. parašų naudotojai renkasi to CA paslaugas, kuris dirba pagal jų reikalavimus atitinkančias sertifikato taisykles.

Kiekvienas CA savo sertifikavimo veiklos nuostatuose turi nurodyti sertifikato taisykles, kurių reikalavimų jis laikosi. Sertifikato taisyklės turi būti laisvai prieinamos internetu.

Šiame skyriuje pateikiami sertifikato taisyklių ir CA sertifikavimo veiklos nuostatų klausimai [25].

## 5.1. Bendrieji klausimai

Sertifikatas - tai asmens tapatybės dokumentas elektroninėje erdvėje. Jame įvardintas asmuo susiejimas su tam asmeniui priklausančiais šifravimo raktais. El. parašo tikrintojas pasirašiusio asmens tapatybę patikrina naudodamas jo sertifikatą.

Kokiu lygiu el. parašų tikrintojai gali pasitikėti sertifikatais, priklauso nuo keleto veiksnių. Šie veiksniai priklauso nuo CA sertifikavimo veiklos nuostatų (**CPS** - *Certification Practice Statement*), nuo pasirašančiųjų asmenų įsipareigojimų (pvz., saugoti privatųjį raktą), nuo CA įsipareigojimų (pvz., garantijų ir atsakomybės ribų).

Sertifikate gali būti nurodyta, kad jis atitinka vienerias arba daugiau sertifikato taisyklių. Sertifikato taisyklės (**CP** - *Certificate Policy*) yra taisyklių rinkinys, įgalinantis spręsti apie sertifikato tinkamumą bendrus saugumo reikalavimus turinčiai parašo naudotojų grupei. CP padeda sertifikatų naudotojams (kuriantiems parašus ir parašų tikrintojams) nuspręsti, ar tas taisykles atitinkantis sertifikatas yra pakankamai patikimas tam tikrai veiklos sričiai.

## 5.2. Pagrindinės sąvokos

Plačiau apibūdinkime dvi glaudžiai susijusias sąvokas: sertifikato taisykles ir CA sertifikavimo veiklos nuostatus.

***Sertifikato taisyklės (CP)***.

Kai CA sudaro sertifikatą, tuo būsimiems sertifikato naudotojams pareiškiama, kad sertifikate nurodytas viešasis raktas yra susijęs su įvardintu asmeniu. Tačiau sertifikato naudotojai turi įvertinti, kokiu laipsniu galima pasitikėti tokiu CA pareiškimu. Gali būti įvairūs sertifikatai, sudaryti laikantis skirtingų veiklos reikalavimų ir procedūrų. Todėl jų naudojimo tikslai ir leistinos taikymo sritys gali skirtis.

CP yra taisyklių rinkinys, leidžiantis bendrus saugumo reikalavimus turinčiai el. parašo naudotojų grupei spręsti apie sertifikato tinkamumą. Pačiame sertifikate nurodoma, kokių CP laikantis buvo sudarytas tas sertifikatas.

CP atpažįstamos pagal jų unikalų identifikatorių (OID – *Object IDentificator*). CP registravimo procesas turi atitikti ISO/IEC ir ITU standartus. Asmuo (institucija), kuris registruoja CP ir suteikia joms identifikatorių, turi viešai paskelbti visą CP tekstą, kad el. parašo naudotojai galėtų susipažinti su CP.

CP yra CA akreditavimo pagrindas. Kiekvienas CA akredituojamas pagal vienerias arba daugiau CP, kurių reikalavimus jis atitinka. Kai aukštesnio lygmens CA sudaro sertifikatą žemesnio lygmens CA, sertifikato sudarytojas turi įvertinti visas žemesnio lygmens CA įgyvendinamas CP (toks įvertinimas gali remtis jo akreditacijos pagal nurodytas CP duomenimis). Įvertintas CP rinkinys nurodomas CA sudaromame sertifikate. Šios nuorodos vėliau yra naudojamos sertifikatų sekos tikrinimo procese. Sertifikatų seka – tai pasirašančio asmens parašą patvirtinančių sertifikatų eilė, susidedanti iš pasirašančio asmens sertifikato, pastarąjį sertifikatą sudariusio ir jį pasirašiusio CA sertifikato ir kitų (arba nė vieno) tokiu būdu susijusių CA sertifikatų, pasibaigianti CA, kuris pats sau sudaro ir pasirašo sertifikatą, sertifikatu.

Sertifikato išplėtimai sertifikato taisyklėms (CP) nurodyti.

Nesiplėsdami į visus sertifikato laukus, kurie yra nustatyti RFC 3280, RFC 3739, ETSI TS 101 862 [24, 27, 4] standartuose, čia akcentuosime tik sertifikato išplėtimus (*extensions*), skirtus sertifikato taisyklėms. Tai išplėtimai:

- ♦ sertifikato taisyklėms (*certificatePolicies*);
- ♦ taisyklių sąsajoms (*PolicyMappings*);
- ♦ draudžiamų sertifikato taisyklių (*inhibit Any-Policy*) išplėtimas.

Šie sertifikato išplėtimai gali būti kritiniai (apribojantys, įpareigojantys) arba nekritiniai (paaiškinamieji).

Nekritiniame išplėtime išvardinamos CP, kurias įgyvendina CA. Tačiau tai neapriboja sertifikato naudojimo vien tik tikslais, nurodytais išvardintose CP. Šiame lauke gali būti nurodytų CP paaiškinimai.

Nekritinis išplėtimas taikomosiose sistemose (el. parašą naudojančiose sistemose) interpretuojamas taip. Kiekviena taikomoji sistema suderinama (pritaikoma) reikiamoms el. parašo taisyklėms (plačiau žiūr. 8 skyriuje PARAŠO TAISYKLĖS). Tikrinant sertifikatų seką, kiekviename sekos sertifikate turi būti nurodytos tos CP, kurioms yra suderinta taikomoji sistema.

Kritinis su CP susijęs sertifikato išplėtimas atlieka aukščiau minėtas aiškinamąsias funkcijas ir turi apribojančią paskirtį. Jame nurodoma, kad sertifikatas gali būti naudojamas laikantis tik vienerių iš sertifikate išvardintų CP. Šio lauko paskirtis yra apsaugoti CA nuo kaltinimų ir reikalavimų padengti galimus nuostolius tų sertifikato naudotojų, kurie sertifikatą naudojo ne pagal CP taisykles. Kritinis CP laukas padeda sumažinti CA riziką nenumatytais atvejais.

CP taisyklių sąsajoms (*PolicyMappings*) skirtas išplėtimas gali būti tik pačių CA sertifikatuose. Šis laukas įgalina CA nurodyti, kad jo įgyvendinamos CP gali būti laikomos ekvivalenčiomis kito CA įgyvendinamoms CP. Abiem tokiems CA sertifikatus turi būti išdavęs tas pats aukštesnio lygmens CA.

Draudžiamų sertifikato taisyklių (*inhibit Any-Policy*) išplėtimas gali būti naudojamas dviems tikslams. Pirma, jame gali būti informacija, suteikianti galimybę CA reikalauti detalių CP nuorodų visuose sertifikatų sekos sertifikatuose. Sertifikatų naudotojai gali matyti, kad sertifikatų sekos pradžios sertifikatai yra sudaryti patikimo teikėjo, t. y. CA pasitikima visais sertifikatų naudojimo atvejais, ir todėl šiame sertifikato lauke nebūtina detaliai nurodyti CP. Tačiau kai CA, kuriuo pasitikima vienoje srityje (domene), prireikia remtis už tos srities ribų, jis gali pareikalauti, kad CP būtų detaliai nurodytos iš eilės einančiame kitame sertifikatų sekos sertifikate.

Kitas draudžiamų sertifikato taisyklių (*inhibit Any-Policy*) išplėtimo galimas panaudojimas yra informacijos, panaikinančios sertifikatų sekos CA įgyvendinamų taisyklių sąsajas (*PolicyMappings*), pateikimas. Gali prireikti atšaukti taisyklių sąsajas, kai reikia liudyti už srities (domeno) ribų.

Sertifikato išplėtimai CP paaiškinimams (*qualifiers*).

Sertifikato taisyklių (*certificatePolicies*) išplėtime šalia CP nuorodos dar gali būti CP paaiškinimai. Galimi tokie CP paaiškinimų tipai:

- sertifikavimo veiklos nuostatų (CPS) nuoroda. Čia pateikiama

nustatyto pavidalo rodyklė (URI – *Uniform Resource Identifier*), kur galima rasti CA sertifikavimo veiklos nuostatus;

- perspėjamasis tekstas asmenims (įskaitant abonentus ir parašų tikrintojus) dėl naudojimosi sertifikatu. CA gali prašyti, kad asmuo patvirtintų, ar jis sutinka su įgyvendinamomis CP.

***Sertifikavimo veiklos nuostatai (CPS).***

CPS – tai pagrindinės CA veiklos taisyklės, kuriose turi būti nurodytos įgyvendinamos sertifikato taisyklės (CP).

CPS gali būti dvejopo pavidalo: CA deklaracijos pavidalo, patvirtinančios atliekamų veiksmų patikimumą, arba kaip CA įstatai ar reglamentas. CPS gali būti nurodomi sutartyse tarp CA ir abonentų. CPS gali būti parengti remiantis daugeliu dokumentų, kaip įstatymai, privačios sutartys ar deklaracijos.

## 5.3. Santykis tarp sertifikato taisyklių ir sertifikavimo veiklos nuostatų

Sertifikavimo veiklos nuostatai (CPS) yra detalus, sertifikatų naudotojams suprantamas CA veiksmų išdėstymas. Detalumo laipsnis gali varijuoti, tačiau visada CPS yra detalesnis dokumentas už sertifikato taisykles (CP).

Tam tikras detalumas yra privalomas, kad sertifikatų naudotojai pajėgtų įvertinti CA patikimumą, nesant akreditacijos ar kitokio jo kokybės įvertinimo. Tačiau CPS nėra tinkama vieta nurodyti skirtingų CA sąveiką. CA sąveikai pagrįsti geriau tinka CP. CA pagal savo CPS gali būti kelerių CP, numatytų skirtingiems tikslams ir naudojamų skirtingose vartotojų grupėse, įgyvendintojas. Taip pat skirtingi CA su skirtingais CPS gali būti vienerių CP įgyvendintojai.

Norimi CP ir CPS bruožai yra šie:

- dauguma organizacijų, besinaudojančių viešaisiais arba keleto institucijų CA, nori, kad CA sertifikavimo veiklos nuostatuose (CPS) būtų dokumentuota organizacijai priimtina tvarka. CPS yra viena iš priemonių, apsauganti CA nuo ginčų su abonentais ir kitais sertifikatų naudotojais bei nustatanti CA santykius su jais;
- kita vertus, yra didelis stimulas taikyti CP plačiam organizacijų ratui. Jei tam tikros CP pripažįstamos ir taikomos plačiai, tai yra pagrindas automatizuoti sertifikatų tikrinimą įvairiose sistemose.

CPS ir CP sudaro visumą, apimančią nemažai tokių pačių klausimų. CP gali būti kaip atskiras dokumentas. CPS taip pat gali būti atskiras dokumentas, kurio kiekvienas elementas (reikalavimas, nuostata, sąlyga)

turi būti susietas su vieneriomis ar daugiau CP. Pagrindinės dalys, kurios turi būti CP ar CPS, yra šios:

- ♦ įvadas;
- ♦ informacijos teikimas ir teikėjo atsakomybė;
- ♦ asmenų tapatybės ir duomenų autentiškumo tikrinimas;
- ♦ sertifikatų tvarkymo reikalavimai;
- ♦ aplinka, valdymas ir darbo kontrolė;
- ♦ techninis saugumas;
- ♦ sertifikatų, CRL ir OCSP profiliai (struktūra);
- ♦ atitikties auditas ir įvertinimas;
- ♦ kiti veiklos ir teisiniai klausimai.

## 5.4. Sertifikato taisyklių ir CA sertifikavimo veiklos nuostatų struktūra

Toliau pateikiama sertifikato taisyklių (CP) struktūra. Panašios struktūros turi būti ir CA sertifikavimo veiklos nuostatai (CPS) [25]. Jei laikomasi standartinės CP ir CPS formos, tai bus lengviau:

- ♦ palyginti dvejas CP kryžminio sertifikavimo atvejais (CP ekvivalentiškumui nustatyti);
- ♦ palyginti CPS su CP tikrinant, ar CPS tiksliai atitinka įgyvendinamas CP;
- ♦ palyginti dvejus CPS (skirtingų CA).

Nežiūrint to, kad ETSI TS 101 456 standartas [1] nereikalauja laikytis vienodos CP ar CPS dokumentų struktūros, tačiau rekomenduojama CP ir CPS struktūra yra tokia:

1. ĮVADAS
1.1. Apžvalga (*santrauka*)
1.2. Pavadinimas ir identifikatorius
1.3. PKI dalyviai (*paslaugų teikėjai, parašo naudotojai*)
1.4. Sertifikatų naudojimo sritys
1.5. Atsakingoji institucija (*kontaktiniai duomenys*)
1.6. Apibrėžimai ir santrumpos

2. INFORMACIJOS TEIKIMAS IR TEIKĖJO ATSAKOMYBĖ
(*CP, CPS, sertifikatų duomenų ir CRL sąrašų teikimo klausimai*)

3. ASMENŲ TAPATYBĖS IR DUOMENŲ AUTENTIŠKUMO TIKRINIMAS
3.1. Reikalavimai vardams
3.2. Pradinis asmens duomenų patikrinimas
3.3. Prašymų pakeisti raktus tikrinimas
3.4. Prašymų atšaukti ar sustabdyti sertifikatų galiojimą tikrinimas

4. SERTIFIKATŲ TVARKYMO REIKALAVIMAI
4.1. Prašymas sudaryti sertifikatą
4.2. Prašymo sudaryti sertifikatą vykdymas
4.3. Sertifikato sudarymas
4.4. Sertifikato galiojimo pradžia
4.5. Raktų porų ir sertifikatų naudojimas
4.6. Sertifikatų atnaujinimas
4.7. Rakto keitimas sertifikate
4.8. Sertifikatų keitimas
4.9. Sertifikatų atšaukimas ir galiojimo sustabdymas
4.10. Sertifikatų statuso informacijos teikimo paslaugos
4.11. Abonemento pabaiga
4.12. Raktų atstatymas

5. APLINKA, VALDYMAS IR DARBO KONTROLĖ
5.1. Fizinės aplinkos reikalavimai (*patalpos, energijos teikimas, apsauga, kt.*)
5.2. Procedūrų kontrolė
5.3. Personalo kontrolė
5.4. Audito procedūros
5.5. Įrašų dėjimas į archyvą
5.6. Raktų keitimas
5.7. Rakto kompromitacijos ir veiklos sutrikimų pasekmių šalinimas
5.8. CA ar RA veiklos nutraukimas

6. TECHNINIS SAUGUMAS
6.1. Raktų porų generavimas ir įdiegimas
6.2. Privačiojo rakto apsauga ir kriptografinio modulio valdymas
6.3. Kiti raktų porų tvarkymo klausimai
6.4. Privačiojo rakto aktyvavimas (*pvz., įvedus PIN kodą, pirštų atspaudus*)
6.5. Kompiuterių sauga
6.6. Techninių priemonių priežiūra
6.7. Tinklo sauga
6.8. Laiko žymų naudojimas

7. SERTIFIKATŲ, CRL IR OCSP PROFILIAI (*struktūra, parametrai*)
7.1. Sertifikatų profilis
7.2. CRL profilis
7.3. OCSP profilis

8. ATITIKTIES AUDITAS IR ĮVERTINIMAS
8.1. Vertinimo dažnis ir aplinkybės
8.2. Vertintojai ir jų kvalifikacija
8.3. Vertintojo ir tikrinamo padalinio ryšiai
8.4. Tikrinamieji dalykai (*topics*)

8.5. Veiksmai pastebėjus trūkumus
8.6. Tikrinimo rezultatų pranešimas

9. KITI VEIKLOS IR TEISINIAI KLAUSIMAI
9.1. Rinkliavos
9.2. Finansinė atsakomybė
9.3. Slaptoji informacija
9.3. Atsakomybė už slaptosios informacijos saugojimą
9.4. Asmens duomenų apsauga
9.5. Intelektinės nuosavybės apsauga
9.6. Atsakomybė ir garantijos
9.7. Garantijų nutraukimas
9.8. Atsakomybės apribojimai
9.9. Civilinės atsakomybės draudimas
9.10. Terminai ir paslaugų nutraukimas
9.11. Individualios pastabos ir ryšiai su PKI dalyviais
9.12. Pataisų darymas
9.13. Ginčų sprendimas
9.14. Teisinė bazė
9.15. Atitikimas teisės aktams
9.16. Kiti klausimai

Įvairių valstybių CA įgyvendinamų sertifikato taisyklių ir sertifikavimo veiklos nuostatų pavyzdžių galima rasti internete [37; 40].

# 6. PATIKIMA SERTIFIKATŲ TVARKYMO SISTEMA

CA sudaromi sertifikatai yra asmens tapatybės dokumentas elektroninėje erdvėje. Todėl CA veiklai keliami aukšti reikalavimai, ir jis savo darbe turi naudoti patikimą kompiuterinę sistemą sertifikatams tvarkyti.

Šiame skyriuje dėstomi reikalavimai CA sertifikatų tvarkymo sistemoms.

## 6.1. Bendrosios nuostatos

Čia aprašomi saugumo reikalavimai kvalifikuotų ir nekvalifikuotų sertifikatų tvarkymo sistemoms, kokias turėtų naudoti CA.

Kvalifikuotus sertifikatus sudarantys CA turi naudoti patikimas sistemas ir priemones, apsaugotas nuo pakeitimų ir garantuojančias technologinį bei kriptografinį procesų saugumą.

Patikimos sertifikatų tvarkymo sistemos (toliau – Sistema) reikalavimai nekvalifikuotų sertifikatų (NQC - *Non-Qualified Certificates*) atveju yra mažesni nei kvalifikuotų sertifikatų (QC – *Qualified Certificates*) atveju. Tolesniame dėstyme atkreipiamas dėmesys į šiuos skirtumus.

Saugumo reikalavimai yra svarbūs Sistemų gamintojams ir CA, diegiantiems tokias Sistemas ir norintiems atitikti nustatytus reikalavimus patiems CA. Gamintojų teikiamos Sistemos turi atitikti CWA 14167-1 standarte [8] nustatytus saugumo reikalavimus. Gamintojas turi pateikti liudijimą (sertifikatą, deklaraciją), kad jo teikiama Sistema atitinka reikalavimus. CA turi naudoti tik saugumo reikalavimus atitinkančią Sistemą.

Reikalavimai Sistemai skaidomi į dalis pagal CA funkcijas. Realiai gali būti taip, kad CA naudos ne vieną Sistemą, o atskiras posistemes, atliekančias tam tikras funkcijas ir skirtas tam tikroms paslaugoms teikti. Tačiau tai nekeičia požiūrio į Sistemą apskritai ir saugumo reikalavimus jai.

Sistema padeda CA atlikti jam pavestas funkcijas. Funkcijos skirstomos į privalomas pagrindines (*Core Functionality*, tai penkios pagrindinės CA funkcijos, žiūr. 4 skyrių SERTIFIKATŲ CENTRAI) ir neprivalomas papildomas (*Supplementary Functionality,* tai parašo kūrimo įrangos SCDev ir laiko žymų teikimo paslaugos). Jeigu CA teikia ir papildomas paslaugas, jos naudojama Sistema turi atitikti ir papildomus reikalavimus. Sistemos funkcijos turi atitikti saugumo reikalavimus, aprašytus CWA 14167-1 standarte [8].

## 6.2. Saugumo reikalavimų lygiai ir reikalavimų grupės

Sistemos saugumo reikalavimai yra dviejų lygių:

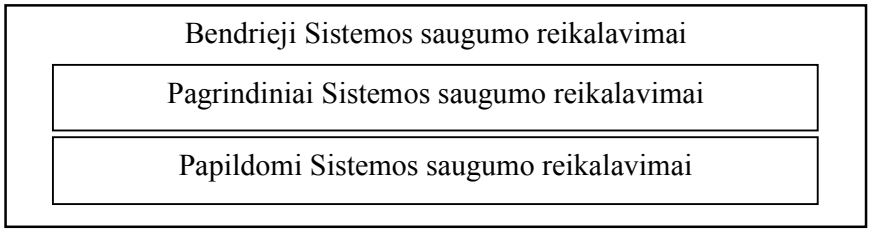
- ♦ reikalavimai Sistemai, kai CA teikia nekvalifikuotus sertifikatus (NQC);
- ♦ reikalavimai Sistemai, kai CA teikia kvalifikuotus sertifikatus (QC).

Sistema turi atitikti vieno lygio reikalavimus, bet ne abu vienu metu.

Sistemos saugumo reikalavimai skirstomi į tokias grupes:

- ♦ bendruosius;
- ♦ pagrindinius;
- ♦ papildomus.

Bendrieji saugumo reikalavimai yra privalomi visoms Sistemos funkcijoms (žiūr. 6.1 pav.).




6.1 pav. Saugumo reikalavimai CA naudojamoms Sistemoms

Į reikalavimus taip pat įeina Sistemoje naudojamų el. parašo algoritmų reikalavimai ir šių algoritmų parametrai [31].

## 6.3. Bendrieji Sistemos saugumo reikalavimai

Bendruosius Sistemos saugumo reikalavimus sudaro šios dalys:

1. Sistemos saugumo užtikrinimas (*Systems and Security Management*)

Sistemoje turi būti priemonės nustatyti ir kontroliuoti su Sistema dirbančių asmenų teises ir pareigas. Sistemą eksploatuoti ir prižiūrėti gali šie pareigūnai:

- ♦ saugumo pareigūnai;
- ♦ registracijos pareigūnai;
- ♦ Sistemos administratoriai;
- ♦ Sistemos operatoriai;
- ♦ Sistemos auditoriai.

Reikalaujama, kad atskirų pareigūnų įtakos zonos nepersidengtų, pavyzdžiui, darbuotojas, kuriam suteikti saugumo pareigūno įgaliojimai, negali būti kartu Sistemos auditorius.

2. Sistemos veikimas (*Systems&Operations*)

Tai reikalavimai tokiems dalykams, kaip:

1) **veiksmų atlikimas** (*Operations Management*). Sistema turi būti eksploatuojama teisingai, kad būtų minimizuota sutrikimų rizika, apsaugota nuo virusų, nuo nesankcionuotų pakeitimų. Sistemos gamintojas turi pateikti sistemos instaliavimo, administravimo ir naudojimo instrukcijas;

2) **CA veiklos nenutrūkstamumas** (*Business Continuity*). CA veikla neturi nutrūkti netgi įvykus Sistemos gedimams. Sertifikatų duomenų, CRL sąrašų teikimas bei prašymų atšaukti sertifikatus aptarnavimas neturi nutrūkti ilgam, panaudojus alternatyvias Sistemas. Sistemos atstatymas neturi turėti įtakos Sistemos patikimumui;

3) **sistemos veiksmų sinchronizavimas laike** (*Time Synchronisation*). Sertifikatų sudarymas ir jų tvarkymas (pvz., galiojimo nutraukimas) yra susijęs su laiku. Sistema turi būti sinchronizuota su standartiniu laiko šaltiniu UTC (*Co-ordinated Universal Time*, Grinvičo laikas). Pastebėkime, kad tai nėra susiję su jokiomis laiko žymomis, apie kurias rašoma 10 skyriuje LAIKO ŽYMA. Sistemos laikrodžio sinchronizavimo su UTC laiku reikalavimai kvalifikuotus sertifikatus sudarantiems CA yra griežtesni negu nekvalifikuotų sertifikatų atveju. Kvalifikuotus sertifikatus sudarančių CA Sistemos privalo būti sinchronizuotas su UTC laiku vienos sekundės tikslumu.

3. Identifikavimas ir autentifikavimas (*Identification & Authentification*)

Tik CA įgalioti asmenys gali kreiptis ir naudoti Sistemą. Tokią kontrolės funkciją turi turėti visi komponentai. Į Sistemą besikreipiančių asmenų identifikavimą ir autentifikavimą gali atlikti atitinkama programinė įranga arba betarpiškai naudojamas komponentas.

Šis reikalavimas skaidomas į tokias dalis:

1) **vartotojų autentifikavimas** (*User Authentification*). Kiekvienas CA darbuotojas turi būti identifikuotas ir suteikti jam įgaliojimai dar iki veiksmų su Sistema darymo;

2) **autentiškumo nepripažinimas** (*Athentification Failure*). Po nustatyto kiekio nesėkmingų autentifikavimo bandymų Sistema turi užblokuoti tolesnius darbuotojo autentifikavimo bandymus ir užfiksuoti tokį faktą;

3) **slaptųjų elementų tikrinimas** (*Verification of Secrets*). Sistemoje turi būti priemonės patikrinti, ar jos komponentų slaptieji elementai (pvz., slaptažodžiai, PIN kodai) atitinka nustatytus reikalavimus. Bet kuriuo atveju Sistemos slaptųjų elementų atskleidimo arba neleistinos prieigos tikimybė turi būti labai maža.

4. Patekimo į Sistemą kontrolė (*System Access Control*)

Tokios kontrolės pagrindinis tikslas yra užtikrinti, kad Sistemos objektus naudotų tik identifikuoti ir atitinkamus įgaliojimus turintys darbuotojai. Tai taikoma visiems CA jautriems objektams. Patekimas į Sistemą gali būti kontroliuojamas atitinkama programine įranga arba betarpiškai naudojamu Sistemos komponentu.

Sistema turi turėti galimybę kontroliuoti ir apriboti identifikuotų asmenų prieigą prie Sistemos arba objektų, nežiūrint ar asmenys yra objektų savininkai ar tik atsakingi už objektus.

Sistema turi apsaugoti nuo prieigos prie viešai neskelbtinos darbo procese išliekančios informacijos.

5. Raktų tvarkymas (*Key Managemet*)

Skiriamos trys CA raktų kategorijos:

- ♦ raktai sertifikatams pasirašyti;
- ♦ infrastruktūriniai raktai saugiam duomenų perdavimui tarp atskirų Sistemos dalių arba saugomiems duomenims (pvz., audito duomenims) pasirašyti;
- ♦ Sistemos kontroliniai raktai, kuriuos naudoja CA darbuotojai, dirbantys su Sistema.

Saugumo reikalavimai šioms trims raktų kategorijoms yra nevienodi. Didžiausi yra sertifikatų pasirašymo raktams, o mažiausi – darbuotojų kontroliniams raktams. Infrastruktūriniai ir kontroliniai raktai gali būti simetrinio arba asimetrinio metodo.

Raktų tvarkymo reikalavimų dalys:

1) **raktų generavimas** (*Key Generation*). Raktai sertifikatams pasirašyti turi būti generuojami ir saugomi saugiame kriptografiniame modulyje, kontroliuojant dviem asmenims. Kriptografinis modulis turi atitikti CWA 14167-2 standarto [9] arba kitokio jį atitinkančio standarto, pvz., FIPS 140-2 Level 3 ar ISO/IEC 15408 [32, 42-45], reikalavimus. Sugeneruoti infrastruktūriniai ir kontroliniai raktai turi būti laikomi aparatūrinėje (*hardware*) kriptografinėje įrangoje. Raktai turi būti generuojami laikantis nustatytų algoritmų ir parametrų [31];

2) **raktų tiekimas** (*Key Distribution*). Atviru pavidalu privatieji raktai asmenims neturi būti tiekiami, o turi būti perduodami nustatytu būdu. Viešieji raktai, kurie nėra dedami į jokį sertifikatą, turi būti laikomi saugiai, kad būtų išvengta jų perėmimo ar manipuliacijų su jais. Tie viešieji raktai, kurie dedami į sertifikatus ir tiekiami abonentams bei parašų tikrintojams, turi būti platinami garantuojant jų vientisumą (neiškraipymą) ir autentiškumą;

3) **raktų naudojimas** (*Key Usage*). Visi saugūs kriptografiniai moduliai, naudojami sertifikatams pasirašyti, infrastruktūriniams ar Sistemos kontroliniams raktams laikyti ir naudoti, turi turėti kreipimosi į juos kontrolės priemones (turi reikalauti PIN kodo ar kt.). Raktas turi būti naudojamas tik tai funkcijai, kuriai jis yra skirtas. Naudojant raktus būtina įsitikinti, kad galioja juos atitinkantys sertifikatai;

4) **raktų keitimas** (*Key Change*). Infrastruktūriniai ir Sistemos kontroliniai raktai turi būti keičiami kasmet. Jei Sistemoje naudojami algoritmai tampa nebepatikimi, raktai turi būti keičiami nedelsiant;

5) **raktų naikinimas** (*Key Destruction*). Pasibaigus sertifikatams pasirašyti naudojamų raktų galiojimo terminui, jie turi būti sunaikinti. Jei Sistemoje yra raktų generavimo funkcija, o sugeneruoto rakto atsisakoma, tai jis turi būti sunaikintas. Naikinant raktus, jų duomenys turi būti ištrinami tiek iš programinės, tiek iš techninės įrangos;

6) **raktų saugojimas, kopijavimas ir atstatymas** (*Key Storage, Backup & Recovery*). Privatieji raktai turi būti laikomi saugiai. Sertifikatams pasirašyti skirtas privatusis raktas turi būti laikomas saugiame kriptografiniame modulyje, atitinkančiame nustatytus reikalavimus. Infrastruktūriniai ir Sistemos kontroliniai privatieji raktai turi būti saugomi aparatūrinėje kriptografinėje įrangoje. Sistema turi leisti tik įgaliotam asmeniui - saugumo pareigūnui - kopijuoti, įrašyti ar atstatyti visų paskirčių privačiuosius raktus. Sertifikatams pasirašyti naudojamas privatusis raktas gali būti kopijuojamas, įrašomas ar atstatomas tik kontroliuojant dviem asmenims. Sistemoje neturi būti priemonių, įgalinančių kopijuoti ar atstatyti CA abonentų raktus;

7) **raktų dėjimas į archyvą**. Sistemoje neturi būti priemonių, įgalinančių archyvuoti abonentams sukurtus privačiuosius raktus.

6. Apskaita ir auditas (*Accounting & Auditing*)

CA veiklos patikimumas turi būti aukštas. Todėl turi būti vedama griežta apskaita, kaupiami audito duomenys ir reguliariai atliekamas auditas.

Reikalavimai apskaitai ir auditui skirstomi į tokias grupes:

1) **audito duomenys** (*Audit Data Generation*). Kaip minimumas turi būti fiksuojami Sistemos įrangos (aplinkos), šifravimo raktų ir sertifikatų tvarkymo darbai, šių darbų pradžios ir pabaigos laikas, audito duomenų parametrų keitimai, kt.;

2) **prieigos prie audito duomenų garantijos** (*Guarantees of Audit Data Availability*). Audito duomenims laikyti turi būti skiriama pakankamai vietos, ankstesnio audito duomenys automatiškai neturi būti ištrinami;

3) **audito duomenų parametrai** (*Audit Data Parameters*). Reikalaujama, kad kiekvienas audito duomenų įrašas turėtų datą ir laiką, būtų nurodytas audito duomenų pobūdis (fiksuojamas įvykis), kas atsakingas už veiksmus, kokie sprendimai buvo priimti dėl įvykio;

4) **audito duomenų pasirinktinė peržiūra** (*Selectable Audit Review*). Sistemoje turi būti galimybė susirasti audito duomenis pagal jų tipą ir/arba pagal vartotoją, su kuriuo tie duomenys yra susiję. Audito duomenys turi būti suprantamos formos;

5) **audito duomenų peržiūros apribojimas** (*Restricted Audit Review*). Reikalaujama, kad Sistema neleistų vartotojams skaityti audito duomenų, išskyrus įgaliotuosius asmenis – Sistemos auditorius. Audito įrašų keitimas yra draudžiamas;

6) **pavojaus signalų generavimas** (*Generation of Alarm*). Sistema turi perspėti apie bandymus pažeisti saugumą. Tuomet turi būti, pavyzdžiui, pasiunčiama el. pašto žinutė Saugumo pareigūnui arba kitaip signalizuojama apie pavojų;

7) **audito duomenų vientisumo garantija** (*Guarantees of Audit Data Integrity*). Sistema turi garantuoti audito duomenų vientisumą, naudojant el. parašą, duomenų santraukas (*hash)* ar kitokias priemones;

8) **audito atlikimo laiko garantija** (*Guarantees of Audit Timing*). Audito duomenų sukūrimo laikui užfiksuoti turi būti naudojamas patikimas laiko šaltinis.

7. Duomenų archyvavimas (*Archiving*)

Archyvavimo reikalavimų dalys yra šios:

1) **archyvuojami duomenys** (*Archive Data Generation*). Sistema turi turėti duomenų archyvavimo priemones. Kaip minimumas į archyvą turi būti dedami šie duomenys: visi sertifikatai, visi CRL sąrašai, visi audito duomenys. Kiekvienas archyvuojamas duomuo turi turėti atsiradimo laiką, o kritinio saugumo duomenys turi būti laikomi užkoduotu pavidalu;

2) **pasirinktinė paieška** (*Selectable Search*). Sistemoje turi būti priemonės įrašų pagal duomenų tipą paieškai archyve;

3) **archyvo duomenų vientisumas** (*Integrity of Archived Data*). Archyvo duomenys turi būti apsaugoti nuo pakeitimo.

8. Duomenų kopijų darymas ir sistemos atstatymas (*Backup & Recovery*)

1) **kopijų darymas** (*Backup Generation).* Sistemoje turi būti priemonės duomenų kopijoms daryti. Turi būti daromos kopijos tik tų duomenų, kurių reikia Sistemos stoviui atstatyti (pvz., po gedimų). Kopijas gali daryti tik įgalioti asmenys – Sistemos operatorius kartu su saugumo pareigūnu;

2) **kopijų informacijos vientisumas ir konfidencialumas** (*Integrity and Confidenciality of Backup Information*). Duomenų kopijos turi būti apsaugotos nuo pakeitimo, naudojant el. parašus, duomenų santraukas (*hash)* ar kitokias priemones;

3) **sistemos atstatymas** (*Recovery*). Sistemoje turi būti priemonės, įgalinančios atstatyti Sistemos stovį (pvz., po gedimų) iš duomenų kopijų. Sistemos atstatymo darbus gali atlikti tik įgalioti asmenys – Sistemos operatorius kartu su saugumo pareigūnu.

## 6.4. Pagrindiniai Sistemos saugumo reikalavimai

Pagrindiniai saugumo reikalavimai skirstomi į tokias grupes:

1. Bendrojo pobūdžio reikalavimai

Visi CA tarnybų siuntinėjami pranešimai turi būti apsaugoti naudojant el. parašus, duomenų santraukas (*hash*) ar kitokias priemones. Pranešimuose turi būti jų sukūrimo laikas, taip pat atsitiktinis skaičius (*nonce*), padedantis apsisaugoti nuo klaidų.

2. Abonentų registravimo reikalavimai (*Registration Service*)

Į CA funkcijas įeina asmenų, prašančių sudaryti sertifikatą, tapatybės ir kitų jų duomenų patikrinimas bei pateiktų duomenų tvarkymas ir saugojimas.

Reikalavimai šioms funkcijoms apima tokius klausimus, kaip:

1) **prašymas sertifikatui gauti** (*Certificate Application*). Registracijos pareigūnas įstatymų leistinomis priemonėmis turi patikrinti prašytojo tapatybę ir jo pateiktus duomenis sertifikatui sudaryti.

Jei prašyme yra asmens privatūs duomenys, tai registravimo tarnyba (RA), siųsdama juos sertifikatų sudarymo tarnybai, turi garantuoti konfidencialumą. Tam Sistema turi turėti atitinkamas priemones.

RA turi būti įdiegusi priemones prašytojo pateikiamam viešajam raktui patikrinti, ar jis atitinka jo turimą privatųjį raktą ir algoritmus.

RA turi surinkti visus duomenis, būtinus kvalifikuotam sertifikatui sudaryti (jei sudaromi tokios rūšies sertifikatai).

Sistema turi sudaryti sąlygas registravimo pareigūnui patvirtinti (pvz., pasirašyti) gautą prašymą, prieš išsiunčiant jį iš RA kitoms CA tarnyboms.

Kvalifikuoto sertifikato atveju prie prašymo turi būti pridedamas jo pateikimo laikas ir sertifikato paskelbimo kontrolinė informacija (per kiek laiko bus sudarytas sertifikatas ir pateiktas sertifikatų duomenų teikimo tarnybai).

RA siunčiami pranešimai turi būti autentifikuoti arba pasirašyti infrastruktūriniu arba kontroliniu raktu;

2) **abonento duomenų tvarkymas** (*Subscriber Data Management*). Sistema turi turėti priemones abonento duomenims apsaugoti nuo iškraipymo ir jų konfidencialumui garantuoti;

3) **RA auditas** (*Registration Service Audit*). RA turi registruoti visus prašymus sertifikatams gauti, įskaitant prašymus pakeisti raktus sertifikatuose.

3. Sertifikatų sudarymo reikalavimai (*Certificate Generation Service*)

Funkcijos ir reikalavimai:

1) **sertifikatų sudarymo procedūra** (*Certificate Generation*). Atėjus iš RA prašymui sudaryti sertifikatą, Sistema sudaro sertifikatą, įtraukdama į jį pateiktą viešąjį raktą. Tokiu būdu abonentas susiejamas su jam priklausančiu viešuoju raktu.

Sistema taip pat gali siųsti CA infrastruktūrinius ar kontrolinius viešuosius raktus sertifikatų sudarymo tarnybai, kad ir jiems būtų sudaryti sertifikatai.

Sudarius sertifikatą, jis gali būti perduotas užsakiusiam asmeniui tiesiogiai per sertifikatų duomenų teikimo tarnybą arba per parašo formavimo įrangos teikimo tarnybą (jei CA tokią turi).

CA tarnyboms sukurti infrastruktūriniai ar kontroliniai sertifikatai gali būti perduodami tiesiogiai.

Reikalaujama, kad sertifikatų sudarymo tarnyba užtikrintų jai atsiųstų prašymų sertifikatui sudaryti vientisumą, šaltinio autentiškumą, o esant reikalui, ir atsiųstų prašymų konfidencialumą.

Gauti prašymai turi būti apdorojami saugiai, turi būti patikrinama, ar jie atitinka CA įgyvendinamas sertifikato taisykles (CP).

Prieš sudarydama sertifikatą Sistema turi patikrinti pareigūno įgaliojimus.

CA privatusis raktas, skirtas pasirašyti kvalifikuotiems sertifikatams, turi būti naudojamas tik šiems tikslams arba atitinkamiems CRL sąrašams pasirašyti.

Turi būti sudaromi tik sertifikatų sudarymo tarnybos saugumo pareigūno nustatyto profilio (struktūros, parametrų) sertifikatai.

Visuose Sistemos sudarytuose nekvalifikuotuose sertifikatuose (NQC) turi būti:

- asmens vardas arba slapyvardis. Jei yra slapyvardis, tas turi būti aiškiai pabrėžta;
- viešasis raktas, atitinkantis asmens privatųjį raktą;

- CA el. parašas, sukurtas naudojant CA privatųjį raktą, skirtą pasirašyti NQC;
- Sistemos suteiktas unikalus sertifikato vardas ir serijos numeris. Tas unikalumas turi būti CA ribose;
- galiojimo pradžios ir pabaigos terminai;
- sertifikato taisyklių (CP) nuoroda.

Visi Sistemos sudaryti kvalifikuoti sertifikatai (QC) turi atitikti jiems nustatytus reikalavimus. Be ką tik minėtų NQC duomenų juose turi būti:

- CA saugus el. parašas, sukurtas naudojant CA privatųjį raktą, skirtą pasirašyti QC;
- Sistemos naudojamas algoritmas sertifikatams pasirašyti, atitinkantis standartų reikalavimus.

Sistemos sudaryti QC turi atitikti ETSI TS 101 456 standarte [1] reikalaujamą profilį (struktūrą, parametrus). Šis standartas reikalauja, kad sertifikate būtų nurodytas ir asmens vardas (arba slapyvardis), sertifikato leidėjas, o sertifikato išplėtimo laukuose (*extentions*) – asmens atributai, sertifikatų taisyklės (CP), rakto naudojimo paskirtis, biometriniai asmens duomenys, požymis, kad sertifikatas yra kvalifikuotas (išsamus, aukštesnio lygio);

2) **sertifikatų atnaujinimas** (*Certificate Reneval*). Sertifikatas gali būti atnaujinamas dar nepasibaigus jo galiojimo terminui. Galimi du atnaujinimo variantai: sudaryti naują sertifikatą, paliekant tą patį viešąjį raktą, arba sudaryti naują sertifikatą, keičiant viešąjį raktą.

Gali būti atnaujinami ne tik abonentų, bet ir Sistemos infrastruktūriniai bei kontroliniai sertifikatai. Sistema turi garantuoti saugų sertifikatų atnaujinimą, kad nebūtų neleistinų pakeitimų sertifikatuose.

Sistemos infrastruktūrinių ir kontrolinių sertifikatų keitimas turi būti atliekamas laikantis standartų reikalavimų (žiūr. 6.3 skyriaus 5 dalies 4 punktą).

Sistema turi užtikrinti, kad privatieji raktai sertifikatams pasirašyti būtų pakeisti dar iki šių raktų galiojimo termino pabaigos. Atnaujinti privatieji raktai turi garantuoti ne mažesnį kaip buvusį saugumo lygį. Tai gali būti atliekama sudarant tarpinius (trumpalaikius) sertifikatus naujiems privatiesiems raktams patvirtinti:

- sudarant sertifikatą senam viešajam raktui, pasirašytą naujuoju privačiuoju raktu;
- sudarant sertifikatą naujam viešajam raktui, pasirašytą senuoju privačiuoju raktu;

- sudarant sau naująjį sertifikatą, pasirašytą naujuoju privačiuoju raktu.

Sistema turi garantuoti saugų asmenų sertifikatų ir/arba raktų keitimą.

Rekomenduojama asmenų sertifikatus keisti dar nesibaigus jų galiojimo terminui, kadangi pranešimų siuntimo tarp asmens ir CA saugumui užtikrinti gali būti panaudoti senieji raktai/sertifikatai;

3) **kryžminis sertifikavimas** (*Cross Certification*). Kryžminis sertifikavimas įgalina sukurti vienos krypties arba abipusį pasitikėjimo mechanizmą tarp dviejų arba daugiau CA. CA-atsakovo Sistema sudaro sertifikatą CA-prašytojo Sistemai, pateikusiai savo viešąjį raktą. CA-atsakovo abonentai dabar gali pasitikėti ir CA-prašytojo sudarytais sertifikatais.

Jei Sistema naudoja kryžminį sertifikavimą vienos krypties arba abipusiam pasitikėjimui tarp dviejų arba daugiau CA užtikrinti, turi būti garantuotas tarp Sistemų siunčiamų pranešimų autentiškumas ir vientisumas, klaidoms išvengti į pranešimus turi būti įterpiamas atsitiktinis skaičius (*nonce*).

CA-atsakovo Sistema turi garantuoti, kad CA-prašytojo Sistemos įgyvendinamos sertifikato taisyklės (CP) ir sertifikavimo veiklos nuostatai (CPS) būtų priimtini ir CA-atsakovo abonentams (asmenims) ir juo pasitikinčioms šalims;

4) **sertifikatų sudarymo auditas** (*Certificate Generation Service Audit*). Sertifikatų sudarymo tarnyba savo veiklos bėgyje turi registruoti tokius duomenis:

- visų CA sertifikatų, naudojamų asmenims sudaromiems sertifikatams pasirašyti ir CA infrastruktūriniams ar kontroliniams tikslams, tvarkymo duomenis;
- visų CA raktų, naudojamų sertifikatams pasirašyti, tvarkymo duomenis;
- visus asmenų sertifikatų tvarkymo duomenis;
- visus kryžminio sertifikavimo duomenis.

4. Sertifikatų duomenų teikimo reikalavimai (*Certificate Dissemination Service)*

1) **sertifikatų duomenų teikimo valdymas** (*Dissemination Management*). Sistema turi teikti sertifikatų duomenis laikydamasi abonentų pateiktų apribojimų;

2) **duomenų importas/eksportas** (*Import/Export of Objects*). Įsteigus sertifikatų duomenų saugyklą (*repository*), turi būti nustatytos duomenų išrinkimo saugumo taisyklės.

Skaityti duomenis turi būti leidžiama tik abonentams ir įgaliotiems asmenims, laikantis abonentų nustatytų apribojimų ir priimtų saugumo taisyklių.

Rašyti duomenis į saugyklą turi būti leidžiama tik įgaliotiems CA asmenims.

5. Sertifikatų atšaukimo valdymo reikalavimai (*Certificate Revocation Management Service)*

1) **prašymas pakeisti sertifikato statusą** (*Certificate Status Change Requests*). Asmeniui įtarus, kad jo privatusis raktas yra atskleistas (sukompromituotas), jis gali sustabdyti savo sertifikato galiojimą, pasiuntęs prašymą CA. Norėdamas atstatyti sertifikato galiojimą, asmuo turi nusiųsti atitinkamą prašymą.

Jei asmuo yra įsitikinęs, kad jo privatusis raktas yra atskleistas, turi būti siunčiamas prašymas atšaukti sertifikatą jį sudariusiam CA.

Kreipęsis į sertifikatų atšaukimo tarnybą, CA gali prašyti pakeisti jo paties infrastruktūrinių ir kontrolinių sertifikatų statusą. Tam turi būti siunčiami autentifikuoti pranešimai, kuriuos CA Sistema gali priimti arba atmesti.

Prašymai atšaukti/sustabdyti sertifikato galiojimą turi būti įvykdomi laiku. Maksimalus laiko tarpas tarp prašymo gavimo ir sertifikato galiojimo atšaukimo/sustabdymo, įskaitant prašytojo autentiškumo nustatymą ir nutraukimo žinios paskelbimą, neturi būti didesnis kaip viena diena.

Visi prašymai sustabdyti sertifikato galiojimą, atsisakyti sustabdymo arba atšaukti (galutinai nutraukti galiojimą) sertifikatą turi būti tinkamai patikrinti ir patvirtinti.

Jei sertifikatas buvo atšauktas, Sistema turi garantuoti, kad jis nebebus atstatytas.

Asmenų sertifikatams pasirašyti naudojami CA sertifikatai bei CA infrastruktūriniai sertifikatai gali būti atšaukti tik kontroliuojant dviem asmenims.

Sertifikato statusas turi būti keičiamas tik dalyvaujant ir leidus:

- ♦ CA saugumo pareigūnui, keičiant CA infrastruktūrinio/kontrolinio sertifikato statusą;
- ♦ registracijos pareigūnui arba saugumo pareigūnui, keičiant asmenų sertifikatų statusą;
- ♦ turint asmens sutikimą dėl jo sertifikato statuso keitimo.

Sertifikato taisyklėse (CP) gali būti nustatyta, kad asmens sertifikato statusą gali pakeisti trečiasis asmuo (pvz., asmens darbdavys), nusiuntęs atitinkamą prašymą CA.

Duomenų bazė su sertifikatų statuso duomenimis turi būti pakoreguota nedelsiant, atlikus būtinas sertifikato galiojimo stabdymo/atšaukimo procedūras.

2) **sertifikato galiojimo stabdymas/atšaukimas** (*Certificate Suspension/ Revocation*). CA yra atsakingas už sertifikatų statuso keitimą ir šios informacijos perdavimą CRL sąrašų teikimo tarnybai. Sistema gali siųsti pranešimus iš sertifikatų atšaukimo tarnybos (ši tarnyba formuoja CRL) į CRL teikimo tarnybą:

- ♦ periodiškai (kas nustatytą laiko tarpą) arba;
- ♦ realiu laiku, kai CRL teikimo tarnyba, gavusi vartotojo užklausą dėl sertifikato statuso, tuoj pat paprašo duomenų iš sertifikatų atšaukimo tarnybos.

Sistema turi būti pajėgi atšaukti sertifikatus netgi po veikimo sutrikimų.

Jei pranešimai (CRL sąrašai, CRL pokyčiai ar pavienių sertifikatų statuso informacija) tarp sertifikatų atšaukimo tarnybos ir CRL teikimo tarnybos siuntinėjami periodiškai, tai Sistema turi atitikti šiuos reikalavimus:

- ♦ jei CRL saugykla vartotojams pasiekiama *offline* būdu (per katalogus, kreipusis gaunamas visas CRL failas), CRL turi būti atnaujinamas bent kartą per dieną;
- ♦ jei CRL saugykla vartotojams pasiekiama *online* būdu (OCSP), CRL turi būti atnaujinamas, kai tik pakeičiamas kurio nors sertifikato statusas ir bent kartą per dieną;
- ♦ kiekviename sertifikatų statuso pranešime turi būti siuntėjo vardas ir jo skaitmeninis parašas;
- ♦ pranešimuose gali būti informacija tik apie tuos sertifikatus, kurių galiojimas sustabdytas/atšauktas;
- ♦ pranešime rekomenduojama kiekvienam CRL sąrašo sertifikatui nurodyti jo serijinį numerį ir statuso keitimo priežastį.

Jei pranešimai tarp sertifikatų atšaukimo tarnybos ir CRL teikimo tarnybos sintinėjami realiu laiku, tai Sistema turi atitikti šiuos reikalavimus:

- ♦ jei CRL teikimo tarnyba paprašo duomenų apie konkretaus sertifikato statusą, sertifikatų atšaukimo tarnyba iš savo CRL duomenų bazės turi pateikti duomenis apie to sertifikato einamąjį statusą;
- ♦ turi būti patikimas duomenų perdavimo kelias tarp sertifikatų atšaukimo tarnybos ir CRL teikimo tarnybos;

- patikimas duomenų perdavimo kelias turi būti nustatytas taip, kad būtų minimizuota galimybė išsiginti pranešimų;
- užklausos ir atsakymai dėl sertifikatų statuso turi būti apsaugoti nuo klastočių (panaudojant *nonce*).

3) **atšauktų sertifikatų tvarkymo auditas** (*Certificate Revocation Management Audit*). Sertifikatų atšaukimo tarnyba turi fiksuoti visus prašymus dėl sertifikatų statuso pakeitimo, nežiūrint ar prašymas buvo patenkintas ar ne.

6. CRL teikimo reikalavimai (*Certificate Revocation Status Service*)

1) **informacija apie atšaukimą** (*revocation status data*). CRL teikimo tarnyba el. parašų naudotojams teikia sertifikatų statuso (galioja ar atšauktas) informaciją. CRL teikimo tarnyba duomenis apie sertifikatų atšaukimą gauna iš CA sertifikatų atšaukimo tarnybos. Tam yra tokie reikalavimai:

- pranešimus į CRL teikimo tarnybą realiu laiku (kai ji užklausia) arba periodiškai (nustatytais laiko tarpais) turi siųsti tik sertifikatų atšaukimo tarnyba;
- Sistema, *on-line* veiksena teikianti sertifikatų statuso informaciją, privalo garantuoti realiu laiku ar periodiškai perduodamų pranešimų vientisumą ir autentiškumą;
- Sistema, *on-line* veiksena teikianti sertifikatų statuso informaciją ir perduodanti ją realiu laiku, privalo užtikrinti, kad sertifikatų statuso duomenų bazės išduotas atsakymas atitiktų užklausoje nurodytą sertifikatą;

2) **užklausa/atsakymas dėl sertifikato statuso** (*status request/ response*). El. parašo tikrintojas, gavęs iš CA sertifikatų duomenų teikimo tarnybos reikiamą sertifikatą parašui patikrinti, turi patikrinti ir sertifikato statusą. Sertifikatų statuso informaciją teikia CRL teikimo tarnyba. CRL teikimo tarnyba tai gali atlikti dviem būdais: *on-line* (sertifikato statuso informacija pateikiama realiu laiku) arba *off-line* (sertifikatų statuso informacija pateikiama periodiškai kas tam tikrą laiko tarpą) veiksena.

*On-line* veiksenos atveju el. parašo tikrintojas siunčia į CRL teikimo tarnybą užklausą dėl sertifikato statuso. CRL teikimo tarnyba realiu laiku kreipiasi į sertifikatų duomenų bazę einamajai informacijai apie sertifikatą gauti arba, jei naudojamas periodinis CRL sąrašų apsikeitimas tarp bazės (bazę formuoja sertifikatų atšaukimo tarnyba) ir CRL teikimo tarnybos, šią informaciją CRL tarnyba ima iš paskutinio periodiškai gaunamo CRL sąrašo.

Klausiančiajam siunčiamas suformuotas atsakymas, kuriame yra informacija tik apie jį dominančio sertifikato statusą.

*Off-line* veiksenos atveju CRL teikimo tarnyba, turėdama paskutinę CRL sąrašo versiją, persiunčia ją el. parašų tikrintojui, kad jis galėtų tikrinti sertifikatų statusus.

Sistema gali reikalauti, kad užklausos būtų pasirašytos klausiančiųjų el. parašu. Užklausas gali generuoti ir pati Sistema, norėdama gauti sertifikatams pasirašyti naudojamų, infrastruktūrinių ir Sistemos kontrolinių raktų sertifikatų statuso informaciją.

Reikalavimai CRL teikimo tarnybos atsakymams:

- *on-line* veiksena išduotas atsakymas turi būti pasirašytas tarnybos el. parašu, gautu naudojant tarnybos infrastruktūrinį raktą. *Off-line* veiksenos atveju siunčiami atsakymai, kuriuose yra vėliausia CRL sąrašo versija. Tokius CRL sąrašus pasirašo jų sudarytojai;
- atsakymams pasirašyti naudojami algoritmai/raktai turi atitikti jiems nustatytus reikalavimus [31];
- atsakyme turi būti nurodytas laikas, kada CRL teikimo tarnyba arba CRL sudarytojas pasirašė atsakymą.

3) **CRL teikimo auditas.** Visus su sertifikatų statuso užklausomis ir atsakymais susijusius specifinius įvykius turi fiksuoti CRL teikimo tarnyba.

## 6.5. Papildomi Sistemos saugumo reikalavimai

Papildomi Sistemos saugumo reikalavimai yra susiję su dviem paslaugomis: laiko žymų teikimu ir parašo formavimo įrangos teikimu (**SCDev** – *Signature Creation Device* arba **SSCD -** *Secure Signature Creation Device)*.

1. Laiko žymų teikimas (*Time Stamp Service*)

Duomenų laiko žyma yra įrodymas, kad duomenys (el. parašas, kt.) buvo sukurti iki žymoje nurodyto laiko. Laiko žymas kuria laiko žymų tarnybos (TSA). TSA, kaip ir CA, savo darbe turi naudoti tam tikrus reikalavimus atitinkančią sistemą ir procesus. Yra keturios grupelės reikalavimų laiko žymos atveju:

1) **užklausų korektiškumo tikrinimas** (*check request corectness*). Šio Sistemos komponento paskirtis yra patikrinti užklausos laiko žymai gauti korektiškumą ir pilnumą. Jei nustatoma, kad užklausa teisinga, atitinkami duomenys persiunčiami laiko žymos formavimo komponentui. Taigi:

- TSA gali tikrinti kiekvienos užklausos šaltinį (pateikėją) prieš tikrindama jos korektiškumą. Tam gali prireikti šaltinio autentifikavimo mechanizmo;
- TSA turi užtikrinti, kad užklausa laiko žymai gauti naudoja leistiną santraukos (*hash*) algoritmą [31];

2) **laiko parametrų generavimas** (*time parameter generation*). Šis komponentas naudoja patikimą tikslaus laiko šaltinį. Gautas laikas naudojamas formuojant laiko žymą. Reikalaujama, kad:

- TSA laikrodis būtų sinchronizuotas su universaliuoju laiku UTC (*Co-ordinated Universal Time*, Grinvičo laikas) ne mažesniu kaip vienos sekundės tikslumu;
- TSA laikrodžio sinchronizavimui su UTC laiku būtų naudojamas patikimas būdas;

3) **laiko žymos formavimas** (*time stamp generation*). Formuojant laiko žymą yra surenkami tokie duomenys: einamasis laikas, unikalus žymos serijinis numeris, laiko žymai sudaryti pateikti ir laiko žymos taisykles atitinkantys duomenys (pvz., *nonce*, TSA sertifikato duomenys). Reikalaujama, kad:

- TSA suteiktas serijinis numeris kiekvienai sukurtai laiko žymai būtų unikalus TSA ribose. Ši savybė turi išlikti netgi po šios paslaugos teikimo sutrikimų;
- kartu su laiku TSA privalo žymoje nurodyti ir laiko šaltinio tikslumą, jei jis yra aukštesnis už reikalaujamą laiko žymos taisyklėse;
- laiko žymoje turi būti laiko žymos taisyklių nuoroda, kurių laikantis buvo sukurta žyma;

4) **laiko žymos pasirašymas** (*time stamp (TST) computation*). Šio komponento paskirtis yra sudaryti tokią laiko žymą, kuri jau bus siunčiama prašytojui. Čia suformuojamas TSA el. parašas iš laiko žymos formavimo komponento gautiems duomenims. Į žymą įtraukiama TSA sertifikato nuoroda, kita su šio sertifikato statusu susijusi informacija (pvz., CRL). Šiam žingsniui yra tokie reikalavimai:

- TSA privatusis raktas laiko žymoms pasirašyti turi būti laikomas saugiame kriptografiniame modulyje;
- kriptografinis modulis turi atitikti CWA 14167-2 standarto [9] arba kitokio jį atitinkančio standarto, pvz., FIPS 140-2 Level 3 ar ISO/IEC 15408 [32, 33, 42-45], reikalavimus;
- TSA kontroliniai raktai turi būti laikomi aparatūrinėje (*hardware*) kriptografinėje įrangoje;

- ♦ TSA privačiojo rakto, skirto žymoms pasirašyti, negalima naudoti kitiems tikslams;
- ♦ TSA turi užtikrinti, kad sudarytose laiko žymose būtų tokie patys reikalaujami duomenys, kurie buvo atsiųsti užklausose;
- ♦ TSA parašo/rakto algoritmai turi atitikti nustatytus reikalavimus [31];

5) **laiko žymos paslaugos auditas** (*time stamping service audit*). Kontrolės tikslams TSA turi fiksuoti visus su laiko žymų teikimu susijusius specifinius įvykius:

- ♦ visus TSA raktų keitimo/atstatymo įvykius;
- ♦ visų TSA pasirašymo raktų gyvavimo ciklo tvarkymo įvykius;
- ♦ visus sutrikimo atvejus, įskaitant laikrodžio tikslumo sutrikimus.

2. Parašo formavimo įrangos teikimas abonentams (*subscriber device provision service*)

1) **SCDev rengimas** (*SignatureCreationDevice preparation*).

Sertifikavimo paslaugų teikėjo Sistema (ją gali turėti ne tik CA, bet ir kitas šios rūšies paslaugos teikėjas), rengdama SCDev, pavyzdžiui, mikroprocesorinę kortelę, sukuria raktų porą ir užrašo privatųjį raktą į SCDev arba pasiunčia komandą į SCDev raktų porai generuoti SCDev viduje. Atliekant šiuos veiksmus reikalaujama:

- ♦ jei asmuo yra įsigijęs SCDev iš trečiojo asmens, Sistema visų pirma turi patikrinti ar SCDev yra tinkamas ir gautas iš sertifikuoto gamintojo;
- ♦ inicializavimo, formatavimo ir failų struktūros kūrimo metu turi būti naudojamos saugios reikšmės, parametrai ir kreipimosi valdymo sąlygos, kad SCDev konfigūracija būtų saugi ir nebūtų galima neleistinai panaudoti SCDev;
- ♦ jei naudojama saugi SCDev (t. y. SSCD), ji turi būti įvertinta ir sertifikuota pagal CWA 14169 standartą [11];
- ♦ jei raktų pora yra sugeneruota ne SCDev viduje, tai raktų porų generavimo kriptografinis įrenginys (CD - *Cryptographic Device*) turi būti patikrintas ir sertifikuotas pagal CWA 14169 standartą;
- ♦ jei raktų pora yra sugeneruota ne SCDev viduje, ji turi būti saugiai perkelta į SCDev. Turi būti patikimas ryšio kanalas tarp kriptografinio įrenginio ir SCDev;
- ♦ kai kriptografiniu įrenginiu sugeneruota raktų pora sėkmingai perkeliama į SCDev, raktų pora kriptografiniame įrenginyje turi būti sunaikinama;

2) **SCDev teikimas** (*SCDev provision*). SCDev teikimas – tai parengtų SCDev perdavimas abonentams. CA turi užtikrinti, kad Sistemos

konfigūracijos dėka SCDev būtų atiduotas numatytam ir autentifikuotam abonentui;

3) **aktyvavimo duomenų kūrimas ir platinimas** (*activation data creation&distribution*):

- pradinius SCDev aktyvavimo duomenis (pvz., PIN kodą) Sistema turi generuoti saugiai;
- Sistema turi užtikrinti, kad CA darbuotojai negalėtų neteisėtai panaudoti parengtos SCDev. Tai gali būti pasiekta naudojant saugias SCDev rengimo ir teikimo procedūras arba pateikiant abonentui priemones, įgalinančias patikrinti, ar privatusis raktas nebuvo panaudotas iki SCDev gavimo;

4) **SCDev teikimo abonentams auditas** (*subscriber device provision service audit*). Sistema turi fiksuoti visus poveikį saugumui turinčius SCDev rengimo įvykius.

## 6.6. Kriptografinis modulis

CA privalo pasirašyti sudarytus sertifikatus ir CRL sąrašus, o laiko žymų teikėjai (TSA) - sukurtas laiko žymas. Jie turi patikimai saugoti savo privačiuosius raktus nuo nesankcionuoto panaudojimo. Tam turi būti priemonės, garantuojančios privačiųjų raktų konfidencialumą. Kriptografinis modulis (toliau - KM) yra ypatingos svarbos elementas Sistemoje.

Skiriamos dvi KM rūšys:

- KM sertifikatams ar laiko žymoms pasirašyti [9];
- KM raktų generavimo paslaugai teikti (CA abonentų raktams generuoti ir rašyti į patikimas laikmenas) [10].

Pirmos rūšies KM-1 gali būti naudojamas CA (arba kitokio sertifikavimo paslaugų teikėjo) raktams sugeneruoti, privačiajam raktui saugoti, sertifikatams ir CRL sąrašams pasirašyti. Tai programinę ir techninę dalis turintis įrenginys, galintis atlikti tokias kriptografines funkcijas:

- generuoti raktus, skirtus sertifikatams pasirašyti;
- pasirašyti sertifikatus, naudojant tam skirtą raktą. Parašui sukurti į KM gali būti paduodama sertifikato duomenų santrauka (*hash*) arba visi sertifikato duomenys, kurių santrauką padaro pats KM (jei tai numatyta).

Papildomai KM turi atlikti dar ir tokias funkcijas:

- autentifikuoti vartotoją;
- kontroliuoti kreipinius į KM raktui sugeneruoti ar sunaikinti;

- kontroliuoti kreipinius į KM, kai norima panaudoti raktą sertifikatams pasirašyti;
- fiksuoti audito duomenis darant KM keitimus, susijusius su saugumu;
- savęs testavimą.

KM naudoja šiuos duomenis:

a) privatųjį raktą, kuris sugeneruojamas ir saugomas KM viduje. Galimos šio rakto atsarginių kopijų kūrimo ir atstatymo funkcijos;

b) pasirašomus duomenis. Pasirašymo metu KM modulyje gali būti tokie duomenys:

- importuota sertifikato santrauka;
- importuoti visi sertifikato duomenys. Jų santrauką apskaičiuoja pats KM;
- visas CRL arba CRL santrauka, laiko žymos duomenys, kai teikiamos tokios paslaugos;
- eksportuojamas sertifikato, CRL ar laiko žymos parašas.

KM turi turėti priemones, kurios leistų dirbti su KM tik įgaliotiems asmenims. Teisę naudoti KM turi turėti šie darbuotojai (CA ar kitokio paslaugos teikėjo):

- kriptografijos pareigūnas (asmuo, įgaliotas įdiegti, suderinti ir prižiūrėti KM, generuoti, naikinti, daryti atsargines kopijas ar atstatyti raktus, kuriuos naudoja paslaugų teikėjas);
- pasirašantysis pareigūnas (asmuo, įgaliotas pasirašyti sertifikatus ar kt. egzistuojančiu paslaugų tiekėjo privačiuoju raktu);
- auditorius, turintis teisę tikrinti KM sukauptus audito duomenis.

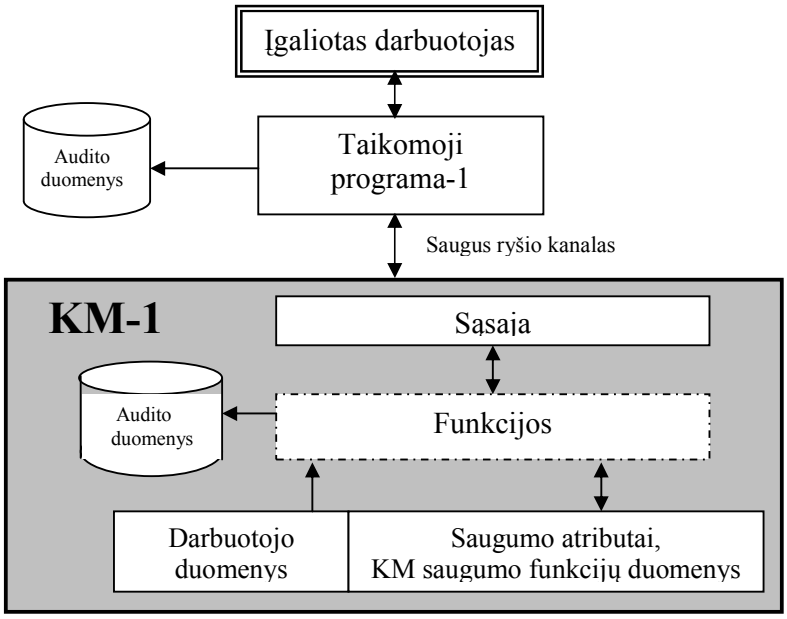
Daugeliu atvejų KM yra kaip atskiras Sistemos komponentas, turintis savo techninę ir programinę įrangą. Naudojant saugius ryšio kanalus, KM susiejamas su taikomąja vartotojo programa (klientine programa). Saugaus ryšio kanalo pavyzdžiai yra kompiuterio PCI, SCSI, USB magistralės.

Logiškai KM yra atsakingas už privačiojo rakto apsaugą nuo atskleidimo, pakeitimo ir nesankcionuoto panaudojimo. Vartotojas betarpiškai palaiko ryšį su taikomąja programa, kuri savo ruožtu kreipiasi į KM. Taikomosios programos atsakomybė yra patikrinti pasirašančiojo asmens autentiškumą, jo įgaliojimus, saugiai perduoti pasirašomus duomenis KM, formuoti ir kaupti audito duomenis. KM struktūra ir jo ryšys su išore pavaizduoti 6.2 pav.

KM saugumo reikalavimai (jie dar vadinami PP - *Protection Profile*) yra išdėstyti CWA 14167-2 standarte [9]. Jie turi atitikti informacinių technologijų bendrųjų saugumo standartų (*Common Criteria*) EAL4 lygį [34].

KM saugumo reikalavimai (PP) visų pirma yra skirti tiems KM, kurie naudojami kvalifikuotiems sertifikatams pasirašyti. Tačiau juos atitinkančius KM gali naudoti ne tik sertifikatų sudarymo tarnybos, bet ir kitokių paslaugų teikėjai, kaip CRL tvarkytojai šiems sąrašams pasirašyti, sertifikatų statuso duomenų *on-line* veiksena (OCSP) teikėjai pranešimams pasirašyti, laiko žymų teikėjai laiko žymoms pasirašyti.

KM turi naudoti standartų nustatytus algoritmus [31].




6.2 pav. Kriptografinio modulio (KM-1) sertifikatams pasirašyti struktūra ir jo ryšys su išore

Antros rūšies KM-2 generuoja raktus ir rašo juos į saugią parašo formavimo įrangą (SSCD). Jis naudojamas tada, kai CA klientams teikia tokias paslaugas ir savo sudėtyje turi parašo formavimo įrangos tarnybą. Tokios paslaugos teikimu gali užsiimti ne tik CA.

Šalia pagrindinių funkcijų – raktų generavimo, privačiojo rakto užrašymo į SSCD ir viešojo rakto perdavimo sertifikatams sudaryti - šis KM gali vykdyti tokias papildomas funkcijas:

- autentifikuoti vartotoją;
- kontroliuoti kreipinius į KM raktams generuoti ir rašyti į SSCD;
- fiksuoti audito duomenis darant KM keitimus, susijusius su saugumu;

- savęs testavimą.

Šis KM operuoja su tokiais duomenimis:

a) parašo formavimo duomenimis (SCDat – *Signature Creation Data*): abonento privačiuoju raktu, kuris generuojamas KM viduje ir užrašomas į SSCD;

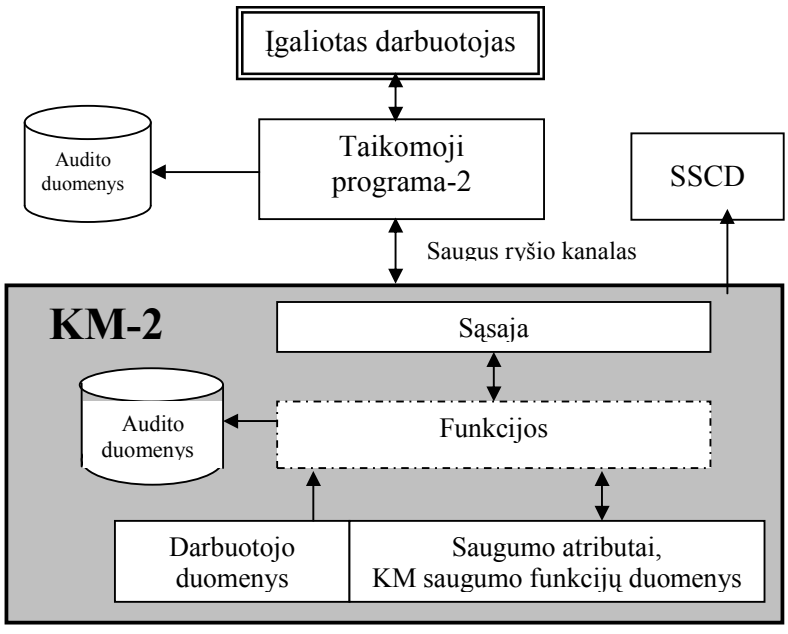
b) parašo tikrinimo duomenimis: abonento viešuoju raktu, kuris generuojamas KM viduje, užrašomas į SSCD ir perduodamas sertifikatų sudarymo taikomajai programai.

Šios mokymo priemonės 9.6 skyriuje „Saugi parašo formavimo įranga (SSCD)“ šis KM atitinka SSCD-1 tipo įrangą, o SSCD, į kurį rašomas privatusis raktas, atitinka SSCD-2.

Teisę naudoti šį KM turi turėti šie darbuotojai (CA ar kitokio paslaugos teikėjo):

- kriptografijos pareigūnas (asmuo, įgaliotas įdiegti, suderinti ir prižiūrėti KM, generuoti ir eksportuoti abonento raktų porą);
- auditorius, turintis teisę tikrinti KM sukauptus audito duomenis.

6.3 pav. pavaizduota raktams generuoti ir rašyti į SSCD skirto KM struktūra ir jo ryšys su išore. Saugumo reikalavimai šios rūšies KM yra CWA 14167-3 standarte [10].




6.3 pav. Kriptografinio modulio (KM-2) abonentų raktams generuoti ir rašyti į SSCD struktūra ir jo ryšys su išore

# 7. ELEKTRONINIO PARAŠO FORMATAI

Šiame skyriuje aprašoma el. parašo struktūra ir jame talpinami informacijos elementai.

## 7.1. El. parašo elementai ir formatai

El. parašas susideda iš informacijos elementų (jie vadinami parašo atributais) visumos ir skaitmeninio parašo [2]. Skaitmeninis parašas kuriamas tai informacijos elementų visumai (t. y. tos visumos santraukai), kurioje gali būti:

♦ ***pasirašytų duomenų tipas*** – informacijos elementas, kuris nurodo pasirašytų duomenų tipą (tekstas, garsas, vaizdas, failo tipas, kt.). Jis yra naudojamas tada, kai nėra griežto reikalavimo pasirašomų duomenų tipui. To reikia, kad tikrintojas stebėtų duomenis tokiomis pat priemonėmis, kaip ir pasirašęs asmuo;

♦ ***pasirašyti duomenys.*** Jų pačiame el. paraše gali ir nebūti. Tuomet turėsime vadinamąjį išorinį el. parašą;

♦ ***pasirašytų duomenų santrauka*;**

♦ ***pasirašiusio asmens sertifikato nuoroda.*** Gali būti pateikiamas visas sertifikatas arba tik sertifikato identifikatorius ir jo santrauka. Tai ypač svarbu, kai pasirašantis asmuo turi keletą sertifikatų, atitinkančių tą patį privatųjį raktą, kad išvengtume el. parašo tikrintojo pretenzijų, jog buvo panaudotas kitos paskirties sertifikatas. Kai pasirašantysis asmuo turi kelis sertifikatus, atitinkančius skirtingus privačiuosius raktus, tai padeda išvengti ginčų dėl to, kad pasirašantysis asmuo pateikė parašo tikrintojui ne tą viešąjį raktą;

♦ ***parašo taisyklių nuoroda*** (kai parašo taisyklės nurodomos akivaizdžiai). Šiuo atveju pateikiamos visos parašo taisyklės arba tik jų identifikatorius ir santrauka. Taip užtikrinama, kad tikrintojas laikytųsi tokių pačių parašo taisyklių, kaip ir pasirašantysis asmuo. Apie parašo taisykles žiūr. 8 skyriuje;

♦ ***pasirašiusio asmens nurodytas pasirašymo laikas;***

♦ ***pasirašytų duomenų laiko žyma*** (įrodymui, kad parašas buvo sukurtas vėliau, nei duomenų laiko žymoje užfiksuotas laikas);

♦ ***pasirašiusio asmens pareigos*** (rolė, įgaliojimai);

♦ ***pasirašiusio asmens nurodyta pasirašymo vieta;***

♦ ***kita papalidoma informacija***, kuri turi būti el. paraše pagal parašo taisykles.

Aukščiau išvardinti el. parašo atributai yra asmens pasirašomi atributai, t. y. jų duomenys patenka į skaitmeninį parašą. El. paraše privalo būti ***pasirašytų duomenų tipo***, ***pasirašytų duomenų santraukos ir pasirašiusio asmens sertifikato nuorodos*** atributai. Kitų pasirašomų atributų naudojimas priklauso nuo pasirinktų el. parašo taisyklių.

Tikrinant el. parašą būtina vienareikšmiškai nustatyti, ar pasirašiusio asmens sertifikatas ir parašo informacijos elementų sertifikatai (jei tokie naudojami) buvo galiojantys pasirašymo metu. Tai reiškia, jog el. parašas turi turėti savo vietą laiko skalėje.

Pirmojo tikrinimo metu, kai nėra papildomos informacijos apie el. parašo sukūrimo laiką (pvz., laiko žymos), laikoma, jog pasirašymo laikas yra artimas laikui, kai vyko pirmasis tikrinimas (nežiūrint to, kad pasirašęs asmuo el. paraše nurodė pasirašymo laiką). El. parašas yra galiojantis, jei sertifikatas pirmojo tikrinimo metu nebuvo atšauktas. Todėl rizika, kad el. parašas bus laikomas negaliojančiu, yra mažesnė, jei pirmąjį tikrinimą atliksime kaip galima greičiau po el. parašo sukūrimo. Pirmojo tikrinimo metu el. parašui sukuriama laiko žyma.

Įprasto tikrinimo metu el. paraše jau turi būti papildoma informacija, leidžianti patikrinti, kad el. parašas buvo sukurtas sertifikato galiojimo metu. Tokia informacija yra:

- laiko žyma, kurią paprašius pasirašiusiam asmeniui arba el. parašo tikrintojui suformuoja laiko žymų teikėjas; arba
- laiko markeris, gaunamas iš saugios audito duomenų bazės, kurioje kaupiami el. parašai ir jų užrašymo toje duomenų bazėje laikai - laiko markeriai.

Rekomenduojama naudoti el. parašų laiko žymas.

El. parašo patvirtinimo duomenys, kurie papildomai dedami į el. parašą, yra:

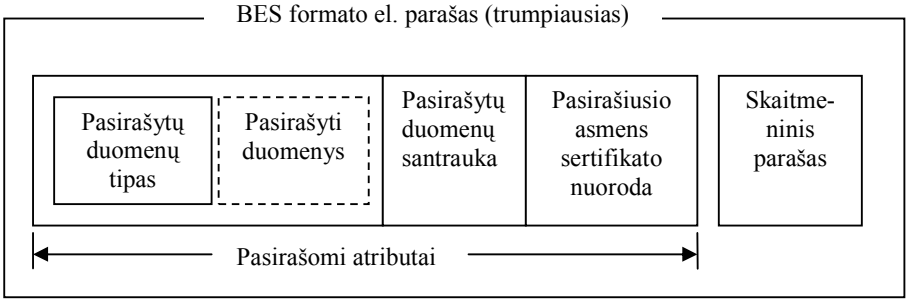
- laiko žyma;
- įvairūs su parašu susiję sertifikatai (ne tik pasirašiusio asmens, bet ir CA, TSA, kt.);
- informacija apie sertifikatų galiojimo statusą (CRL sąrašai).

Tai asmens nepasirašomi atributai. Juos pasirašo ir už juos garantuoja atitinkami sertifikavimo paslaugų teikėjai (CA, TSA).

El. paraše nebūtinai turi būti visi aukščiau išvardinti atributai. Todėl yra leistini tokie el. parašo formatai:

1) BES (***B****asic* ***E****lectronic* ***S****ignature*) formato el. parašas. Jis susideda iš informacijos elementų rinkinio ir to rinkinio skaitmeninio parašo. 7.1 pav.

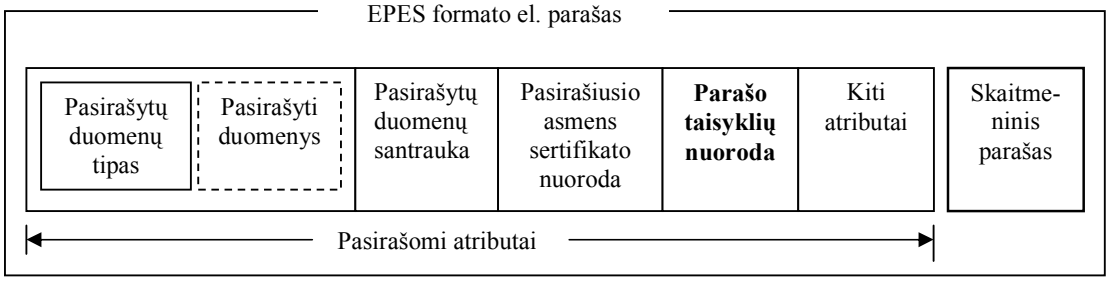
schemiškai parodytas trumpiausio pavidalo BES formato el. parašas. Jis tenkina Europos Sąjungos Direktyvos 1999/93/EC [46] reikalavimus, garantuoja pasirašytų duomenų autentiškumą ir pasirašiusio asmens tapatybę bei gali būti sukurtas nenaudojant jokių papildomų paslaugų (pvz., laiko žymos teikėjų). Tačiau pasibaigus pasirašiusio asmens sertifikato galiojimo laikui toks el. parašas tampa negaliojantis.




7.1 pav. BES formato el. parašas

Atkreipkime dėmesį į sąvokų „skaitmeninis parašas“ ir „elektroninis parašas“ naudojimą. Skaitmeninis parašas yra tik el. parašo viena iš dalių.

2) EPES (***E**xplicit **P**olicy-based **E**lectronic **S**ignature*). Šio formato el. paraše, lyginant jį su BES formato parašu, yra akivaizdžiai nurodomos parašo taisyklės (žiūr. 7.2 pav.). Tai reiškia, kad galioja tik toks el. parašas, kuris atitinka nurodytas parašo taisykles. BES ir EPES formatų el. parašuose gali būti ir kiti šio skyriaus pradžioje išvardinti pasirašomi atributai.

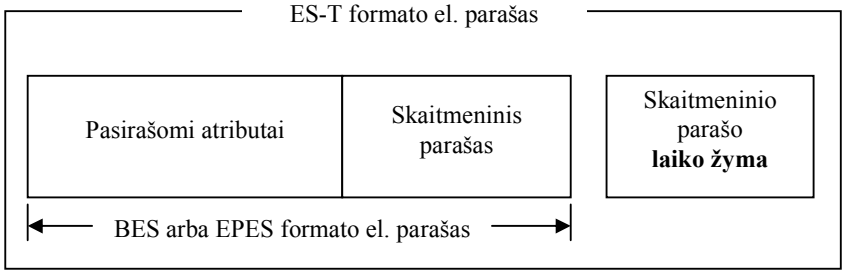



7.2 pav. EPES formato el. parašas

3) ES-T (***E**lectronic**S**ignature-**T**ime*) formato el. parašas papildomas:

- laiko žyma, kuri gaunama iš TSA, arba
- laiko markeriu, gautu iš saugios audito duomenų bazės.

Tai užtikrina ilgalaikį el. parašo galiojimą. Laiko žyma arba laiko markeris gali būti dedamas BES ir EPES formatų parašams. 7.3 pav. shemiškai pavaizduota ES-T formato el. parašo struktūra.




7.3 pav. ES-T formato el. parašas

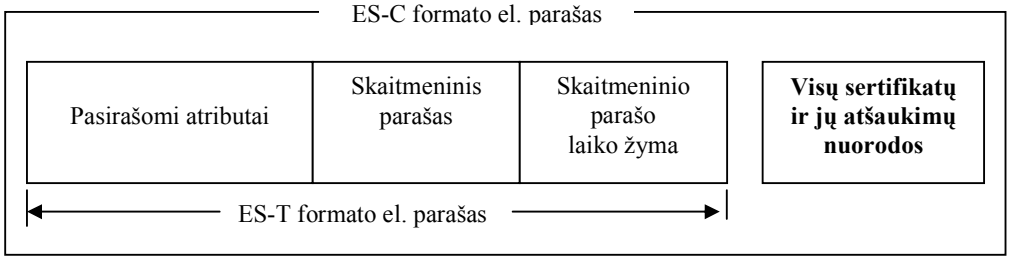
4) ES-C (***E**lectronic **S**ignature with **C**omplete validation data references*) formato el. parašas susideda iš ES-T formato parašo plius visų su el. parašu susijusių sertifikatų nuorodų bei visų šių sertifikatų atšaukimų (CRL ir/arba OCSP atsakymų) nuorodų. Čia turima galvoje ne tik pasirašiusio asmens sertifikatas, bet ir CA, TSA bei kitų paslaugos teikėjų sertifikatai. Patys sertifikatai, CRL, OCSP atsakymai gali būti saugomi bet kurioje vietoje. El. paraše nurodoma tik jų laikymo vieta, nes kitaip parašų apimtis pasidarytų labai didelė.

7.4 pav. schemiškai pavaizduota jo struktūra.

El. parašo galiojimą patvirtinantys duomenys gali būti saugomi kartu su parašu arba kur nors kitur. ES-C turi dvi formas:

a) ES-C, leidžiančią patvirtinančius duomenis laikyti kur nors kitur (pvz., centrinėje saugykloje);

b) ES-X, leidžiančią tuos duomenis laikyti kartu su ES-T formato el. parašu.




7.4 pav. ES-C formato el. parašas

5) ES-X (***ES** with e**X**tended validation data*) formato el. parašas. Jis gaunamas pridėjus visus jį patvirtinančius duomenis (ne tik šių patvirtinančių duomenų nuorodas). Jis pavaizduotas 7.5 pav.

Pirmiausiai ES-X el. parašo formatas yra naudojamas tuomet, kai parašą tikrinantis asmuo neturi patikimos prieigos prie:

- pasirašiusio asmens sertifikato;
- CA, sudarančių visą sertifikatų seką, sertifikatų;
- susijusių CRL sąrašų, nuorodytų ES-C formato el. paraše.

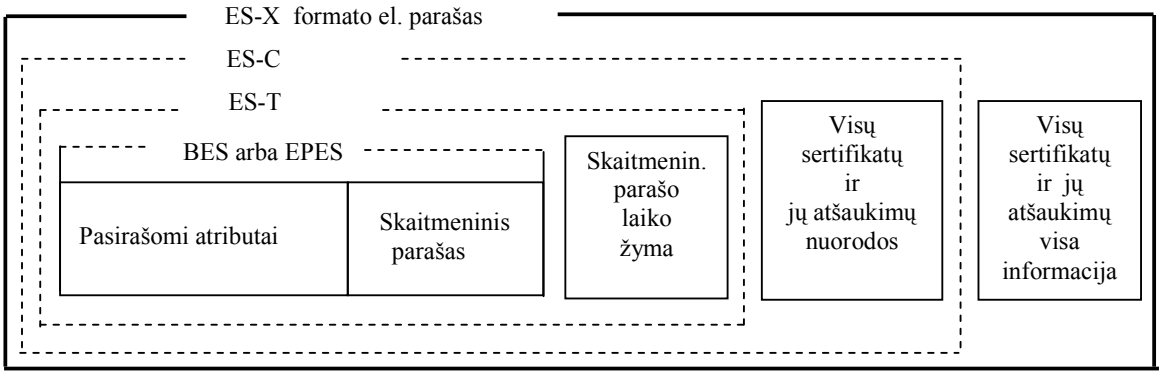
Tokiu atveju reikalingų sertifikatų ir CRL sąrašų visi duomenys (ne vien nuorodos į juos) taip pat pridedami prie ES-C formato el. parašo. Taip gaunamas išplėstinis ilgas el. parašas (*X-Long*).

Dar viena priežastis dėl kurios naudojamas ES-X formatas, tai CA privačiojo rakto kompromitacijos (rakto atskleidimas tretiesiems asmenims, matematinio metodo tapimas nepatikimu, kt.) galimybė. Jei daroma prielaida jog taip gali atsitikti, tai reikia tik ES-C formato el. parašą papildyti laiko žyma, gauta šiems duomenims:

- ES-C formato el. parašui, taip suformuojant pirmojo tipo ES-X formato el. parašą (ES-X Type 1); arba

- tik visų sertifikatų ir jų atšaukimų nuorodoms, taip suformuojant antrojo tipo ES-X formato el. parašą (ES-X Type 2).

Norint išvengti neigiamų pasekmių dėl pirmosios (kai nėra patikimos prieigos prie sertifikatų) ir antrosios (kai CA raktas, kuris naudojamas sertifikatams pasirašyti, tampa nebepatikimas) priežasčių, galima dėti abi laiko žymas: pirmą - ES-C formato el. parašui, ir antrą - visų sertifikatų ir jų atšaukimų nuorodoms. Taip gaunamas ilgas išplėstinio formato el. parašas su laiko žymomis (*X-Long-Timestamped*).




7.5 pav. ES-X formato el. parašas

## 7.2. Į archyvą dedamų dokumentų el. parašas

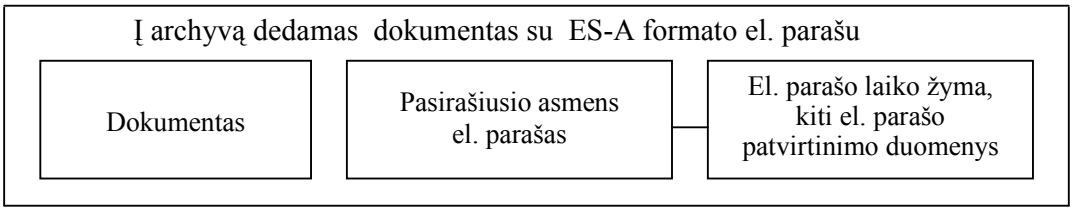
Į archyvą dedami dokumentai turi turėti tokias dalis:

- ♦ patį dokumentą;
- ♦ el. parašą su papildomais parašo galiojimą patvirtinančiais duomenimis (ne tik pasirašiusio asmens sertifikatą). Laiko žyma yra vienas iš papildomų, parašo galiojimą patvirtinančių duomenų.

Tokia į archyvą dedamo dokumento struktūra yra būtina dėl šių priežasčių. Pirma, dokumentą pasirašiusio asmens sertifikato galiojimo

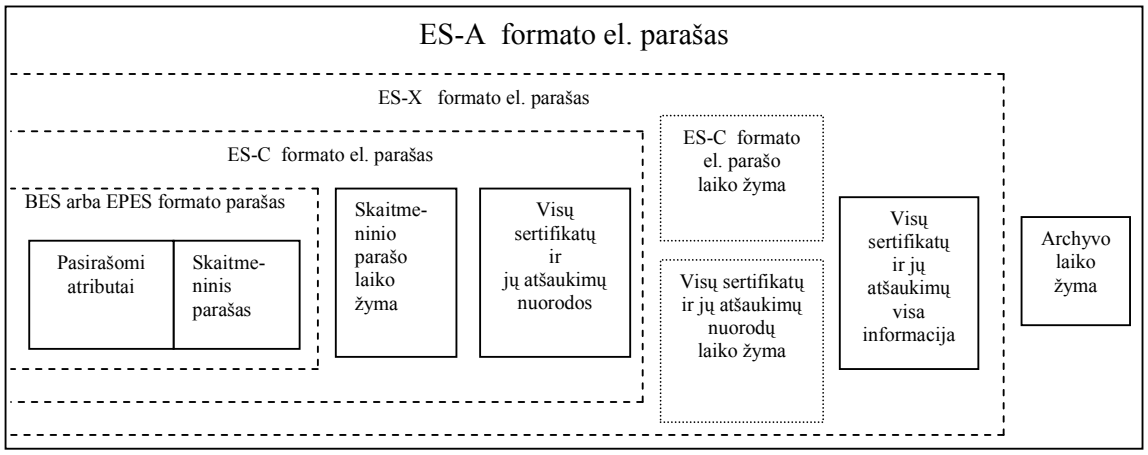
terminas gali būti pasibaigęs. Laiko žyma šiuo atveju tarnauja kaip įrodymas, kad parašas buvo sukurtas dar pasirašiusio asmens sertifikato galiojimo laikotarpiu. Antra, parašo technologijoje naudojami duomenų santraukos ir kriptografiniai algoritmai, buvę patikimi dokumento pasirašymo metu, prabėgus daug metų, kai bus tikrinamas archyvuoto dokumento parašas, jau gali būti tapę nepatikimi. Tačiau laiko žymų teikėjo (TSA) naudoti algoritmai žymoms kurti turi būti išlikę patikimi.

7.6 pav. schemiškai pavaizduota į archyvą dedamo pasirašyto dokumento struktūra.




7.6 pav. Į archyvą dedamo dokumento struktūra

7.7 pav. parodytas į archyvą dedamo dokumento el. parašas.




7.7 pav. ES-A formato el. parašas

# 8. PARAŠO TAISYKLĖS

Parašo taisyklės yra dokumentas, apibrėžiantis konkrečią el. parašo struktūrą, jo kūrimo ir tikrinimo procedūras, naudojimo sritis, sąlygas. Jos suteikia kontaktuojančioms šalims papildomos informacijos, padedančios labiau pasitikėti el. parašu. El. parašas laikomas potencialiai galiojančiu, jei jis buvo sukurtas laikantis parašo taisyklių. Parašo taisyklės gali būti nurodomos pačiame el. paraše arba kontaktuojančios šalys apie jas informuojamos kitokiais būdais - per sutartis, teisės aktus.

Parašo taisykles rengia el. parašo naudotojų grupės atstovai (pvz., kažkuris bankas, valstybės institucija, darbuotojų asociacija), tvirtina rengėjas. Jos turi būti laisvai prieinamos internetu.

Šiame skyriuje nagrinėjami parašo taisyklių klausimai.

## 8.1. Įžanga

Valdymo institucijų, verslo atstovų, šalies gyventojų kontaktavimas informacinių technologijų (IT) priemonėmis turi būti saugus. Perduodamų duomenų saugumui užtikrinti be el. parašo dar reikia papildomos informacijos, kuri didintų pasitikėjimą el. parašu. El. versle ir kitur partneriai turi apsibrėžti sąlygas, esant kurioms duotame veiklos kontekste el. parašas būtų laikomas galiojančiu. Visos tokios taisyklės ir sąlygos yra el. parašo galiojimo pagrindas. Jos gali būti surašytos viename dokumente, kuris vadinamas parašo taisyklėmis (*signature policy*) [2, 7, 28].

**Parašo taisyklės (*signature policy*)** – unikalų identifikatorių turintis techninių ir procedūrinių taisyklių rinkinys parašui kurti ir tikrinti. Parašo naudotojų grupė pati rengia šias taisykles arba pasirenka kitų parengtas ir jiems tinkančias taisykles. Parašo taisykles tvirtina jas parengęs asmuo.

Parašo taisyklės gali būti parašytos naudojant plačiai pripažintą formalųjį ASN.1 žymėjimą (ASN.1 – *Abstract Syntax Notation One*), XML kalbą arba laisvo teksto pavidalą, aiškiai apibrėžiant visus reikalavimus. Kai dvi arba daugiau šalių pranešimus vieni kitiems siuntinėja elektroninėmis priemonėmis, jiems iškyla poreikis apibrėžti parašo naudojimo sąlygas. Parašo taisyklės apibrėžia el. parašo naudojimo sritis ir koks jis turi būti (pvz., kokius atributus turintis) duoto konteksto transakcijose.

Viešųjų raktų infrastruktūra (PKI), be kurios neįmanomas el. parašo diegimas, reikalauja detaliai nurodyti įvairius el. parašo naudojimo ir gyvavimo ciklo technologinius, organizacinius ir teisinius aspektus. PKI atžvilgiu parašo taisyklės apibrėžia el. parašo naudojimo sąlygas tam

tikrame kontekste. Kontekstas gali būti suprantamas kaip operacijos (transakcijos) tipas, teisinis režimas, pasirašančiojo pareigos, kt.

Parašo taisyklės gali būti traktuojamos kaip kontaktuojančių šalių pasitikėjimą vienas kitu didinanti priemonė. Parašo taisyklės gali pagerinti PKI naudojimo sąlygas, kadangi jos įgalina pasirašantįjį asmenį perteikti daugiau informacijos parašo gavėjui, tuo darydamos transakciją skaidresnę. Dar daugiau, parašo taisyklės yra tinkama vieta nurodyti tam tikriems aspektams, kurie gali būti svarbūs sertifikavimo paslaugų teikėjams, pvz., informacijos elementai, kuriuos galima atskleisti tretiesiems asmenims (teisėsaugos institucijoms, kt.), sąlygos, kada galima atskleisti tą informaciją, kt.

## 8.2. Parašo taisyklių kontekstas

Parašo taisyklių paskirtis yra suteikti kontaktuojančioms šalims kiek galima daugiau informacijos apie partnerį. Parašo taisyklės sietinos su transakcijomis, nes formalizuoja tam tikrus transakcijų elementus ir jų naudojimą el. parašuose. Platesniam el. parašo naudojimui būtina išnagrinėti įvairių tipų transakcijas, kurioms galėtų būti taikomos pasirinktos parašo taisyklės.

Nevaržomos privačios transakcijos yra ta sritis, kur el. parašas galėtų būti labiausiai naudingas. Privačiose transakcijose nėra privalomų reikalavimų tvirtinti transakciją parašu. Formalioms transakcijoms, kurioms teisės aktai nustato specifinę formą, procedūras, kt., parašo taisyklės gali būti naudingos nurodyti transakcijos tikrinimo ir el. parašo naudojimo ribas. Parašo taisyklių naudotojams taip pat gali prireikti specifiškai apibrėžti transakcijas, kurioms parašo taisyklės yra reikalingos ar privalomos.

Praktiniu požiūriu yra naudinga turėti vieningas parašo taisykles, kurios tiktų įvairioms transakcijoms. Parašo taisyklių poreikį būtina susieti su poreikiu formalizuoti tam tikrus transakcijų informacijos elementus ir el. parašo naudojimą. Toks informacijos elementų formalizavimas būtinas automatiniam el. parašo informacijos apdorojimui ir pasitikėjimui juo padidinti, įrodymų ginčų atveju surinkimui.

### 8.2.1. Transakcijų kontekstas

Kadangi parašo taisyklės atspindi tam tikrus reikalavimus transakcijoms, būtina tam tikrų parašo taisyklių pagrindinius elementus susieti su tokį formalizavimą iššaukusiais reikalavimais. Transakcijos gali būti susiję su komercine, administracine ar privačiąja veikla arba bet kokia jų kombinacija. Transakcijų kontekstas apsprendžia bendrąsias parašo kūrimo taisykles. Tokios taisyklės gali būti kilusios iš įstatymų, pvz.,

operacija turi būti atliekama, užpildant specifinę formą, esant tam tikroms sąlygoms, kt. Specifinės transakcijų taisyklės, susijusios su pasirašymo teise ar specifinėmis parašo pripažinimo sąlygomis, gali būti įtrauktos į parašo taisykles.

### 8.2.2. Parašo taisyklės ir viešųjų raktų infrastruktūra (PKI)

PKI aplinka reikalauja, kad duomenis pasirašantis asmuo nurodytų savo parašo specifinę prasmę (paskirtį). El. parašas gali reikšti, kad asmuo veikia laikydamasis jam suteiktų įgaliojimų arba kad parašas naudojamas tik autentiškumui patvirtinti. Kai parašas turi specifinę prasmę, pasirašantis asmuo turi įtraukti į el. parašą atributą, nurodantį parašo paskirties tipą.

Reikalavimas nurodyti parašo paskirties tipą gali būti parašo taisyklėse, ir tokio reikalavimo egzistavimą pasirašantis asmuo turi perduoti pasirašytų duomenų gavėjams, kad jie geriau pasitikėtų parašu.

Parašo taisyklės, kuriomis vadovaujasi pasirašantis asmuo, gali būti tiesiogiai nurodomos unikaliu identifikatoriumi, dedamu į el. parašą. Parašo gavėjas gali spręsti, ar jam priimtinos pasirašiusio asmens naudotos ir nurodytos parašo taisyklės. Jei parašo taisyklės yra priimtinos, parašo tikrintojas, remdamasis jomis, pasitiki pasirašytais duomenimis.

Parašo taisyklės, kuriomis remiasi pasirašantis asmuo, gali būti nurodomos ir netiesiogiai. Tuomet tam tikra informacija, kuri padėtų susieti pasirašytus duomenis su parašo taisyklėmis, turi būti patalpinta kitur, ne pačiame paraše, o, pavyzdžiui, teisės aktuose ar sutartyse, parašo tikrintojams prieinamoje vietoje. Kad galima būtų naudotis šiuo informacijos apie parašo taisykles perdavimo būdu, transakcijos prasmė jau turi būti žinoma. Praktikoje šis būdas netinka laisvo pavidalo tekstams, bet jis yra geras apibrėžtos formos duomenims.

Yra du parašo taisyklių netiesioginio nurodymo būdai:

- dokumentas (pvz., teisės aktas, sutartis), nurodantis, kad tam tikros parašo taisyklės tinka jose išvardintų formų duomenims;
- dokumentas, nurodantis, kad tam tikros formos duomenims vartotinos atitinkamos parašo taisyklės.

<u>Parašo taisyklės uždaroje aplinkoje (uždarose sistemose)</u>

Nors PKI geriau tinka atvirų transakcijų ir komunikacijų atveju, tačiau PKI dažnai naudojama ir uždarose aplinkose. Uždarų aplinkų (**CUG** – *Closed User Groups*) bruožas yra išankstinės žinios apie veiklos partnerius. Tokiose aplinkose PKI naudojama todėl, kad ji geriau nei kitos technologijos atitinka saugumo reikalavimus.

Parašo taisyklių leidėjas taisykles perduoda (platina) vienašališkai nustatytomis priemonėmis, kurios atitinka sutartas veiklos ribas. Su parašo taisyklėmis sutinkantys vartotojai turi pasirašyti dvišalį susitarimą dėl šių taisyklių naudojimo dvišalėse transakcijose, arba tai patvirtinti kitokiu būdu.

Uždaroje aplinkoje kontaktuojančios pusės gali pritarti parašo taisyklėms ir jų naudojimo sąlygoms, nurodydamos tai pasirašomose sutartyse.

Parašo taisyklės atviroje aplinkoje

Jei uždarose aplinkose apibrėžtoms transakcijoms gali būti taikomi paprastesni reikalavimai, tai atvirose aplinkose naudojamos parašo taisyklės turi būti kruopščiai parengtos ir atitikti numatomas transakcijas. Tik labai atsakingai parengtos parašo taisyklės ir atitinkančios specifinius teisės aktų reikalavimus gali būti naudojamos atviroje aplinkoje.

Parašo taisyklės turi neatsiejamą poveikį pasitikėjimui tarp veiklos partnerių. Pasitikėjimas tarp šalių atsiranda tada, kai jos viena kitą pažįsta ir bendradarbiauja pagal žinomas normas. Nesant tokių aplinkybių, parašo taisyklių uždavinys atviroje aplinkoje yra padidinti kontaktuojančių šalių pasitikėjimą el. parašu.

Parašo taisykles šalys gali gauti atvirais tinklais. Parašo taisyklės padeda jų leidėjams paskleisti el. parašo naudojimo sąlygas neapibrėžtam parašo naudotojų ratui.

Parašo taisyklių formos ir turinio standartizavimas prisideda prie platesnio taisyklių pripažinimo ir geresnės šalių sąveikos atviroje aplinkoje.

### 8.2.3. Parašo taisyklių tipai

Parašo taisyklės gali atspindėti įvairius kontaktuojančių šalių transakcijų aspektus. Jos gali būti susijusios su vieno parašo transakcijomis arba kelis parašus turinčiomis transakcijomis.

Vieno parašo transakcijų parašo taisyklės leidžia priimti sprendimą, ar parašas yra galiojantis, ar ne.

Kelis parašus turinčiose transakcijose duomenis būna pasirašę keli asmenys. Kaip pavyzdys gali būti dviejų šalių sandoris, kurį tvirtina notaras. Tokiame dokumente bus trys parašai. Čia svarbi ir parašų sukūrimo eilės tvarka. Kitas pavyzdys – krovinio siuntėjas, ekspeditorius, gavėjas, t.t.

Minėtų transakcijų atvejais turi būti atitinkamos parašo taisyklės.

### 8.2.4. Parašo taisyklių ir sertifikato taisyklių santykis

Kadangi taisyklės yra bendras būdas elektroninės komercijos veiklos sąlygoms išreikšti, todėl parašo taisyklės turi skirtis nuo kitokio tipo taisyklių, tame tarpe ir nuo sertifikato taisyklių. Parašo taisyklėse yra nuorodos, kuriomis vadovaujantis galima nustatyti sertifikato taisykles, atitinkančias duotas parašo taisykles. Tai padeda apriboti sertifikatų ratą, kurie gali būti naudojami el. parašams patvirtinti, esant konkrečioms parašo taisyklėms. Juk sertifikatuose nurodomas sertifikato taisyklių identifikatorius (OID), kurių laikantis sertifikatai yra sudaromi ir tvarkomi. Kita vertus, sertifikato taisyklėse gali būti nuoroda į parašo taisykles, parodanti, kad sertifikato taisyklės atitinka kažkurias parašo taisykles. Tačiau sertifikato taisyklės ir parašo taisyklės visada yra atskiri dokumentai, nes skiriasi jų paskirtis ir veikimo sritys.

## 8.3. Parašo taisyklių leidėjai ir naudotojai

### 8.3.1. Parašo taisyklių leidėjai

Parašo taisyklių leidėjas apibrėžia el. parašo naudojimą nustatyto tipo transakcijoms ir tam tikram parašo naudotojų ratui. Parašo taisyklių leidėju gali būti:

- juridinis asmuo, t. y. organizacija, nustatanti el. parašo naudojimo sąlygas savo atstovams ir klientams ryšiams su ja;
- fizinis asmuo, pavyzdžiui, notaras, kt. profesijos atstovas (arba profesijos atstovų asociacija), nustatantis el. parašo naudojimo sąlygas klientams, ryšiams su juo profesiniais klausimais.

### 8.3.2. Parašo taisyklių naudotojai

Fizinis asmuo, veikiantis savo arba kito asmens vardu pagal profesinį ar tarnybinį įgaliojimą, yra pasirašantis asmuo tam tikro konteksto transakcijose. El. parašą gali tikrinti fizinis asmuo arba tai gali būti atliekama automatiškai.

Pasirašantis asmuo

Už el. parašą visų pirma yra atsakingas jį sukūręs asmuo. Todėl pasirašantis asmuo turi žinoti parašo taisykles. Apskritai, pasirašantis asmuo yra atsakingas už informacijos apie el. parašo naudojimo sąlygas perdavimą veiklos partneriams.

Pasirašantis asmuo gali pasirašinėti savo iniciatyva arba vykdydamas jam patikėtas pareigas. Kalbant apie patikėtas pareigas, skiriami du atvejai:

paraše jos gali būti nurodytos be jokio patvirtinimo arba paraše gali būti nuoroda į pareigas patvirtinantį specialų sertifikatą (pareigų sertifikatą).

Parašo tikrintojas

Parašo tikrintojas yra asmuo, tikrinantis gautą pasirašytą dokumentą. Jis visų pirma turi įsitikinti, kad el. paraše nurodytos parašo taisyklės atitinka jo veiklos reikalavimus. Pagal el. paraše esančią nuorodą atsisiuntęs parašo taisykles, jis turi įsitikinti taisyklių autentiškumu (ar taisyklės nėra suklastotos, iškraipytos).

## 8.4. Reikalavimai parašo taisyklėms

### 8.4.1. Reikalavimai parašo taisyklių pavidalui

Parašo taisyklės gali būti naudojamos įvairiais laiko momentais. Jų gali prireikti pasirašančiam asmeniui, kad įsitikintų, jog taisyklės atitinka jo atliekamų transakcijų kontekstą. Tuo metu jam reikia tokio pavidalo (formato) parašo taisyklių, kad galėtų perskaityti jas.

Pasirašančio asmens pasirinktose parašo taisyklėse esančias sąlygas turi gebėti suprasti ne tik žmogus, bet ir techninė bei programinė įranga, kuri naudojama parašui kurti.

Pasirašytų duomenų parašo tikrintojas turi nustatyti, kokiomis parašo taisyklėmis vadovavosi pasirašantis asmuo. Todėl parašo taisyklės tikrintojui turėjo būti perduotos arba iki parašo tikrinimo momento, arba turi būti pateiktos parašo tikrinimo metu. Šiais atvejais taisyklės turi būti žmogui perskaitomo pavidalo. Automatiniu būdu tikrinant el. parašą, parašo taisyklės turi būti pateiktos kompiuteriui (kt. mašinai) suprantamu pavidalu.

Taigi, parašo taisyklės turi būti dviejų pavidalų:

- ♦ žmogui perskaitomo pavidalo;
- ♦ mašinai suprantamo pavidalo.

### 8.4.2. Bendroji parašo taisyklių informacija

Parašo taisyklėse turi būti tokia bendroji informacija:

- ♦ parašo taisyklių leidėjo pavadinimas. Tai atsakingo už parašo taisyklių leidimą asmens vardas;
- ♦ parašo taisyklių identifikatorius. Parašo taisyklės turi turėti identifikatorių (OID), kurio paskutinis dešinėje esantis skaičius reikštų taisyklių versiją duotu metu;

- pasirašymo periodas. Tai pradžios laikas ir data ir, jeigu reikia, pabaigos laikas ir data, kuomet gali būti kuriami elektroniniai parašai, vadovaujantis tomis parašo taisyklėmis;
- parašo taisyklių išleidimo data;
- parašo taisyklių taikymo sritis. Čia bendrais bruožais turi būti nurodomas teisinis, sutartinis arba taikomasis kontekstas (aplinkybės, sąlygos), kur parašo taisyklės galėtų būti taikomos, ir elektroninio parašo naudojimo specifiniai tikslai.

Transakcijų šalių prisiimti tam tikri įsipareigojimai taip pat gali būti įtraukiami į parašo taisykles. Tai galėtų būti kažkokio įsipareigojimo identifikatorius (OID), platesnis jo paaiškinimas.

### 8.4.3. Parašo patvirtinimo taisyklės ir duomenys

Asmuo, gavęs pasirašytą dokumentą, prieš imdamasis tolesnių transakcijos kontekstą atitinkančių veiksmų, turi patikrinti el. parašą. Parašą tikrinančios šalys dar surenka tokius informacijos elementus, kaip pasirašiusio asmens sertifikato galiojimą patvirtinantys duomenys ir parašo galiojimą patvirtinantys duomenys. Jei parašo tikrintojas nusprendžia, kad parašo taisyklės atitinka teisinio/sutartinio konteksto reikalavimus, tai reiškia, kad jis sutinka su el. parašo naudojimo sąlygomis, kurios yra aiškiai ar netiesiogiai atspindėtos pasirašytuose duomenyse.

Parašo taisyklės tikrinamos tada, kai asmuo gauna pasirašytus duomenis, ir tai gali būti padaryta betarpiškai dalyvaujant žmogui arba automatiniu būdu.

Techniniai parašo taisyklių reikalavimai kartu su visais parašo tikrinimo duomenimis yra vadinami **parašo patvirtinimo taisyklėmis** (tai parašo taisyklių dalis). Tai tokios taisyklės, kuriomis reikia vadovautis tikrinant parašus.

Parašo patvirtinimo taisyklės pasirašančiam asmeniui nurodo, kokius informacijos elementus (atributus) jis turi pateikti paraše, o parašo tikrintojui – kokie informacijos elementai turi būti paraše, kad jis pagal parašo reikalavimus būtų laikomas potencialiai galiojančiu.

Pasirašantis asmuo gali naudoti skirtingo paskirties tipo parašus (pvz., duomenims patvirtinti, duomenų gavimo faktui patvirtinti, kt.), nors bendrosios parašo taisyklės yra tos pačios. Kad kiekvienam parašų paskirties tipui nereikėtų kurti vis naujų parašo taisyklių, jose galima apibrėžti bendras taisykles, tinkančias visiems parašų paskirties tipams, bei keletą specifinių taisyklių, taikomų tik tam tikriems parašų paskirties tipams. Tokiu būdu tam tikros parašo taisyklės gali būti naudojamos

įvairiems parašų paskirties tipams, jeigu pasirašantis asmuo sukurtame paraše aiškiai nurodo parašo paskirties tipą.

Todėl parašo taisyklės gali būti padalintos į dvi dalis:

a) bendras visiems parašų tipams taisykles (Bendrąsias taisykles);

b) specifinių parašų tipų taisykles (Specialiąsias taisykles).

Šias dalis galima apibūdinti taip:

a) bendrųjų taisyklių dalis tinka visų tipų parašams. Šios taisyklės apima sertifikatų, laiko žymų ir atributų (pvz., pareigų atributas, kuris gali būti nurodytos el. paraše ir patvirtintas specialiu sertifikatu) patikimumo sąlygas, nepriklausomai nuo bet kokių apribojimų atributams, kurie gali būti el. parašo sudėtyje;

b) specialiųjų taisyklių dalis yra skirta duotiems specifinės paskirties parašų tipams. Jos taip pat apima sertifikatų, laiko žymų ir atributų patikimumo sąlygas, nepriklausomai nuo bet kokių apribojimų atributams, kurie gali būti el. parašo sudėtyje.

Parašo patvirtinimo duomenys

Parašui patvirtinti reikalingi elementai (duomenys) gali būti nurodomi Bendrųjų ir/arba Specialiųjų taisyklių dalyje, tačiau jokiu būdu jie negali prieštarauti vieni kitiems. Parašo taisyklių leidėjas turi nustatyti tokius parašui patikrinti būtinus elementus (duomenis), kurie atitiktų puoselėjamas parašo patvirtinimo taisykles.

Parašo patvirtinimo taisyklėse turi būti šie elementai (duomenys):

a) taisyklės, kaip naudotis CA;

b) taisyklės pasirašiusių asmenų sertifikatams tikrinti;

c) tikrinimo, kad parašas buvo sukurtas pasirašiusio asmens sertifikato galiojimo laikotarpiu (t. y. kaip naudoti parašo laiko žymą), taisyklės;

d) taisyklės, susijusios su atidėjimo periodu (tai privalomas laiko tarpas, kuris turi praeiti nuo parašo sukūrimo iki jo tikrinimo, kad tikrintojas būtų labiau tikras, jog pasirašantis asmuo nepaprašė panaikinti savo sertifikato galiojimo tuoj po parašo sukūrimo. Praeina tam tikras laiko tarpas, kol CA tarnybos, gavusios prašymą, panaikina sertifikato galiojimą);

e) CRL sąrašų informacijos naudojimo taisyklės;

f) apsisaugojimo nuo CA privačiojo rakto sukompromitavimo ir kriptografijos metodo silpnųjų pusių atskleidimo pasekmių taisyklės;

g) parašo kūrimo aplinkos taisyklės;

h) informacijos elementai (parašo atributai), kuriuos pasirašantysis asmuo turi pateikti paraše, o parašo tikrintojas turi patikrinti;

i) visi parašo algoritmų ir šifravimo raktų ilgio apribojimai;

j) pasirašančiųjų asmenų pareigų (rolių) nurodymo taisyklės;

k) reikalavimai sertifikatų sekai. Sertifikatų seka – tai pasirašančiojo asmens sertifikato ir CA, kuriais pasitikima, sertifikatų grandinė. Visi tokios sekos sertifikatai turi būti tikrinami.

### 8.4.4. Kitos parašo taisyklių ypatybės

Parašo taisyklėse gali būti ir papildomi reikalavimai, pavyzdžiui, susiję su el. parašo naudotojų aplinka (namų aplinka, įstaigos aplinka, mobilioji aplinka, kt.). Papildomos taisyklės gali būti pateiktos žmogui įprasta kalba ir kompiuteriui suprantamu pavidalu (ASN.1, XML formato).

### 8.4.5. Parašo taisyklių apsauga

Tiek pasirašantis asmuo, tiek parašo tikrintojas, prieš naudodamas parašo taisykles, turi įsitikinti jų autentiškumu. Jei pasirašantis asmuo paraše nurodo parašo taisyklių identifikatorių, jis turi pridėti ir tų taisyklių santrauką (*hash*) bei santraukos algoritmo identifikatorių.

Parašo taisyklių skelbimas

Pasirašantis asmuo, kurdamas parašą, turi būti tikras dėl naudojamų parašo taisyklių autentiškumo. Lygiai taip pat parašo tikrintojas turi būt tikras, kad vadovaujasi autentiškomis parašo taisyklėmis. Tam reikalingi šių taisyklių autentiškumą ir vientisumą (neiškraipymą) užtikrinantys skelbimo ir perdavimo būdai. Parašo taisyklių leidėjams rekomenduojama naudoti vieną iš trijų parašo taisyklių saugaus perdavimo parašo naudotojams būdų:

a) naudoti patikimus perdavimo kanalus – talpinti parašo taisykles saugiuose WWW puslapiuose (naudoti TLS/SSL protokolus) arba siuntinėti naudotojams parašo taisykles, pasirašytas leidėjo el. parašu;

b) naudoti patikimas parašo taisyklių saugyklas (*repository*). Parašo taisyklės patikimų sertifikavimo paslaugų teikėjų (trečiųjų asmenų) prižiūrimoje saugykloje turėtų būti saugomi tol, kol bus poreikis naudotis jais, netgi parašo taisyklių leidėjams nutraukus savo veiklą;

c) naudoti patikimas duomenų laikmenas, pavyzdžiui, kompaktinius diskus (CD-ROM), iš kur bet kada galima būtų parašo taisykles perskaityti.

### 8.4.6. Bendroji parašo taisyklių struktūra

Parašo taisyklės yra el. parašo kūrimo ir tikrinimo taisyklių rinkinys, kuriomis remiantis kontaktuojančios šalys gali laikyti parašą galiojančiu tam tikroje veiklos srityje (santykių kontekste). Parašo taisyklės apibrėžia el. parašo naudojimo sąlygas, veiklos sritis ir koks jis turi būti duotos srities transakcijose.

Parašo taisyklių identifikavimas: nuorodose į parašo taisykles be parašo taisyklių identifikatoriaus dar turi būti parašo taisyklių santraukos (*hash*) algoritmo identifikatorius ir parašo taisyklių santraukos reikšmė.

Toliau pateikiama bendroji parašo taisyklių struktūra:

1. BENDROJI INFORMACIJA
1.1. Parašo taisyklių identifikatorius
1.2. Parašo taisyklių išleidimo data
1.3. Parašo taisyklių leidėjas
1.4. Parašo taisyklių taikymo sritys
1.5. Kita bendroji informacija

2. PARAŠO PATVIRTINIMO TAISYKLĖS
2.1. Parašo taisyklių naudojimo laikotarpis (periodas)
2.2. Bendrosios taisyklės
2.2.1. Pasirašančiojo asmens taisyklės
2.2.1.1. Pasirašomas dokumentas parašo struktūroje (t. y. į parašą įtraukiamas visas dokumentas ar tik jo santrauka)
2.2.1.2. Parašo vidiniai atributai (kokie informacijos elementai – asmens pasirašomi atributai turi būti paraše, kurių rinkiniui kuriamas skaitmeninis parašas)
2.2.1.3. Parašo išoriniai atributai (laiko žymos, kt.)
2.2.1.4. Pasirašančiojo asmens sertifikato nuoroda (nurodyti tik pasirašančiojo sertifikatą ar visą sertifikatų seką)
2.2.1.5. Kitos taisyklės
2.2.2. Parašo tikrintojo taisyklės
2.2.2.1. Parašo išoriniai atributai (laiko žymos, kt.)
2.2.2.2. Pasirašiusiojo asmens sertifikato tikrinimas
2.2.2.3. Kitos parašo tikrintojo taisyklės
2.2.3. Pasirašiusiojo asmens sertifikato patikimumo sąlygos
2.2.3.1. Reikalavimai sertifikatams:
a) sertifikatų sekos CA, sudariusio sau sertifikatą, nuoroda;
b) leistinas sertifikatų sekos ilgis;
c) taikytinos sertifikato taisyklės;
d) reikalavimai CA vardams (internetiniams adresams);
e) kitos sąlygos
2.2.3.2. Sertifikatų galiojimo tikrinimo reikalavimai:
a) galinių sertifikatų (pasirašančiojo asmens, atributinės informacijos ar laiko žymos teikėjo) galiojimo tikrinimas:
- naudojant atšauktų sertifikatų sąrašą (CRL);
- sertifikatų statuso tikrinimas *on-line* protokolu (OCSP);
- naudojant atšauktų sertifikatų sąrašų (CRL) pokyčius;

- kiti tikrinimai;

b) sertifikatus sudarančių CA sertifikatų galiojimo tikrinimas:
- naudojant atšauktų sertifikatų sąrašą (CRL);
- sertifikatų statuso tikrinimas *on-line* protokolu (OCSP);
- naudojant atšauktų sertifikatų sąrašų (CRL) pokyčius;
- kiti tikrinimai

2.2.4. Laiko žymos patikimumo sąlygos
2.2.4.1. Taisyklės laiko žymų teikėjo viešajam raktui paliudyti
2.2.4.2. Laiko žymų galiojimo nutraukimo reikalavimai
2.2.4.3. Reikalavimai laiko žymų teikėjų vardams (internetiniams adresams)
2.2.4.4. Parašo tikrinimo atidėjimo (angl. *grace*) periodas
2.2.4.5. Maksimalus laiko skirtumas tarp pasirašiusiojo asmens nurodyto laiko ir laiko žymos laiko
2.2.5. Parašo vidinių atributų patikimumo sąlygos
2.2.5.1. Pasirašančiojo asmens atributai
2.2.5.2. Atributo sertifikato tikrinimo sąlygos
2.2.5.3. Atributo sertifikato galiojimo nutraukimo reikalavimai
2.2.5.4. Atributų apribojimai
2.2.6. Algoritmų apribojimai
2.2.6.1. Pasirašančiojo asmens naudojamų algoritmų apribojimai:
a) parašo kūrimo algoritmai (santraukos, kriptografijos, kombinuotieji - santraukos + kriptografijos);
b) minimalus raktų ilgis;
c) kiti apribojimai
2.2.6.2. Sertifikatus pasirašantiesiems asmenims sudarančio CA naudojamų algoritmų apribojimai
2.2.6.3. Sertifikatus kitiems CA sudarančio CA naudojamų algoritmų apribojimai
2.2.6.4. Parašo vidinių atributų informaciją (pvz., pasirašančiojo asmens pareigas) liudijančių paslaugų teikėjų (AA – *Attribute Authority*) naudojamų algoritmų apribojimai
2.2.6.5. TSA naudojamų algoritmų apribojimai
2.2.7. Kitos bendrojo pobūdžio taisyklės
2.3. Specialiosios taisyklės
2.3.1. Specifinės paskirties parašo tipo identifikatorius

Kiti 2.3 skyriaus punktai turi būti tokie patys (kurių reikia) kaip ir 2.2 skyriaus, tačiau juose neturi būti pasikartojančių ar prieštaraujančių reikalavimų.

### 8.4.7. Parašo taisyklių pavyzdys

*I. BENDROJI PARAŠO TAISYKLIŲ INFORMACIJA*

1. Parašo taisyklių identifikatorius:

*Identifikatorius (OID):* *2.16.440.9999.1.1.1.*

*Parašo taisykles galima rasti internete adresu:*

*www.xxxx.lt/parasotaisykles*

2. Parašo taisyklių išleidimo data: *2004 m. sausio 1 d.*
3. Parašo taisyklių leidėjas:

*XXXX komitetas ar kita organizacija*

*Vilniaus g.. 99, Vilnius, Lietuva*

4. Parašo taisyklių taikymo sritis:

*Lietuvos Respublikos valstybės institucijų ir savivaldybių tarpusavio susirašinėjimui, susirašinėjimui su verslo atstovais, valstybės gyventojais.*

*II. BENDROSIOS PARAŠO GALIOJIMO TAISYKLĖS*

5. Parašo taisyklių naudojimo laikotarpis:

*nuo 2004 m. sausio 1 d.*

*iki 2008 m. gruodžio 31 d.*

6. Pasirašančiojo asmens ir parašo tikrintojo taisyklės:

6.1. Pasirašančiojo asmens taisyklės:

6.1.1. Visi pasirašomi duomenys neturi būti dedami į parašą. Į sukurtą parašą kaip viena iš jo sudėtinių dalių (pasirašomas atributas) turi būti įtraukta pasirašomų duomenų santrauka.

6.1.2. Sukurtame paraše turi būti tokios jo sudėtinės dalys - pasirašomi atributai:

| *Nr.* | *Pasirašomo atributo pavadinimas* | *Atributo identifikatorius* |
|---|---|---|
| *1* | *Pasirašomų duomenų tipas* | *1.2.840.113549.1.9.3* |
| *2* | *Pasirašomų duomenų santrauka* | *1.2.840.113549.1.9.4* |
| *3* | *Pasirašymo laikas* | *1.2.840.113549.1.9.5* |
| *4* | *Pasirašančiojo asmens sertifikato nuoroda* | *1.2.840.113549.1.9.16.2.12* |
| *5* | *Parašo taisyklių nuoroda* | *1.2.840.113549.1.9.16.2.15* |
| *6* | *Pasirašančiojo asmens pareigos* | *1.2.840.113549.1.9.16.2.18* |

6.1.3. Sukurtą parašą pasirašantysis asmuo turi papildyti tokiais duomenimis – nepasirašomais atributais:

| *Nr.* | *Nepasirašomo atributo pavadinimas* | *Atributo identifikatorius* |
|---|---|---|
| *1* | *Laiko žyma* | *1.2.840..113549.1.9.16.2.14* |
| *2* | *Visų su parašu susijusių sertifikatų (išskyrus pasirašančiojo asmens) nuorodos* | *1.2.840..113549.1.9.16.2.21* |
| *3* | *Visų su parašu susijusių sertifikatų statuso informacijos šaltinių nuorodos* | *1.2.840..113549.1.9.16.2.22* |

6.1.4. Parašo pasirašomame atribute *"Pasirašančiojo asmens sertifikato nuoroda "* (6.1.2. ketvirtas punktas) turi būti pateikiama tik pasirašančiojo asmens sertifikato nuoroda.

6.2. Parašo tikrintojo taisyklės:

6.2.1. Parašo tikrintojas turi papildyti tikrinamąjį parašą tokiais duomenimis – nepasirašomais atributais, jei jų nepateikė pasirašantysis asmuo:

| *Nr.* | *Nepasirašomo atributo pavadinimas* | *Atributo identifikatorius* |
|---|---|---|
| *1* | *Laiko žyma* | *1.2.840..113549.1.9.16.2.14* |
| *2* | *Visų su parašu susijusių sertifikatų (išskyrus pasirašančiojo asmens) nuorodos* | *1.2.840..113549.1.9.16.2.21* |
| *3* | *Visų su parašu susijusių sertifikatų statuso informacijos šaltinių nuorodos* | *1.2.840..113549.1.9.16.2.22* |

7. Pasirašiusiojo asmens sertifikato patikimumo sąlygos

7.1. Sertifikatų seka:

7.1.1. Sertifikato, kurį sertifikatų centras (CA) pasidarė sau, nuoroda:

www.xxxx.lt/ltca0001 + *sha1* + *sertifikato santraukos reikšmė*

7.1.2. Sertifikatų sekos ilgio apribojimai - *nėra*

7.1.3. Pripažįstamos sertifikato taisyklės:

| *Nr.* | *Sertifikato taisyklių leidėjas* | *Sertifikato taisyklių identifikatorius* |
|---|---|---|
| *1* | *XXXX komitetas* | *1.16.440.1.1.1.1* |

7.1.4. Apribojimai sertifikatų centrų (CA) vardams - *nėra.*

7.1.5. Sertifikato taisyklių akivaizdžios nuorodos turi būti kiekviename sertifikatų sekos sertifikate.

7.2. Sertifikato statuso tikrinimas.

7.2.1. Pasirašiusiojo asmens sertifikato statusas turi būti tikrinamas naudojant bent vieną iš šių būdų: peržiūrint atšauktų sertifikatų sąrašo (CRL) paskutinę versiją arba tikrinant sertifikatų statusą *on-line* protokolu *(arba tikrinimas nebūtinas).*

7.2.2. Sertifikatų centrų (CA) sertifikatų statusas turi būti tikrinamas naudojant bent vieną iš šių būdų: peržiūrint atšauktų sertifikatų sąrašo paskutinę versiją arba tikrinant sertifikatų statusą *on-line* protokolu *(arba tikrinimas nebūtinas).*

8. Laiko žymos patikimumo sąlygos.

8.1. Laiko žymų teikėjo (TSA) sertifikatų seka.

8.1.1. Sertifikato, kurį sertifikatų centras (CA) pasidarė sau, nuoroda www.xxxx.lt/ltca0001 + *sha1 + sertifikato santraukos reikšmė*

8.1.2. Sertifikatų sekos ilgio apribojimai - *nėra.*

8.1.3. Pripažįstamos sertifikato taisyklės

| *Nr.* | *Sertifikato taisyklių leidėjas* | *Sertifikato taisyklių identifikatorius* |
|---|---|---|
| *1* | *XXXX komitetas* | *1.16.440.1.1.1.1* |

8.1.4. Apribojimai sertifikatų centrų (CA) vardams - *nėra.*

8.1.5. Sertifikato taisyklių akivaizdžios nuorodos turi būti kiekviename sertifikatų sekos sertifikate.

8.2. Laiko žymų teikėjo (TSA) sertifikato statuso tikrinimas

8.2.1. Laiko žymos teikėjo (TSA) sertifikato statusas turi būti tikrinamas naudojant bent vieną iš šių būdų: peržiūrint atšauktų sertifikatų sąrašo (CRL) paskutinę versiją arba tikrinant sertifikatų statusą *on-line* protokolu *( arba tikrinimas nebūtinas)*

8.2.2. Sertifikatų centro (CA), išdavusio sertifikatą laiko žymos teikėjui (TSA) sertifikatų statusas turi būti tikrinamas naudojant bent vieną iš šių būdų: peržiūrint atšauktų sertifikatų sąrašo (CRL) paskutinę versiją arba tikrinant sertifikatų statusą *on-line* protokolu (OCSP) *( arba tikrinimas nebūtinas)*

8.3. Apribojimai laiko žymos teikėjų (TSA) vardams - *nėra.*

8.4. Atidėjimo periodas – leistinas maksimalus skirtumas tarp pasirašiusiojo asmens sertifikato atšaukimo laiko ir laiko parašo laiko žymoje – *24 val.*

8.5. Leistinas maksimalus skirtumas tarp laiko parašo laiko žymoje ir laiko, kurį pasirašęs asmuo nurodo parašo pasirašomame atribute *“Pasirašymo laikas”* (6.1.2. trečias punktas) - *7 dienos.*

9. Parašo atributų patikimumo sąlygos

9.1. Sertifikuojami parašo pasirašomi atributai - *nėra.*

9.2. Parašo pasirašomame atribute *“Pasirašančiojo asmens pareigos” (6.1.2. šeštas punktas)* turi būti nurodomos pasirašančiojo asmens pareigos.

10. Algoritmų apribojimai

10.1. Pasirašančiojo asmens naudojamų algoritmų apribojimai:

| *Nr.* | *Algoritmo pavadinimas* | *Minimalus rakto ilgis* | *Algoritmo identifikatorius* |
|---|---|---|---|
| *1* | *Santraukos algoritmas SHA1* | | *1.3.14.3.2.26* |
| *2* | *Šifravimo algoritmas RSA* | *1024* | *1.2.840.113549.1.1.1* |
| *3* | *Kombinuotasis algoritmas SHA1suRSA* | *1024* | *1.2.840.113549.1.1.5* |

10.2. Sertifikatų centro (CA), sudarančio sertifikatus pasirašantiesiems asmenims, naudojamų algoritmų apribojimai.

| *Nr.* | *Algoritmo pavadinimas* | *Minimalus rakto ilgis* | *Algoritmo identifikatorius* |
|---|---|---|---|
| *1* | *Santraukos algoritmas SHA1* | | *1.3.14.3.2.26* |
| *2* | *Šifravimo algoritmas RSA* | *2048* | *1.2.840.113549.1.1.1* |
| *3* | *Kombinuotasis algoritmas SHA1suRSA* | *2048* | *1.2.840.113549.1.1.5* |

10.3. Sertifikatų centro (CA), sudarančio sertifikatus kitiems sertifikatų centrams (CA), naudojamų algoritmų apribojimai.

| *Nr.* | *Algoritmo pavadinimas* | *Minimalus rakto ilgis* | *Algoritmo identifikatorius* |
|---|---|---|---|
| *1* | *Santraukos algoritmas SHA1* | | *1.3.14.3.2.26* |
| *2* | *Šifravimo algoritmas RSA* | *2048* | *1.2.840.113549.1.1.1* |
| *3* | *Kombinuotasis algoritmas SHA1suRSA* | *2048* | *1.2.840.113549.1.1.5* |

10.4. Laiko žymos teikėjų (TSA) naudojamų algoritmų apribojimai.

| *Nr.* | *Algoritmo pavadinimas* | *Minimalus rakto ilgis* | *Algoritmo identifikatorius* |
|---|---|---|---|
| *1* | *Santraukos algoritmas SHA1* | | *1.3.14.3.2.26* |
| *2* | *Šifravimo algoritmas RSA* | *2048* | *1.2.840.113549.1.1.1* |
| *3* | *Kombinuotasis algoritmas SHA1suRSA* | *2048* | *1.2.840.113549.1.1.5* |

PASTABA: šiame pavyzdyje pateikti atributų ir kitų objektų unikalieji identifikatoriai (OID) yra tikslintini.

# 9. ELEKTRONINIO PARAŠO KŪRIMAS

Čia aprašomi saugumo reikalavimai kompiuterių programoms, skirtoms kurti (formuoti) saugius, pasirašančių asmenų kvalifikuotais sertifikatais paremtus el. parašus, naudojant saugią parašo formavimo įrangą (**SSCD** - *Secure Signature Creation Device*). Tokie parašai trumpiau vadinami kvalifikuotais parašais (toliau – parašas). Pateikiami:

- parašo kūrimo aplinka, funkcinis modelis [12];
- bendrieji reikalavimai modelyje nurodytoms funkcijoms;
- reikalavimai kiekvienai parašo kūrimo taikomųjų programų funkcijai;
- reikalavimai SSCD [11].

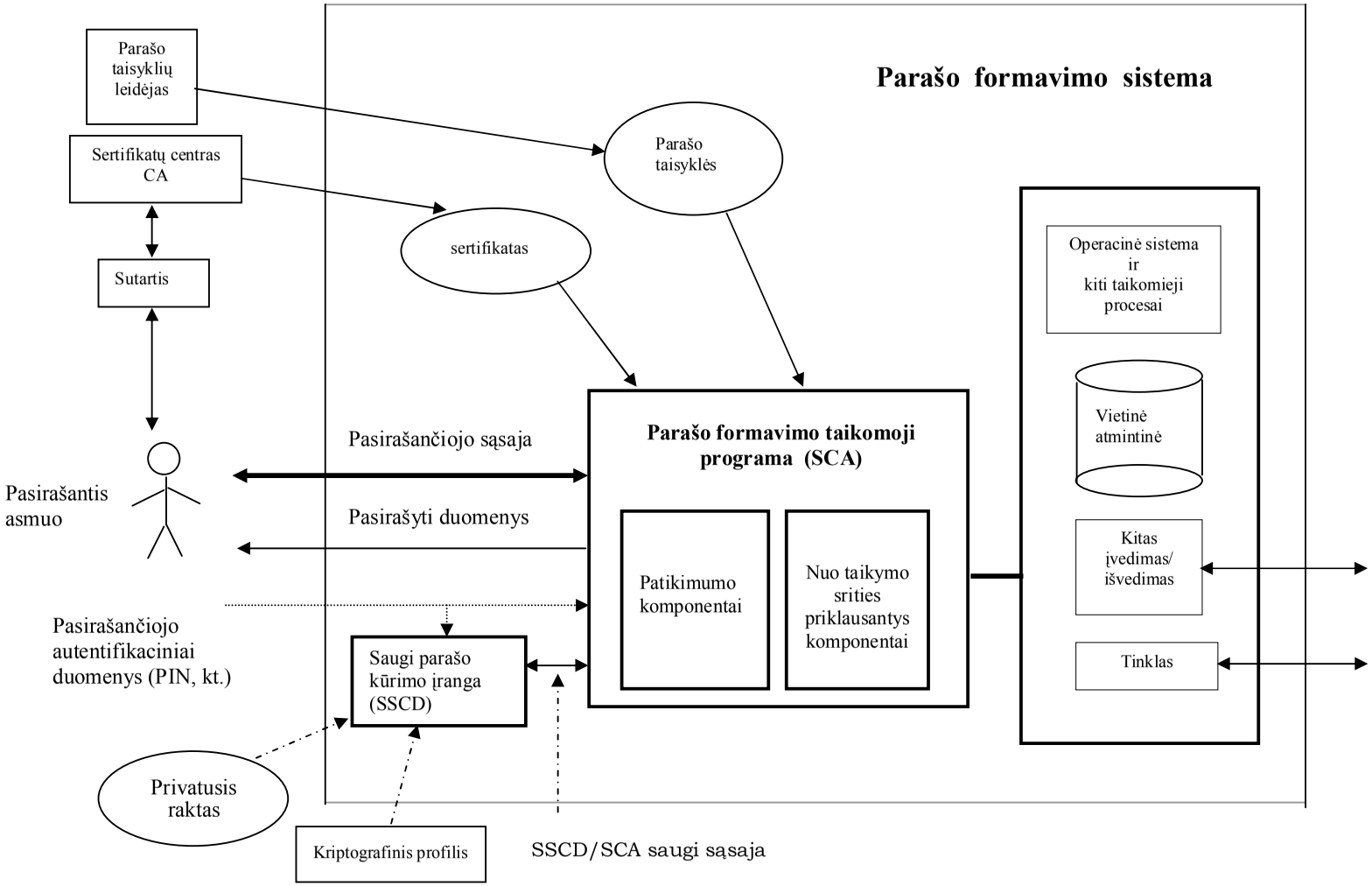
## 9.1. Parašo kūrimo funkcinis modelis

Parašo kūrimo aplinka (PKA) apima pasirašantį asmenį ir parašo formavimo sistemą. Parašo formavimo sistema (toliau – **Sistema**) susideda iš parašo formavimo taikomosios programos (**SCA** - *Signature Creation Aplication*) ir saugios parašo formavimo įrangos (SSCD). 9.1 pav. pavaizduotas parašo kūrimo funkcinis modelis. SCA ir SSCD turi paimti pasirašomą dokumentą ir parašo atributus, iš jų suformuoti pasirašomus duomenis (t. y. jų santrauką), sukurti parašą ir gauti pasirašytą dokumentą.

Pagrindines funkcijas atliekantys SCA komponentai yra skirstomi į dvi grupes: patikimumo komponentus ir nuo taikomosios srities priklausančius komponentus. Be parašo kūrimo funkcijų dar atliekamos ir kitos, kurios turi įtakos saugumui. Išvardinkime jas:

- operacinės sistemos funkcijos. Pastaroji sistema pasirašymo metu padeda palaikyti ryšį tarp pasirašančio asmens ir SCA, iš SCA perduoti pasirašančio asmens informaciją į SSCD, gauti parašo taisyklių informaciją ir sertifikatų duomenis, valdyti vietinę atmintį;
- SSCD sąsajos funkcijos. SSCD yra išorinis įrenginys SCA atžvilgiu. Jis turi sąveikauti su SCA priimdamas pasirašančio asmens autentifikavimo duomenis ir pasirašomus duomenis bei grąžindamas sukurtą parašą;
- SCA vietinė atmintis gali būti naudojama laikinam duomenų įsiminimui pasirašymo procese. Tai taip pat gali turėti įtakos saugumui.

SCA gali turėti ir kitų funkcijų, kurios nėra susijusios su parašo kūrimu. Pavyzdžiui, duomenų įvedimas/išvedimas, ryšys su kompiuterių tinklu, kas taip pat gali turėti įtakos saugumui.




9.1 pav. Parašo kūrimo funkcinis modelis [12]

Parašo kūrimo metu (aplinkoje) susiduriama su tokia informacija:

- kriptografiniu profiliu (parametrais, charakteristikomis, kt.);
- sutartimi tarp pasirašančio asmens ir CA, sudariusio jam sertifikatą;
- parašo atributais;
- privačiuoju raktu;
- sukurtu parašu;
- pasirašančio asmens autentifikavimo duomenimis (PIN, kt.);
- pasirašančio asmens sertifikatais;
- SSCD informacija (pvz., kriptografinė informacija, SSCD savininko vardas);
- pasirašytais duomenimis;
- pasirašančio asmens dokumentais.

SCA darbas valdomas naudojant tokias sąsajas ir sąveikas:

- pasirašomam dokumentui pasirinkti ar įvesti;
- parašo atributams pasirinkti ar įvesti, įskaitant sertifikatą, atitinkantį kuriamą parašą;
- norimam pasirašytų duomenų tipui pasirinkti, nurodyti jų reikiamą formatą ir turinį;
- pasirašančio asmens autentifikavimo duomenims įvesti ir perduoti SSCD, jei į šį procesą įtraukiama SCA;
- pasirašomiems duomenims ir parašo atributams peržiūrėti (stebėti) prieš pasirašant;
- sąsaja su paslaugų teikėjais (CA, kt.) sertifikatams, CRL sąrašams ir parašo taisyklėms gauti;
- pasirašymo procesui sąmoningai pradėti;
- patikimam SCA ir SSCD ryšiui;
- parašui išvesti.

Yra vidinės ir viešosios parašo kūrimo aplinkos (PKA), kurios turi skirtingus saugumo reikalavimus. Vidinės PKA pavyzdys galėtų būti įmonė, kuri naudoja parašą vidaus poreikiams, o viešosios PKA pavyzdys - bankas.

## 9.2. Parašo kūrimo informacinis modelis

Duomenys, iš kurių formuojamas parašas, apima pasirašomą dokumentą ir pasirinktus parašo atributus. Dažniausiai visų pirma sukuriama pasirašomo dokumento santrauka ir toliau naudojama ji. Pasirašomo dokumento formatas (.doc, .pdf, kt.) yra nurodomas duomenų formato atribute, kuris yra vienas iš parašo atributų. Prisiminkime, kad parašo atributai yra tam tikri duomenys, pvz., pasirašančio asmens

sertifikato, parašo taisyklių nuorodos, kt., kurie įtraukiami į parašą kartu su pasirašomo dokumento santrauka [2].

Iš pasirašomo dokumento ir parašo atributų suformuojami reikalingo formato duomenys. Šie duomenys pasirašomi ir vėliau naudojami tikrinant parašą.

Pasirašytą dokumentą sudaro pats dokumentas, suformatuoti asmens pasirašomi duomenys (ES formato parašas, žiūr. skyrių ELEKTRONINIO PARAŠO FORMATAI) ir kita pagalbinė informacija – asmens nepasirašomi atributai (pvz., laiko žyma, CRL nuorodos, kt.). Parašo kūrimo informacinis modelis parodytas 9.2 pav.

## 9.3. Parašo formavimo taikomosios programos (SCA) sudėtis

9.3 pav. pavaizduota SCA sudėtis. SCA yra sudaryta iš patikimumo komponentų ir nuo taikymo srities priklausančių komponentų. Trumpai apžvelkime kiekvieną iš šių komponentų.

### 9.3.1. Patikimumo komponentai

***Pasirašomo dokumento teikimo komponentas***

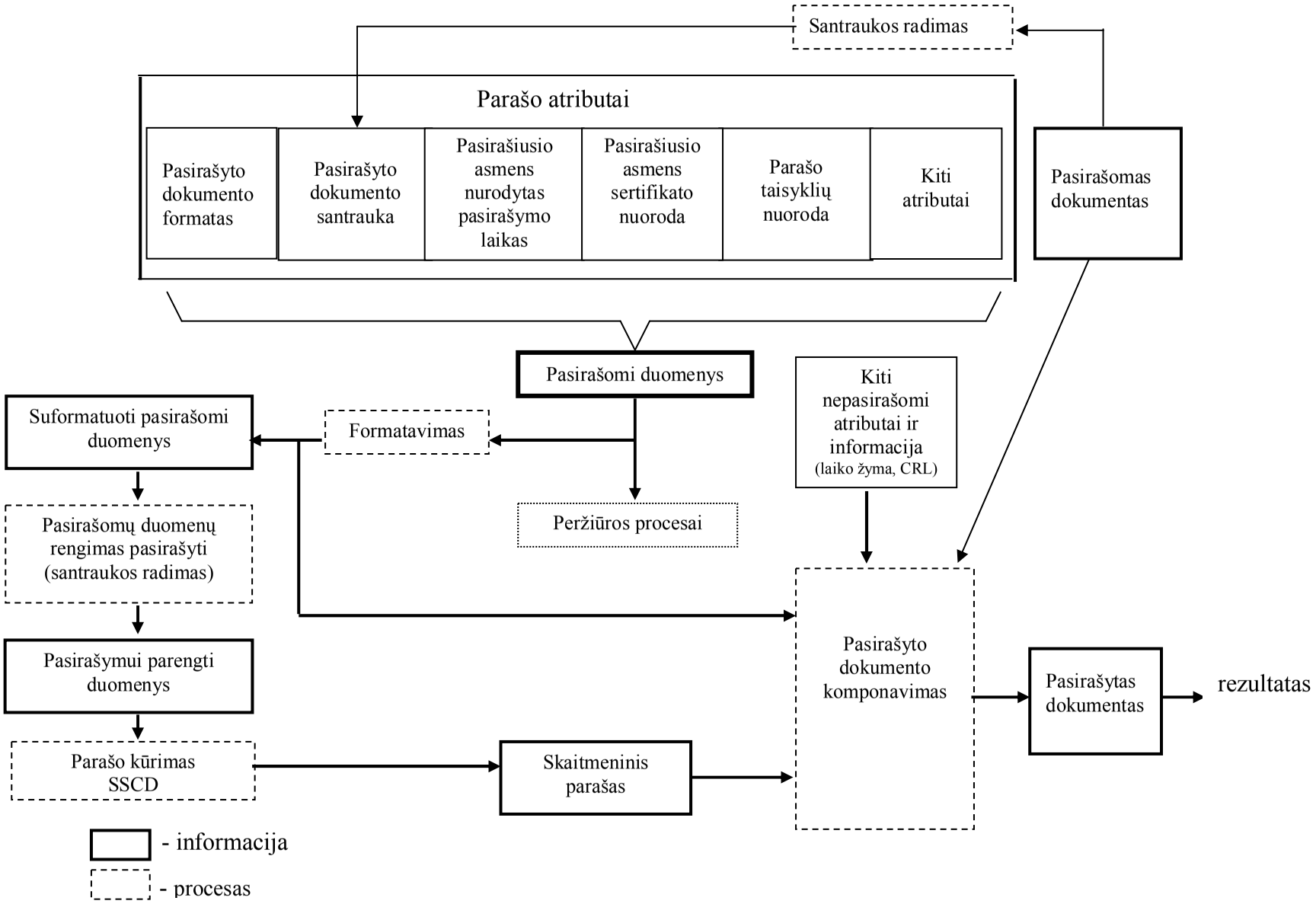
Šis komponentas padeda pasirašančiam asmeniui paimti norimą dokumentą taip, kad jis nebūtų sugadintas ar pakeistas. Kiekvienas pasirašomas dokumentas turi apibrėžtą formatą (.doc, .pdf, kt.). Pasirašyto dokumento tikrintojui taip pat turi būti žinomas dokumento formatas. Dokumento (duomenų) formatas gali būti aiškiai nurodytas pačiame paraše arba nustatomas netiesiogiai, pasinaudojus parašo taisyklėmis, bendraujančių šalių sutartimis, kt. Pasirašomo dokumento teikimo komponentas turi perspėti, jei norima pasirašyti nenumatyto formato dokumentą.

***Parašo atributų teikimo komponentas***

Šio komponento paskirtis yra užtikrinti, kad į parašą būtų įtraukti reikiami informacijos elementai (parašo atributai). Pasirašantis asmuo gali turėti galimybę keisti tam tikrų parašo atributų turinį. Pavyzdžiui, galimybė pasirinkti reikiamą sertifikatą yra būtina, nes pasirašantis asmuo gali turėti kelis sertifikatus, kurių naudojimas priklauso nuo veiklos srities.

***Pasirašomų duomenų formatavimo komponentas***

Šis komponentas paima pasirašomą dokumentą (dažniausiai jo santrauką), parašo atributus ir suformuoja pasirašymui reikalingo formato duomenis. Šiam komponentui yra keliamas vienintelis saugumo reikalavimas: SCA turi parengti tokius pasirašomus duomenis, kokie yra numatyti pasirašančio asmens pasirinktose parašo taisyklėse.




9.2 pav. Parašo kūrimo informacinis modelis [12]

***Sąveikos su pasirašančiu asmeniu komponentas***

Per šį komponentą Sistema palaiko tiesioginį ryšį su pasirašančiu asmeniu. Šiam komponentui keliami aukšti reikalavimai. Prieš kurdama parašą, Sistema turi gauti iš pasirašančio asmens tam tikrą prašymą, kad jis nori kurti parašą. Tik gavusi prašymą sistema turi pradėti tam tikrus veiksmus. Sistema neturi turėti galimybių sukurti parašą atsitiktinai, asmeniui to nesuvokiant. Sistema turi nutraukti pasirašymo procesą, jei, pateikus asmens autentifikacijos duomenis, parašo kūrimas užtrunka pernelyg ilgai. Šis reikalavimas yra keliamas todėl, kad pašaliniai asmenys neperimtų autentifikacijos duomenų ir nespėtų sukurti fiktyvių parašų. Jei pasirašantis asmuo naudoja viešąją SCA, tai tokia SCA turi užtikrinti informacijos apie pasirašantį asmenį gavimą. SCA kūrėjai turi atkreipti dėmesį į tokius sąsajos su vartotoju aspektus, kaip parašo kūrimo nuoseklumas, sąsajos spalvos, atsakomoji reakcija, saugumo pažeidimų aptikimas, neteisingas pasirinkimas, žmogaus ir Sistemos neigiamo dialogo išvengimas, pasirašančio asmens tapatybės nustatymas, sertifikatų nurodymas, laikas, kt.

***Pasirašančio asmens autentifikavimo komponentas***

Šis komponentas yra atsakingas už pasirašančio asmens autentifikavimą. Parašas yra susietas su pasirašančiu asmeniu. Saugi parašo formavimo įranga (SSCD) nustato, ar norintis kurti parašą asmuo turi teisę naudoti tą SSCD. Tai atliekama paprašius slaptažodžio ar PIN kodo arba biometrinėmis priemonėmis (pirštų atspaudais, akies rainele, kt.). Saugi parašo formavimo sistema turi patikrinti asmens autentifikacinius duomenis, nustatyti, ar jie yra teisingi, taip pat turi sudaryti galimybę pasirinkti autentifikacijos būdą.

***Duomenų santraukos (hash) komponentas***

Šis komponentas ima surinktus pasirašymui duomenis ir parengia juos pasirašymui (suformuoja jų santrauką). Šiam komponentui yra taikomi trys saugumo reikalavimai:

- ♦ turi būti naudojamas patikimas santraukos algoritmas;
- ♦ parašui formuoti parengti duomenys turi atitikti leistiną formatą;
- ♦ turi būti korektiškai formuojami ir rodomi pasirašomi duomenys.

***SSCD/SCA sąveikos komponentas***

Šis komponentas yra atsakingas už sąveiką tarp SCA ir SSCD. Saugumo prasme tai labai svarbus komponentas, nes kiekvienas sutrikimas gali baigtis tuo, kad bus sukurtas blogas parašas. SCA turi turėti tam tikrą

fizinę sąsają su SSCD. Ši sąsaja gali būti nuolatinė arba dinamiškai sukuriama. Tiek vienu, tiek kitu atveju yra tam tikri saugumo reikalavimai. Kalbant apie šį komponentą, būtina atkreipti dėmesį į informacijos iš SSCD gavimą, SSCD funkcijų pasirinkimą daugelio programų sistemų atveju (*mutli-application platform*), parašo kūrimui reikalingų duomenų pasirinkimą, pasirašančio asmens patikrinimą, parašo formavimą ir parašo įsiminimą (*logging*). Šiam komponentui keliamais saugumo reikalavimais siekiama panaikinti šias grėsmes:

- klaidingą parašo sukūrimą dėl fizinės sąsajos sutrikimų;
- tarpinį, nepageidaujamą poveikį bevielio ryšio atveju;
- klaidingą privačiojo rakto pasirinkimą;
- klaidingą parašo sukūrimą dėl šio komponento gedimo.

***SSCD/SCA autentifikavimo komponentas***

Šis komponentas naudojamas tik tam tikrose parašų kūrimo sistemose saugiam ryšiui tarp SSCD ir SCA sukurti (dažniausiai viešojo naudojimo SCA). Naudojamas tuomet, kai reikalaujamas pasitikėjimo sąveika SSCD/SCA lygis negali būti pasiektas tam tikromis organizacinėmis priemonėmis.

### 9.3.2. Nuo taikymo srities priklausomi komponentai

Nuo taikymo srities priklausomų komponentų tarpe svarbesni yra:

1) ***pasirašomo dokumento kūrimo priemonė*** (tekstų rengyklė, pvz., *MS Word*, kt.);

2) ***pasirašyto dokumento komponavimo komponentas***. Šis komponentas iš pasirašomo dokumento ir asmens pasirašomų parašo atributų (pvz., pasirašančiojo sertifikato nuorodos), jų skaitmeninio parašo, asmens nepasirašomų atributų ir informacijos (pvz., laiko žymos, CRL) suformuoja pasirašytą dokumentą;

3) ***parašų įsiminimo (logging) komponentas***. Dažnai būna naudinga išsaugoti bent paskutinius 20 sukurtų parašų. Jų kiekį apriboja SSCD atminties talpa. Pavyzdžiui, gali būti įsimenama tokia informacija: sukurtų parašų kiekis, parašo sukūrimo data ir laikas, duomenų santrauka, parašas, pasirašyto dokumento identifikatorius, SCA arba SSCD identifikatorius, pasirašiusio asmens sertifikato identifikatorius, parašo taisyklių nuoroda;

4) ***sąveikos su sertifikavimo paslaugų teikėju komponentas*** informacijai apie sertifikatus, laiko žymoms, CRL gauti;

5) ***SSCD savininko indikatorius***, kuriame rodomas SSCD savininko vardas.

### 9.3.3. Sąsaja duomenims įvesti/išvesti

Duomenų įvedimo/išvedimo procesuose yra tam tikra rizika, kad duomenis gali perimti ir pakeisti tretieji asmenys. Tai sertifikatų gavimo (importavimo), pasirašomų dokumentų bei parašo atributų gavimo, SCA komponentų atsisiuntimo, pasirašytų duomenų išsiuntimo (eksportavimo) procesai. Todėl SCA ryšiui su išore keliamais saugumo reikalavimais siekiama sumažinti šių grėsmių tikimybę:

- ♦ SCA komponentų sugadinimo virusais;
- ♦ komponentų sugadinimo dėl įsibrovėlių.

### 9.3.4. SCA aplinka ir sąsajos su SSCD

SCA gali būti įdiegta tokiose aplinkose:

- ♦ asmeniniame kompiuteryje;
- ♦ nešiojamame kompiuteryje (*laptop*);
- ♦ mobiliajame telefone;
- ♦ asmeniniame skaitmeniniame asistente.

SSCD funkcijos yra saugoti privatųjį raktą, tikrinti pasirašančio asmens autentifikacinius duomenis ir kurti el. parašą (žiūr. 9.6 skyrių). SSCD gali būti realizuotas kaip:

- ♦ intelektualioji (mikroprocesorinė) kortelė;
- ♦ įrenginys su USB jungtimi (strypelis - *stick, token*);
- ♦ įrenginys su PCMCIA;
- ♦ saugos dėžė (*security box*).

## 9.4. Bendrieji SCA saugumo reikalavimai

Visi objektų identifikatoriai turi vienareikšmiškai nurodyti objektus.

Įrangos atitiktis nustatytiems reikalavimams turi būti grindžiama tiekėjo deklaracijomis.

***Pagrindiniai patikimų kanalų reikalavimai***:

a) SCA turi užtikrinti pasirašomų duomenų ir pagalbinės informacijos (pvz., pasirašančiojo sertifikato nuorodos), jų santraukos (*hash*) bei visos kitos pasirašančio asmens pateikiamos informacijos perdavimo tarp SCA ir SSCD vientisumą;

b) SCA turi išlaikyti pasirašomų duomenų ir pasirašančio asmens autentifikacinių duomenų konfidencialumą.

***Reikalavimai viešosioms parašo kūrimo sistemoms***:

a) SCA turi patikimai sunaikinti visą darbinę informaciją, susijusią su parašo kūrimu, iškart po parašo suformavimo;

b) aplinkos stebėjimo kameros (*Closed Circuit Televisions*) negali būti išdėstytos taip, kad galėtų užfiksuoti pasirašančiojo asmens autentifikacinius duomenis. SCA turi būti tokiose vietose, kad niekas tų duomenų negalėtų nei pamatyti nei nufilmuoti.

***Reikalavimai dokumento ir pasirašomų duomenų (parašo atributų) apdorojimui***: SCA turi užtikrinti, kad tik vartotojo pasirinkti pasirašomi duomenys būtų pateikti tolesniam procesui.

***Reikalavimai paskirstytoms (išsklaidytoms) parašo kūrimo sistemoms***: Bet kokie pasirašančio asmens autentifikaciniai duomenys ir pasirašomi duomenys, kurie cirkuliuoja tarp išsklaidytos SCA komponentų, turi būti perduodami saugiais kanalais, užtikrinančiais duomenų vientisumą ir konfidencialumą.

***Reikalavimai dėl pašalinių procesų ir nebūtinų ryšio kanalų naudojimo:*** sistemos ir programinės įrangos elementus, išorinius įrengimus ir duomenų perdavimo kanalus, kurie nėra būtini SCA veikimui, draudžiama naudoti pasirašymo procese.

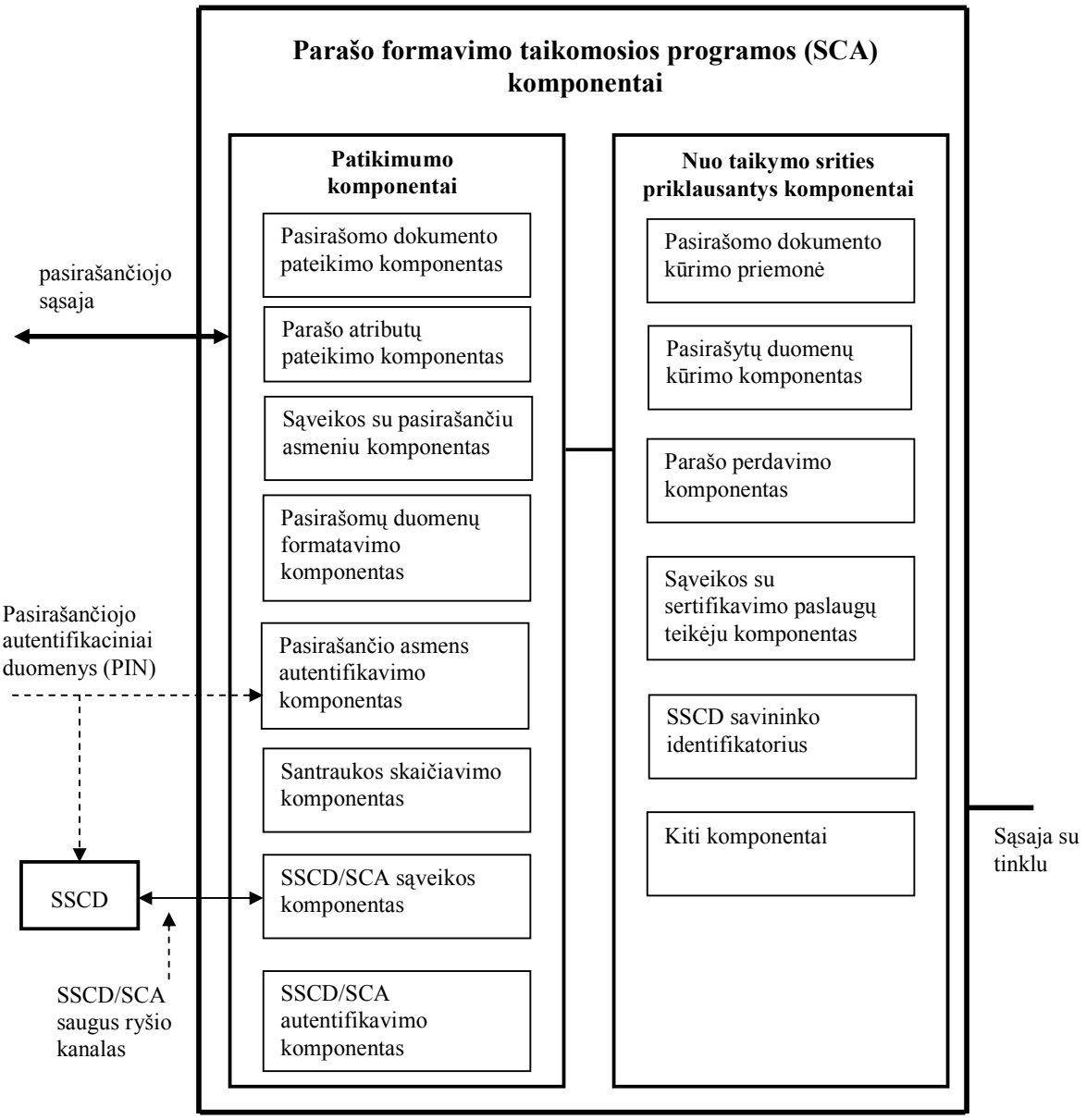
***Pasirašytų duomenų tikrinimas po pasirašymo***: pasirašantis asmuo turi turėti galimybę patikrinti, ar jo sukurtas parašas iš tikro atitinka pasirinktus duomenis ir parašo atributus.

***Reikalavimai pasirašomiems duomenims (parašo atributams):***

a) pasirašomuose duomenyse turi būti informacija apie patį pasirašomą dokumentą (jei ne visas dokumentas, tai jo santrauka), apie pasirašančio asmens sertifikatą, parašo taisykles, parašo paskirties tipą (jei parašo taisyklės leidžia asmenims iš kelių galimų parašo paskirties tipų pasirinkti vieną);

b) jei programinė įranga ar parašo taisyklės leidžia naudoti kelis dokumentų formatus, tai pasirašomuose duomenyse turi būti informacija ir apie pasirašomo dokumento formatą.

Kiti parašo atributai gali būti įtraukti į pasirašomus duomenis priklausomai nuo taikomosios srities.




9.3 pav. Parašo formavimo taikomosios programos (SCA) sudėtis [12]

## 9.5. Saugumo reikalavimai SCA komponentams

### 9.5.1. Patikimumo komponentai

***Pasirašomo dokumento pateikimo komponentas (PDPK)***

Reikalavimai PDPK:

1) PDPK turi leisti naudoti parašo taisyklėse nurodyto formato dokumentus arba leisti dokumento formatą (EDI, HTML, XML, failo tipą, kt.) nurodyti atitinkamame parašo atribute;

2) jei nurodomas neleistinas dokumento formatas, PDPK apie tai turi įspėti vartotoją;

3) PDPK gamintojai turi nurodyti, kokie dokumentų formatai yra palaikomi ir kokios galimos pasekmės, jei naudojami kitokio formato dokumentai. PDPK turi perspėti vartotoją apie formato neatitikimą prieš kuriant parašą;

4) turi atvaizduoti vartotojui tokį dokumentą, kokį jis ketina pasirašyti, ir kad būtent toks dokumentas bus pasirašytas;

5) PDPK turi informuoti vartotoją apie tai, kad pasirašomame dokumente yra dalys, kurias yra pasirašę kiti asmenys;

6) PDPK neturi keisti pasirašomo dokumento;

7) PDPK turi perspėti vartotoją, jei negali pateikti visų dokumento dalių pagal parašo atribute nurodytą dokumento formatą;

8) PDPK turi įspėti vartotoją apie paslėptojo teksto, makrosų (makro komandų) ar aktyviojo kodo buvimą pasirašomame dokumente.

***Parašo atributų pateikimo komponentas (PAPK)***

PAPK reikalavimai:

1) vartotojas turi turėti galimybę peržiūrėti parašo atributus ir turi būti užtikrinama, kad pateikiami būtent tie atributai, kuriuos jis pasirinko ir kurie bus naudojami pasirašymo metu;

2) turi būti užtikrintas parašo atributų vientisumas ir autentiškumas;

3) vartotojas turi būti įspėjamas apie paslėptojo teksto, makrosų ar aktyviojo kodo buvimą parašo atributuose.

4) PAPK turi leisti vartotojui peržiūrėti daugumą komponentų pasirinkto sertifikato, kuris įtraukiamas į parašo atributų rinkinį (pasirašomus duomenis).

***Sąveikos su pasirašančiuoju asmeniu komponentas (SSPK)***

Šiam komponento reikalavimai:

1) prieš pasirašymo proceso inicijavimą SSPK turi paprašyti vartotojo įvesti neįprastą kreipimąsi dėl parašo kūrimo. Šis kreipimasis turi būti toks, kad nebūtų pasirašoma atsitiktinai.

2) SSPK‘e turi būti nustatytas laikas, per kurį reikia suspėti sukurti parašą. Jei šis laikas išsenka, parašo kūrimo procesas turi būti nutrauktas ir vartotojas iš naujo turi pateikti autentifikacinius duomenis.

Kuriant šį komponentą reikia atsižvelgti ir į keletą sąsajos su vartotoju aspektų: spalvų parinkimą, grįžtamąjį ryšį, aplinką (viešoji ar uždaroji), saugumą, kalbą, pranešimų apie klaidas informatyvumą, veiksmo pakartojimo galimybę, t.t.

***Pasirašančio asmens autentifikacijos komponentas (PAAK)***

Pasirašančiam asmeniui autentifikuoti yra galimi du būdai. Vienas iš jų paremtas žinojimu (žinau slaptažodį, PIN), kitas turėjimu – biometriniais duomenimis (pirštų atspaudais, akies rainele, kt.). Galimos šių būdų kombinacijos. Biometrinis autentifikavimo būdas yra sunkiau įgyvendinamas.

Saugumo reikalavimai autentifikavimui, paremtam žinojimu (slaptažodžiu, PIN):

1) SCA turi turėti priemones, įgalinančias pasirašantį asmenį pateikti savo autentifikacinius duomenis SSCD;

2) SCA turi garantuoti pasirašančiojo asmens autentifikacinių duomenų konfidencialumą ir panaikinti juos tuoj pat, kai jie nebereikalingi;

3) jei pasirašantis asmuo netyčia pateikia blogus autentifikacinius duomenis neviršydamas leistino kartų skaičių, jam turi būti pranešama apie klaidą ir leidžiama bandyti tuos duomenis vesti iš naujo, jei tik SSCD tų duomenų įvedimo neužblokavo;

4) pasirašančiam asmeniui tam tikrą skaičių kartų klaidingai pateikus autentifikacinius duomenis, SSCD turi liautis tai leidusi, apie tai perspėdama SCA, kuri savo ruožtu informuoja vartotoją;

5) saugus kanalas autentifikaciniams duomenis perduoti į SSCD turi eiti per SCA;

6) jei SCA ir SSCD leidžia, vartotojui turi būti suteikta galimybė keisti savo autentifikacinius duomenis. Nauji autentifikaciniai duomenys turi būti įvedami du kartus ir tikrinamas jų sutapimas;

7) įvedami asmens autentifikaciniai duomenys neturi būti matomi, tačiau vartotojas turi matyti tam tikrą informaciją, kai SCA įveda simbolį;

8) vartotojui norint pakeisti savo autentifikacinius duomenis, naujieji duomenys turi būti įvedami du kartus ir tikrinamas jų sutapimas.

Saugumo reikalavimai, susiję su biometriniais autentifikavimo duomenimis:

1) turi būti patikimas kanalas tarp biometrinio sensoriaus ir SSCD;

2) turi būti naudojama kriptografija biometrinių duomenų autentiškumui užtikrinti ir kad jie nebūtų panaudoti neleistinai (jei šie duomenys naudotini viešosiose vietose).

***Pasirašomų duomenų formatavimo komponentas (PDFK)***

Vienintelis reikalavimas šiam komponentui yra tas, kad jis turi suformatuoti pasirašomus duomenis (parašo atributus) kaip to reikalauja pasirašančio asmens pasirinktos parašo taisyklės.

***Duomenų santraukos (hash) komponentas (DSK)***

Šiam komponentui keliami tokie reikalavimai:

1) turi būti naudojami tik standartuose [31] leistini santraukos algoritmai;

2) pasirašymui parengti ir perduodami į SSCD duomenys (pasirašomų duomenų santrauka) turi atitikti nustatytą formatą;

3) SCA turi užtikrinti, kad pasirašymui parengti duomenys (*hash*) bus gauti iš duomenų rinkinio (parašo atributų), kurio reikalauja standartai.

***SSCD/SCA sąveikos komponentas***

Šiam komponentui keliami saugumo reikalavimai yra šie:

1) komponentas turi turėti visus fizinės sąsajos elementus bei jų savybes, kad užtikrintų tinkamą įvairių SSCD tipų veikimą;

2) jei tarp SCA ir SSCD naudojamas bevielis ryšys, SCA turi būti atitinkamos priemonės slaptam pasiklausymui ir pašaliniam įsikišimui išvengti;

3) komponentas turi užtikrinti, kad būti parinktos tinkamos SSCD funkcijos, jei naudojama SSCD ir SCA tai leidžia daryti (pvz., SSCD gali turėti kelis privačiuosius raktus).

4) komponentas turi būti apsaugotas nuo bet kokių neleistinų pakeitimų.

***SSCD/SCA autentifikavimo komponentas***

Vienintelis reikalavimas šiam komponentui yra tas, kad turi būti tikrinamas tarp SCA ir SSCD perduodamos informacijos autentiškumas, kad būtų užtikrintas saugus informacijos perdavimas. Tuo siekiama išvengti suklastotos SCA panaudojimo.

### 9.5.2. Nuo taikymo srities priklausomi komponentai

Nuo taikymo srities priklausomiems komponentams konkrečių reikalavimų, sietinų su parašo kūrimu, nėra. Priminsime, kad svarbesni iš šių komponentų yra:

- pasirašomo dokumento kūrimo priemonė (tekstų rengyklė, kt.);
- pasirašyto dokumento komponavimo komponentas;
- parašų įsiminimo (logging) komponentas;
- sąveikos su sertifikavimo paslaugų teikėju komponentas;
- SSCD savininko indikatorius.

## 9.6. Saugi parašo formavimo įranga (SSCD)

Šiandieną plintanti el. parašo technologija yra paremta asimetrinio šifravimo metodu - viešaisiais ir privačiaisiais šifravimo raktais. Privatieji

raktai dar vadinami el. parašo formavimo duomenimis (**SCDat** - *Signature Creation Data*), o viešieji raktai - parašo tikrinimo duomenimis (**SVD** - *Signature Verification Data*). El. parašo saugumui didelę įtaką turi saugus šifravimo raktų poros generavimas, privačiojo rakto perdavimas asmeniui, šio rakto laikymas ir naudojimas kuriant el. parašus. Visuose šiuose etapuose turi būti naudojama saugi parašo formavimo įranga (SSCD), užtikrinanti privačiojo rakto slaptumą.

El. parašų kūrimo metu SSCD įranga savo funkcijas atlieka tik tarpininkaujant taikomąjai el. parašo formavimo taikomajai programai (SCA), apie kurią rašyta aukščiau.

Skiriami trys SSCD įrangos tipai:

1) SSCD-1. Tai įranga, kurios paskirtis generuoti šifravimo raktų poras SCDat/SVD. Ji el. parašams kurti nenaudojama. Sugeneruoti raktai saugiai perkeliami į SSCD-2 tipo įrangą ir tik tuomet naudojami el. parašams kurti;

2) SSCD-2. Tai el. parašo kūrimo įranga, į kurią privatusis raktas SCDat įrašomas iš SSCD-1 tipo įrangos;

3) SSCD-3. Tai įranga, kurios viduje sugeneruojama šifravimo raktų pora SCDat/SVD ir kuri vėliau naudojama el. parašams kurti. Privatusis raktas SCDat iš šio tipo įrangos į išorę niekada neperduodamas.

9.4 pav. parodyta dviejų tipų SSCD įranga. SSCD-1 tipo įranga skirta generuoti šifravimo raktų SCDat/SVD porai. Privatusis raktas SCDat saugiu kanalu perduodamas ir įrašomas į SSCD-2 tipo įrangą.

SSCD-2 yra personalizuota įranga, skirta tik vienam vartotojui (pvz., tai gali būti intelektualioji kortelė). Vartotojas, norėdamas kurti el. parašą SSCD-2 įranga, turi įvesti savo autentifikacinius duomenis (pvz., PIN kodą). Jei SSCD-2 neturi betarpiškos sąsajos su vartotoju, tai turi būti saugus ryšio kanalas tarp SSCD-2 ir parašo formavimo taikomosios programos (SCA), per kurią vartotojas palaiko ryšį su SSCD-2.

SSCD-1 įranga nėra personalizuota. Tačiau su ja dirbti, t. y. generuoti SCDat/SVD raktus ir eksportuoti juos, gali tik įgalioti asmenys (pvz., sistemos administratorius).

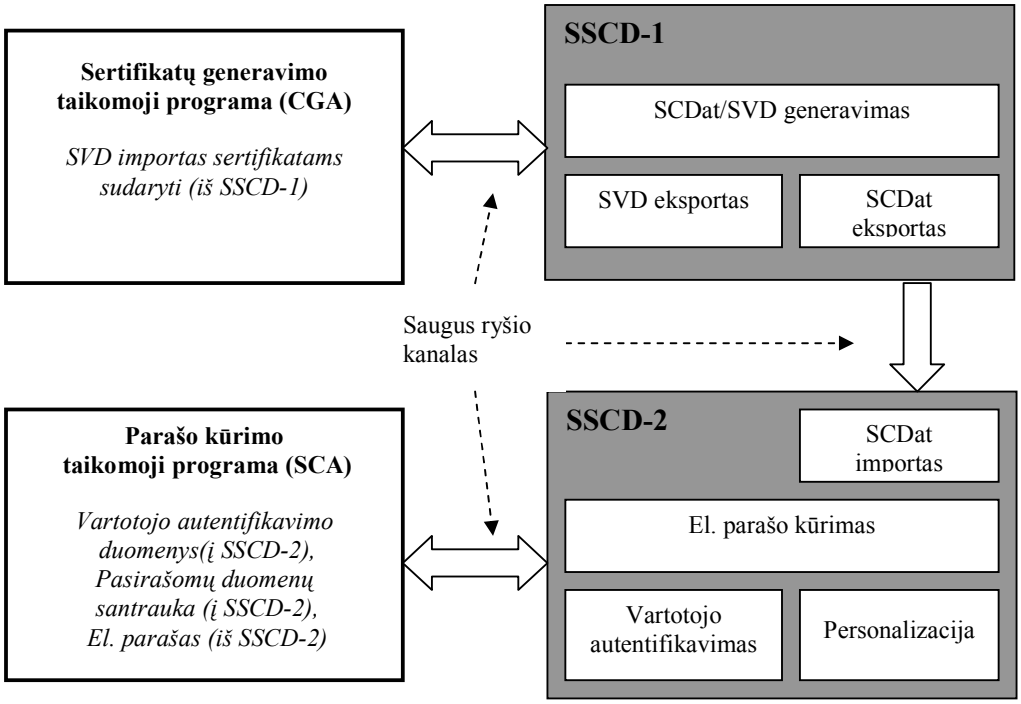
9.5 pav. pavaizduota SSCD-3 tipo įranga. Pastarosios funkcijos yra analogiškos abiejų SSCD-1 ir SSCD-2 funkcijoms kartu paėmus. Viso to privalumas, kad privatusis raktas SCDat nėra eksportuojamas, ir taip užtikrinamas aukštesnis jo saugumas.

Viešasis raktas SVD tiek SSCD-1, tiek SSCD-3 įrangos atveju turi būti eksportuojamas saugiu kanalu, nes jis reikalingas sudarant sertifikatus.

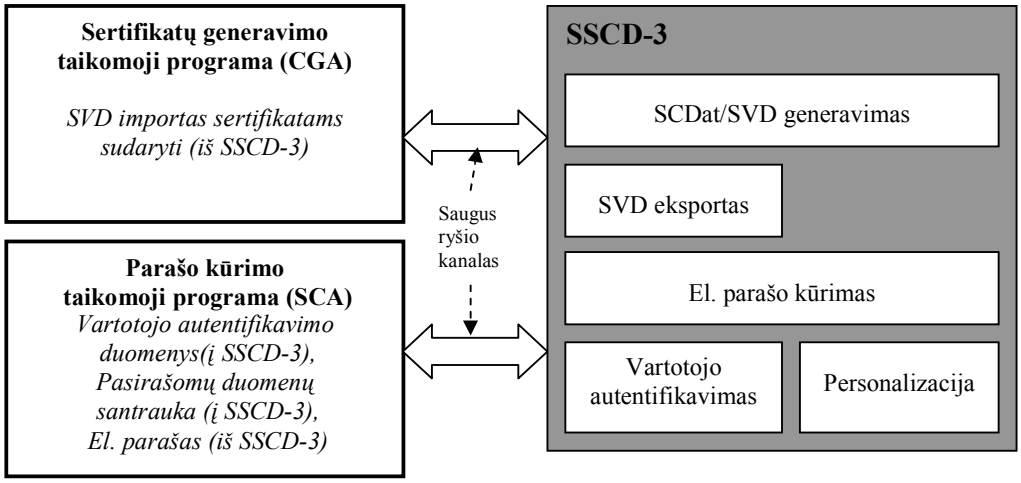
SSCD apima atitinkamą techninę įrangą, savąją operacinę sistemą, SCDat/SVD raktų generavimą, privačiojo rakto SCDat saugojimą, parašo kūrimo funkciją. Parašo formavimo taikomoji programa (SCA) ir sertifikatų

generavimo (sudarymo) taikomoji programa (CGA – *Certificate Generation Application*) yra aplinka, su kuria SSCD betarpiškai kontaktuoja. Tarp jų turi būti saugus ryšio kanalas. Taip pat saugus ryšio kanalas turi būti tarp žmogaus ir SCA autentifikavimo duomenims įvesti.

SSCD saugumo reikalavimai (PP - *Protection Profile*) yra smulkiai išdėstyti CWA 14169 standarte [11].




9.4 pav. SSCD-1 ir SSCD-2 tipų įrangos funkcijos




9.5 pav. SSCD-3 tipo įrangos funkcijos

# 10. LAIKO ŽYMA

Laiko žyma yra įrodymas, kad el. parašas arba kitokie el. duomenys buvo sukurti (arba, pvz., išsiųsti el. paštu) iki žymoje nurodyto laiko. El. parašams jos yra ypač svarbios, nes su parašais susiję sertifikatai turi ribotą galiojimo terminą. Parašas yra negaliojantis, jei jis buvo sukurtas pasibaigus sertifikato galiojimui. Parašams naudojant laiko žymas, suformuotas pasirašiusio asmens sertifikato galiojimo laikotarpiu, užtikrinamas ilgalaikis el. parašų galiojimas. Kitokių el. duomenų atveju laiko žyma gali pasitarnauti, pavyzdžiui, kaip autorinių teisių arba duomenų išsiuntimo iki nurodyto laiko įrodymas. El. komercijoje, finansiniuose atsiskaitymuose to gali labai prireikti.

Laiko žymas kuria patikimi tretieji asmenys - laiko žymos tarnybos (TSA - *Time Stamping Authorities*).

Šiame skyriuje supažindinama su laiko žymos kūrimo klausimais, reikalavimais TSA [3, 6, 29].

## 10.1. Laiko žymos samprata

El. duomenų laiko žyma yra įrodymas, kad duomenys buvo sukurti iki žymoje nurodyto laiko. Jos yra svarbios el. parašams, nors gali būti naudojamos ir kitais tikslais, pavyzdžiui, kaip el. duomenų autorinių teisių įrodinėjimo priemonė.

El. parašu pasirašantieji asmenys turi turėti CA sudarytus sertifikatus. Sertifikatuose šalia kitų duomenų yra sertifikato galiojimo pradžios ir pabaigos terminai. Tačiau sertifikato galiojimas dėl įvairių priežasčių gali būti nutrauktas anksčiau, nei sertifikate nurodytas pabaigos terminas. Parašas, sukurtas po sertifikato galiojimo nutraukimo, yra negaliojantis. Todėl ateityje, pavyzdžiui, archyve esantiems el. dokumentams, būtina turėti galimybę patikrinti, kad asmenys juos pasirašė atitinkamų sertifikatų galiojimo laikotarpiu.

Kad galėtume įrodyti, jog parašas buvo sukurtas atitinkamo sertifikato galiojimo laikotarpiu, be laiko žymos dar reikalingi ir to sertifikato duomenys. Informacija apie sertifikatus, kurių galiojimo laikas pasibaigęs (nutrauktas), saugoma juos išdavusių CA atšauktų sertifikatų sąrašuose (CRL). Parašui laiko žyma turi būti sukurta pasirašiusio asmens sertifikato galiojimo laikotarpiu.

Laiko žymas kuria patikimi tretieji asmenys - laiko žymų tarnybos (TSA – *Time Stamping Authorities*).

Laiko žymos gavimo procesas yra toks: prašytojas (klientas) siunčia užklausą į TSA laiko žymai gauti, o TSA grąžina prašytojui atsakymą. Užklausoms ir atsakymams formuoti, analizuoti, perduoti prašytojai ir TSA turi būti apsirūpinę atitinkama įranga.

## 10.2. Laiko žymų teikėjų (TSA) veiksmai

Asmuo, norintis savo el. duomenims (pvz., el. parašui) gauti laiko žymą, siunčia užklausą į TSA. Reikalaujama, kad TSA, rengdama atsakymą :

1) naudotų patikimą laiko šaltinį;

2) įtrauktų teisingą laiko reikšmę į kiekvieną laiko žymą;

3) įtrauktų unikalų sveikąjį skaičių (*nonce*) į kiekvieną kuriamą laiko žymą (*nonce* atsiunčia prašytojas. Jo reikia tam, kad galima būtų atskirti užklausas, kai tiems patiems duomenims žymos prašo skirtingi prašytojai);

4) kurtų laiko žymą, gavusi iš prašytojo tik teisingą užklausą;

5) įtrauktų į kiekvieną laiko žymą laiko žymos taisyklių (*policy*), kurių laikantis žyma buvo sukurta, identifikatorių (OID*)*;

6) kurtų laiko žymą tik prašytojo atsiųstai el. duomenų santraukai (*hash*), apskaičiuotai pagal algoritmą, kurio OID nurodytas užklausoje;

7) tikrintų, ar santraukos reikšmės ilgis atitinka užklausoje nurodytą santraukos algoritmą (pvz., SHA-1 algoritmas duoda 160 bitų ilgio santrauką, MD5 – 128 bitų);

8) niekaip nenagrinėtų santraukos reikšmės, kuriai prašoma sukurti laiko žymą (tikrinamas tik santraukos reikšmės ilgis, kaip nurodyta ankstesniame punkte);

9) netrauktų į laiko žymą jokių prašytoją identifikuojančių duomenų;

10) pasirašytų kiekvieną laiko žymą el. parašu, naudodama tik šiam tikslui skirtą privatųjį raktą, ir turėtų šią rakto paskirtį patvirtinantį sertifikatą;

11) įtrauktų papildomą informaciją į laiko žymą, jei to prašoma užklausos išplėtimų (*extensions*) lauke ir TSA palaiko (gali apdoroti) tokius užklausų išplėtimus. Jei tai neįmanoma, TSA privalo nusiųsti prašytojui atsakymą su perspėjimu apie klaidą.

## 10.3. Laiko žymų prašytojų veiksmai

Laiko žymai gauti prašytojas siunčia užklausą TSA. Gavęs užklausą, TSA suformuoja atsakymą prašytojui. Prašytojas, gavęs iš TSA atsakymą, turi patikrinti klaidų lauko turinį, t. y. ar atsakyme nėra perspėjimo apie klaidą. Jei klaidos nėra, prašytojas turi patikrinti įvairius laiko žymos laukus ir TSA el. parašo laiko žymoje galiojimą. Ypač svarbu patikrinti, ar duomenys, kuriems buvo sukurta žyma, atitinka tuos, kuriems buvo

prašoma sukurti žymą. Prašytojas turi patikrinti, ar laiko žymoje yra teisingas TSA sertifikato identifikatorius, ar nepakeista duomenų santraukos reikšmė ir ar teisingas santraukos algoritmo identifikatorius OID. Prašytojas turi patikrinti atsakymo savalaikiškumą, palygindamas atsakyme nurodytą žymos laiką su tikruoju vietos laiku, jei tai įmanoma, ir patikrindamas, ar atsakyme įterptas toks pats unikalus sveikasis skaičius (*nonce*; tai 64 bitų ilgio atsitiktinis skaičius), kuris buvo siųstas užklausoje.

Jeigu bet kurio iš aukščiau išvardintų tikrinimų metu pastebimas neatitikimas, laiko žyma turi būti atmesta.

Kadangi TSA sertifikato galiojimas gali būti nutrauktas (pasibaigęs), turėtų būti tikrinamas ir šio sertifikato statusas, t. y. ar jis dar galioja. Tuo tikslu prašytojui reikėtų kreiptis į CRL sąrašą,, esantį TSA sertifikatą išdavusiame CA.

Po to prašytojo programinė įranga turėtų tikrinti iš TSA gauto atsakymo lauką, kuriame nurodomas laiko žymų taisyklių (*policy*) identifikatorius, kad nustatytų, ar naudotos taisyklės priimtinos prašytojui.

## 10.4. Užklausų ir atsakymų formatai

Kad geriau suprastume laiko žymos mechanizmą, jos kūrimo procesą, detalizuokime prašytojų užklausas ir TSA išduodamus atsakymus.

***Užklausų formatas***

Prašytojo siunčiamos į TSA užklausos laiko žymai gauti (*TimeStampReq*) formatas, naudojant ASN.1 (*Abstract Syntax Notation One*) sintaksę, RFC 3161 standarte [29] yra apibrėžtas taip:

```
TimeStampReq ::= SEQUENCE  {
version                  INTEGER { v1(1) },
messageImprint           MessageImprint,
    -- a hash algorithm OID and the hash value of the data
    -- to be time stamped
reqPolicy                TSAPolicyId              OPTIONAL,
nonce                    INTEGER                  OPTIONAL,
certReq                  BOOLEAN                  DEFAULT FALSE,
extensions               IMPLICIT Extensions      OPTIONAL  }
```

*version* lauke nurodoma užklausos laiko žymai gauti versija (v1).

*messageImprint* lauke (žiūr. žemiau) turi būti duomenų santrauka, kuriems norima sukurti žymą. Santrauka pateikiama kaip baitų seka. Šios sekos ilgis privalo atitikti santraukos reikšmės ilgį, gaunamos atitinkamu algoritmu (20 baitų = 160 bitų SHA-1 algoritmui arba 16 baitų = 128 bitų MD5 algoritmui).

```
MessageImprint ::= SEQUENCE  {
hashAlgorithm       AlgorithmIdentifier,
hashedMessage       OCTET STRING  }
```

*hashAlgorithm* lauke privalo būti panaudoto santraukos algoritmo identifikatorius OID.

*reqPolicy* lauke, jei jis įtrauktas, nurodomas laiko žymos taisyklių (*policy*), kurių laikantis turi būti sukurta laiko žyma, identifikatorius OID.

*nonce* laukas, jei jis įtrauktas, leidžia prašytojui patikrinti, kad atsakymas išduotas tikrai į jo pateiktą užklausą. *nonce* lauke įrašomas didelis atsitiktinis sveikasis skaičius. Labai maža tikimybė, kad prašytojas sugeneruotų tokį patį skaičių (64 bitų ilgio sveikąjį skaičių) antrą kartą. *nonce* reikšmę, gautą užklausoje, TSA privalo įtraukti į atsakymą. Jei ji neįtraukta, iš TSA gautas atsakymas turi būti atmestas.

*certReq* laukas. Jei šis laukas yra ir jame įrašyta reikšmė TRUE, tai pagal tokią užklausą TSA privalo pateikti prašytojui savo viešojo rakto sertifikato nuorodą. Šiame lauke gali būti ir kitų sertifikatų nuorodos. Jei *certReq* laukas užklausoje yra praleistas arba jo reikšmė FALSE, tai atsakyme duomenų apie TSA sertifikatą neturi būti.

*extensions* laukas yra bendrasis būdas pridėti papildomą informaciją užklausose. *extensions* lauko struktūra yra apibrėžta standarte RFC 3280 [24], susijusiame su sertifikatais. Jei TSA laiko žymos serveris nepažįsta (nepriima) kurio nors užklausoje esančio *extension* lauko, tai serveris neturi formuoti laiko žymos ir grąžinti atsakymą su perspėjimu apie klaidą (*unacceptedExtension*).

Užklausose prašytojo tapatybė nenurodoma, nes tokia informacija rengiant TSA atsakymus nereikalinga. Tais atvejais, kai TSA vis tik prašo prašytojo tapatybės duomenų, gali būti naudojamos kitokios identifikavimo/autentifikavimo priemonės ( pvz., RFC 2246 arba RFC 2630 standartais apibrėžtomis priemonėmis).

***TSA atsakymų formatas***

TSA atsakymo (*TimeStampResp*) prašytojams formatas yra:

```
TimeStampResp ::= SEQUENCE  {
status                  PKIStatusInfo,
timeStampToken          TimeStampToken      OPTIONAL  }
```

*status* lauke savo ruožtu yra laukas *PKIStatusInfo:*

```
PKIStatusInfo ::= SEQUENCE {
status                  PKIStatus,
statusString            PKIFreeText     OPTIONAL,
failInfo                PKIFailureInfo  OPTIONAL  }
```

Kai *PKIStatusInfo* lauke *status* turi reikšmę 0 arba 1, TSA atsakyme turi būti laiko žyma. Kai *status* reikšmė yra kitokia, laiko žymos neturi būti. Vieną iš žemiau nurodytų reikšmių *status* privalo turėti:

```
PKIStatus ::= INTEGER  {
    granted                 (0),
        -- when the PKIStatus contains the value zero
        -- a Time Stamp Token, as requested, is present.
    grantedWithMods         (1),
        -- when the PKIStatus contains the value one
        -- a Time Stamp Token, with modifications, is present.
    rejection               (2),
    waiting                 (3),
    revocationWarning       (4),
        -- this message contains a warning
        -- that a revocation is imminent
    revocationNotification  (5)
        -- notification that a revocation has occurred  }
```

Laiko žymos serveriai neturi išduoti jokių kitokių reikšmių. Prašytojai gali ignoruoti bet kokias kitokias gautas reikšmes.

Kai laiko žyma nėra pateikiama, *failInfo* nurodo priežastį, kodėl užklausa laiko žymai gauti buvo atmesta, ir gali turėti vieną iš šių reikšmių :

```
PKIFailureInfo ::= BIT STRING  {
badAlg                  (0),
  -- unrecognized or unsupported Algorithm Identifier
badRequest              (2),
  -- transaction not permitted or supported
badDataFormat           (5),
  -- the data submitted has the wrong format
timeNotAvailable        (14),
  -- the TSA's time source is not available
unacceptedPolicy        (15),
  -- the requested TSA policy is not supported by the TSA
unacceptedExtension     (16),
  -- the requested extension is not supported by the TSA
addInfoNotAvailable     (17)
 -- the additional information requested
 -- could not be understood or is not available  }
```

Tai yra tik tos *PKIFailureInfo* reikšmės, kurios yra palaikomos. Laiko žymos serveriai neturi išduoti kitokių reikšmių. Prašytojai gali ignoruoti bet kokias kitokias gautas reikšmes.

*PKIStatusInfo* lauke *statusString* gali būti įrašytas tekstas, nurodantis, dėl kokių priežasčių nebuvo sukurta laiko žyma.

TSA atsakymo *TimeStampToken* lauke yra laukas *ContentInfo*, nurodantis duomenų tipą, kuriems dedama laiko žyma, ir laukas *content*, kuriame yra laiko žymos reikšmė (*TSTInfo*).

Laiko žymoje turi būti TSA parašas.

Laiko žymoje yra tokia informacija:

```
TSTInfo ::= SEQUENCE  {
    version                 INTEGER  { v1(1) },
    policy                  TSAPolicyId,
    messageImprint          MessageImprint,
      -- MUST have the same value as the similar field in
      -- TimeStampReq
    serialNumber            INTEGER,
      -- Time Stamps users MUST be ready to accommodate
      -- integers up to 160 bits
    genTime                 GeneralizedTime,
    accuracy                Accuracy                OPTIONAL,
    ordering                BOOLEAN                 DEFAULT FALSE,
    nonce                   INTEGER                 OPTIONAL,
      -- MUST be present if the similar field was present in
      -- TimeStampReq. In that case it MUST have the same value
    tsa                     GeneralName             OPTIONAL,
    extensions              IMPLICIT Extensions     OPTIONAL }
```

*version* lauke nurodoma laiko žymos versija (šiuo metu v1). Laiko žymos serveriai privalo teikti v1 versijos laiko žymas.

Iš leistinų (OPTIONAL) laukų, privalomas yra tik *nonce* laukas.

Prašytojai turi mokėti suprasti v1 versijos laiko žymas su visais jose leistinais laukais, bet neprivalo suprasti kai kurių *extensions* laukų semantikos, jei jie yra.

*policy* lauke turi būti nurodytas laiko žymos taisyklių, kurias įgyvendina TSA, identifikatorius. Jei laiko žymos taisyklių identifikatorius buvo nurodytas užklausoje, tuomet atsakyme šis identifikatorius turi būti toks pats kaip ir užklausoje. Priešingu atveju prašytojui turi būti išsiųstas atsakymas su pranešimu apie klaidą (unacceptedPolicy). Laiko žymos taisyklėse gali būti tokio tipo informacija (šis sąrašas nėra išsamus):

- sąlygos, kurioms esant laiko žyma gali būti naudojama;

- reikalavimas įsiminti (*log*) laiko žymas, kas leistų vėliau patikrinti, ar laiko žyma yra autentiška.

*messageImprint* laukas turi turėti tokią pat duomenų santraukos reikšmę, kaip ir atitinkamas užklausos, atsiųstos laiko žymai gauti, laukas, o santraukos ilgis turi būti toks, koks yra būdingas algoritmui, nurodytam užklausos *hashAlgoritm* lauke.

*serialNumber* lauke TSA kiekvienai laiko žymai įrašo sveikąjį skaičių – unikalų žymos serijinį numerį (t. y. TSA vardas ir numeris laiko žymai identifikuoti). Atkreiptinas dėmesys, kad numerio unikalumo savybė turi būti išsaugota netgi po galimo paslaugų teikimo sutrikimo.

*genTime* lauke įrašomas laikas, kada TSA sukūrė laiko žymą. Pagal ASN.1 sintaksę *GeneralizedTime* parametre sekundės gali būti nurodomos su trupmenine dalim. Kai nėra aukštesnio tikslumo poreikio, laikas turi būti nurodomas vienos sekundės tikslumu.

Ši sintaksė yra tokia : YYYYMMDDhhmmss[.s...]Z

Pavyzdys : 20010706001326.34352Z

Kodavimas turi būti nutraukiamas, pasiekus "Z"(*zero*). Jei yra sekundės trupmeninė dalis, ji atskiriama tašku. Trupmeninės dalies gale neturi būti bereikalingų nulių. Jei trupmeninė dalis visa lygi nuliui, turi būti praleidžiamas ir taškas.

Vidurnakčio laiko formatas turi būti toks: "YYYYMMDD000000Z", kur "YYYYMMDD" yra dienos po vidurnakčio data.

Keletas galiojančių laiko atvaizdavimo pavyzdžių :

"20010521000000Z"
"20010622123421Z"
"20010722132100.3Z"

*accuracy* laukas nurodo *GeneralizedTime* parametre (žiūr. *genTime* lauką) patalpinto laiko nukrypimą nuo UTC laiko.

```
Accuracy ::= SEQUENCE  {
seconds          INTEGER           OPTIONAL,
millis           INTEGER (1..999)  OPTIONAL,
micros           INTEGER  (1..999) OPTIONAL  }
```

Jei sekundės, milisekundės arba mikrosekundės yra praleidžiamos, praleistame lauke turi būti rašomas nulis.

*accuracy* reikšmę (laiko paklaidą) pridėję prie *GeneralizedTime* parametre patalpinto laiko, galime gauti viršutinę laiko ribą, kada TSA kūrė laiko žymą. Analogiškai, atėmę *accuracy* reikšmę iš *GeneralizedTime*, gausime apatinę laiko ribą. *accuracy* reikšmėje gali būti sekundės, milisekundės (1-999) ir mikrosekundės (1-999). Kiekviena iš jų turi būti išreiškiama sveikuoju skaičiumi. Jei *accuracy* laukas praleidžiamas (šis

laukas nebūtinas, *optional*), tai laiko tislumas gali būti gaunamas kitais keliais, t. y. per *PolicyInformation* parametrą.

Jei *ordering* laukas yra praleistas arba esančio lauko reikšmė yra FALSE, tuomet *genTime* laukas nurodo tik laiką, kada TSA kūrė laiko žymą. Tokiu atveju tos pačios TSA arba skirtingų TSA sukurtų laiko žymų eiliškumą įmanoma nustatyti tik tada, jei skirtumas tarp *genTime* reikšmės vienoje laiko žymoje ir *genTime* reikšmės kitoje laiko žymoje yra didesnis už *genTime* reikšmių tikslumų (*accuracy* laukų reikšmių*)* sumą.

Jei *ordering* laukas yra ir jame įrašyta reikšmė TRUE, tos pačios TSA sukurtų laiko žymų eiliškumas visuomet gali būti nustatytas remiantis *genTime* laukais, nepaisant *genTime* reikšmių tikslumo.

*nonce* laukas atsakyme privalo būti, jei toks laukas buvo užklausoje. Šiuo atveju *nonce* reikšmė turi būti tokia pati, kaip ir atsiųstos užklausoje (*nonce* – sveikasis atsitiktinis 64 bitų ilgio skaičius, kurį sugeneruoja prašytojas ir įdeda į užklausą).

*tsa* lauke nurodomas TSA vardas. Jei šis laukas yra, jame nurodytas vardas turi sutapti su TSA sertifikate įrašytu vardu.

*extensions* laukas yra bendrasis būdas pridėti papildomą informaciją. Konkretus *extention* lauko tipas gali būti apibrėžtas standartuose, arba jį gali apibrėžti ir užregistruoti bet kuri organizacija ar bendruomenė.

## 10.5. Pranešimų perdavimas

Pranešimų (užklausų laiko žymai gauti, TSA atsakymų) perdavimo mechanizmui nėra jokių privalomų reikalavimų. Žemiau aprašomi mechanizmai yra leistini (*optional*) ; ateityje gali atsirasti nauji mechanizmai.

***Pranešimų perdavimas el. pašto žinutėmis***

Pranešimai gali būti siunčiami ir priimami naudojant bendrąsias MIME (*Multi-Purpose Internet Mail Extensions*) priemones, todėl paprastasis interneto el. pašto transportas gali būti naudojamas laiko žymų pranešimams perduoti.

***Pranešimų perdavimas failais***

Perduodamame faile, kuriame yra laiko žyma, turi būti tik vienas DER-kodo TSA pranešimas, t. y. jame neturi būti pašalinių (nesusijusių) antraščių ar priedų. Toks failas gali būti perduodamas, pvz., FTP (*File Transfer Protocol*) būdu.

Užklausos laiko žymai gauti failo vardo plėtinys turėtų būti ".tsq" (*TimeStampQuery*), o atsakymo apie laiko žymą – ".tsr" (*TimeStampReply*).

***Pranešimų perdavimas prisijungus prie serverio***

Paprastasis TCP protokolas gali būti naudojamas TSA pranešimams perduoti. Šis protokolas tinka tais atvejais, kai prašytojas prisijungia prie TSA serverio ir klausdamas gauna atsakymą. Šio protokolo esmė yra ta, kad TSA dirba kaip paslaugos teikėjas (atsakovas) ir gali priimti užklausas žinomu (*well-defined*) prievadu (IP jungties numeris 318).

Tipiniu atveju prašytojas prisijungia prie šio prievado ir pateikia užklausą TSA. TSA grąžina atsakymą su laiko žyma ir/arba su atitinkamu numeriu, kurį panaudojus vėliau iš TSA galima gauti laiko žymos duomenis.

Jei TSA į gautą užklausą siunčia tik atitinkamą numerį, tai kartu siunčiama ir nuoroda, kaip vėliau galima būtų gauti laiko žymos duomenis. Kai prašytojas iš TSA gauna galutinį pranešimą (*finalMsgRep*), tai TSA nebeteikia jokių naujų nuorodų.

Prašytojas siunčia į TSA atitinkamo tipo pranešimą-užklausą (*direct TCP-based TSA message*). TSA siunčia prašytojui panašaus tipo pranešimą-atsakymą.

TSA pranešimo sudėtis: *length* (32-bitai), *flag* (8-bitai), *value* (apibrėžiama žemiau, naudojant ASN.1 sintaksę). *length* lauke užrašomas likusios pranešimo dalies ilgis baitais (*value* lauko baitų kiekis plius *flag* lauko baitas).

RFC 3161 standarte [29] TSA pranešimai apibrėžiami taip:

| pranešimo-pavadinimas (*Message name*) | požymis (*flag*) | duomenys (*value*) |
|---|---|---|
| **tsaMsg** | '00'H | DER-encoded TSA message |
| -- TSA message | | |
| **pollRep** | '01'H | polling reference (32 bits), time-to-check-back (32 bits) |
| -- poll response where no TSA message response ready; | | |
| -- use polling reference value (and estimated time value) for | | |
| -- later polling | | |
| **pollReq** | '02'H | polling reference (32 bits) |
| -- request for a TSA message response to initial message | | |
| **negPollRep** | '03'H | '00'H |
| -- no further polling responses (i.e., transaction complete) | | |
| **partialMsgRep** | '04'H | next polling reference (32 bits), time-to-check-back (32 bits), DER-encoded TSA message |
| -- partial response (receipt) to initial message plus new polling | | |
| -- reference (and estimated time value) to use to get next part | | |
| -- of response | | |

**finalMsgRep** '05'H DER-encoded TSA message
-- final (and possibly sole) response to initial message
**errorMsgRep** '06'H human readable error message
-- produced when an error is detected (e.g., a polling
-- reference is received which doesn't exist or
-- is finished with)

Pranešimų eilės tvarka gali būti tokia :

a) prašytojas siunčia *tsaMsg* tipo užklausą ir iš TSA gauna *pollRep, negPollRep, partialMsgRep* arba *finalMsgRep* tipo atsakymą;

b) prašytojas siunčia *pollReq* tipo užklausą ir iš TSA gauna *negPollRep, partialMsgRep, finalMsgRep* arba *errorMsgRep* tipo atsakymą.

*time-to-check-back* parametras (žiūr. *pollRep* arba *partialMsgRep* tipo pranešimus) yra 32 bitų ilgio sveikasis skaičius, nurodantis sekundžių kiekį, po kurio vėl bus galima siųsti kitą užklausą *pollReq* (prašytojas gali siųsti daug *pollReq* tipo užklausų, kol negaus *finalMsgRep* tipo atsakymo).

***Pranešimų perdavimas HTTP priemonėmis***

Užklausos laiko žymai gauti ir TSA atsakymai gali būti perduodami internetu, naudojant bendrąjį HTTP protokolą. Todėl TSA pranešimams perduoti galima naudoti paprastąjį naršyklės-serverio būdą. Gavęs užklausą, TSA serveris turi atsakyti, išduodamas atitinkamą atsakymą su laiko žyma arba HTTP pranešimą apie klaidą.

## 10.6. Saugumo klausimai

Steigiant TSA turi būti atkreiptas ypatingas dėmesys į šias aplinkybes, turinčias įtakos laiko žymų teisėtumui ir patikimumui:

1) atsiradus priežasčiai, dėl kurios nebegalima toliau pasitikėti TSA, nors TSA privatusis raktas nėra sukompromituotas (nėra prarasta privačiojo rakto kontrolė), TSA sertifikatas turi būti atšauktas. Bet kuriuo metu vėliau TSA privačiuoju raktu pasirašytos laiko žymos laikomos negaliojančiomis;

2) kai TSA privatusis raktas sukompromituojamas, atitinkamas sertifikatas turi būti atšauktas. Šiuo atveju bet kuri laiko žyma, pasirašyta šiuo raktu, negali būti laikoma patikima. Dėl šios priežasties reikalaujama, kad TSA privatusis raktas būtų laikomas ir naudojamas saugiai, kad būtų minimizuota jo sukompromitavimo galimybė. Kai TSA privatusis raktas sukompromituojamas, TSA sukurtų ir išsaugotų laiko žymų auditas (*audit trail*) gali padėti atskirti nesuklastotas ir suklastotas laiko žymas. Dviejų laiko žymų, gaunamų iš skirtingų TSA, naudojimas yra kitas šios problemos sprendimo būdas;

3) TSA privatusis raktas laiko žymoms pasirašyti turi būti pakankamo ilgio, kad išliktų patikimas pakankamai ilgą laiką. Netgi išpildžius šį reikalavimą, rakto galiojimo laikas bus baigtinis. Todėl, galiojimo terminui pasibaigus, bet kuri TSA anksčiau pasirašyta žyma vėliau turėtų būti pasirašoma iš naujo naujuoju TSA privačiuoju raktu (jei yra prieinamos autentiškos TSA sertifikatų kopijos senuose CRL sąrašuose) arba patvirtinta notaro (jei jie tokie yra), kad būtų labiau pasitikima žymomis. Laiko žymos taip pat galėtų būti saugomos įrodymų registravimo tarnyboje (*Evidence Recording Authority*), kas padėtų išlaikyti pasitikėjimą žymomis;

4) programinėje įrangoje, besikreipiančioje į TSA, turėtų būti nustatyta laiko trukmė, kiek galima laukti atsakymo. Tarpininko (*man-in-the-middle*) veiksmai gali įnešti užlaikymą. Todėl bet kuris atsakymas, negautas per nustatytą laiką, turėtų būti laikomas įtartinu. Kadangi kiekvienas pranešimų perdavimo metodas turi skirtingas užlaikymo charakteristikas, priimtina laiko periodo trukmė priklausys nuo pranešimų perdavimo metodo ir nuo kitų aplinkos veiksnių;

5) jei skirtingi asmenys prašo laiko žymų tiems patiems duomenims ir nurodo tokį patį duomenų santraukos algoritmą arba vienas asmuo gauna kelias laiko žymas tiems patiems duomenims, tai į sukurtas laiko žymas bus įtraukta tokia pati duomenų santrauka; laiko žymų tikrintojai turi žinoti, kad kelios laiko žymos gali būti susijusios (priklausyti) su tais pačiais duomenimis;

6) gali pasitaikyti, kad tyčia ar netyčia atsiranda keli atsakymai į užklausas, turinčias tokį patį santraukos algoritmą ir tokią pačią duomenų santraukos reikšmę. Netyčiniai atsakymai atsiranda tada, kai prašytojas išsiunčia tą pačią užklausą į TSA daugiau kaip vieną kartą, esant kompiuterių tinklo sutrikimams. Tyčiniai atsakymai atsiranda tada, kai įsilaužėlis (*middleman*) kėsinasi pakeisti TSA atsakymus. Tokioms situacijoms nustatyti yra keletas būdų. *nonce* parametras (atsitiktinis skaičius užklausoje, kuris perkeliamas į atsakymą) visada padeda aptikti pasikartojančius atsakymus ir todėl yra rekomenduotinas. Kita galimybė – tai vietinio laiko (*local clock*) ir laiko tarpo (*moving time window*), kurio metu prašytojas išsaugo visas siųstas santraukas, stebėjimas. Gavęs atsakymą, prašytojas įsitikina, kad atsakymo laikas patenka į nurodytą laiko tarpą ir kad tuo metu buvo naudota vienintelė santraukos reikšmė.

## 10.7. Reikalavimai laiko žymų prašytojų ir TSA įrangai

El. parašo naudotojai, norintys gauti laiko žymą savo sukurtiems el. parašams, turi kreiptis į TSA, pasiųsdami atitinkamą užklausą. Į gautą

užklausą TSA turi išduoti atitinkamą atsakymą. Tam prašytojų ir TSA naudojama įranga turi atitikti nustatytus reikalavimus. Kokie parametrai turi būti užklausose ir atsakymuose, kokie algoritmai turi būti naudojami juos formuojant, kokiomis priemonėmis turi būti perduodamos užklausos ir atsakymai, yra nustatyta ETSI TS 101 861 standarte [3]. Pastarajame įvesta nemažai apribojimų, lyginant su RFC 3161 standartu [29].

### 10.7.1. Reikalavimai prašytojų įrangai

Prašytojų naudojama įranga turi formuoti nustatyto formato užklausas ir sugebėti priimti nustatyto formato atsakymus iš TSA:

1. Reikalavimai užklausoms:

a) užklausos parametrai: prašytojų suformuotose užklausose neturi būti *extensions* laukų (pagal RFC 3161 standartą [29] tokie laukai buvo leistini);

b) naudotini algoritmai: duomenų, kuriems norima gauti laiko žymą, santraukai sukurti gali būti naudojami šie algoritmai: SHA-1, MD5 arba RIPEMD-160. Rekomenduojami SHA-1 arba RIPEMD-160;

2. Reikalavimai susiję su TSA atsakymais:

a) reikalavimai atsakymų laukams:
- turi būti palaikomas ir suprantamas laiko tikslumo laukas *accuracy*;
- turi būti palaikomos *ordering* lauko reikšmės - *missing* (praleistas) arba FALSE;
- turi būti palaikomas *nonce* parametras;
- *extensions* laukų gali nebūti;

b) naudotini algoritmai: laiko žymoje TSA parašas turi būti sukurtas naudojant SHA-1 ir RSA algoritmus;

c) reikalavimas raktų ilgiams: TSA parašo kūrimo RSA algoritme turi būti naudojami 1024 bitų ilgio raktai. Turėtų būti galimybė naudoti ir 2048 bitų ilgio raktus.

### 10.7.2. Reikalavimai TSA serveriui

TSA serveris, priimdamas užklausas, turi suprasti (palaikyti) jose esančius laukus ir sukurti atitinkamų reikalavimų atsakymus.

1. Reikalavimai, susiję su užklausų priėmimu:

a) turi būti priimami šie užklausų laukai ir parametrai:
- *nonce* lauko parametras;
- *certReq* lauko parametras;
- *extensions* laukų gali nebūti;

b) naudotini algoritmai: duomenų santrauka, atsiųsta laiko žymai uždėti, turi būti apskaičiuota SHA-1, MD5 arba RIPEMD-160 algoritmu.

2. Reikalavimai atsakymams:

a) atsakymo parametrai:

- turi būti *genTime* parametras ne mažesniu kaip vienos sekundės tikslumu;
- *accuracy* lauke turi būti nurodomas ne mažesnis kaip vienos sekundės tikslumas;
- turi būti *ordering* parametras su *missing* arba FALSE reikšme;
- *extensions* laukų gali nebūti;
- jei *extensions* laukai yra, jis neturi būti kritinis (jo informacija neesminė, aiškinamoji, patariamoji);

b) pasirašant žymas santraukoms apskaičiuoti naudotini SHA-1, MD5 arba RIPEMD-160 algoritmas. El. parašas turi būti kuriamas naudojant SHA-1 ir RSA algoritmus;

c) reikalavimas raktų ilgiams: RSA algoritme turi būti naudojami 1024 bitų ilgio raktai. Turėtų būti galimybė naudoti ir 2048 bitų ilgio raktus.

## 10.8. Reikalavimai TSA

### 10.8.1. Bendrieji klausimai

El. parašo laiko žyma yra įrodymas, kad el. parašas buvo sukurtas iki žymoje nurodyto laiko. Taip užtikrinamas ilgalaikis el. parašo galiojimas, nes galima bus įrodyti, kad asmuo sukūrė el. parašą dar jam priklausančio sertifikato galiojimo periodu.

Reikalavimai apibrėžia, kaip TSA turi kurti žymas ir valdyti žymos kūrimo procesą, kad jomis galėtų pasitikėti vartotojai.

Reikalaujama, kad TSA sudarytose laiko žymose būtų nurodomas universalusis laikas (*UTC – universal co-ordinated time;* Grinvičo laikas) ir žymos būtų pasirašytos TSA el. parašu.

***Keletas sąvokų apibrėžimų***

TSA veiklos skelbimas – pareiškimų apie TSA veiklą ir reikalavimus rinkinys, informuojantis laiko žymos vartotojus.

TSA veiklos nuostatai – pagrindinės veikimo taisyklės, kurių laikosi TSA, teikdama laiko žymas.

TSA sistema – informacinių technologijų priemonių visuma, reikalinga laiko žymoms teikti.

Laiko žymos taisyklės – laiko žymų sudarymo ir naudojimo taisyklės, nustatančios TSA, laiko žymos naudotojų teises ir pareigas. Laiko žymos

taisykles renkasi laiko žymos naudotojai, tvirtina ir įgyvendina TSA. Laiko žymos taisyklės rengiamos laiko žymos naudotojų grupės iniciatyva, TSA arba pasirenkamos iš standartų.

Laiko žymos kūrimo blokas – techninė ir programinė įranga, kuri yra valdoma kaip atskiras vienetas ir turi savo privatųjį raktą laiko žymoms pasirašyti.

Abonentas – asmuo, prašantis TSA teikti laiko žymas jo duomenims ir tiesiogiai ar netiesiogiai išreiškęs sutikimą su TSA sąlygomis.

Vartotojai – TSA abonentai ir laiko žymomis pasitikinčios šalys (parašų tikrintojai).

***Kai kurių sąvokų platesnis apibūdinimas***

TSA yra atsakinga už visas su laiko žymų teikimu susijusias paslaugas. TSA pasirašo laiko žymas savo el. parašu. Laiko žymoje turi būti nurodyta ją sukūrusi TSA.

TSA sudėtyje gali būti keli aiškiai atskirti laiko žymas teikiantys padaliniai (serveriai). Kiekvienas padalinys laiko žymoms pasirašyti turi naudoti savo privatųjį raktą.

TSA abonentu gali būti tiek organizacija (grupė vartotojų, juridinis asmuo), tiek individualus vartotojas. Jei abonentas yra organizacija, tai už kai kurių organizacijos įsipareigojimų vykdymą yra atsakingi ir jos nariai. Tačiau bet kuriuo atveju atsako organizacija, jei jos nariai nekorektiškai vykdo organizacijos prisiimtus įsipareigojimus, ir jos pareiga yra tinkamai informuoti savo narius. Jei abonentas yra individualus vartotojas, tuomet jis yra tiesiogiai atsakingas už įsipareigojimų vykdymą.

***Laiko žymos taisyklių ir TSA veiklos nuostatų tikslai***

Apskritai, laiko žymos taisyklės nurodo “kas turi būti daroma”, o TSA veiklos nuostatai - “kaip turi būti daroma”, t. y. apibrėžia laiko žymos kūrimo procesą ir TSA laikrodžio parodymų tikslumo palaikymą. Laiko žymos taisyklės nustato bendruosius laiko žymos paslaugų reikalavimus. TSA savo veiklos nuostatuose nurodo, kaip tos taisyklės yra įgyvendinamos.

Laiko žymos taisyklės yra rengiamos nepriklausomai nuo specifinių TSA darbinės aplinkos detalių, tuo tarpu TSA veiklos nuostatai atspindi TSA organizacinę struktūrą, darbines procedūras, galimybes, kompiuterinę aplinką.

Laiko žymos taisyklės turi turėti unikalų identifikatorių. Tų taisyklių identifikatoriai, kurias įgyvendina TSA, turi būti nurodyti TSA veiklos nuostatuose.

Laiko žymos taisyklės turi būti laisvai prieinamos internetu, kad su jomis galėtų susipažinti vartotojai.

Ar TSA tinkamai įgyvendina pasirinktas taisykles, įvertina nepriklausomi auditoriai.

### 10.8.2. Pareigos ir atsakomybė

***TSA pareigos***

- TSA turi užtikrinti, kad visi jai keliami reikalavimai, kurie detalizuoti žemiau, yra įgyvendinami laikantis pasirinktų laiko žymos taisyklių;
- TSA turi užtikrinti procedūrų atitikimą nustatytiems reikalavimams, netgi jei procedūras atlieka TSA subrangovai;
- TSA turi teikti visas laiko žymos paslaugas, laikydamasi savo veiklos nuostatų;
- TSA turi laikytis savo abonentams prisiimtų laiko žymos teikimo sąlygų, įskaitant teikiamų paslaugų tinkamumą ir tikslumą.

***Laiko žymos vartotojų pareigos***

- gavę laiko žymą, vartotojai turi patikrinti, ar TSA ją pasirašė teisingai ir ar žymai pasirašyti panaudotas privatusis raktas nėra sukompromituotas;
- vartotojai turi laikytis laiko žymos naudojimo apribojimų, nustatytų laiko žymos taisyklėse;
- vartotojas turi laikytis sutartyse su TSA ar kitur nurodytų atsargumo priemonių.

***Atsakomybė***

- TSA už neteisėtus veiksmus atsako ir padarytą žalą vartotojams atlygina įstatymų nustatyta tvarka;
- TSA gali atsisakyti arba apriboti savo atsakomybę, susijusią su laiko žymų teikimu, jeigu tai neprieštarauja galiojantiems įstatymams.

### 10.8.3. TSA veiklos reikalavimai

***TSA veiklos nuostatai ir jų skelbimas***

- TSA savo veikla turi užtikrinti patikimą laiko žymos paslaugų teikimą;
- TSA turi parengti savo veiklos nuostatus ir juos bei laiko žymos paslaugų teikimo sąlygas paskelbti internete visiems vartotojams.

***Raktų tvarkymas***

- TSA turi užtikrinti, kad bet kokie kriptografiniai raktai būtų generuojami laikantis standartų;
- TSA turi užtikrinti savo privačiojo rakto konfidencialumą ir vientisumą;
- TSA turi užtikrinti pasitikinčioms šalims platinamo TSA viešojo rakto ir bet kurių kitų susijusių parametrų vientisumą ir autentiškumą;

- TSA sertifikato galiojimo ir atitinkamo privačiojo rakto naudojimo trukmė turi būti ribota, atsižvelgiant į naudojamus duomenų santraukos apskaičiavimo ir parašo kūrimo algoritmus bei laiko žymoms pasirašyti naudojamo rakto ilgį;
- TSA turi užtikrinti, kad jos privatusis raktas laiko žymoms pasirašyti nebebūtų naudojamas pasibaigus sertifikate nustatytam terminui;
- TSA turi užtikrinti laiko žymoms pasirašyti naudojamo kriptografinio modulio saugumą viso jo gyvavimo ciklo metu.

***Laiko žymos kūrimas***

- TSA turi užtikrinti, kad laiko žymos būtų kuriamos saugiai ir į jas būtų įtraukiamas teisingas laikas;
- TSA turi užtikrinti, kad jos laikrodis paskelbtu tikslumu būtų sinchronizuotas su universaliuoju laiku UTC.

***TSA valdymas ir darbas***

- TSA turi užtikrinti, kad administracinės ir valdymo procedūros atitiktų pripažintus standartus;
- TSA turi užtikrinti, kad jos informacija ir kitoks turtas būtų tinkamai apsaugoti;
- TSA turi užtikrinti, kad personalas ir samdomi darbuotojai stiprintų ir palaikytų TSA veiksmų patikimumą ir kad darbuotojų sukčiavimo galimybės būtų sumažintos iki minimumo;
- TSA turi užtikrinti, kad fizinė prieiga prie kritinių paslaugos vietų (laiko žymos formavimo ir pasirašymo) būtų kontroliuojama ir fizinis pavojus jos turtui būtų minimizuotas;
- TSA turi užtikrinti, kad TSA sistemos komponentai būtų saugūs ir būtų naudojami teisingai, su minimaliu sutrikimų pavojumi;
- TSA turi užtikrinti, kad tik įgalioti asmenys turėtų prieigą prie TSA sistemos;
- TSA sistemoje turi būti naudojami komponentai (kriptografinis modulis, kt.), apsaugoti nuo modifikavimo;
- TSA turi užtikrinti, kad atsitikus įvykiams, turintiems įtakos laiko žymų teikimo saugumui, įskaitant TSA privačiojo rakto kompromitaciją arba pastebėjus laikrodžio sutrikimus, vartotojai būtų tinkamai informuojami;
- TSA turi užtikrinti, kad būtų minimizuota potenciali vartotojų žala TSA nutraukiant veiklą, ir, kas ypač svarbu, kad būtų nepertraukiamai teikiama informacija, reikalinga anksčiau sukurtų laiko žymų teisingumui patikrinti;

- TSA turi užtikrinti, kad nebūtų pažeidžiami įstatymų ir kitų teisės aktų reikalavimai, pvz., asmens duomenų apsauga;
- TSA turi užtikrinti, kad visa reikiama informacija, susijusi su laiko žymų kūrimu, audito tikslams būtų užrašoma ir saugoma atitinkamą laiką, kad, reikalui esant, galima būtų ją panaudoti kaip įrodinėjimo priemonę teisme.

## 10.9. Laiko žymos taisyklės

Reikalavimai TSA apibrėžia, kaip TSA turėtų kurti žymas ir valdyti žymos kūrimo procesą, kad jomis galėtų pasitikėti parašo naudotojai, visų pirma turintys kvalifikuotus sertifikatus.

Kiekvienas TSA savo veikloje turi vadovautis laiko žymų taisyklėmis (*policy*). Kaip tos taisyklės detaliai yra įgyvendinamos, nurodoma TSA nuostatuose.

**Laiko žymos taisyklės** – laiko žymų sudarymo ir naudojimo taisyklės, nustatančios TSA, laiko žymos naudotojų teises ir pareigas. Laiko žymos taisykles renkasi laiko žymos naudotojai, tvirtina ir įgyvendina TSA. Laiko žymos taisyklės rengiamos laiko žymos naudotojų grupės iniciatyva, TSA arba pasirenkamos iš standartų [6].

Parašo naudotojai, kuriems reikalingos laiko žymos, turi susipažinti su laiko žymų taisyklėmis ir TSA veiklos nuostatais.

Laiko žymos taisyklių pavyzdį galime rasti adresu [38].

# 11. ELEKTRONINIO PARAŠO TIKRINIMAS

Šiame skyriuje skaitytojai supažindinami su el. parašo tikrinimu bei atkreipiamas dėmesys į laiko žymų svarbą parašų tikrinimui prabėgus keleriems metams. Apibrėžiamas parašo tikrinimo procesas ir naudotina parašo tikrinimo sistema (techninė ir programinė įranga) įvairiose aplinkose [13].

## 11.1. Bendrosios nuostatos

Kiekvienas el. parašu pasirašantis asmuo turi turėti sertifikatą, kas įgalina parašų tikrintojus nustatyti pasirašiusiojo asmens tapatybę, jo įgaliojimus, kt. Sertifikatus sudaro sertifikatų centrai (CA).

Sertifikatas turi būti pasirašytas jį sudariusio CA el. parašu. Tam CA turi būti gavęs sertifikatą iš aukštesnį statusą turinčio CA, o aukščiausio statuso (*root*) CA sertifikatą sau sudaro pats. Visi šie sertifikatai sudaro vadinamąją sertifikatų seką.

Sertifikate yra nurodomi jo galiojimo pradžios ir pabaigos terminai. Sertifikatas dėl įvairių priežasčių gali būti atšauktas ir anksčiau, nei nurodytas pabaigos terminas. Parašas, sukurtas po sertifikato atšaukimo, yra negaliojantis.

Praėjus kažkiek laiko, pavyzdžiui, jau archyve esantiems pasirašytiems duomenims, būtina turėti galimybę patikrinti, kad asmenys juos pasirašė atitinkamų sertifikatų galiojimo laikotarpiu. Tam parašo naudotojai el. duomenims ir el. parašams turi naudoti laiko žymas. Laiko žymas teikia laiko žymų tarnybos (TSA). El. parašo laiko žyma yra įrodymas, kad parašas buvo sukurtas iki žymoje nurodyto laiko.

El. parašo tikrinimo reikalavimai ir reikalingi el. parašo elementai (atributai) priklauso nuo numatytos el. parašo gyvavimo trukmės. Skiriami trys el. parašų variantai:

- epizodiniai (mažos galiojimo trukmės). Tai parašai, kurių nebereikia saugoti gavus informaciją apie jų galiojimo nutraukimą;
- trumpalaikiai. Tai parašai, kuriuos tikrinti gali reikėti tol, kol nesibaigė pasirašančiojo asmens sertifikato galiojimo laikas;
- ilgalaikiai. Tai parašai, kuriuos tikrinti gali reikėti pasibaigus pasirašančiojo asmens sertifikato galiojimo laikui ir, galbūt, netgi pasibaigus CA, sudariusio sertifikatą pasirašančiajam asmeniui, sertifikato galiojimo laikui.

Šiame skyriuje pagrindinis dėmesys skiriamas trumpalaikių ir ilgalaikių el. parašų tikrinimui.

Parašo naudotojų pasirinktos parašo taisyklės yra parašų kūrimo ir tikrinimo pagrindas. Šiame skyriuje naudojamų sąvokų apibrėžimai:

**sertifikatų seka** (*certification path*) – pasirašančiojo asmens parašą patvirtinančių sertifikatų eilė, susidedanti iš pasirašančiojo asmens sertifikato, pastarąjį sertifikatą sudariusio ir jį pasirašiusio CA sertifikato ir kitų (arba nė vieno) tokiu būdu susijusių CA sertifikatų, pasibaigiantis CA, kuris pats sau sudaro ir pasirašo sertifikatą, sertifikatu;

**kvalifikuotas parašas** – tai saugus el. parašas, paremtas kvalifikuotu (išsamiu, aukštesnio lygio) sertifikatu ir sukurtas saugia parašo formavimo įranga (SSCD);

**parašo naudotojai** - asmenys, kurie savo veikloje naudoja el. parašą arba iš kitų asmenų gauna pasirašytus duomenis.

Kad du vienas nuo kito nepriklausomi parašo naudotojai gautų vienodus to paties el. parašo tikrinimo rezultatus, jie turi vadovautis vienodomis taisyklėmis. Todėl yra svarbu, kad pasirašančiojo asmens pasirinktos parašo taisyklės be jokių iškraipymų būtų perduodamos parašų tikrintojams, t. y. turi būti tenkinamos šios sąlygos:

- parašo taisyklės turi būti aiškiai apibrėžtos ir prieinamos visiems parašo naudotojams. Ši sąlyga reikalauja iš parašo taisyklių leidėjų užtikrinti parašo taisyklių teikimą parašo naudotojams saugiomis priemonėmis;
- parašo taisykles, laikantis kurių duomenys buvo pasirašyti, parašų tikrintojai turi atpažinti vienareikšmiškai. Ši sąlyga reikalauja iš pasirašančiųjų asmenų nurodyti pasirinktas parašo taisykles kuriamuose parašuose. Parašo taisyklės gali būti nurodomos aiškiai, naudojant unikalų identifikatorių, arba netiesiogiai, pavyzdžiui, per teisės aktus ar sutartis.

## 11.2. Parašo tikrinimo procesas

### 11.2.1. Pirmasis ir vėlesnieji parašo tikrinimai

Parašo tikrinimo procesas yra veiksmų seka, kurios metu, vadovaujantis parašo taisyklėmis, tikrinamas parašas. Skiriami du el. parašo tikrinimo atvejai:

- pirmasis tikrinimas. Kvalifikuotiems parašams jis turi būti atliekamas kaip galima greičiau po parašo sukūrimo, kad gautume papildomą informaciją (pvz., laiko žymą, sertifikatų duomenis, kt.)

ilgalaikiam parašo galiojimui užtikrinti. Šitokį tikrinimą gali atlikti tiek pasirašantysis asmuo, tiek parašo tikrintojas;

- vėlesnieji tikrinimai. Jie gali būti atliekami praėjus netgi keleriems metams po parašo sukūrimo. Šie tikrinimai nereikalauja naujos informacijos gavimo, kaip to reikėjo pirmojo tikrinimo metu. Tačiau yra viena išimtis: jei parašams kurti naudota kriptografija tapo pažeidžiama, reikia papildomos informacijos, kad galima būtų pratęsti parašo galiojimą.

### 11.2.2. Pirmojo tikrinimo duomenys

Parašo tikrinimo metu asmuo visų pirma turi sužinoti, kokiomis parašo taisyklėmis jis turi vadovautis, bei patikimu būdu gauti tų taisyklių kopiją. Pasirašančiojo asmens naudotas parašo taisykles tikrintojas gali sužinoti iš atitinkamos nuorodos paraše arba, kai tokios nuorodos nėra, remdamasis pasirašytų duomenų tipu (papildomai pasitelkiant teisės aktus ar sutartis).

Kai parašo taisyklės paraše yra nurodytos aiškiai, tikrintojas turi įsitikinti, kad jis turi patikimą parašo taisyklių kopiją. Tikrintojas, perskaitęs parašo taisykles arba spręsdamas pagal parašo taisyklių identifikatorių, taip pat turi įsitikinti, kad parašo taisyklės atitinka jo poreikius (veiklos kontekstą).

Jei parašo taisyklių nuorodos paraše nėra, tikrintojas turi susipažinti su pasirašytais duomenimis ir, pasitelkęs kitus dokumentus (pvz., sutartis tam tikros srities operacijoms atlikti), įsitikinti, kad tokiam duomenų tipui paprastai taikomos tam tikros parašo taisyklės.

El. parašo pirmasis tikrinimas reikalauja, kad parašo tikrinimo sistema būtų pajėgi apdoroti, iš vienos pusės, aiškiai nurodytas arba pagal pasirašytų duomenų tipą nustatytas parašo taisykles, o iš kitos pusės:

- pasirašytus duomenis (tai pasirašančiojo asmens parengti duomenys);
- tų duomenų el. parašą;
- kitus el. parašo patvirtinimo duomenis (šie duomenys suformuojami pirmojo tikrinimo metu).

Prisiminkime, kad paprasčiausias BES formato el. parašas susideda iš informacijos elementų visumos (pasirašomų parašo atributų) ir skaitmeninio parašo. Skaitmeninis parašas kuriamas informacijos elementų visumai (t. y. tos visumos santraukai-*hash*), kurioje turi būti:

- pasirašytų duomenų tipas;
- pasirašyti duomenys arba jų santrauka;
- pasirašančiojo asmens sertifikato nuoroda.

Papildomai el. paraše dar gali būti:

- ♦ parašo taisyklių nuoroda;
- ♦ pasirašančiojo asmens nurodomas pasirašymo laikas;
- ♦ pasirašomų duomenų laiko žyma;
- ♦ pasirašančiojo asmens pareigos (rolė, įgaliojimai);
- ♦ pasirašančiojo asmens nurodoma pasirašymo vieta.

Tikrinant el. parašą būtina nustatyti, ar pasirašančiojo asmens sertifikatas ir parašo informacijos elementų sertifikatai (jei tokie naudojami, pvz., asmens pareigų sertifikatas) buvo galiojantys pasirašymo metu.

Pirmojo tikrinimo metu, kai dar nėra papildomos informacijos apie parašo sukūrimo laiką (pvz., laiko žymos), laikoma, jog pasirašymo laikas yra artimas pirmojo tikrinimo laikui. Parašas yra galiojantis, jei pasirašančiojo asmens sertifikatas pirmojo tikrinimo metu nebuvo atšauktas. Todėl rizika, kad parašas bus laikomas negaliojančiu, yra mažesnė, jei pirmąjį tikrinimą atliksime kaip galima greičiau po parašo sukūrimo.

Taigi, pirmojo tikrinimo įeities duomenys yra šie:

- ♦ parašo taisyklės;
- ♦ pasirašyti duomenys;
- ♦ BES formato parašas.

Vėlesniojo tikrinimo metu paraše jau turi būti papildoma informacija (tai asmens nepasirašomi parašo atributai), leidžianti patikrinti, kad parašas buvo sukurtas sertifikato galiojimo metu. Ilgalaikiam el. parašo galiojimui užtikrinti pirmojo tikrinimo metu BES formato el. parašas turi būti papildytas tokia informacija:

- ♦ laiko žyma, kurias suformuoja laiko žymų teikėjai (TSA);
- ♦ įvairių su parašu susijusių sertifikatų nuorodomis (ne tik pasirašančiojo asmens, bet ir paslaugų teikėjų CA, TSA, kt.);
- ♦ informacija apie sertifikatų galiojimo statusą (gaunama iš CA tvarkomų CRL sąrašų).

### 11.2.3. Pirmojo tikrinimo rezultatai

Pirmojo tikrinimo rezultatai yra tokie: tikrinimo statusas ir parašo patvirtinimo duomenys.

Pirmojo tikrinimo statusas gali būti:

- ♦ sėkmingas;
- ♦ nesėkmingas;
- ♦ nebaigtas.

Sėkmingas tikrinimas reiškia, jog parašas atitiko visus parašo taisyklių reikalavimus.

Nesėkmingas tikrinimas reiškia, jog parašas neatitiko parašo taisyklių reikalavimų, pvz., buvo ne toks duomenų tipas, neatitiko pasirašytų duomenų santrauka, nebegaliojo pasirašiusiojo asmens sertifikatas.

Nebaigtas tikrinimas reiškia, jog pasirašytų duomenų tipas yra leistinas, atitinka pasirašytų duomenų santrauka, tačiau nepakanka informacijos, kad galima būtų patikrinti, ar parašas atitinka visus parašo taisyklių reikalavimus. Tokiu atveju turi būti galimybė parašą tikrinti vėliau, kai bus gauta trūkstama informacija. Priklausomai nuo trūkstamos informacijos, tikrinančiajam turėtų būti pasirinkimo galimybė, ką daryti su tokiu parašu.

Pirmojo tikrinimo metu tikrintojas privalo surinkti parašo patvirtinimo duomenis – laiko žymą, sertifikatų duomenis, CRL sąrašų informaciją - kurie turi atitikti visus parašo taisyklių reikalavimus. Ateityje, vėlesniojo tikrinimo metu parašo patvirtinimo duomenys bus kaip įrodymas, jog visi sertifikatų sekos sertifikatai kuriant parašą buvo galiojantys. Tai reiškia, jog turi būti surinkti duomenys apie visus sertifikatus (pasirašančiojo asmens, CA, kt.) bei jų galiojimo statusą.

Kad ateityje vėlesniojo tikrinimo metu galėtume įrodyti, jog visi duomenys buvo gauti dar iki sertifikatų galiojimo nutraukimo, reikalinga el. parašo laiko žyma. Tiek pasirašantysis asmuo, tiek parašo tikrintojas gali kreiptis į laiko žymų tarnybą (TSA) parašo laiko žymai gauti.

Pasirašantysis asmuo savo nuožiūra gali kurti ES-C formato el. parašus, turinčius visus patvirtinimo duomenis (žiūr. 7 skyrių ELEKTRONINIO PARAŠO FORMATAI). Tokiu atveju visi parašo patvirtinimo duomenys turės būti perduodami ir parašų tikrintojams.

Jei el. parašo vėlesniojo tikrinimo metu pastebima, kad pasirašantysis asmuo nebuvo suformavęs ES-T formato el. parašo (parašo su laiko žyma), tai tikrintojas, pirmą kartą gavęs BES formato el. parašą, turi parengti ES-T formato el. parašą. Pridėta laiko žyma bus nepriklausomas įrodymas, kad el. parašas jau egzistavo tuo metu ir pasirašęs asmuo negalės jo išsižadėti. El. parašo laiko žyma turi būti sukurta kiek galima greičiau po parašo sukūrimo. Kai pasirašantysis asmuo nepateikia ES-C formato el. parašo, tai tokio formato el. parašą turi sukomplektuoti tikrintojas, jei CRL sąrašo informacija ir kiti el. parašo patvirtinimo duomenys dar yra prieinami. Ką turi padaryti pasirašantysis asmuo ir ką - parašo tikrintojas, nustatoma parašo taisyklėse.

Bendruoju atveju ES-C formato el. parašas negali būti sukurtas tuo pačiu metu kaip ir BES formato el. parašas, nes po parašo sukūrimo iki jo tikrinimo būtina palaukti tam tikrą laiko tarpą. Tai vadinamasis atidėjimo periodas *(grace period)* arba laikas, kuris sugaištamas sertifikatui atšaukti (jis reikalingas apsaugai nuo klastočių, kai asmuo pasirašo, uždeda laiko žymą ir tuoj pat prašo atšaukti sertifikatą). Jei sertifikato galiojimas tikrinimo metu buvo tik sustabdytas, tai būtina palaukti, kol baigsis sustabdymo laikotarpis.

ES-C formato el. parašai gali būti išplėsti iki ES-X formato el. parašų. Tam prie ES-C parašo dar pridedami:

- pasirašiusiojo asmens visas sertifikatas;
- sertifikatų seką sudarančių CA visi sertifikatai, į kuriuos yra nuorodos ES-C el. paraše;
- CRL sąrašų informacija, į kuriuos yra nuorodos ES-C el. paraše.

ES-X formato el. paraše gali būti saugomas tik pasirašiusiojo asmens sertifikatas, o sertifikatų seką sudarančių CA sertifikatus ir jų CRL sąrašų duomenis saugoti kur nors kitur centrinėje vietoje. Atminties taupymo prasme taip yra efektyviau, kai el. parašai yra gaunami iš daugelio asmenų, kuriems sertifikatus yra sudaręs tas pats CA.

Parašo tikrintojams gali prireikti įrodymų, kad sertifikatų sekos sertifikatai ir CRL sąrašų informacija ES-X parašo kūrimo metu buvo galiojanti. Tam gali tekti naudoti papildomas laiko žymas.

El. parašo technologijoje naudojami algoritmai ir šifravimo raktai gali pasidaryti nesaugūs. Gali pasibaigti laiko žymų tarnybų (TSA) sertifikatų galiojimo terminai. Todėl laiko žymos gali būti dedamos surinkus visą parašo patvirtinimo duomenų komplektą. Pakartotinai laiko žymos gali būti dedamos, kai tik parašo patvirtinimo duomenys tampa pažeidžiami. Tokiu būdu el. parašo patvirtinimo duomenys gali turėti įdėtines laiko žymas.

### 11.2.4. Tikrinimo proceso taisyklės

Kvalifikuotas el. parašas laikomas galiojančiu, jei:

- jame yra parašo taisyklių nustatytas pasirašomų atributų rinkinys;
- jame yra tinkami el. parašo patvirtinimo duomenys, kaip CA sertifikatų duomenys, CRL sąrašų informacija, laiko žyma (tai asmens nepasirašomi atributai, juos pasirašo atitinkami sertifikavimo paslaugų teikėjai);
- tikrinimas atliekamas patikima parašo tikrinimo sistema.

#### *11.2.4.1. Pasirašančiojo asmens sertifikatas*

Yra leistini tokie el. parašai ir pasirašančiųjų asmenų sertifikatų reikalavimai:

- kvalifikuoti el. parašai. Juos kuriantys asmenys turi turėti kvalifikuotus sertifikatus ir naudoti saugią parašo formavimo įrangą (SSCD). Sertifikato išplėtimų lauke turi būti nurodytos atitinkamos sertifikato taisyklės ir kad sertifikatas yra kvalifikuotas, ir asmuo turi naudoti SSCD. Tokius reikalavimus atitinka, pavyzdžiui, ETSI 101 456 standarte [1] apibrėžtos sertifikato taisyklės "*QCP public+SSCD*";
- kvalifikuotais sertifikatais paremti el. parašai. Tokių parašų kūrėjai turi turėti kvalifikuotus sertifikatus, o SSCD naudojimas neprivalomas *(*sertifikato taisyklės *"QCP public");*
- el. parašai. Jais pasirašantys asmenys gali turėti paprastus sertifikatus ir nebūtinai naudoti SSCD.

#### *11.2.4.2. Sertifikatų sekos sužinojimas ir tikrinimas*

El. parašo galiojimui patvirtinti sertifikatų tikrinimas gali turėti apribojimus, nustatytus parašo taisyklėse. Tai patikimų taškų ir sertifikatų sekos apribojimų kombinacija.

**Sertifikatų seka** (*certification path*) – pasirašančiojo asmens parašą patvirtinančių sertifikatų eilė, susidedanti iš pasirašančiojo asmens sertifikato, pastarąjį sertifikatą sudariusio CA sertifikato ir kitų (arba nė vieno) tokiu būdu susijusių CA sertifikatų, pasibaigiantis CA, kuris pats sau sudaro sertifikatą, sertifikatu;

**Patikimi taškai** – tai CA, kurie sertifikatus sau sudaro patys (*root* CA). Jei vienas iš patikimų taškų yra keičiamas, turi būti išleidžiama nauja parašo taisyklių versija. Parašo galiojimui patvirtinti būtina, kad egzistuotų sertifikatų seka nuo CA, sudariusio pasirašančiojo asmens sertifikatą, iki vieno iš patikimų taškų, nurodytų parašo taisyklėse.

Parašo galiojimui patvirtinti būtina atsižvelgti į bet kokius sertifikatų tikrinimo apribojimus sertifikatų sekoje. Svarbiausi yra sertifikato taisyklėse išdėstyti apribojimai ir vardų apribojimai:

- sertifikato taisyklės apriboja sertifikatų seką nuo pasirašančiojo asmens sertifikato iki patikimo taško sertifikato;
- vardų apribojimai – tai vardų formos apribojimai.

Vardų apribojimai yra ypač svarbūs, kai parašo taisyklėse nurodoma daugiau kaip vienas patikimas taškas. Šiuo atveju konkretaus patikimo

taško sertifikatas gali būti naudojamas tikrinti tik atitinkamų pasirašančiųjų asmenų parašus.

Sertifikato taisyklių apribojimus yra lengviau apdoroti, bet tam sertifikatų sekos sertifikatuose turi būti nuorodyti sertifikato taisyklių identifikatoriai.

Bendruoju atveju sertifikatų sekos apdorojimas prasideda nuo vieno iš parašo taisyklėse nurodytų patikimų taškų ir baigiasi pasirašančiojo asmens sertifikatu.

Parašo taisyklėse apibrėžiami šie sertifikatų sekos klausimai:

- sertifikatų sekos CA, sudariusio sau sertifikatą, nuoroda;
- leistinas sertifikatų sekos ilgis;
- taikytinos sertifikato taisyklės;
- reikalavimai CA vardams (internetiniams adresams);
- kitos sąlygos sertifikatų sekai.

#### *11.2.4.3. CRL sąrašų informacijos naudojimas*

Parašo taisyklės apibrėžia CRL sąrašais ir/arba tiesioginės prieigos protokolu (OCSP) gaunamos sertifikatų statuso informacijos naudojimo tvarką sertifikatų galiojimui patikrinti.

Tikrintojas gali pasiremti pasirašiusio asmens sertifikate esančia informacija, spręsdamas, kaip geriausia būtų gauti ir patikrinti sertifikato galiojimo statuso informaciją.

Tikrintojas turi būti tikras, kad pasirašymo metu privatųjį raktą turėjo tik teisėtas jo savininkas. Tačiau yra neišvengiamas užlaikymas tarp rakto kompromitacijos (pametimo, pavogimo, kt.) pastebėjimo ir pranešimo apie rakto (t. y. atitinkamo sertifikato) atšaukimą išplatinimo. Pasitikėjimui parašu padidinti parašo taisyklėse turi būti nustatytas *atidėjimo periodas*, tik praėjus kuriam parašas gali būti tikrinamas. Tikrintojas turi palaukti šį laiką iki kreipimosi sertifikato statuso informacijai gauti.

Tikrintojas turi atkreipti ypatingą dėmesį į tokią situaciją:

- ***t1*** yra pasirašančiojo asmens nurodytas parašo sukūrimo laikas;
- laiku ***t2*** sukuriama parašo laiko žyma, kur ***t2*** yra vėlesnis už ***t1***;
- atidėjimo periodas pridedamas prie laiko ***t2*** ir jis baigiasi laiku ***t3***;
- sertifikato galiojimas panaikinamas laiku ***t4***, kas gali būti anksčiau arba vėliau už ***t3***;
- pirmasis parašo tikrinimas atliekamas laiku ***t5***, kuris negali būti ankstesnis už ***t3.***

Jei sertifikato galiojimas buvo panaikintas iki ***t3*** laiko, tai tikrinamasis parašas yra negaliojantis. Jei sertifikato galiojimas buvo panaikintas po ***t3*** laiko, tai parašas yra galiojantis [13].

Jei pasirašančiojo asmens sertifikatas buvo atšauktas ir tikrintojas neturi įrodymų, kad buvo sukurta parašo laiko žyma, parašas negali būti laikomas galiojančiu.

#### *11.2.4.4. Laiko žymų arba laiko markerių naudojimas*

Naudojant laiko žymas, turi būti laikomasi šių taisyklių. Nuo pasirašymo momento, kurio laiką pasirašantysis asmuo nurodo paraše, iki parašo laiko žymos sukūrimo praeina kažkiek laiko. Kuo šis laikas yra ilgesnis, tuo didesnė rizika, kad parašas bus negaliojantis pasirašančiajam asmeniui praradus privatųjį raktą (parašo formavimo duomenis) arba tyčia nutraukus sertifikato galiojimą. Parašo taisyklėse turi būti nustatytas maksimalus skirtumas (užlaikymas) tarp pasirašančiojo asmens nurodomo pasirašymo laiko ir laiko žymoje esančio laiko. Jei užlaikymo trukmė nenurodoma, tai parašo laiko žyma turi būti sukurta ne vėliau kaip sertifikato galiojimo pabaigos terminas.

TSA kiekvieną sukurtą laiko žymą pasirašo savo el. parašu. TSA sertifikatui patikrinti, kaip ir kitų pasirašančiųjų asmenų atveju, taip pat yra sertifikatų seka su savo patikimais taškais ir apribojimais.

#### *11.2.4.5. Apribojimai algoritmams ir raktų ilgiams*

Parašo taisyklėse gali būti nustatyti parašo kūrimo algoritmai (santraukos, šifravimo, kt.) ir leistini minimalūs raktų ilgiai. Juos gali naudoti:

- pasirašantieji asmenys, kurdami parašus;
- CA, pasirašydami asmenims arba kitiems CA sudaromus sertifikatus;
- paslaugų teikėjai, pasirašydami sudaromus parašo atributų (pvz., pasirašančiojo asmens pareigų) sertifikatus;
- laiko žymų teikėjai (TSA), pasirašydami žymas.

#### *11.2.4.6. Pasirašančiųjų asmenų pareigų tikrinimas*

El. parašuose gali būti nurodomos pasirašančiojo asmens pareigos (rolė). Galimi du jų nurodymo būdai: pasirašantysis asmuo laisvai nurodo pareigas arba nurodomas sertifikatas, liudijantis pasirašančiojo asmens pareigas, t. y. *pareigų sertifikatas*.

Pareigos gali būti vienu iš parašo informacijos elementų (atributų). Gali būti tokie sertifikavimo paslaugų teikėjai, kurie sudaro parašo atributų sertifikatus (šiuo atveju – pareigų sertifikatus).

Mašininiam parašo tikrinimui svarbu, kad pasirašančiųjų asmenų pareigos būtų užkoduotos mašinai suprantamu pavidalu.

Jei parašo taisyklės reikalauja nurodyti paraše pasirašančiojo asmens pareigų sertifikatą, tai tikrinant parašą būtina tikrinti ir šį sertifikatą bei jį sudariusį sertifikavimo paslaugų teikėją (**AA** - *Attribute Authority*). Patikimų taškų išvardinimas ir apribojimai parašo atributų sertifikatų teikėjams (AA) gali būti taikomi lygiai taip pat, kaip ir CA ar TSA.

#### *11.2.4.7. Kitos parašo taisyklių nuostatos*

Parašo taisyklėse gali būti papildomi reikalavimai, pavyzdžiui, susiję su pasirašančiojo asmens pasirašymo aplinka. Šie reikalavimai turi būti pateikti žmogui suprantama forma ir mašininiam apdorojimui tinkama forma.

### 11.2.5. Vėlesniojo tikrinimo duomenys

Parašui patikrinti prabėgus daug metų po jo sukūrimo tikrintojas privalo vienareikšmiškai sužinoti pasirašiusio asmens naudotas parašo taisykles. Tai gali būti atlikta pasinaudojus paraše esančia parašo taisyklių nuoroda arba, nesant jos, remiantis pasirašytų duomenų tipu. Toliau tikrintojas privalo gauti parašo taisykles ir įsitikinti, kad jos atitinka tikrinančiojo poreikius.

Vėlesnysis tikrinimas reikalauja, kad parašo tikrinimo sistema (techninė ir programinė įranga) būtų pajėgi apdoroti:

- parašo taisykles;
- pasirašytus duomenis (tai pasirašančiojo asmens parengti duomenys);
- tų duomenų el. parašą;
- kitus el. parašo patvirtinimo duomenis.

Vėlesnysis tikrinimas yra panašus į pirmąjį tikrinimą, išskyrus tai, kad jau yra visi patvirtinimo duomenys. Ypatingai svarbu yra nustatyti, ar pasirašančiojo asmens sertifikatas ir parašo informacijos elementų (parašo atributų) sertifikatai buvo galiojantys tuo metu, kai buvo kuriamas parašas. Todėl paraše turi būti laiko žyma.

Laiko žyma tiksliai nenurodo, kada buvo sukurtas parašas. Tai galima nustatyti nebent remiantis paraše paties pasirašančiojo asmens nurodytu parašo sukūrimo laiku. Parašo taisyklėse gali būti nustatyta, kad laikas parašo laiko žymoje turi būti pakankamai arti laiko, kurį pasirašantysis asmuo nurodo paraše. “Pakankamai arti” gali būti kelios minutės, valandos ar net dienos, t. y. kaip nurodyta parašo taisyklėse.

### 11.2.6. Vėlesniojo tikrinimo rezultatai

Vėlesnysis tikrinimas atliekamas laikantis parašo taisyklių. Vienintelis tokio tikrinimo rezultatas – parašo tikrinimo statusas, kuris gali būti dvejopas:

- tikrinimas sėmingas, t. y. parašas atitiko visus parašo taisyklių reikalavimus ir yra galiojantis;
- tikrinimas nesėkmingas, t. y. parašas neatitiko parašo taisyklių reikalavimų ir yra negaliojantis.

## 11.3. Parašo tikrinimo sistemos

### 11.3.1. Pirmojo tikrinimo sistema

Pirmojo tikrinimo sistemoje (techninėje ir programinėje įrangoje) turi būti [13]:

a) saugus parašo tikrinimo procesas (nustatyta veiksmų seka);

b) vartotojo sąsaja (interfeisas) paimti pasirašytiems duomenims ir pasirinkti norimą tikrinti parašą (pasirašytuose duomenyse gali būti keli parašai);

c) sąsaja tikrinimo laikui gauti;

d) vartotojo sąsaja pasirašytiems duomenims (tekstui, garsui, vaizdui) pavaizduoti reikiamu formatu;

e) vartotojo sąsaja parašo taisyklėms pasižiūrėti;

f) vartotojo sąsaja informacijai apie pasirašiusįjį asmenį ir parašo tikrinimo statusą (parašas galioja ar ne) gauti;

g) galima vartotojo sąsaja el. parašui užrašyti į audito duomenų bazę, kurią tvarko nepriklausomas sertifikavimo paslaugų teikėjas;

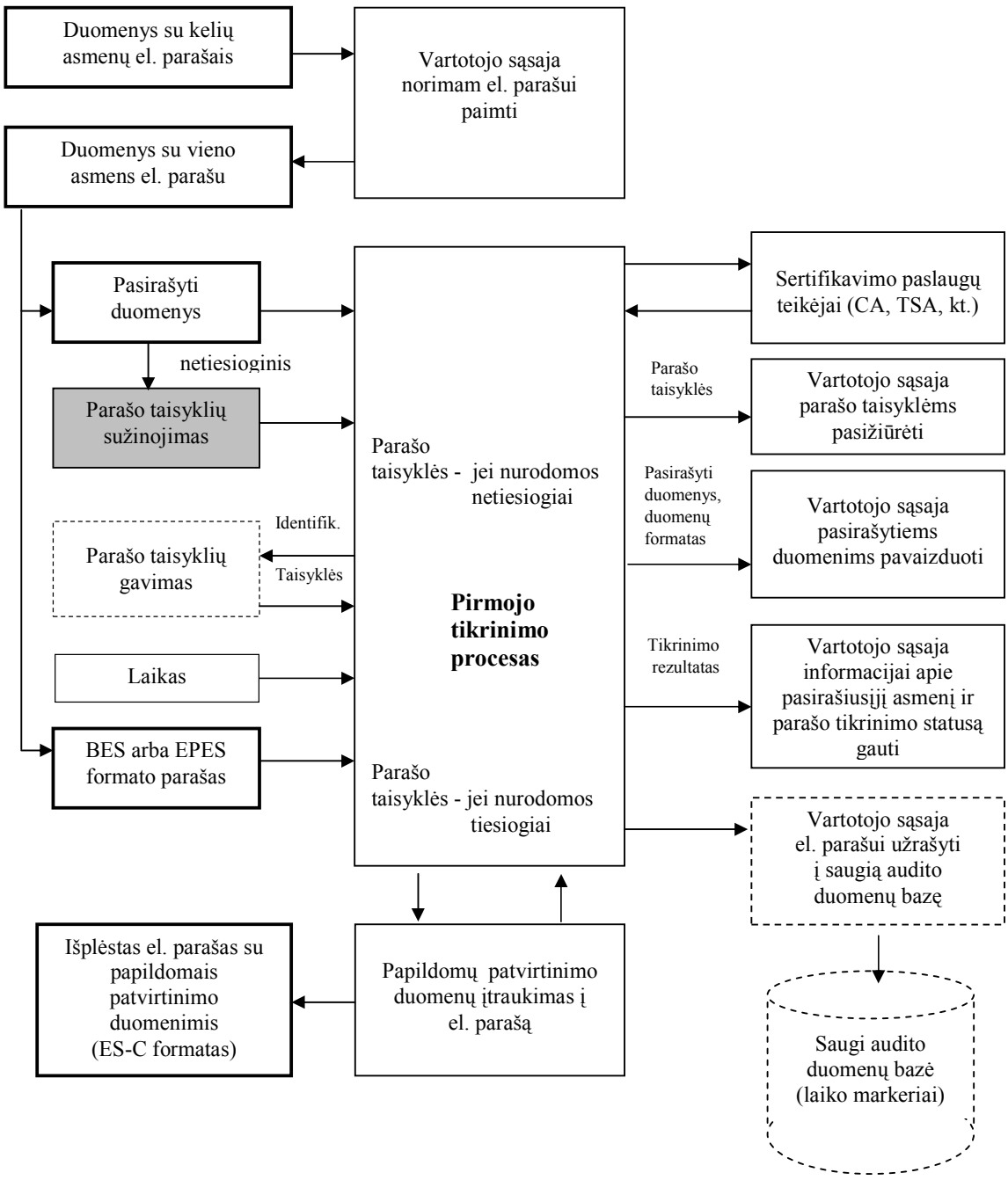
h) vartotojo sąsaja su kompiuterių tinklu sertifikavimo paslaugų teikėjų (CA, CRL, OCSP, TSA, kt.) informacijai gauti, jei jos nebūna pateikęs pasirašantysis asmuo;

i) galima vartotojo sąsaja parašo taisyklėms gauti.

11.1 pav. parodyta el. parašo pirmojo tikrinimo sistemos schema.

Jei parašo taisyklės yra nurodomos netiesiogiai, t. y. paraše nėra jų nuorodos, tuomet parašo taisyklės pirmajam tikrinimui gaunamos ne pirmojo tikrinimo sistemos priemonėmis.

Jei vietoje laiko žymų yra naudojami laiko markeriai, tai turi būti paslaugų teikėjas, įgaliotas kaupti ir saugoti el. parašus patikimoje audito duomenų bazėje.




11.1 pav. El. parašo pirmojo tikrinimo sistemos schema [13]

### 11.3.2. Vėlesniojo tikrinimo sistema

Vėlesniojo tikrinimo sistemoje (techninėje ir programinėje įrangoje) turi būti [13]:

a) saugus parašo tikrinimo procesas (nustatyta veiksmų seka);

b) vartotojo sąsaja (interfeisas) paimti pasirašytiems duomenims ir pasirinkti norimą tikrinti parašą (pasirašytuose duomenyse gali būti keli parašai);

c) sąsaja tikrinimo laikui gauti;

d) vartotojo sąsaja pasirašytiems duomenims (tekstui, garsui, vaizdui) pavaizduoti reikiamu formatu;

e) vartotojo sąsaja parašo taisyklėms pažiūrėti;

f) vartotojo sąsaja informacijai apie pasirašiusįjį asmenį ir parašo tikrinimo statusą (parašas galioja ar ne), kai pirmasis tikrinimas jau seniai būna atliktas, gauti;

g) galima vartotojo sąsaja el. parašo laiko markeriui gauti iš saugios audito duomenų bazės, kurią tvarko nepriklausomas sertifikavimo paslaugų teikėjas;

h) galima vartotojo sąsaja parašo taisyklėms gauti.

11.2 pav. parodyta el. parašo vėlesnio tikrinimo sistemos schema.

Jei parašo taisyklės yra nurodomos netiesiogiai, t. y. paraše nėra jų nuorodos, tuomet parašo taisyklės įprastam tikrinimui gaunamos ne įprasto tikrinimo sistemos priemonėmis.

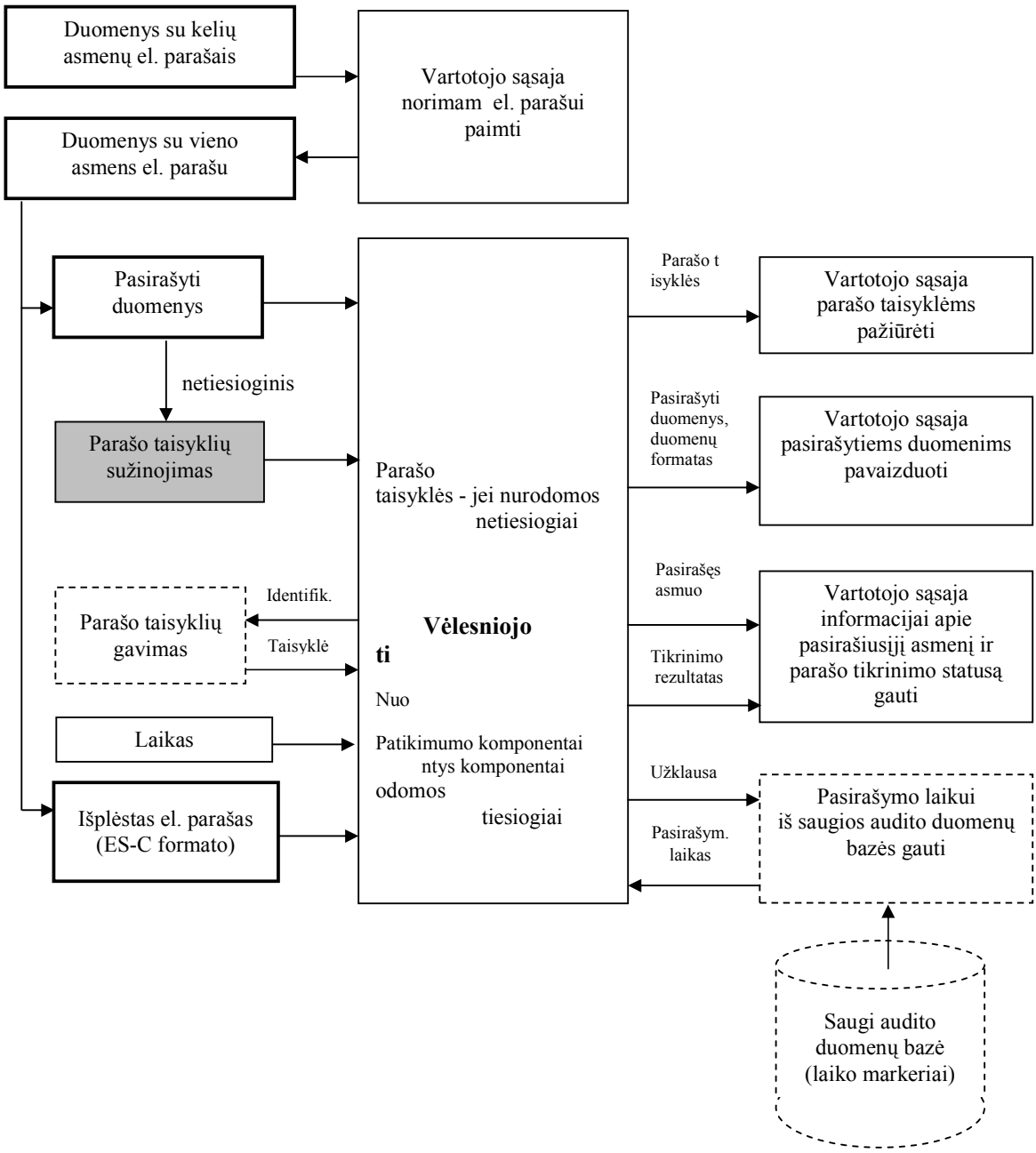
Jei pasirašytų duomenų el. paraše yra naudojamas laiko markeris vietoje laiko žymos, tai reikalinga vartotojo sąsaja duomenų pasirašymo laikui gauti iš patikimos audito duomenų bazės.

### 11.3.3. Parašo tikrintojai

Parašą gali tikrinti asmuo, kuriam yra adresuoti pasirašyti duomenys, mašina arba tretieji asmenys.

Kai parašą tikrina asmuo, jis turi turėti priemones (parašo tikrinimo sistemą), kurių pakeitimai po jų įkėlimo (instaliavimo) į kompiuterį turi būti pastebimi. Tarp tikrintojo ir kompiuterio turi būti šios vartotojo sąsajos:

- ♦ norimam elektroniniam parašui pasirinkti;
- ♦ parašo taisyklėms pažiūrėti;
- ♦ pasirašytiems duomenims pavaizduoti;
- ♦ informacijai apie pasirašiusįjį asmenį ir parašo tikrinimo statusą pavaizduoti;
- ♦ parašo patvirtinimo duomenims (pvz., sertifikatų duomenų, CRL informacijos, laiko žymų) gauti.




11.2 pav. El. parašo vėlesniojo tikrinimo sistemos schema [13]

Kai parašą tikrina mašina, nėra jokių vartotojo sąsajos reikalavimų. Parašas yra tikrinamas nedalyvaujant žmogui. Patikrinimo rezultatai fiksuojami, kad juos bet kada vėliau galėtų peržiūrėti žmogus.

Parašus gali tikrinti ir tretieji asmenys. Tai gali būti kaip paslauga, išlaisvinanti parašo naudotojus nuo gana sudėtingo tikrinimo proceso.

## 11.4. Parašo tikrinimo aplinkos

Parašai gali būti tikrinami namų aplinkoje, įstaigoje, viešosiose vietose ir mobilioje aplinkoje. Keliai priimtinam tikrinimo patikimumo lygiui užtikrinti yra nevienodi. Bendruoju atveju saugumą užtikrina techninių, procedūrinių ir organizacinių priemonių visuma. Kiekvienai iš aplinkų minėtų priemonių svoris yra nevienodas.

### 11.4.1. Namų aplinka

Privačiai parašo naudotojų aplinkai yra teikiama patikima įranga, kurią išimtinai prižiūri privatus asmuo, ir ja naudojasi nedidelė vienas kitu pasitikinčių žmonių grupė. Gali būti naudojama įvairi techninė įranga:

- asmeninis kompiuteris;
- interaktyvi televizija (*smart TV*);
- į kompiuterių tinklą įjungta įranga;
- asmeninis skaitmeninis asistentas (*PDA – Personal Digital Assist.*);
- interneto telefonas (*Internet Phone* ).

Parašo tikrinimo programinė įranga yra naudojama ir gyvuoja greta kitos programinės įrangos (operacinės sistemos, taikomųjų programų). Turi būti garantuojama, kad ta kita programinė įranga negali piktavališkai įsiterpti į parašų tikrinimo programinės įrangos darbą.

Parašo tikrinimo programinę įrangą parašo naudotojas gali būti iš anksto įkėlęs (instaliavęs) į savo kompiuterį arba ji įkeliama tik tuomet, kai jos prireikia. Abiem atvejais parašo naudotojai turi pasitikėti šios programinės įrangos teikėju.

Jei naudojama iš anksto įkelta parašo tikrinimo programinė įranga, tai ji turi būti gauta iš patikimo pardavėjo tam tikros formos paketu. Ant paketo(ų) aiškiai turi būti nurodytos įrangos charakteristikos, ypač:

- parašo formatas, kurį palaiko įranga;
- parašo taisyklės, kurias palaiko įranga;
- duomenų formatai, kuriuos įranga gali pavaizduoti.

Pirmos dvi charakteristikos gali būti sujungtos į vieną, tačiau trečioji turi būti nurodoma atskirai, kad ją galima būtų atnaujinti (išplėsti) naujais duomenų formatais.

Paketai taip pat turi turėti aiškias žymes (*logo*).

Parašo tikrinimo programinės įrangos įkėlimo į kompiuterį saugumo lygiui padidinti, parašo tikrinimo programinė įranga gali būti pasirašyta gamintojo el. parašu.

Jei parašo tikrinimo programinė įranga įkeliama į kompiuterį tik tuomet, kai jos prireikia, tai įranga turi būti pasirašyta gamintojo el. parašu ir įkeliama vėliausia įrangos versija. Įkėlimo proceso saugumui užtikrinti naudojamas gamintojo viešasis raktas, kuris pateikiamas kartu su įranga arba parašo naudotojas būna jau užfiksavęs jį.

Kadangi parašo naudotojas tiesiogiai dalyvauja programinės įrangos įkėlimo procese, jis yra atsakingas už šių procedūrų korektišką atlikimą.

Parašo naudotojas turi pasirūpinti, kad niekas negalėtų modifikuoti įkeltos į jo kompiuterį parašo tikrinimo programinės įrangos to nepastebint. Tai galima pasiekti tik fizinėmis saugos priemonėmis (pvz., užrakinant kabineto duris) arba naudojant fizinių saugos priemonių ir atitinkamos programinės įrangos (pvz., pradinės įkrovos (*boot*) apsaugos, priešvirusinės, kietojo disko užšifravimo) kombinaciją.

### 11.4.2. Įstaigos aplinka

Įstaigose (organizacijose) už adekvačių parašo tikrinimo priemonių pateikimą savo darbuotojams kasdieniniam naudojimui yra atsakinga pati įstaiga. Gali būti naudojama įvairi techninė įranga:

- ♦ asmeninis kompiuteris;
- ♦ nešiojamasis kompiuteris (*laptop*);
- ♦ asmeninis skaitmeninis asistentas;
- ♦ mobilusis telefonas.

Parašo tikrinimo programinę įrangą iš anksto įkelti į asmenų technines priemones (pvz., kompiuterius, mobiliuosius telefonus) gali tik įstaigos įgalioti žmonės. Šią programinę įrangą gali įsikelti ir patys asmenys kiekvieną kartą, kai tik jos prireikia.

Jei naudojama iš anksto įkelta parašo tikrinimo programinė įranga, tai organizacija turi pasitikėti šaltiniu, iš kur ši įranga yra gauta. Įranga turi būti gauta iš patikimo pardavėjo tam tikros formos paketu. Ant paketo(ų) aiškiai turi būti nurodytos įrangos charakteristikos, ypač:

- ♦ parašo formatas, kurį palaiko įranga;
- ♦ parašo taisyklės, kurias palaiko įranga;
- ♦ duomenų formatai, kuriuos įranga gali pavaizduoti.

Paketai taip pat turi turėti aiškias žymes (*logo*).

Įstaigos įgalioti žmonės parašo tikrinimo programinę įrangą gali įkelti į kompiuterį dirbdami kiekvieno pasirašančiojo asmens darbo vietoje, imdami

šią programinę įrangą iš patikimo įstaigos serverio, arba tai atlikti iš nutolusios darbo vietos (*remotely*).

Kai parašo tikrinimo programinė įranga įkeliama į kompiuterį, kiekvieną kartą jos prireikus, asmuo turi pasitikėti iš išorės pateikiama programine įranga. Programinė įranga turi būti pasirašyta gamintojo el. parašu ir pateikiama vėliausia jos versija. Įkėlimo proceso saugumui užtikrinti yra naudojamas gamintojo viešasis raktas, kuris pateikiamas kartu su programine įranga arba įstaigos įgaliotas asmuo būna vieną kartą užfiksavęs šį raktą asmens kompiuteryje.

Kadangi asmuo tiesiogiai nedalyvauja įkraunant parašo tikrinimo programinę įrangą, jis nėra tiesiogiai atsakingas už įkrovimo procedūros korektišką atlikimą.

Įkrovusi parašo tikrinimo programinę įrangą savo darbuotojams, įstaiga turi pasirūpinti, kad niekas negalėtų jos modifikuoti to nepastebint. Tai galima pasiekti naudojant fizinių saugos priemonių ir atitinkamos programinės įrangos (pvz., pradinės įkrovos (*boot*) apsaugos, priešvirusinės, kietojo disko užšifravimo) kombinaciją.

### 11.4.3. Viešosios vietos

Už parašo tikrinimo sistemos viešojoje vietoje patikimumą yra atsakinga organizacija, kuriai nuosavybės teise priklauso ši sistema. Gali būti tokie taškai viešosiose vietose:

- ♦ mažmeninės prekybos taškas (*POS – retail Point-of-Sale*);
- ♦ automatinis kasininkas (*ATM – Automated Teller Machine*);
- ♦ viešųjų paslaugų taškas.

Už sistemos įrengimą yra atsakinga organizacija, kuriai nuosavybės teise priklauso sistema. Ant sistemos turi būti aiškiai užrašyti tos organizacijos pavadinimas ir adresas, o ryšiui su organizacija užmegzti - telefono numeris, pašto adresas, el. pašto adresas arba WWW adresas. Organizacija privalo užtikrinti, kad niekas negalėtų modifikuoti instaliuotos įrangos be prižiūrėtojų žinios.

Parašo tikrinimo sistemos turi būti įrengiamos tokiose vietose, kur būtų sunku nepastebėtam instaliuoti suklastotą sistemą.

Vartotojai apie parašo tikrinimo sistemas viešosiose vietose turėtų būti informuojami individualiai arba skelbiant spaudoje.

### 11.4.4. Mobilioji aplinka

Mobilioji aplinka sukuriama naudojant kai kuriuos jau minėtus namų ar įstaigos aplinkos įrenginius, pavyzdžiui, nešiojamąjį kompiuterį (*laptop*), kaip pavienį įrenginį, prijungtą prie telefoninės ryšio linijos. Kai kurie pavieniai įrenginiai, kaip mobilusis telefonas, paprastai naudojami tik

prisijungus prie tinklo. Vartotojas pasitiki privačiu įrenginiu todėl, kad, visų pirma, gamintojas garantuoja už teikiamo įrenginio savybes, o, antra, įreginį kontroliuoja tik vartotojas, kuris žino specifinius duomenis, saugomus, pavyzdžiui, SIM kortelėje.

Parašo tikrinimo programinę įrangą iš anksto įkelti į mobilųjį įrenginį gali įrenginio gamintojas arba įrenginio vartotojas. Vartotojas gali įkėlinėti šią programinę įrangą ir kiekvieną kartą, kai tik jam jos prireikia.

Kiekvieną kartą įkeliamą parašo tikrinimo programinę įrangą turi pateikti telefonų kompanija. Įkrovimo saugumą užtikrina ryšio protokolas tarp mobilaus įrenginio ir telefonų tinklo.

Programinės įrangos autentiškumui nustatyti turi būti naudojami kontroliniai duomenys (programinės įrangos santrauka-*hash*). Juos vartotojas rankiniu būdu gali būti įkėlęs į mobilųjį įrenginį. Tai atliekama gavus informaciją iš tam tikros vietos. Vėliau kiekvieną kartą įkeliamos programinės įrangos santrauka palyginama su santrauka, kuri buvo įkelta nesinaudojant radijo bangų ryšiu. Minėtus kontrolinius duomenis įkelti į mobilų įrenginį gali ir gamintojas, įrašydamas juos į SIM ar WIM kortelę.

Parašo tikrinimo programinė įranga, kuri į mobilų įrenginį įkeliama pastoviai arba įkeliama kiekvieną kartą, kai jos prireikia, turi turėti parašo taisyklių šaltinio autentiškumo patvirtinimo savybę.

## 11.5. Teisiniai aspektai

### 11.5.1. Teisinis techniškai korektiško parašo negaliojimas

Pagal Lietuvos Respublikos elektroninio parašo įstatymą (Žin., 2000, Nr. 61-1827) saugus el. parašas, sukurtas saugia parašo formavimo įranga ir patvirtintas galiojančiu sertifikatu, el. duomenims turi tokią pat teisinę galią kaip parašas rašytiniuose dokumentuose ir yra leistinas kaip įrodinėjimo priemonė teisme. Tokie parašai turi būti techniškai korektiški, t. y. turi būti korektiškas skaitmeninis parašas, korektiška sertifikatų seka, nė vienas šios sekos sertifikatas neturi būti atšauktas, t. t. Tačiau yra atvejai, kai pasirašančiajam asmeniui priskirtinas parašas gali būti užginčytas (laikomas negaliojančiu).

Ginčų atveju sprendimą dėl techniškai korektiško parašo negaliojimo teisėjas gali priimti papildomai išsiaiškinęs pasirašymo sąlygas arba operacijos (transakcijos) tipą. Šios aplinkybės nebūtinai gali būti susijusios su iš anksto nustatytais parašo techniniais standartais. Jos gali priklausyti nuo tokių ginčytinų veiksnių, kaip taikymo sritis, operacijos tipas, naudojimo sąlygų, sandorių praktikos, t. t.

Parašas gali būti laikomas galiojančiu (teismo sprendime) tik įvertinus parašo pripažinimą trukdančias aplinkybes, kurios gali būti susijusios su pasirašančiuoju asmeniu, parašo paskirties tipu, nustatytu parašo taisyklėse, arba parašų kiekiu ir jų eilės tvarka, nustatyta įstatymuose tam tikroms operacijoms (transakcijoms).

Su pasirašančiuoju asmeniu susijusios trukdančios aplinkybės yra tokios: pasirašantysis asmuo veikė per prievartą (pasirašė grasinant), yra ribotų protinių sugebėjimų (t. y. nepajėgia suvokti sandorio) arba asmuo gali įrodyti, kad duomenys pasirašymui buvo pateikti neteisingai, pavyzdžiui, jo naudojama peržiūros programa (*browser*) negalėjo perskaityti visų pasirašomų duomenų, buvo paslėpto teksto. Remdamasis teisės aktais, asmuo, kuris paskelbė savo norus kitos arba trečiosios šalies verčiamas neteisėtu arba moralei prieštaraujančiu būdu, gali reikalauti anuliuoti tokią operaciją.

Su parašo taisyklėse nustatytomis pasirašančiojo pareigomis (parašo tipu) susijusios trukdančios aplinkybės yra tos, kai parašo taisyklės, kurias leidžiama naudoti tik tam tikroje srityje (pvz., automobilių nuoma), buvo panaudotos pasirašant kitos srities sutartį (pvz., nekilnojamojo turto sandorį).

Dar viena trukdanti aplinkybė yra ta, kai trūksta vieno parašo, o jų lygiagrečiai turėtų būti daugiau kaip vienas. Pvz., teisės aktai gali reikalauti, kad mokestiniai pavedimai, kurių suma viršija nustatytą dydį, yra laikomi teisėtais, jei juos pasirašė buhalteris ir įstaigos vadovas.

Trukdanti aplinkybė, susijusi su vienas į kitą įterpiamų (*embedded*) parašų eilės tvarkos pažeidimu, gali atsirasti specifiniame teisiniame kontekste nustatant operacijos teisėtumą (pvz., nekilnojamojo turto sandoris). Notaras sandorį turi patvirtinti savo el. parašu tik tuomet, kai sandorį jau yra pasirašę pirkėjas ir pardavėjas. Sandoris turi būti anuliuotas, jei trijų techniškai korektiškų parašų eilės tvarka yra klaidinga.

Atkreiptinas dėmesys į tam tikro tipo sandorius. Jei teisės aktai reikalauja, kad aukštesnio patikimumo sumetimais kažkokie sandoriai turi būti pasirašomi ranka rašytu parašu, tai jie neturėtų būti sudaromi elektroniniu būdu, pasirašant el. parašu. Techniškai korektiškas el. parašas tokiu atveju turėtų būti laikomas negaliojančiu.

### 11.5.2. Rizika, susijusi su sertifikatų atšaukimu

Dėl pasirašančiojo asmens sertifikato atšaukimo atsiranda tam tikra rizika, kuri pasiskirsto tarp pasirašančiojo asmens (sertifikato savininko) ir parašo tikrintojo (sertifikatu pasitikinčios šalies). Kai tik asmeniui iškyla

reikalas keisti savo sertifikato statusą (pvz., pametus, pavogus privatųjį raktą), jis privalo nedelsdamas informuoti sertifikatą sudariusį CA. CA per tam tikrą laiko tarpą turi pakeisti sertifikato statuso informaciją viešai prieinamose saugyklose, t. y. CRL sąraše ir tiesioginės prieigos sertifikatų statuso (*OCSP*) serveryje. CRL sąrašas yra atnaujinamas periodiškai, o tiesioginės prieigos sertifikatų statuso OCSP sistemos veikia reliame laike. Sertifikatų saugyklų naudojimo sąlygos yra nustatomos CA veiklos nuostatuose.

Sertifikatų statuso (galioja arba nebegalioja) informacija gali būti laikoma patikima, jei tikrinimas atliekamas tik praėjus atidėjimo periodui. Atidėjimo periodas nustatomas parašo taisyklėse. Jei sertifikatas buvo atšauktas praėjus nustatytam atidėjimo periodui, pasirašantysis asmuo gali atsakyti tik už kokius nors nuostolius, atsiradusius iki sertifikato atšaukimo paskelbimo.

Jeigu atidėjimo periodas parašo taisyklėse nėra apibrėžtas, tikrintojas turi remtis CA sertifikavimo veiklos nuostatuose (CPS) nurodytomis sertifikato taisyklėmis, atitinkančiomis pasirašančiojo asmens sertifikatą. Prieš tikrinimą jis turi pridėti maksimalų laiką, kurio reikia CA asmens sertifikatui atšaukti, prie maksimalaus laiko, kurio reikia asmeniui pranešti apie įvykusią jo privačiojo rakto kompromitaciją.

Jei tokios informacijos nėra, tikrinimo rezultatai negali būti patikimi. Atitinkamai tokio tikrinimo statusas yra *nebaigtas*, paliekant tikrintojui riziką priimti ar atmesti el. parašą.

Pasirašantieji asmenys yra susiję su nuostolių rizika, jei CA išsigina atšaukęs sertifikatą, paprašius teisės to daryti neturinčiam asmeniui. Tokiai rizikai išvengti CA turi būt įdiegęs saugią infrastruktūrą ir užklausų kontrolės mechanizmą.

CA turi turėti patikimas priemones besikreipiančio asmens tapatybei nustatyti ir patikrinti, ar tas asmuo turi įgaliojimus kreiptis dėl sertifikato atšaukimo.

Pasirašantysis asmuo taip pat yra susijęs su nuostolių rizika, kai CA neatšaukia sertifikato per nustatytą laiką.

Su sertifikatų atšaukimu viešųjų raktų infrastruktūroje (PKI) susijusiems teisinės atsakomybės neapibrėžtumams valdyti siūloma naudoti privačiosios teisės mechanizmą, kaip nesutartinių įsipareigojimų (*non-contractual disclaimers*) pasirašymą, sutartines priemones rizikai ir draudimui tarp sandorio šalių paskirstyti, naujų teisės aktų kūrimą.

### 11.5.3. Ginčų sprendimas

Su el. parašais susiję teisiniai ginčai gali kilti tada, kai viena šalis bando įrodyti arba paneigti sandorio egzistavimą. Tokiu atveju visų pirma būtina patikrinti, ar pasirašančiojo asmens sertifikatas galiojo pasirašymo metu.

Jei pasirašančiojo asmens privatusis raktas buvo sukompromituotas (pvz., pamestas, pavogtas), to asmens sertifikato atšaukimo laikas turi būti palyginamas su parašo laiko žymoje esančiu laiku.

Pirma, jei parašo laiko žymoje nurodytas laikas yra ankstesnis už sertifikato atšaukimo laiką, reiškia, kad buvo pasirašyta iki sertifikato atšaukimo, ir todėl parašas yra galiojantis. Priešingu atveju parašas yra negaliojantis.

Antra, turi būti atsižvelgta į atidėjimo periodą, leistiną tarp prašymo atšaukti sertifikatą pateikimo ir informacijos apie sertifikato atšaukimą paskelbimo. Tai reiškia, kad skirtumas tarp žymoje nurodyto laiko ir sertifikato atšaukimo laiko turi būti didesnis už atidėjimo periodą. Jei šis skirtumas yra mažesnis arba laiko žymos iš viso nėra, parašas yra negaliojantis.

Tuo atveju, kai pasirašančiojo asmens privatusis raktas nebuvo sukompromituotas iki sertifikate nurodyto sertifikato galiojimo pabaigos termino, būtina įrodyti, kad parašas buvo sukurtas iki sertifikato galiojimo pabaigos termino.

Šių klausimų sprendimas yra sudėtingas, todėl siūloma spręsti ginčus betarpiškai. Svarbi aplinkybė sprendžiant ginčus yra pasirašančiojo asmens gyvenamoji vieta ir tos vietos jurisdikcija (skirtingų valstybių, valstijų, žemių ar kt. teisės normos gali skirtis).

# 12. PASLAUGŲ IR ĮRANGOS ATITIKTIES VERTINIMAS

## 12.1. Sertifikatų centrų (CA) atitikties reikalavimams vertinimas

Visų CA atitiktis turi būti įvertinta pagal CWA 14172-2 vadovą [15]. Šis vadovas reikalauja vertinti kvalifikuotus sertifikatus sudarančius CA pagal Europos standarto ETSI TS 101 456 reikalavimus [1] (Lietuvoje šis standartas įteisintas kaip LST ETSI TS 101 456 v1.2.1:2002 "Strateginiai reikalavimai, keliami kvalifikuotus sertifikatus išduodantiems sertifikavimo paslaugų teikėjams" standartas).

### 12.1.1. Sertifikatų centrų (CA) atsakomybė

ETSI TS 101 456 standartas [1] apibrėžia reikalavimus kvalifikuotus sertifikatus sudarantiems CA. Už teikiamų paslaugų pažeidimus CA atsako pagal įstatymus. CA turi savo privatųjį šifravimo raktą, kuriuo jis pasirašo visus savo klientams sudarytus sertifikatus. Sertifikate turi būti įvardintas CA, sudaręs tą sertifikatą.

CA gali pasitelkti subrangovus (trečiąsias šalis) paslaugoms teikti. Tačiau CA yra atsakingas už savo ir subrangovų teikiamas paslaugas ir turi užtikrinti, kad būtų laikomasi įstatymų, sertifikato taisyklių, sertifikavimo veiklos nuostatų.

### 12.1.2. Įvadas į CA atitikties nustatymą

ETSI TS 1010 456 standarto [1] reikalavimai apima tokias CA veiklos sritis, kaip sertifikatą norinčių gauti asmenų registracija ir jų tapatybės patikrinimas, sertifikatų sudarymas, sertifikatų duomenų teikimas parašų tikrintojams ir parašo formavimo įrangos rengimas pasirašantiems asmenims (jei CA imasi teikti tokią paslaugą). Taip pat reikalavimai apima CA veiklos valdymą, paslaugų teikimo patikimumą, personalo kvalifikaciją.

ETSI TS 1010 456 standartu gali naudotis nepriklausomos organizacijos, vertindamos CA atitiktį nustatytiems reikalavimams. Atitiktį vertinančios organizacijos turi viešai paskelbti išvadas apie CA atitiktį, tačiau CA vidinės veiklos bei saugumo informacija neturi būti platinama.

### 12.1.3. Reikalavimai atitiktį vertinančioms organizacijoms, vertintojams ar vertintojų grupėms

Organizacija, vertinanti CA atitiktį ETSI TS 101 456 standarto [1] reikalavimams, pati turi atitikti patikimumo ir kompetencijos EN 45000 serijos standartą.

Kiekvienas atitikties vertintojas:

a) privalo turėti išsilavinimą, kuris leistų adekvačiai elgtis atliekant visas šio darbo procedūras;

b) turi turėti ne mažesnę nei ketverių metų pilnu etatu praktinės veiklos patirtį informacinių technologijų srityje, iš jų, bent dvejus metus būtų dirbęs informacijos apsaugos ir/ar PKI srityje;

c) turi gerai žinoti standarto ETSI TS 101 456 reikalavimus;

d) turi išmanyti valdymo sistemų principus;

e) turi išmanyti informacijos apsaugos ir PKI klausimus;

f) turi suprasti atitikties įvertinimo riziką ir valdymo procesų įvertinimo riziką;

g) turi būti sėkmingai užbaigęs bent penkių dienų trukmės sistemų ir procesų vertinimo mokomąjį kursą;

h) turi pasižymėti šiomis asmeninėmis savybėmis: kritiškumu, analitiškumu, realistiškumu, nuoseklumu ir griežtumu;

i) turi turėti atitikties vertimo žinių bei praktinių įgūdžių;

j) privalo nuolat atnaujinti savo žinias informacinių sistemų saugumo, PKI bei valdymo sistemų vertinimo srityse;

k) turi būti atlikęs ne mažiau kaip keturis skirtingus atitikties vertinimus, kurių atlikimo bendra trukmė - 20 dienų. Šie atitikties vertinimai turi būti atlikti prižiūrint vadovaujančiam vertintojui (auditoriui) ir apimti dokumentų peržiūrą, vertinimo išvadų parengimą ir pristatymą;

l) atitikčiai įvertinti reikalingos žinios neturi būti pasenusios;

Atitikties vertintojų grupės vadovas papildomai turi:

m) būti atlikęs bent tris vertinimus jam vadovaujant;

n) turėti pakankamas žinias ir sugebėjimus valdyti vertinimo procesą;

o) turėti efektyvaus bendravimo žodžiu ir raštu įgūdžius.

Pastaba: Pradžioje visai realu, kad vertinimo organizacijos gali ir neturėti vertintojų, atitinkančių b), k) ir m) reikalavimus. Jeigu organizacija vis tik nori suformuoti minėtus kriterijus neatitinkančių vertintojų grupę, ji turėtų pasirūpinti raštiškais įrodymais apie vertintojų patirtį kitose artimose srityse.

CA atitikties vertintojai turi laikytis bent šių elgesio taisyklių ir moralės normų:

a) elgtis teisingai ir objektyviai organizacijos, kurioje jie dirba, ir CA, kurį jie tikrina, atžvilgiu;

b) elgtis nepriklausomai ir bešališkai; informuoti vertintojo organizaciją apie visus turimus ar turėtus ryšius su tikrinamu CA, apie visus galimus interesų konfliktus;

c) nepriimti jokių paskatinimų, dovanų, rinkliavų, nuolaidų ar kitų vertybių iš tikrinamo CA ar su juo susijusių asmenų;

d) neplatinti jokios informacijos ar atitikties vertinimo išvadų tretiesiems asmenims, išskyrus tuos, kuriuos raštiškai yra nurodę vertinamoji CA ir vertintojo organizacija;

e) nedaryti veiksmų, kurie galėtų pakenkti organizacijos, kuriai jie atstovauja, reputacijai;

f) įvykus bet kokiems elgesio taisyklių (kodekso) pažeidimams iki galo dalyvauti bet kokioje apklausos procedūroje;

Reikalavimai atitikties vertintojų grupei:

a) vertintojų grupėje turi būti bent vienas nepriklausomos organizacijos kriterijus atitinkantis vertintojas, kuris:

- galėtų vadovauti grupei;
- išmanytų sertifikavimo paslaugų ir informacijos saugumą reguliuojančius teisės aktus;
- išmanytų naujausius PKI techninius klausimus;
- mokėtų įvertinti su informacijos saugumu susijusią riziką, nustatyti priežastinį/pasekminį ryšį CA valdymo grandinėje, labiausiai pažeidžiamas grandis;
- žinotų organizacinius patikimumo aspektus;

b) vertintojų grupė turi būti pakankamai kompetentinga surasti CA sistemoje saugumo pažeidimo įvykius (valdymo ar technologiniame lygiuose) ir atsekti šiuos saugumo pažeidimo įvykius sukėlusias priežastis.

Pastaba: vertintojų grupė gali būti sudaryta iš vieno žmogaus, jeigu jis atitinka visus aukščiau išvardintus reikalavimus.

Vertintojų grupės kompetencijai užtikrinti gali būti kviečiami išoriniai ekspertai, išmanantys ETSI TS 101 456 standarto reikalavimus, valdymo sistemų principus, informacijos apsaugos ir PKI klausimus, nors ir neatitinkantys kitų reikalavimų. Tokie ekspertai visada turi būti atsakingi grupės vadovui ir nedaryti veiksmų nepriklausomai nuo kitų grupės narių.

### 12.1.4. Atitikties nustatymo procesas

Vertintojas pradžioje turi nustatyti, kurie CA dokumentai ir informacija yra konfidencialūs ir kurių negalės nagrinėti. Vertintojas turi nuspręsti, ar numatomi nagrinėti dokumentai ir informacija yra pakankami atitikčiai įvertinti. Jeigu vertinanti organizacija nusprendžia, kad tinkamas atitikties įvertinimas pagal pateiktus dokumentus negarantuojamas, ji turi apie tai informuoti CA ir perspėti, kad atitiktis bus vertinama tik pasirašius papildomas konfidencialumo sutartis, garantuojančias prieigą prie atitinkamos slaptos CA informacijos.

CA organizacinė struktūra gali būti tokia, kad paslaugos yra teikiamos keliose skirtingose vietose. Tokiu atveju atitiktį vertinanti organizacija gali pati pasirinkti vietas, kuriose vertins atitiktį, laikantis visų vertinimo procedūrų ir reikalavimų.

Prieš pradėdama atitikties vertinimą pasirinktose CA vietose, vertinanti organizacija turėtų pristatyti šių vietų parinkimo metodologiją.

Jeigu CA teikia paslaugas keliose vietose, žiūrima, kad:

a) visos CA paslaugų teikimo vietos būtų valdomos naudojant vienodą centralizuotai prižiūrimą valdymo sistemą, kuri yra tikrinimo objektas;

b) visose vietose būtų atliktas vidinis auditas pagal visas vidines CA tikrinimo procedūras;

c) atitiktį vertinanti organizacija parinktų pakankamą vietų kiekį, atsižvelgdama į:

- CA valdymo sistemos sudėtingumą;
- skirtingose vietose esančių informacinių sistemų sudėtingumą;
- atliekamų darbų skirtumus;
- atliekamų funkcijų skirtumus;
- visų CA padalinių, įskaitant centrinį padalinį, vidinio audito rezultatus;
- valdymo sistemos apžvalgos rezultatus;
- atskirų CA padalinių dydžio skirtumus;
- atskirų CA padalinių funkcijų skirtumus;
- galimą tikrinamų padalinių sąveiką su kritine sistemų informacija arba informacinėmis sistemomis, kurios apdoroja kritinę (slaptą) informaciją;
- įvairius juridinius reikalavimus;

d) patikros vietos turėtų būti dalinai parenkamos pagal c) punkte išvardintus kriterijus ir dalinai atsitiktine tvarka;

e) kiekviena svarbų vaidmenį vaidinanti CA paslaugos tiekimo vieta turi būti įtraukta į tikrinamų vietų sąrašą;

f) vertintojas turi sudaryti periodiško tikrinimo priežiūros programą. Skirtingų vietų vėlesnės atitikties priežiūros programa turi apimti visas atitikčiai patikrinti parinktas vietas, tačiau su laiku reikia stengtis apimti ir visas CA sertifikavimo paslaugos teikimo vietas;

g) jeigu buvo rasti trūkumai nors vienoje CA vietoje arba visoje CA sistemoje, taisymo procedūros turi būti taikomos visai CA sistemai ir padaliniams.

Tikrinant atitiktį turi būti laikomasi ISO 10011-1:1990 standarto reikalavimų.

Vertinanti organizacija CA valdymo sistemos atitiktį turėtų vertinti bent dviem etapais. Toliau šie etapai atitinkamai vadinami "valdymo sistemos atitikties vertinimo 1 etapas" bei "valdymo sistemos atitikties vertinimo 2 etapas". Žemiau aprašomi pagrindiniai kiekvieno etapo tikslai ir minimalios tikrinimų apimtys.

Vertinanti organizacija prieš atitikties vertinimą turi įsitikinti, ar CA gali įrodyti, kad jo naudojama valdymo sistema yra dokumentuota, įgyvendinta ir gali būti pademonstruotas jos veikimas.

***Valdymo sistemos atitikties vertinimo 1 etapas.***

Šiame vertinimo etape vertinančioji organizacija privalo gauti ir peržiūrėti visą CA valdymo sistemos dokumentaciją, išsiaiškinti CA valdymo sistemą ir gerai suplanuoti antrą atitikties vertinimo etapą. CA valdymo sistemos dokumentacijos peržiūra – tai pagrindinis, bet nebūtinai vienintelis šio etapo darbas. Kiti galimi darbai - tai įrašų atitikimo teisės aktams, atsakomybės paskirstymo, vidinio audito ir valdymo peržiūra. Vertinančioji organizacija ir CA turi susitarti, kada ir kur bus vykdomas valdymo sistemos atitikties pirmas vertinimo etapas. Tačiau bet kokiu atveju dokumentacijos peržiūra (1 etapas) turi būti baigta iki valdymo sistemos atitikties vertinimo 2 etapo pradžios.

Pirmo valdymo sistemos atitikties vertinimo etapo rezultatai turi būti dokumentuoti raštiškai. Pabaigus pirmą etapą, vertinančioji organizacija turi nutarti ar pereiti prie 2 etapo, o jeigu taip, tai parinkti tam reikalingos kompetencijos vertinimo grupės narius.

Vertinanti organizacija turi įspėti CA, kokie dokumentai ar/ir informacija bus reikalingi detaliam nagrinėjimui antrajame vertinimo etape.

***Valdymo sistemos atitikties vertinimo 2 etapas.***

Šis etapas visada vykdomas CA patalpose. Naudodamasi visais pirmo atitikties vertinimo etapo pastebėjimais, vertinanti organizacija apsibrėžia antro etapo darbų planą.

Antro atitikties vertinimo etapo tikslai:

a) patvirtinti, kad CA laikosi sertifikato taisyklių, tikslų ir procedūrinių reikalavimų;

b) patvirtinti, kad CA įdiegta valdymo sistema atitinka standartų reikalavimus ir siekia tikslų, numatytų CA įgyvendinamose sertifikato taisyklėse.

ETSI TS 101 456 punkte 7.4.10 reikalaujama, kad CA atitiktų teisės aktų reikalavimus, ypač duomenų apsaugos srityje. CA yra atsakingas už teisės aktų laikymąsi. Atitiktį vertinanti specialistų grupė turi tik patikrinti, ar CA valdymo sistemoje yra funkcijos, užtikrinančios veiklos tikslų įgyvendinimą laikantis teisės aktų.

Leistina, kad CA dokumentacija apimtų ne tik CA valdymo sistemą, bet ir kitas valdymo sistemas (pvz., kokybės, darbuotojų sveikatos ir saugumo, aplinkosaugos), kad galima būtų perprasti CA valdymo sistemos sąveiką su kitomis sistemomis.

CA valdymo sistemos ir kitokių sistemų (pvz., kokybės, aplinkosaugos ir t.t.) atitiktis gali būti vertinama kartu. Tokiu atveju į bendrą sistemų atitikties vertinimą turi būti įtrauktos visos CA valdymo sistemos tikrinimo procedūros. CA atitikties vertinimo kokybė dėl kombinuoto tikrinimo pobūdžio jokiu būdu neturi nukentėti.

Vertinančios organizacijos sprendimo dėl CA atitikties nustatytiems reikalavimams pagrindas turi būti aiškios ataskaitos, kuriose pateikiama pakankamai informacijos.

Vertinimo organizacijai skirtas ataskaitas parengia jos sudaryta vertinimo grupė. Ataskaitose turi būti:

a) CA organizacinės struktūros aprašas, apimantis ir CA subrangovus, jų panaudojimą ir kiekvieno jų struktūrą;

b) peržiūrėtų dokumentų santrauka ir vertinimo nuomonė;

c) CA informacijos saugumo rizikos analizė ir vertinimo nuomonė;

d) CA organizacinės struktūros patikimumo vertinimo nuomonė;

e) vertinimui sugaištas laikas, detali sunaudoto laiko CA dokumentams išnagrinėti ir valdymo sistemai įvertinti specifikacija;

f) neatitikimų sąrašas (jeigu tokių yra);

g) vertinimo metu pateiktų klausimų seka, šių klausimų pagrindimas, naudota metodologija;

h) vertintojų grupės rekomendacijos vertinimo organizacijai dėl sprendimo priėmimo, ar CA atitinka kvalifikuotų sertifikatų išdavėjų reikalavimus.

Vertinančios organizacijos asmuo ar komitetas, priimantis sprendimą dėl CA atitikties kvalifikuotų sertifikatų išdavimo reikalavimams, turi turėti pakankamų žinių ir patyrimo sprendimui pagal vertinimo grupės išvadas priimti. Jeigu lieka nepašalinti nors keli neatitikimai, CA negali būti patvirtintas kaip atitinkantis reikalavimus.

Dokumentas, patvirtinantis CA atitiktį reikalavimams, turi apsiriboti CA deklaruojamais tikslais, veikla, buvimo vieta, organizacijos aprašymu, kuriame CA būtų įvardintas kaip juridinis asmuo arba (jeigu taip reikia) juridinio asmens dalis, kuri teikia kvalifikuotų sertifikatų išdavimo paslaugas. Papildomai turi būti identifikuotos trečiosios šalys (jeigu jos yra), teikiančios atskiras kvalifikuotų sertifikatų sudarymo paslaugas arba paslaugų dalis duotam CA.

Vertinanti organizacija turi reikalauti, kad CA, kuriam buvo išduotas atitiktį patvirtinantis dokumentas, nedelsiant informuotų vertinusią organizaciją apie bet kokius reikšmingesnius savo veiklos taisyklių, valdymo, darbo ir procesų pasikeitimus, kurie gali įtakoti CA atitiktį kvalifikuotų sertifikatų sudarymo reikalavimams. Tokie CA pasikeitimai gali iššaukti papildomą, pakartotiną patikrinimą arba net atitikties deklaracijos suspendavimą. Atitiktis yra suspenduojama iki to momento, kol ji vėl nebus patvirtinta. Vertinanti organizacija pati turi nusistatyti korektišką reagavimo į pasikeitimus veiksmų seką.

Vertinanti organizacija turi nustatyti CA periodiškų tikrinimų programą. Periodiškų tikrinimų tikslas – nustatyti, ar CA vis dar atitinka reikalavimus. Daugeliu atveju, periodiškumas turėtų būti mažesnis kaip vieneri metai.

Papildomai visada turi būti peržiūrimi praeitų patikrinimų duomenys. Ypač svarbu, kad šiuose duomenyse būtų laikomi visi praeityje pastebėti neatitikimai.

Vertinanti organizacija privalo laikytis aiškiai apsibrėžtų sąlygų, kurioms esant bus tvirtinama, kad CA atitinka reikalavimus. Jeigu periodiško tikrinimo metu pastebimi neatitikimai, CA turi pašalinti neatitikimus per sutartą laiką. Jeigu per sutartą laiką neatitikimai nėra pašalinami, atitikties deklaracija turi būti suspenduota arba netgi nutraukta. Neatitikimams pašalinti skiriamas laikas turi atitikti neatitikimo svarbą ir keliamą riziką.

## 12.2. El. parašo įrangos atitikties reikalavimams vertinimas

### 12.2.1. Trumpa apžvalga

Pateikiamos rekomendacijos (patarimai), kaip reikėtų tikrinti el. parašo kūrimo ir tikrinimo įrangos atitiktį CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms" [12] bei CWA 14171 "Elektroninio parašo tikrinimo procedūros" [13] dokumentuose nustatytiems reikalavimams.

Atitikties vertinimo rekomendacijos skiriamos el. parašo kūrimo ir tikrinimo įrangos gamintojams, operatoriams (operatoriai – tai viešųjų paslaugų teikėjai, naudojantys gamintojų sukurtą įrangą).

Dėl el. parašo kūrimo ir tikrinimo procesų sudėtingumo bei didelės šių procesų techninio realizavimo įvairovės, formaliai nustatyti tam naudojamos įrangos ir procedūrų atitiktį reikalavimams yra sunku. Todėl geriausia atitikties keliamiems reikalavimams nustatymo eiga būtų paties gamintojo deklaracijų peržiūra. Jeigu tokią įrangą naudoja viešąsias el. parašo kūrimo ir/ar tikrinimo paslaugas teikiantis operatorius, pastarasis irgi turėtų paskelbti deklaraciją dėl naudojamos įrangos atitikties nustatytiems reikalavimams, remdamasis įrangos gamintojų deklaracijomis. Jeigu el. parašo kūrimo ir/ar tikrinimo įranga yra integruota į dar didesnę sistemą (pvz., CA naudojamą patikimą sertifikatų tvarkymo sistemą), tai tokios sistemos atitikties nustatymo vadovas ir formalios procedūros bus platesnės nei išdėstytos šiame rašinyje (pvz., CA atveju sistema turės atitikti CWA 14172-3 "Saugumo reikalavimai patikimoms elektroninių parašų sertifikatų tvarkymo sistemoms" standartą [16]).

Gamintojams nėra privalomas jų išleidžiamos įrangos atitikties deklaravimas, tačiau tikėtina, kad įranga, kurios atitiktį gamintojas yra deklaravęs, bus laikoma labiau patikima negu ta, kurios atitikties gamintojas dėl tam tikrų priežasčių nebus deklaravęs.

Atitiktį gali nustatyti pati deklaruojanti šalis arba trečioji šalis, pvz., kurios paslaugos yra orientuotos į atitikties nustatymą. Tačiau nepriklausomai nuo atitikties nustatymo procedūros, tik atitiktį deklaruojanti šalis atsako už deklaracijos teisingumą.

Pagrindinės rekomendacijų įrangos gamintojams ir paslaugų teikimo operatoriams dalys yra šios:

1) bendrosios atitikties deklaravimo rekomendacijos;

2) rekomendacijos (*guidance*) gamintojams, deklaruojantiems parašo kūrimo įrangos atitiktį reikalavimams CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms" [12] (pagrindinis reikalavimas gamintojui – turėti įsidiegus ISO 9001 sertifikuotą Kokybės Valdymo Sistemą gamyboje). Rekomenduojama atitikties deklaracijos forma pateikta 1 priede;

3) rekomendacijos operatoriams, deklaruojantiems viešose vietose naudojamos el. parašo kūrimo įrangos atitiktį reikalavimams CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms"[12] (pagrindinis reikalavimas operatoriui – turėti įsidiegus ISO 9001 sertifikuotą Kokybės Valdymo Sistemą paslaugų teikime). Mokymo medžiagos 1 priede parodyta rekomenduojama atitikties deklaracijos forma;

4) rekomendacijos gamintojams, deklaruojantiems parašo tikrinimo įrangos atitiktį reikalavimams, išdėstytiems dokumente CWA 14171 "Elektroninio parašo tikrinimo procedūros" [13] (pagrindinis reikalavimas gamintojui – turėti įsidiegus ISO 9001 sertifikuotą Kokybės Valdymo Sistemą gamyboje). Rekomenduojama atitikties deklaracijos forma pateikta 2 priede;

5) rekomendacijos operatoriams, deklaruojantiems viešose vietose naudojamos el. parašo tikrinimo įrangos atitiktį reikalavimams, išdėstytiems dokumente CWA 14171 "Elektroninio parašo tikrinimo procedūros"[13] (pagrindinis reikalavimas operatoriui – turėti įsidiegus ISO 9001 sertifikuotą Kokybės Valdymo Sistemą paslaugų teikime). Mokymo medžiagos 2 priede parodyta rekomenduojama atitikties deklaracijos forma.

### 12.2.2. Rekomendacijos

***1) bendrosios atitikties deklaravimo rekomendacijos***

Dėl el. parašo kūrimo ir tikrinimo procesų sudėtingumo bei didelės šių procesų techninio realizavimo įvairovės, sunku formaliai nustatyti naudojamos įrangos ir procedūrų atitiktį nustatytiems reikalavimams.

Gamintojams nėra privalomas įrangos atitikties deklaravimas, tačiau tikėtina, kad įranga, kurios atitiktį gamintojas yra deklaravęs, bus laikoma labiau patikima negu ta, kurios atitikties gamintojas dėl tam tikrų priežasčių nėra deklaravęs.

Atitiktį gali nustatyti pati deklaruojanti šalis arba trečioji šalis, pvz., kurios paslaugos yra orientuotos į atitikties nustatymą. Tačiau nepriklausomai nuo atitikties nustatymo procedūros, tik atitiktį deklaruojanti šalis atsako už deklaracijos teisingumą.

Patariama, kad įrangos gamintojas arba parašo kūrimo ar tikrinimo paslaugų teikėjas (operatorius) vadovautųsi [EN 45014:1989] *"General Criteria for Suppliers Declaration of Conformity"* dokumentu, nusakančiu bendruosius atitikties deklaravimo kriterijus. Deklaracijos tikslas – parodyti, kad el. parašo kūrimo ir/ar tikrinimo įranga atitinka keliamus reikalavimus (šiuo atveju CWA 14170 "Saugumo reikalavimus parašo kūrimo sistemoms"[12] ir CWA 14171 "Elektroninio parašo tikrinimo procedūroms"[13]);

***2) rekomendacijos gamintojams, deklaruojantiems parašo kūrimo įrangos atitiktį CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms"standarto [12] reikalavimams***

2.1. Gamintojai, deklaruojantys jų išleidžiamos elektroninio parašo kūrimo įrangos atitiktį nustatytiems reikalavimams, turėtų būti įsidiegę ISO 9001 sertifikuotą Kokybės Valdymo Sistemą. Šioje kokybės valdymo sistemoje turi būti identifikuoti procesai bei procedūros, garantuojančios el. parašo kūrimo įrangos atitiktį visų jos komponentų specifikavimo, projektavimo, gamybos ir pristatymo etapuose. Taip pat gamintojas turi pateikti visas vartojimo ir diegimo instrukcijas įrangos pirkėjui/vartotojui suprantama ir patogia forma. Ypatingas dėmesys turi būti atkreiptas į specifinius įrangos diegimo aspektus. Programinės įrangos gamintojams ISO 9001 standartas gali būti pakeistas CMM (*Capability Maturity Model*) sertifikavimu arba SPICE (*Software Process Impovement and Capability*, ISO/IEC 15504) Kokybės Valdymo Sistemų standartu.

2.2. Gamintojas įrangos atitikties deklaraciją turėtų pateikti 1 priede "Gamintojo deklaracija dėl elektroninio parašo kūrimo įrangos atitikties" nurodyta forma. Deklaracijoje be įrangos atitikties CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms" [12] turi būti nurodyta:

a) kontaktiniai gamintojo duomenys, norint gauti paaiškinimus dėl deklaracijos;

b) nuoroda, kad gamintojas yra įdiegęs ISO 9001 Kokybės Valdymo Sistemą (nurodant sertifikavusią organizaciją ir sertifikato numerį);

c) gamintojo laidavimas už visą įrangą, t. y. už visus privalomus ir specifinius įrangos komponentus;

d) nuorodos į papildomus normatyvinius dokumentus, kuriuos atitinka įranga;

e) visų specifinių įrangos komponentų atitiktį patvirtinantys dokumentai;

f) bet kokie ribojimai, kuriems esant atitikties deklaracija negaliotų;

g) gamintojo arba trečiosios šalies akredituotų (EN ISO 17025) testavimo laboratorijų, patvirtinusių įrangos atitiktį standartams ir normatyviniams dokumentams, sąrašas;

***3) rekomendacijos operatoriams, deklaruojantiems viešose vietose naudojamos el. parašo kūrimo įrangos atitiktį CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms" standarto [12] reikalavimams***

3.1. CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms"[12] skiria dvi fizines aplinkas, kuriose gali būti naudojama el. parašo kūrimo

įranga. Pirmosios aplinkos atveju, kuomet gamintojo pagamintą įrangą tiesiogiai naudoja operatorius - fizinis arba juridinis asmuo, jiems pakanka turėti gamintojo paskelbtą įrangos atitikties deklaraciją. Atroji aplinka yra tokia, kai operatorius, naudodamas gamintojo išleistą įrangą, "viešai, nuotoliniu būdu" teikia parašo kūrimo įrangą savo klientams. Šiuo atveju operatorius turi prisiimti atsakomybę už savo paslaugų korektiškumą bei deklaruoti įdiegtos ir naudojamos įrangos atitiktį.

3.2. Operatoriai, deklaruojantys naudojamos įrangos atitiktį el. parašo kūrimo reikalavimams, turėtų būti įsidiegę ISO 9001 sertifikuotą Kokybės Valdymo Sistemą. Tokioje kokybės valdymo sistemoje turi būti identifikuoti procesai bei procedūros, kurios garantuotų operatoriaus naudojamos sistemos atitiktį jos įdiegimo ir naudojimo etapuose. Taip pat operatorius turi pateikti informaciją apie save patį bei naudojamą sistemą vartotojams suprantama ir patogia forma. Ypatingas dėmesys turi būti atkreiptas į specifinius įrangos aspektus.

3.3. Operatorius savo deklaraciją dėl naudojamos įrangos atitikties turėtų pateikti forma, nurodyta 1 priedo "Paslaugų teikėjo (operatoriaus) deklaracija dėl elektroninio parašo kūrimo įrangos atitikties" dalyje. Deklaracijoje be įrangos atitikties CWA 14170 "Saugumo reikalavimai parašo kūrimo sistemoms"[12] turi būti nurodyta:

a) kontaktiniai operatoriaus duomenys, norint gauti paaiškinimus dėl deklaracijos;

b) nuoroda, kad operatorius yra įdiegęs ISO 9001 Kokybės Valdymo Sistemą (nurodant sertifikavusią organizaciją ir sertifikato numerį);

c) nuorodas į naudojamos įrangos gamintojų paskelbtas atitikties deklaracijas;

d) nuorodos į papildomus normatyvinius dokumentus, kuriuos atitinka įranga;

e) visų specifinių įrangos komponentų atitiktį patvirtinantys dokumentai;

f) bet kokie ribojimai, kuriems esant atitikties deklaracija negaliotų;

***4) rekomendacijos gamintojams, deklaruojantiems parašo tikrinimo įrangos atitiktį CWA 14171 "Elektroninio parašo tikrinimo procedūros" standarto [13] reikalavimams***

4.1. Gamintojai, deklaruojantys jų išleidžiamos el. parašo tikrinimo įrangos atitiktį nustatytiems reikalavimams, turėtų būti įsidiegę ISO 9001 sertifikuotą Kokybės Valdymo Sistemą. Šioje kokybės valdymo sistemoje turi būti identifikuoti procesai bei procedūros, garantuojančios el. parašo tikrinimo įrangos atitiktį visų jos komponentų specifikavimo, projektavimo,

gamybos ir pristatymo etapuose. Taip pat gamintojas turi pateikti visas vartojimo ir diegimo instrukcijas įrangos pirkėjui/vartotojui suprantama ir patogia forma. Ypatingas dėmesys turi būti atkreiptas į specifinius įrangos diegimo aspektus. Programinės įrangos gamintojams ISO 9001 standartas gali būti pakeistas CMM (*Capability Maturity Model*) sertifikavimu arba SPICE (*Software Process Impovement and Capability*, ISO/IEC 15504) Kokybės Valdymo Sistemų standartu.

4.2. Gamintojas įrangos atitikties deklaraciją turėtų pateikti 2 priedo "Gamintojo deklaracija dėl elektroninio parašo tikrinimo įrangos atitikties" nurodyta forma. Deklaracijoje be įrangos atitikties CWA 14171 "Elektroninio parašo tikrinimo procedūros"[13] turi būti nurodyta:

a) kontaktiniai gamintojo duomenys, norint gauti paaiškinimus dėl deklaracijos;

b) nuoroda, kad gamintojas yra įdiegęs ISO 9001 Kokybės Valdymo Sistemą (nurodant sertifikavusią organizaciją ir sertifikato numerį);

c) gamintojo laidavimas už visą įrangą, t. y. už visus privalomus ir specifinius įrangos komponentus;

d) nuorodos į papildomus normatyvinius dokumentus, kuriuos atitinka pagaminta įranga;

e) visų specifinių įrangos komponentų atitiktį patvirtinantys dokumentai;

f) bet kokie ribojimai, kuriems esant atitikties deklaracija negaliotų;

g) gamintojo arba trečiosios šalies akredituotų (EN ISO 17025) testavimo laboratorijų, patvirtinusių įrangos atitiktį standartams ir normatyviniams dokumentams, sąrašas;

***5) rekomendacijos operatoriams, deklaruojantiems viešose vietose naudojamos el. parašo tikrinimo įrangos atitiktį CWA 14171 "Elektroninio parašo tikrinimo procedūros" standarto [13] reikalavimams***

5.1. CWA 14171 "Elektroninio parašo tikrinimo procedūros" [13] skiria dvi fizines aplinkas, kuriose gali būti naudojama el. parašo tikrinimo įranga. Pirmosios aplinkos atveju, kuomet gamintojo pagamintą įrangą tiesiogiai naudoja operatorius - fizinis arba juridinis asmuo, jiems pakanka turėti gamintojo paskelbtą įrangos atitikties deklaraciją. Atroji aplinka yra tokia, kai operatorius, naudodamas gamintojo išleistą įrangą, "viešai, nuotoliniu būdu" teikia parašo tikrinimo paslaugas savo klientams. Šiuo atveju operatorius turi prisiimti atsakomybę už savo paslaugų korektiškumą bei deklaruoti įdiegtos ir naudojamos įrangos atitiktį.

5.2. Operatoriai, deklaruojantys naudojamos įrangos atitiktį el. parašo tikrinimo reikalavimams, turėtų būti įsidiegę ISO 9001 sertifikuotą Kokybės Valdymo Sistemą. Tokioje kokybės valdymo sistemoje turi būti identifikuoti procesai bei procedūros, kurios garantuotų operatoriaus naudojamos sistemos atitiktį jos įdiegimo ir naudojimo etapuose. Taip pat operatorius turi pateikti informaciją apie save patį bei naudojamą sistemą vartotojams suprantama ir patogia forma. Ypatingas dėmesys turi būti atkreiptas į specifinius įrangos aspektus.

5.3. Operatorius savo deklaraciją dėl naudojamos įrangos atitikties turėtų pateikti forma, nurodyta 2 priedo "Paslaugų teikėjo (operatoriaus) deklaracija dėl elektroninio parašo tikrinimo įrangos atitikties" dalyje. Deklaracijoje be įrangos atitikties "Elektroninio parašo tikrinimo procedūrų" reikalavimams turi būti nurodyta:

a) kontaktiniai operatoriaus duomenys, norint gauti paaiškinimus dėl deklaracijos;

b) nuoroda, kad operatorius yra įdiegęs ISO 9001 Kokybės Valdymo Sistemą (nurodant sertifikavusią organizaciją ir sertifikato numerį);

c) nuorodas į naudojamos įrangos gamintojų paskelbtas atitikties deklaracijas;

d) nuorodos į papildomus normatyvinius dokumentus, kuriuos atitinka įranga;

e) visų specifinių įrangos komponentų atitiktį patvirtinantys dokumentai;

f) bet kokie ribojimai, kuriems esant atitikties deklaracija negaliotų.

# SANTRUMPOS

AA – *Attribute Authority,* Informacijos apie asmens atributus (pareigas, narystę draugijose, kt.) teikimo tarnyba;
ASN.1 – *Abstract Syntax Notation 1,* Abstraktaus žymėjimo sintaksė 1;
CA – *Certification Authority,* Sertifikatų centras;
CGA – *Certificate Generation Application,* Sertifikatų sudarymo taikomoji programa;
CPS – *Certification Practice Statement,* Sertifikavimo veiklos nuostatai;
CRL – *Certificate Revocation List,* Atšauktų sertifikatų sąrašas;
CWA – *CEN Workshop Agreement,* CEN komiteto susitarimas;
ES – *Electronic Signature,* Elektroninis parašas;
EESSI – *European Electronic Signature Standardisation Initiative,* Europos elektroninio parašo standartizavimo iniciatoriai;
ETSI – *European Telecommunication Standardisation Institute,* Europos telekomunikacijų standartizavimo institutas;
IETF – *Internet Engineering Task Force,* Interneto problemų sprendėjai;
NQC – *Non-Qualified Certificate,* Nekvalifikuotas sertifikatas;
OID – *Object IDentifier,* Unikalus objekto identifikatorius;
OCSP – *Online Certificate Status Protocol,* Tiesioginės prieigos protokolas sertifikatų statuso informacijai gauti;
PIN – *Personal IdentificationNumber,* Asmens identifikacinis skaičius;
PKI – *Public Key Infrastructure,* Viešojo rakto infrastruktūra;
QC – *Qualified Certificate,* Kvalifikuotas sertifikatas;
QCP – *Qualified Certificate Policy,* Kvalifikuoto sertifikato taisyklės;
RA – *Registration Authority,* Registravimo tarnyba;
RFC – *Request For Comments,* "Prašome komentarų" standartizavimo tarnyba;
RSA – *Rivest-Shamir-Adlemann algorithm,* RSA asimetrinio šifravimo algoritmas;
SHA-1 – *Secure Hash Algorithm1,* Saugus santraukos algoritmas 1;
SCA – *Signature Creation Application,* Parašo formavimo programinė įranga;
SCDev – *Signature Creation Device,* Parašo formavimo įranga;
SCDat – *Signature Creation Data*, Parašo formavimo duomenys (privatusis raktas);
SSCD – *Secure Signature Creation Device,* Saugi parašo formavimo įranga;
SVD – *Signature Verification Data,* Parašo tikrinimo duomenys (viešasis raktas);
TSA – *Time Stamping Authority,* Laiko žymų tarnyba;
UTC – *Coordinated universal Time,* Universalusis laikas (Grinvičo laikas).

# ŠALTINIAI

***ETSI (European Telecommunication Standard Institute) standartai***

http://www.etsi.org/WebSite/Technologies/ElectronicSignature.aspx

(žiūrėta 2008 m. vasarį)

1. ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, 2006-01.
2. ETSI TS 101 733 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures, 2005-09.
3. ETSI TS 101 861 Time stamping profile, 2006-01.
4. ETSI TS 101 862 Qualified Certificate Profile, 2006-01.
5. ETSI TS 102 042 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, 2005-06.
6. ETSI TS 102 023 Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, 2003-01.
7. ETSI TR 102 041 Signature policies report, 2002-02.

***CWA (CEN Workshop Agreement) standartai***

http://www.uninfo.polito.it/WS_Esign/docs.htm#published (žiūrėta 2008 m. vasarį)

8. CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, 2003-06.
9. CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP), 2004-05.
10. CWA 14167-3 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP), 2004-05.
11. CWA 14169 Secure Signature-Creation Devices, version 'EAL 4+', 2004-03.
12. CWA 14170 Security Requirements for Signature Creation Applications, 2004-05.
13. CWA 14171 General Guidelines for Electronic Signature Verification, 2004-05.
14. CWA 14172-1 EESSI Conformity Assessment Guidance - Part:1: General, 2004.

15. CWA 14172-2 EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes, 2004.
16. CWA 14172-3 EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures, 2004.
17. CWA 14172-4 EESSI Conformity Assessment Guidance - Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification, 2004.
18. CWA 14172-5 EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices, 2004.
19. CWA 14355 Guidelines for the implementation of Secure Signature Creation Devices, 2004-03.
20. CWA 14365 Guidelines on the use of Electronic Signatures, 2004-03.

***IETF (Internet Engineering Task Force) RFC (Request For Comments) standartai***

http://www.ietf.org/rfc.html (žiūrėta 2008 m. vasarį)

21. IETF RFC 1321: The MD5 message-digest algorithm http://www.ietf.org/rfc/rfc1321.txt
22. IETF RFC 2313: RSA Encrytion
23. IETF RFC 3447: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, 2003.
24. IETF RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and CRL Profile, 2002.
25. IETF RFC 3647: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework, 2003.
26. IETF RFC 3852: Cryptographic Message Syntax (CMS), 2004.
27. IETF RFC 3739: Internet X.509 Public Key Infrastructure. Qualified Certificate Profile, 2004
28. IETF RFC 3125: Electronic Signature Policies
29. IETF RFC 3161: Internet X.509 Public Key Infrastructure. Time-stamp protocol (TSP)
30. IETF RFC 3174: US Secure Hash Algorithm (SHA-1)

***Kiti šaltiniai***

31. ETSI SR 002 176 Electronic Signatures and Infrastructures (ESI): Algorithms and Parameters for Secure Electronic Signatures, 2005-07. http://www.etsi.org/deliver/etsi_sr/002100_002199/002176/01.01.01_60/sr_002176v010101p.pdf (žiūrėta 2008 m. vasarį).

32. FIPS PUB 140-2 Security Requirements for Cryptographic Modules, 2002. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
33. ISO/IEC 15408:2005(E) Information technology – Security techniques – Evaluation criteria for IT security. http://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm (žiūrėta 2008 m. rugsėjį).
34. CEN Hardware Security Modules for CSPs, CC Protection Profile, EESSI Area 2.
35. V.Stakėnas. Kriptologija (paskaitų konspektai) // Matematinės informatikos katedra, Matematikos ir informatikos fakultetas, Vilniaus universitetas. http://www.mif.vu.lt/matinf/asm/vs/vs0.htm (žiūrėta 2008 m. vasarį).
36. Goteborgs universitet CA http://www.swupki-pca.umu.se/CA/0C.txt (žiūrėta 2008 m. vasarį). http://www.swupki.su.se/ (žiūrėta 2008 m. vasarį).
37. GlobalSign Certificate Policy, version v.2.0, Date: 05/09/05 http://www.globalsign.net/repository (žiūrėta 2008 m. vasarį).
38. Certum Time-stamping Authority Policy. Poland, 2005-05. http://www.certum.pl/repository/ (žiūrėta 2008 m. vasarį).
39. E.Gerck, Overview of Certification Systems: X.509, CA, PGP and SKIP http://www.blackhat.com/presentations/bh-usa-99/EdGerck/certover.pdf (žiūrėta 2008 m. vasarį).
40. www.pki-page.com (žiūrėta 2008 m. vasarį).
41. Informacinės visuomenės plėtros komiteto prie LRV interneto puslapis www.ivpk.lt (žiūrėta 2008 m. vasarį).
42. LST ISO/IEC 15408-1:1999(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general mode. http://webstore.iec.ch/preview/info_isoiec15408-1%7Bed3.0%7Den.pdf (žiūrėta 2008 m. vasarį).
43. LST ISO/IEC 15408-2:1999(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. http://webstore.iec.ch/preview/info_isoiec15408-2%7Bed3.0%7Den.pdf (žiūrėta 2008 m. vasarį).
44. LST ISO/IEC 15408-3:1999(E) Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. http://webstore.iec.ch/preview/info_isoiec15408-3%7Bed3.0%7Den.pdf (žiūrėta 2008 m. vasarį).
45. LST ISO/IEC 17799:2000(E) Information technology – Code of practice for information security management

46. EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA dėl Bendrijos elektroninių parašų reguliavimo sistemos 1999/93/EB, 1999. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:LT:PDF

47. LIETUVOS RESPUBLIKOS ELEKTRONINIO PARAŠO ĮSTATYMAS, Nr. VIII-1822, 2000. http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=105849

48. LIETUVOS RESPUBLIKOS VYRIAUSYBĖS 2002 m. gruodžio 31 d. NUTARIMAS Nr. 2108 „Dėl reikalavimų kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams, reikalavimų elektroninio parašo įrangai, kvalifikuotus sertifikatus sudarančių sertifikavimo paslaugų teikėjų registravimo tvarkos ir elektroninio parašo priežiūros reglamento patvirtinimo“. http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=198003

# PRIEDAI

## 1 priedas. El. parašo kūrimo įrangos atitikties deklaracijos

### *Gamintojo deklaracija dėl elektroninio parašo kūrimo įrangos atitikties*

Mes <<gamintojo pavadinimas>>,
įsikūrę <<gamintojo adresas>>
šiuo dokumentu, mūsų asmenine atsakomybe, deklaruojame, kad elektroninio parašo kūrimo įranga

<<įrangos vardas & specifikacija, tipas ar modelis (ir versijos numeris)>>

visiškai atitinka šiuos reikalavimus [jei yra, ir papildomus normatyvinius dokumentus]:

"Saugumo reikalavimai elektroninio parašo kūrimo įrangai"

<<šiuo metu galiojančio dokumento versija/leidimas ir data>>

[jei yra papildomi dokumentai: <<Standarto ar kito normatyvinio dokumento pavadinimas ir/ar numeris bei data>>].

<<Gamintojo pavadinimas>>
suprojektavo, sukūrė, pagamino ir pateikė
<<įrangos vardas & specifikacija >>
įrangą pagal ISO 9001 [jei yra: CMM arba SPICE] Kokybės Valdymo Sistemą,
sertifikatas <<sertifikato numeris ir išdavimo data>>,
sertifikatą išdavė <<sertifikatą išdavusios organizacijos pavadinimas>> ,
ir šiuo dokumentu laiduoja visos įrangos, t. y. visų įrangos privalomų ir specifinių komponentų, atitiktį. [*jei yra:* Ši atitikties deklaracija yra dalinai paremta atskirų įrangos komponentų atitikties dokumentais:
<<schemų ir jas pritaikiusiųjų (pavadinimas ir šalis) sąrašas>> ]

Ribojimai:
jokių arba <<išvardinami šios atitikties deklaracijos ribojimai>>

Kontaktinė informacija:
<<gamintojo pavadinimas>>
Su šia deklaracija susijusius paaiškinimus galima gauti adresais
<<pašto adresas/telefono numeris/www ir el. pašto adresai>>

## *Paslaugų teikėjo (operatoriaus) deklaracija dėl elektroninio parašo kūrimo įrangos atitikties*

Mes <<operatoriaus pavadinimas>>,
įsikūrę <<operatoriaus adresas>>
šiuo dokumentu, mūsų asmenine atsakomybe, deklaruojame, kad elektroninio parašo kūrimo sistema <<sistemos pavadinimas>>,
esanti <<adresas, vieta>>,
ir naudojanti šią įrangą
<<įrangos vardas & specifikacija, tipas ar modelis (ir versijos numeris)>>,
visiškai atitinka šiuos reikalavimus [jei yra ir papildomus normatyvinius dokumentus]:
"Saugumo reikalavimai elektroninio parašo kūrimo įrangai"
<<šiuo metu galiojančio dokumento versija/leidimas ir data>>
[jei yra papildomi dokumentai: <<Standarto ar kito normatyvinio dokumento pavadinimas ir/ar numeris bei data>>].

Deklaruojama įranga atitinka tuos pačius reikalavimus, kurie nurodyti gamintojo(ų) deklaracijoje(se):
<<gamintojų deklaracijų sąrašas>>
<<Paslaugos teikėjo (operatoriaus) pavadinimas>>
įsidiegė ir valdo šią <<įrangos pavadinimas>>
įrangą pagal ISO 9001 [*jei yra:* CMM arba SPICE] Kokybės Valdymo Sistemą,
sertifikato <<sertifikato numeris ir išdavimo data>>,
sertifikatą išdavė <<sertifikatą išdavusios organizacijos pavadinimas>>,
ir šiuo dokumentu laiduoja visos įrangos, t. y. visų įrangos privalomų ir specifinių komponentų, atitiktį.

[*jei yra*: ši atitikties deklaracija yra dalinai paremta atskirų įrangos komponentų atitikties dokumentais:
<<schemų ir jas pritaikiusiųjų (pavadinimas ir šalis) sąrašas>> ]

Ribojimai:
jokių arba <<išvardinami šios atitikties deklaracijos ribojimai>>

Kontaktinė informacija:
<<paslaugos teikėjo (operatoriaus) pavadinimas>>
Su šia deklaracija susijusius paaiškinimus galima gauti adresais
<<pašto adresas/telefono numeris/www ir el. pašto adresai>>

# 2 priedas. El. parašo tikrinimo įrangos atitikties deklaracijos

## *Gamintojo deklaracija dėl elektroninio parašo tikrinimo įrangos atitikties*

Mes <<gamintojo pavadinimas>>,
įsikūrę <<gamintojo adresas>>
šiuo dokumentu, mūsų asmenine atsakomybe, deklaruojame, kad elektroninio parašo tikrinimo įranga

<<įrangos vardas & specifikacija, tipas ar modelis (ir versijos numeris)>>

visiškai atitinka šiuos reikalavimus [*jei yra:* ir papildomus normatyvinius dokumentus]:

"Saugumo reikalavimai elektroninio parašo tikrinimo įrangai"
<<šiuo metu galiojančio dokumento versija/leidimas ir data>>

[jei yra papildomi dokumentai: <<Standarto ar kito normatyvinio dokumento pavadinimas ir/ar numeris bei data>> ].

<<Gamintojo pavadinimas>>
suprojektavo, sukūrė, pagamino ir pateikė
<<įrangos vardas & specifikacija >>
įrangą pagal ISO 9001 [*jei yra:* CMM arba SPICE] Kokybės Valdymo Sistemą,
sertifikatas <<sertifikato numeris ir išdavimo data>>,
sertifikatą išdavė <<sertifikatą išdavusios organizacijos pavadinimas>> ,
ir šiuo dokumentu laiduoja visos įrangos, t. y. visų įrangos privalomų ir specifinių komponentų, atitiktį. [*jei yra:* Ši atitikties deklaracija yra dalinai paremta atskirų įrangos komponentų atitikties dokumentais:
<<schemų ir jas pritaikiusiųjų (pavadinimas ir šalis) sąrašas>> ]

Ribojimai:
jokių arba <<išvardinami šios atitikties deklaracijos ribojimai>>

Kontaktinė informacija:
<<gamintojo pavadinimas>>
Su šia deklaracija susijusius paaiškinimus galima gauti adresais
<<pašto adresas/telefono numeris/www ir el. pašto adresai>>

***Paslaugų teikėjo (operatoriaus) deklaracija***
***dėl elektroninio parašo tikrinimo įrangos atitikties***

Mes <<operatoriaus pavadinimas>>,
įsikūrę <<operatoriaus adresas>>
šiuo dokumentu, mūsų asmenine atsakomybe, deklaruojame, kad elektroninio parašo tikrinimo sistema
<<sistemos pavadinimas>>,
esanti <<adresas, vieta>>,
ir naudojanti šią įrangą
<<prekės vardas & specifikacija, tipas ar modelis (ir versijos numeris)>>,
visiškai atitinka šiuos reikalavimus [*jei yra:* ir papildomus normatyvinius dokumentus]:
"Saugumo reikalavimai elektroninio parašo tikrinimo įrangai"
<<šiuo metu galiojančio dokumento versija/leidimas ir data>>
[jei yra papildomi dokumentai: <<Standarto ar kito normatyvinio dokumento pavadinimas ir/ar numeris bei data>> ].

Deklaruojama įranga atitinka tuos pačius reikalavimus, kurie nurodyti gamintojo(ų) deklaracijoje(se): <<gamintojų deklaracijų sąrašas>>

<<Paslaugos teikėjo (operatoriaus) pavadinimas>>
įsidiegė ir valdo šią
<<įrangos pavadinimas>>
įrangą pagal ISO 9001 [*jei yra:* CMM arba SPICE] Kokybės Valdymo Sistemą,
sertifikato <<sertifikato numeris ir išdavimo data>>,
sertifikatą išdavė <<sertifikatą išdavusios organizacijos pavadinimas>>,
ir šiuo dokumentu laiduoja visos įrangos, t. y. visų įrangos privalomų ir specifinių komponentų, atitiktį. [*jei yra:* ši atitikties deklaracija yra dalinai paremta atskirų įrangos komponentų atitikties dokumentais:
<<schemų ir jas pritaikiusiųjų (pavadinimas ir šalis) sąrašas>> ]

Ribojimai:
jokių arba <<išvardinami šios atitikties deklaracijos ribojimai>>

Kontaktinė informacija:
<<paslaugos teikėjo (operatoriaus) pavadinimas>>
Su šia deklaracija susijusius paaiškinimus galima gauti adresais
<<pašto adresas/telefono numeris/www ir el. pašto adresai>>