KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS SISTEMŲ KATEDRA

Vida Undzėnienė

ELEKTRONINIO PARAŠO SERTIFIKATŲ CENTRO ĮRANGA

Magistro darbas

Darbo vadovas
Vilniaus universiteto
Matematikos ir informatikos fakulteto
doc. dr. V.Undzėnas

KAUNAS, 2005

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
INFORMACIJOS SISTEMŲ KATEDRA

TVIRTINU
Katedros vedėjas
doc. dr. R. BUTLERIS
2005-01-10

ELEKTRONINIO PARAŠO SERTIFIKATŲ CENTRO ĮRANGA

Informatikos inžinerijos magistro baigiamasis darbas

Recenzentas
doc. dr. S.Gudas

2005-01-07

Vadovas
Vilniaus universiteto
Matematikos ir informatikos fakulteto
doc. dr. V.Undzėnas
2005-01-06

Atliko
IFN-2 gr. stud.
V. Undzėnienė
2005-01-05

KAUNAS, 2005

KAUNO TECHNOLOGIJOS UNIVERSITETO REKTORIUS

ĮSAKYMAS
DĖL 2004 – 2005 M. M. MAGISTRO STUDIJŲ KVALIFIKACIJOS KOMISIJŲ

2004 m. gruodžio 27 d. Nr. A-649
Kaunas

Magistro kvalifikaciniam laipsniui suteikti,

į s a k a u sudaryti šių studijų programų kvalifikacijos komisijas:

15. INFORMACINIŲ TECHNOLOGIJŲ (62107T103), INFORMACINIŲ SISTEMŲ INŽINERIJOS (62107T104)

Pirmininkas –	Raimundas Stulpinas, UAB „Strauja“ generalinis direktorius;
Sekretorius –	Antanas Lenkevičius, docentas;
Nariai:	Rimantas Butleris, docentas,
	Valentinas Kiauleikis, docentas,
	Jonas Kazimieras Matickas, docentas,
	Bronius Paradauskas, docentas,
	Dalius Rubliauskas, docentas,
	Aleksandras Targamadzė, profesorius.

Rektorius Ramutis Bansevičius

I.Milišiūnaitė, (8~37) 30 00 41

Undzėnienė Vida. Equipment of Electronic Signature Certification Authority. Information Technologies master‘s thesis/ Tutor associate professor Dr. V.Undzėnas; Vilnius University, faculty of Mathematics and Informatics. - Kaunas, 2005, 86 p.

SUMMARY

Project aim – preparation of electronic signature certification authority (CA) project and certificate managing software (information system) prototype.

The work reviews the problems of electronic signature infrastructure development in Lithuania. The analytical survey of electronic signature CA was carried out. The standards determining the structure of electronic signature Certificate, CA activities, requirements for Trustworthy Systems Managing Certificates were examined.

The organizational structure of CA was prepared and working model was worked out. The workflow model was worked out to depict the hierarchy of certification processes. The use case model were created for certificate issuing, data processing and providing data of revoked certificates. Detail descriptions of information streams between the system and computerized tasks are provided. Structural diagrams on the information streams were created. According to information flows the entity relations diagram was created, the logical structure of data bases (DB) for certificates was developed.

The DB *Esign* of valid certificates and DB *Esign_archives* of revoked certificates were created. Specification of program modules was made up. Three types of manuals were prepared for system users – a manual for the client, a manual for the user and a manual for the programmer. The certificate managing system prototype was tested. The results of the experiment are presented.

For practical realization of the project the Organization activity modeling system ProVision WorkbenchTMv.3.1 was used, as well as the data base management system MySQL, programming interpreter PHP and Web server.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Plėtojant elektroninę komerciją, sudarant sutartis elektroniniu būdu, verslo partneriams yra svarbūs bendravimo konfidencialumo bei duomenų autentiškumo klausimai. Tinklais perduodamų elektroninių duomenų autentiškumui garantuoti elektroniniai dokumentai pasirašomi elektroniniu parašu, kuris šiandien yra paremtas asimetriniu šifravimu. Šiuolaikinės programinės priemonės, kuriomis galima sukurti šifravimo raktų poras, yra prieinamos kiekvienam informatikos specialistui. Todėl duomenų gavėjas negali būti visiškai įsitikinęs, kas yra siuntėjas ir ar nėra kokios klastotės.

Apsisaugoti nuo nesąžiningų, nusikalstamų veikų elektroninėje aplinkoje galima tik teisinėmis-organizacinėmis priemonėmis. Todėl turi būti gerai išvystyta elektroninio parašo infrastruktūra - teisės aktų, normatyvinių dokumentų, standartų, organizacinių ir techninių priemonių visuma. Vienas iš pagrindinių elektroninio parašo infrastruktūros dalyvių - sertifikatų centrai. Asmuo, norintis pasirašinėti elektroniniu parašu, turi registruotis sertifikatų centre. Už nedidelį mokestį (50-100 Lt metams) kiekvienam pasirašančiajam sertifikatų centras sudaro sertifikatą – elektroninį liudijimą, kuris susieja parašo tikrinimo duomenis (viešąjį raktą) su asmeniu ir patvirtina to asmens tapatybę. Sugeneruotas sertifikatas išduodamas abonentui ir kartu patalpinamas internetu laisvai prieinamoje duomenų bazėje. Tokiu būdu pasirašytų duomenų gavėjai turi galimybę pasitikrinti, ar šifravimo raktai iš tikro priklauso pasirašytus duomenis atsiuntusiam asmeniui, ir ar sertifikatas galiojo pasirašymo metu.

Norint užtikrinti nepriekaištingą elektroninio parašo sertifikatų centro veiklą, reikia sertifikatų centre įdiegti patikimą sertifikatų tvarkymo sistemą.

Šiame darbe, remiantis ETSI TS 101 456 standartu "Reikalavimai kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams" bei užsienio valstybių sertifikatų centrų veiklos pavyzdžiais, formuluojami reikalavimai sertifikatų centro įrangai, pateikiami prototipai priemonių, reikalingų sertifikatų centro veikloje.

Magistrinio darbo tema pasirinkta siekiant įgyta žinių ir patirties elektroninio parašo infrastruktūros vystymo srityje, o tuo pačiu puoselėti elektroninį parašą Lietuvoje.

Projekto tikslas – elektroninio parašo sertifikatų centro projekto ir programinės įrangos prototipo sukūrimas.

Uždaviniai:

- suformuluoti elektroninio parašo sertifikatų centro įrangai keliamus reikalavimus, atitinkančius ES standartų nuostatas**;**
- sukurti elektroninio parašo sertifikatų centro organizacinės struktūros ir programinės įrangos projektą;
- sukurti prototipus priemonių, reikalingų sertifikatų centro veikloje;

- išbandyti prototipus ir parengti jų galimo panaudojimo rekomendacijas;
- įgyti patirtį šioje srityje, kuri galėtų praversti plėtojant Lietuvoje elektroninio parašo infrastruktūrą.

Pagrindiniai darbo rezultatai:

- sukurtas elektroninio parašo sertifikatų centro programinės įrangos projektas, paremtas IETF RFC 2459, IETF RFC 3039, ETSI TS 101 862 standartų [9, 11, 2] reikalavimais;
- parengtas sertifikatų centro informacinės sistemos prototipas ir vartotojo dokumentacija, remiantis ETSI TS 101 456, CWA 14167-1, CWA 14167-2 [1, 3, 4] standartais;

Projektui realizuoti buvo naudoti šie instrumentai:

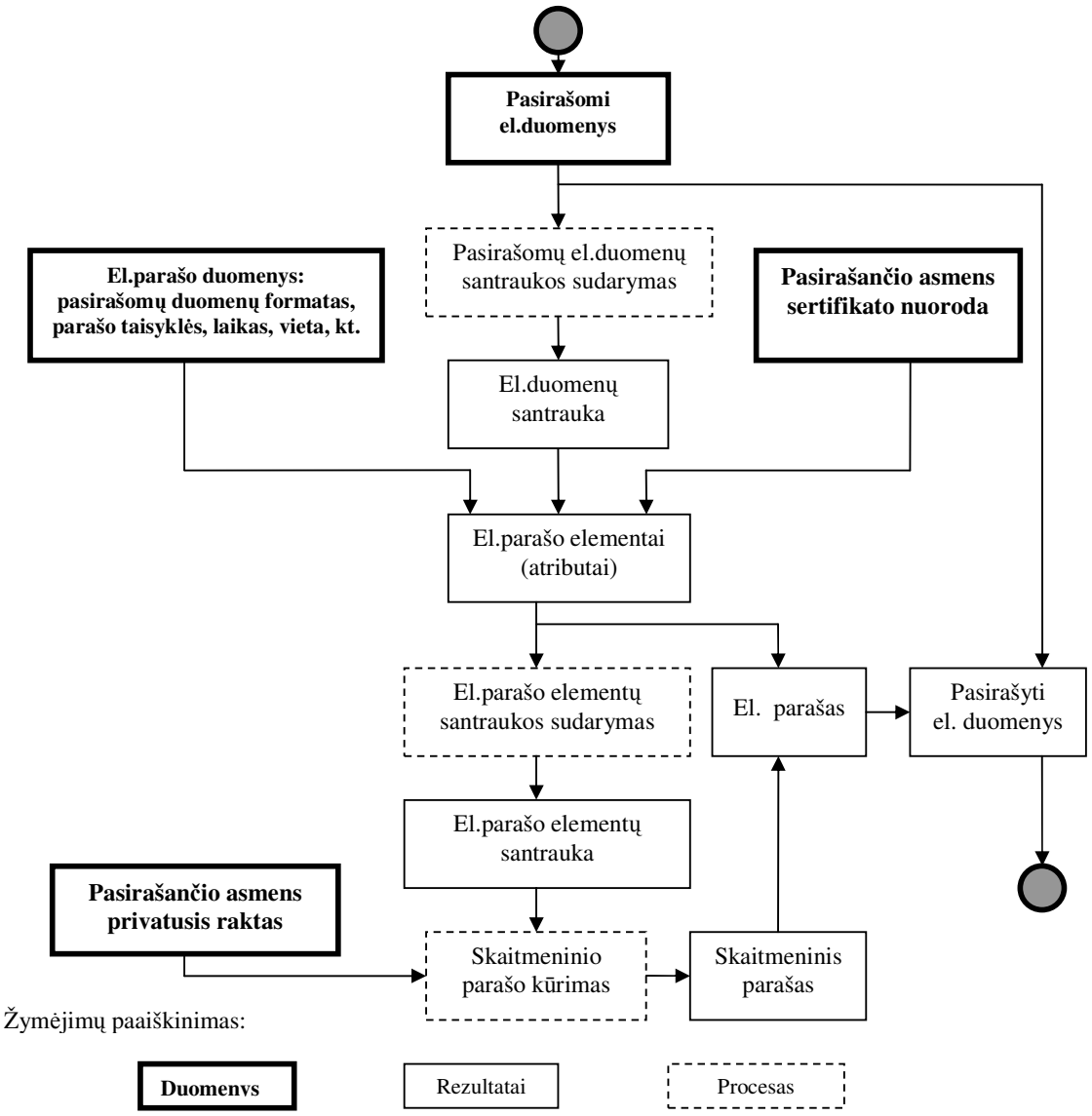
- organizacijų veiklos modeliavimo sistema *ProVision Workbench^{TM}v.3.1*,
- reliacinė duomenų bazių valdymo sistema *MySQL*,
- programavimo interpretatorius *PHP*,
- *Web* serveris.

1. ANALITINĖ DALIS

1.1. ELEKTRONINIO PARAŠO KŪRIMAS IR TIKRINIMAS

Panagrinėkime, kaip kuriamas elektroninis parašas (1.1 pav.). Kuriant parašą naudojami pasirašomi elektroniniai duomenys. Kadangi pasirašomų duomenų apimtis gali būti įvairi, visų pirma sukuriama fiksuoto ilgio duomenų santrauka (angliškai ji vadinama įvairiai: *hash, message digest, imprint*). Dažniausiai ji būna 128 arba 160 bitų ilgio. Šiuo metu dažniausiai naudojami *SHA-1* (*Secure Hash Algorithm*; 160 bitų santrauka) [12], *MD5* (*Message Digest algorythm 5*; 128 bitų santrauka) [8], *RIPEMD-160* (*Race Integrity Primitives Evaluation Message Digest 160*; 160 bitų santrauka) duomenų santraukos algoritmai. Šie algoritmai vadinami vienos krypties, kolizijoms atspariais santraukos algoritmais, kadangi pasižymi tokiomis savybėmis:

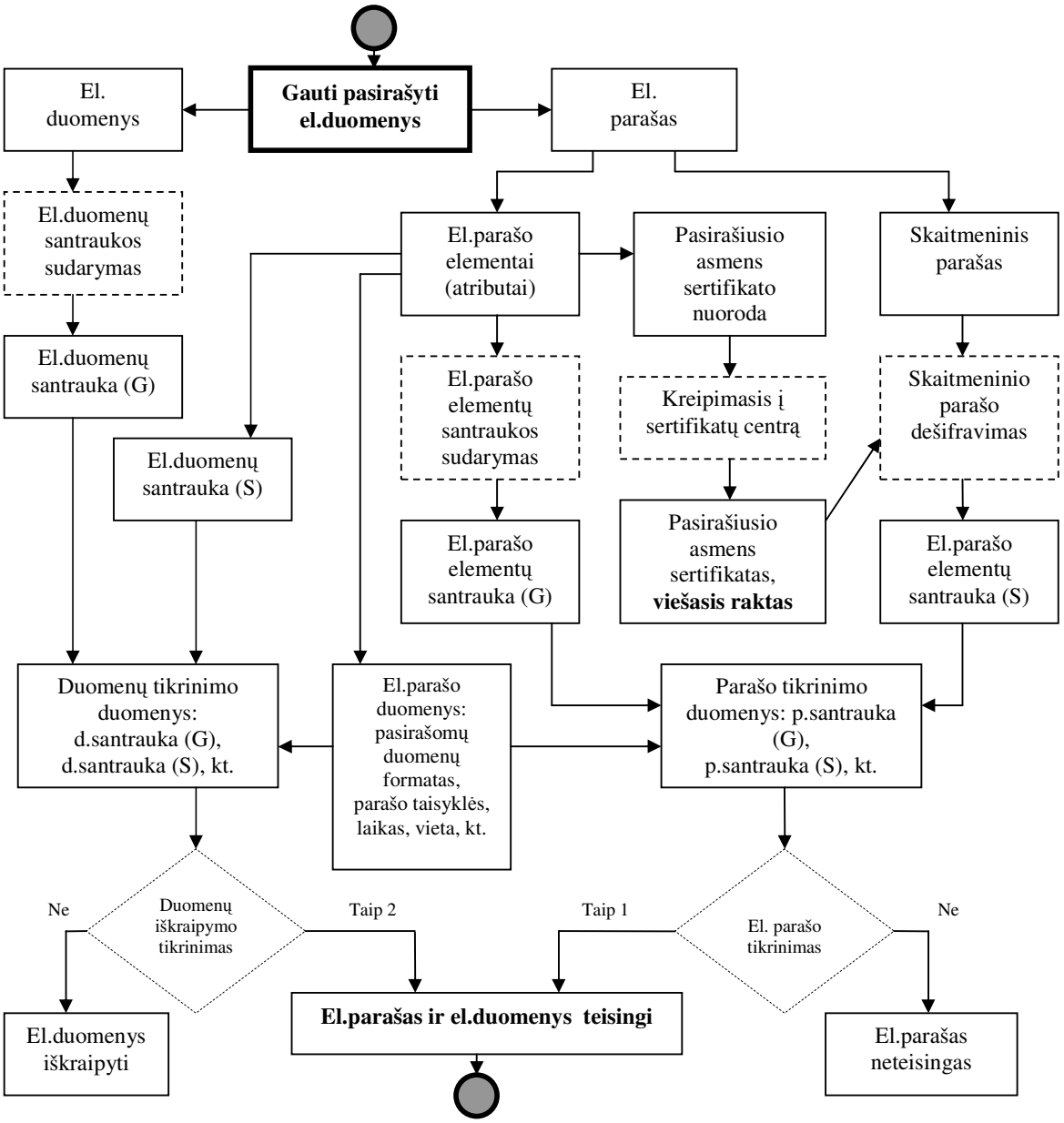
- iš santraukos neįmanoma atstatyti pačių duomenų;
- praktiškai neįmanoma rasti dviejų skirtingų duomenų, kurių santraukos būtų vienodos.



1.1 pav. Elektroninių duomenų pasirašymas

Nagrinėjant įvairią literatūrą dažniausiai sutinkamas toks elektroninio parašo apibrėžimas: ***elektroninis parašas*** **-** tai duomenų santrauka ir kita papildoma informacija (pvz., nuoroda į pasirašančiojo asmens sertifikatą, kt.), šalia kurių yra tų duomenų ir informacijos šifras, gautas koduojant asmens privačiuoju raktu. **Pasirašyti duomenys** – tai duomenys plius parašas. 1.1 pav. parodyta duomenų pasirašymo schema.

Pasirašytų duomenų gavėjas parašui tikrinti naudoja atitinkamą įrangą ir siuntėjo viešąjį raktą. Tam gavėjas taip pat sukuria atsiųstų duomenų santrauką. Toliau, atšifruojant parašą siuntėjo viešuoju raktu, atstatoma siuntėjo sukurta duomenų santrauka. Palyginus šias dvi santraukas, įsitikinama parašo tikrumu, t.y. ar duomenys nebuvo iškraipyti ir ar parašą sukūrė asmuo, turintis privatųjį raktą, kuris atitinka atšifravimui naudotą viešąjį raktą. 1.2 pav. parodyta elektroninio parašo patvirtinimo schema.



1.2 pav. Elektroninio parašo tikrinimas (S – siuntėjas, G – gavėjas)

Viešasis raktas yra pasirašiusio asmens sertifikate, o šio asmens sertifikato nuoroda siunčiama elektroniniame paraše kartu su pasirašytais duomenimis. Galimybę pasitikrinti, ar pasirašytus duomenis ir sertifikato nuorodą iš tikro atsiuntė prisistatęs asmuo, suteikia sertifikatų sudarytojai - sertifikatų centrai *(CA – Certification Authorities*). Tikrinant parašą taip pat svarbu įsitikinti, ar parašo kūrimo metu galiojo pasirašiusio asmens sertifikatas, ar nepažeisti sertifikate nustatyti apribojimai ir parašo taisyklės. Parašo tikrinimo įranga ir procedūra turi atitikti nustatytus reikalavimus [7].

Elektroninio parašo labai svarbus komponentas yra nuoroda į pasirašiusio asmens sertifikatą.

1.2. STANDARTŲ, NUSTATANČIŲ SKAITMENINIO SERTIFIKATO STRUKTŪRĄ, APŽVALGA

Elektroniniu parašu pasirašantis asmuo turi turėti sertifikatą. Sertifikatus sudaro ir jų duomenis parašų tikrintojams teikia sertifikatų centrai. Asmenys, norintys gauti sertifikatus, privalo sertifikatų centro registravimo tarnybai pateikti tapatybę patvirtinančius dokumentus ir kitą būtiną informaciją (įskaitant viešąjį šifravimo raktą, jei asmuo raktų porą susigeneravo kitur).

Sertifikatas – tai elektroninio pavidalo liudijimas, patvirtinantis, kad viešasis šifravimo raktas, o tuo pačiu ir jį atitinkantis privatusis šifravimo raktas, priklauso sertifikate nurodytam asmeniui.

Skiriamos dvi sertifikatų rūšys:

- paprasti sertifikatai;
- kvalifikuoti sertifikatai;

Pagrindinis dokumentas nustatantis sertifikato struktūrą yra IETF RFC 2459 standartas [9]. IETF RFC 3039 standarte [11] išdėstyti reikalavimai kvalifikuotiems sertifikatams, patikslinti reikalavimai kai kurių sertifikato laukų turiniui. ETSI TS 101 862 standartas [2] įveda papildomus laukus į sertifikatą, siekiant glaudesnio ryšio su Europos Sąjungos teisės aktais (elektroninio parašo Direktyva 1999/93/EC).

Sertifikato struktūra, naudojant ASN.1 (*Abstract Syntax Notation One*) standarto sintaksę, IETF RFC 2459 standarte pateikta taip:

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

TBSCertificate  ::=  SEQUENCE  {
 version          [0]  EXPLICIT Version DEFAULT v1,
 serialNumber          CertificateSerialNumber,
 signature             AlgorithmIdentifier,
 issuer                Name,
 validity              Validity,
 subject               Name,
 subjectPublicKeyInfo  SubjectPublicKeyInfo,
 issuerUniqueID  [1]   IMPLICIT UniqueIdentifier OPTIONAL,
                 -- If present, version shall be v2 or v3
```

```
subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                  -- If present, version shall be v2 or v3
extensions      [3]  EXPLICIT Extensions OPTIONAL
                  -- If present, version shall be v3}
```

Atsižvelgiant į IETF RFC 2459 [9], IETF RFC 3039 [11] ir ETSI TS 101 862 [2] standartus, matoma, kad kvalifikuotą sertifikatą turėtų sudaryti tokie laukai:

1.1 lentelė

Kvalifikuoto sertifikato laukai

Sertifikato laukas	Paaiškinimas
sertifikato versijos numeris (**version):**	dabar naudojama v3 versija;
sertifikato serijinis numeris (**serialNumber**):	serijinį numerį suteikia sertifikatų centras;
algoritmo, kurį sertifikatų centras naudoja pasirašyti sertifikatams, identifikatorius (**signature**):	RSA ar kt. algoritmo identifikatorius;
sertifikatų centro, kuris sudarė ir pasirašė sertifikatą, pavadinimas (**issuer)**:	nurodoma valstybė, kurioje yra sertifikatų centras, organizacija, organizacijos padalinio vardas ir kiti sertifikatų centrą identifikuojantys duomenys;
sertifikato galiojimo laikas (**validity):**	nuo kokios datos ir laiko, iki kokios datos ir laiko galioja sertifikatas;
asmuo, kuriam sudarytas sertifikatas (**subject**):	fizinio arba juridinio asmens vardas, kuriam priklauso sertifikate nurodytas viešasis raktas;
asmeniui priklausantis viešasis raktas (**subjectPublicKeyInfo)**:	algoritmo identifikatorius ir viešojo rakto reikšmė;
sertifikatų centro unikalus identifikatorius **(issuerUniqueID)**:	(nebūtinas laukas sertifikate);
asmens unikalus identifikatorius **(subjectUniqueID)**:	(nebūtinas laukas sertifikate);
sertifikato išplėtimo laukai (**extentions)**:	(nebūtini laukai sertifikate), nurodoma įvairi papildoma informacija;
algoritmo, kurį sertifikatų centras naudoja pasirašyti sertifikatams, identifikatorius (**signatureAlgorithm**):	SHA-1 su RSA ar kt. algoritmo identifikatorius;
sertifikatų centro elektroninis parašas(**signatureValue)**:	parašo reikšmė.

Panagrinėkime, kokia informacija gali būti sertifikato išplėtimo laukuose. Kiekvienas sertifikate nurodytas išplėtimo laukas turi turėti identifikatorių (pavadinimą). Šie laukai gali būti pažymėti kaip “kritiniai” ir “nekritiniai”.

1.2 lentelė

Kvalifikuoto sertifikato išplėtimo laukai

Sertifikato išplėtimo laukas	Lauke teikiama informacija
Sertifikatų centro raktą, naudojamą pasirašyti sertifikatams, identifikuojanti informacija (***Authority Key Identifier)***	✓ Sertifikatų centro rakto identifikatorius ***(keyIdentifier);*** ✓ Sertifikatų centro sertifikatą sudaręs aukštesnio lygmens sertifikatų centras (***authorityCertIssuer)***; ✓ Sertifikatų centro sertifikato serijinis numeris ***(authorityCertSerialNumber);***

1.2 lentelės tęsinys kitame puslapyje

1.2 lentelės tęsinys

Sertifikato išplėtimo laukas	Lauke teikiama informacija
Asmens, kuriam sertifikatų centras išdavė sertifikatą, rakto identifikatorius (***subjectKey Identifier)***	Naudojamas ypatingos paskirties raktų atvejais (pvz., kitam sertifikatų centrui išduotas raktas, kurį jis naudos sudarytiems sertifikatams pasirašyti).
Rakto naudojimo paskirtis (***key usage***),	Nurodomos rakto paskirtys. Pvz., *keyCertSign* – pasirašyti sertifikatams, *cRLSign* – pasirašyti CRL sąrašams, ir/arba kitos. Kai kurių rakto paskirčių kombinacijos yra neleistinos.
Privačiojo rakto naudojimo terminas ***(Private Key Usage Period)***	Terminas gali skirtis nuo sertifikato galiojimo termino. Pvz., sudarant naują sertifikatą gali būti naudojami senieji raktai.
Sertifikato taisyklės (***Certificate Policies***)	Nurodomi vienerių arba keleto taisyklių identifikatoriai. Taip pat gali būti paaiškinimai, kur galima rasti tas taisykles, sertifikatų centro sertifikavimo veiklos nuostatus , kt.
Asmens papildomi duomenys ***(SubjectAltName)***	Užrašomi asmens elektroninio pašto adresas, internetinis adresas, kt..
Sertifikatų centro papildomi duomenys ***(IssuerAltName)***	Užrašomi sertifikatų centro elektroninio pašto adresas, internetinis adresas, kt..
Asmens atributai (***Subject Directory Attributes***)	Laukas nerekomenduojamas. Jis gali būti vietinėse aplinkose.
Baziniai (bazės) apribojimai ***(Basic Constraints)***	Nurodoma, koks gali būti sertifikatų sekos ilgis. Jei šiame lauke yra reikšmė TRUE, tai sertifikatas priklauso sertifikatų centrui. Eiliniams asmenims turi būti FALSE reikšmė, todėl šio išplėtimo lauko jų sertifikatuose nebūna
Vardų apribojimai ***(Name Constraints)***	Naudojamas tik sertifikatų centrų sertifikatuose. Jame nurodomi leistini sertifikatų centro vardai ir jų ilgis sertifikatų sekoje. Apribojimai apibrėžiami leistinų arba draudžiamų pomedžių terminais.
Sertifikato taisyklių apribojimai ***(PolicyConstraints)***	Gali būti tik sertifikatų centrų sertifikate.
Išplėstinis parašo naudojimo paskirties laukas ***(Extended key usage field)***	Nurodomi sertifikato naudojimo tikslai, papildant arba vietoje lauko “rakto naudojimo paskirtis” .
CRL sąrašų vietos ***(CRL Distribution Points)***	Nurodoma, kur galima gauti CRL informaciją.
Nuosavas Interneto plėtinys ***(Private Internet Extensions)***	Skirtas PKI naudojimo Internetu reikmėms

Siekiant prisiderinti prie Europos Sąjungos reikalavimų, RFC 2459 standartas [9] papildomas RFC 3039 standarto [11] nuostatomis, kurios privalomos kvalifikuotiems sertifikatams.

1.3 lentelė

Pagrindinių laukų, nustatytų RFC 2459 standarto, papildymas RFC 3039 standarto nuostatomis

Sertifikato laukas	**Lauko reikšmės paaiškinimas**
Sertifikatų centro, kuris sudarė ir pasirašė sertifikatą, pavadinimas *(issuer)*	Turi būti atitinkami duomenys iš šio sąrašo: domeno komponentas, valstybės pavadinimas, valstijos ar provincijos pavadinimas, organizacijos pavadinimas, organizacijos padalinio pavadinimas, serijinis numeris.
Asmuo, kuriam sudarytas sertifikatas *(subject)*	Turi būti atitinkami duomenys iš šio sąrašo: valstybės pavadinimas, bendrasis vardas, pavardė, vardas, slapyvardis, serijinis numeris, organizacijos pavadinimas, organizacijos padalinio pavadinimas, valstijos arba provincijos pavadinimas, buvimo vietos pavadinimas, pašto adresas.

1.4 lentelė

Išplėtimo laukų, nustatytų RFC 2459 standarto, papildymas RFC 3039 standarto nuostatomis

Sertifikato išplėtimo laukas	Lauko reikšmės paaiškinimas
Asmens atributai (*Subject Directory Attributes*)	Rašomi reikalingi duomenys iš šio sąrašo: titulas; gimimo data; gimimo vieta; lytis; kurios valstybės pilietis yra; valstybė, kurioje gyvena.
Sertifikato taisyklės (*Certificate Policies*)	Turi būti bent vienerių taisyklių identifikatorius, kurias įgyvendina sertifikatų centras. Lauke turi būti visa taisyklių informacija, reikalinga sertifikato galiojimui patvirtinti.
Rakto naudojimo paskirtis (*key usage*)	Nurodoma rakto naudojimo paskirtis, leistinos rakto naudojimo kombinacijas.
Asmens biometriniai duomenys (*Biometric Information*)	Nurodoma asmens biometrinės informacijos saugojimo vieta ir šios informacijos santrauka (*hash*).

ETSI TS 101 862 standartu [2] nustatomi patikslinti ir papildomi reikalavimai kvalifikuotiems sertifikatams, kurie yra išdėstyti RFC 3039 standarte [11].

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

Sertifikato savybei, kad jis yra kvalifikuotas, nurodyti turi būti atskiras išplėtimo laukas (*qCStatements extension*). Jame nurodomi tokie požymiai: sertifikatas yra kvalifikuotas; leistina operacijų (transakcijų) piniginė vertė, kada sertifikatas gali būti naudojamas; kiek laiko sertifikatas bus saugomas archyve pasibaigus jo galiojimui.

Lietuva savo elektroninio parašo įstatyminę bazę kūrė remiantis standartų RFC 2459, RFC 3039, ETSI TS 101 862 nustatytais reikalavimais [2, 9, 11]. Lietuvos Respublikos elektroninio parašo įstatyme nurodoma, kad :

Sertifikatas **-** elektroninis liudijimas, kuris susieja parašo tikrinimo duomenis (viešąjį raktą) su pasirašančiu asmeniu ir patvirtina arba leidžia nustatyti pasirašančio asmens tapatybę.

Lietuvos elektroninio parašo įstatyme paprastiems sertifikatams nėra numatyta specialių reikalavimų. Specialūs reikalavimai numatyti tik kvalifikuotiems sertifikatams.

Kvalifikuotas sertifikatas **-** sertifikatas, kurį sudarė Vyriausybės ar jos įgaliotos institucijos nustatytus reikalavimus atitinkantis sertifikavimo paslaugų teikėjas.

Lietuvos elektroninio parašo įstatyme nurodyta, kad kvalifikuotame sertifikate turi būti tokie duomenys:

1) užrašas, kad tai yra kvalifikuotas sertifikatas;

2) sertifikavimo paslaugų teikėjo ir jo buveinės šalies identifikatoriai;

3) pasirašančio asmens vardas ir pavardė arba slapyvardis;

4) pasirašančio asmens specialūs atributai, jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus;

5) parašo tikrinimo duomenys (viešasis raktas), atitinkantys pasirašančio asmens turimus parašo formavimo duomenis (privatųjį raktą);

6) sertifikato galiojimo pradžios ir pabaigos terminai;

7) sertifikato identifikatorius, suteiktas sertifikavimo paslaugų teikėjo;

8) sertifikavimo paslaugų teikėjo saugus elektroninis parašas;

9) sertifikato naudojimo paskirties apribojimai, jei tai nustatyta;

10) leistina operacijų piniginė vertė, kada sertifikatas gali būti naudojamas, jei tai nustatyta.

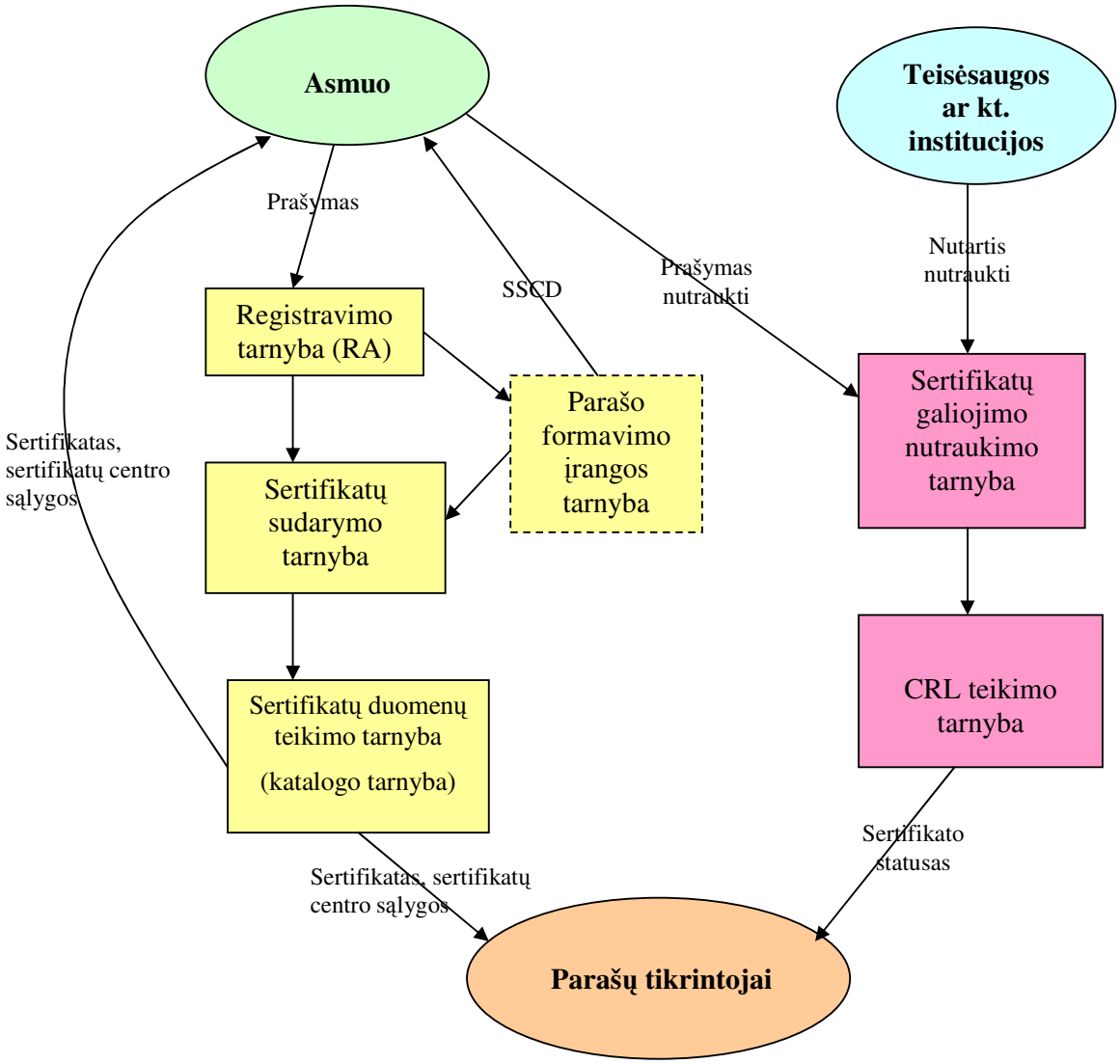
Lietuvos elektroninio parašo įstatyme nurodoma, kad sertifikatai turi būti patvirtinti sertifikatų centro elektroniniu parašu. Todėl sertifikatų centras savo ruožtu turi būti gavęs sertifikatą iš aukštesnio lygmens sertifikatų centro. Aukščiausiojo lygmens sertifikatų centras sertifikatą pasidaro pats.

1.3. ELEKTRONINIO PARAŠO SERTIFIKATŲ CENTRO SUDĖTIS

Lietuvos elektroninio parašo įstatyme nurodoma, kad Sertifikatų centro paskirtis yra sudaryti sertifikatus asmenims, norintiems savo veikloje naudoti elektroninį parašą, ir sertifikatų duomenis teikti elektroninių parašų tikrintojams. Pagrindinėms funkcijoms vykdyti sertifikatų centras turi turėti tokius padalinius, kaip:

- *registravimo tarnyba (RA-Registration Authority)*. Ji iš asmenų priima būtinus duomenis sertifikatams sudaryti, patikrina juos ir perduoda sertifikatų sudarymo tarnybai. sertifikatų centras gali turėti kelias tokias tarnybas įvairiose šalies vietovėse;
- *sertifikatų sudarymo tarnyba*. Ji iš registravimo tarnybos gautų asmens duomenų ir viešojo rakto, gauto iš asmens kartu su jo duomenimis arba iš parašo formavimo įrangos tarnybos (tokia tarnyba gali būti sertifikatų centre), sudaro sertifikatą, pasirašo jį savo elektroniniu parašu ir atiduoda sertifikatų duomenų teikimo tarnybai;
- *sertifikatų duomenų teikimo tarnyba* (*katalogo tarnyba - directory service*). Sertifikatas atiduodamas jo savininkui ir užrašomas į galiojančių sertifikatų duomenų bazę - katalogą. Iš pastarosios duomenų bazės pagal užklausas sertifikatų duomenys teikiami parašų tikrintojams;
- *sertifikatų galiojimo nutraukimo tarnyba*. Šios tarnybos funkcijos yra laiku nutraukti sertifikato galiojimą pačiam sertifikato savininkui paprašius, teisėsaugos institucijų sprendimu, paprašius asmeniui, kuriam atstovauja sertifikato savininkas, arba pasibaigus sertifikate nurodytam jo pabaigos galiojimo terminui. Informacija apie nebegaliojančius sertifikatus kaupiama atitinkamame sąraše (CRL - *Certificate Revocation List*), kuris periodiškai perduodamas CRL teikimo tarnybai;
- *CRL teikimo tarnyba*. Ji informaciją apie nebegaliojančius sertifikatus laiko pas save ir operatyviai pagal užklausas teikia parašų tikrintojams. Tie parašai, kurie buvo sukurti sertifikato galiojimo laikotarpiu, išlieka galiojantys. Elektroninis parašas, sukurtas negaliojant sertifikatui, yra negaliojantis.

Sertifikatų centro veiklos procesai ir naudojama įranga turi atitikti standartų ETSI TS 101 456, CWA 14167-1, CWA 14167-2 nustatytus reikalavimus [1, 3, 4]. 1.3 pav. parodyta sertifikatų centro struktūros schema.



1.3 pav. Sertifikatų centro struktūra

Sudarant sertifikatus jau turi būti sugeneruoti šifravimo raktai. Viešasis raktas dedamas į sertifikatą, o privatusis raktas saugiai įrašomas į laikmeną (pvz., į intelektualiąją kortelę ar diskelį) ir atiduodamas tik užsakiusiam asmeniui. Raktų poroms generuoti sertifikatų centras gali turėti atitinkamą tarnybą – parašo formavimo įrangos tarnybą. Tačiau tokios tarnybos sertifikatų centre gali ir nebūti.

Raktų poras generuoti ir privačiuosius raktus rašyti į saugias laikmenas, gali tuo besiverčiantys kiti sertifikavimo paslaugų teikėjai (nebūtinai sertifikatų centras). Šiuo atveju asmuo, norėdamas gauti sertifikatą, pateikia sertifikatų centrui viešąjį raktą. Viešasis raktas yra visiems laisvai prieinamas, o

privatusis raktas yra prieinamas tik vienam asmeniui. Jis juo pasinaudoti gali tik žinodamas slaptažodį, PIN kodą ar kt. Sertifikatų centras sudaro sertifikatą, jį perduoda užsakiusiam asmeniui ir sertifikatų duomenų teikimo tarnybai.

Parašo formavimo įrangos, t.y. raktų sugeneravimas ir privačiojo rakto laikmenos jiems saugoti ir naudoti parengimas yra kritinis elektroninio parašo infrastruktūros klausimas, lemiantis parašo saugumą. Saugi parašo formavimo įranga (SSCD – *Secure Signature Creation Device*) turi tenkinti standartų CWA 14168**,** CWA 14169 nustatytus reikalavimus [5, 6]**.**

Nepriekaištingam funkcionavimui sertifikatų centras turi paruošti savo sertifikavimo veiklos nuostatus, kurie atitiktų pasirinktas sertifikato taisykles. Sertifikato taisyklės – sertifikato sudarymo ir naudojimo taisyklės, nustatančios paslaugų teikėjo, pasirašančio asmens, parašo naudotojo teises ir pareigas. Sertifikato taisykles apibrėžia ETSI TS 101 456 ir RFC 2527 standartai [1, 10] bei Lietuvos Respublikos Vyriausybės 2002 m. gruodžio 31 d. nutarimas Nr. 2108 ir Lietuvos standartas LST ETSI TS 101 456 „Strateginiai reikalavimai, keliami kvalifikuotus sertifikatus išduodantiems sertifikavimo paslaugų teikėjams“.

1.4. STANDARTO REIKALAVIMAI PATIKIMŲ SERTIFIKATŲ TVARKYMO SISTEMŲ SAUGUMUI

Kad vartotojai pasitikėtų elektroniniu parašu, sertifikatų centrai turi tinkamai atlikti savo funkcijas, laikytis saugumo reikalavimų. Sertifikatų centrai turi naudoti patikimas sistemas ir priemones, apsaugotas nuo pakeitimų ir garantuojančias technologinį bei kriptografinį atliekamų procesų saugumą.

Patikimai sertifikatų centrų veiklai užtikrinti yra nustatyti saugumo reikalavimai patikimoms sertifikatų tvarkymo sistemoms (toliau – Sistema). Sistemos saugumo reikalavimai yra pateikti CWA 14167-1 standarte[3]. Sertifikatų centrai turi naudoti tik saugumo reikalavimus atitinkančią Sistemą. Sistema padeda sertifikatų centrui vykdyti pavestas funkcijas. Jos skirstomos į:

- privalomas pagrindines:
  - ✓ klientų registravimo;
  - ✓ sertifikatų sudarymo;
  - ✓ sertifikatų duomenų teikimo;
  - ✓ sertifikatų galiojimo nutraukimo;
  - ✓ CRL teikimo.
- neprivalomas papildomas*,* tai parašo kūrimo įrangos teikimo bei laiko žymos paslaugos.

Jeigu sertifikatų centras teikia ir papildomas paslaugas, tai naudojama Sistema turi atitikti ir papildomus reikalavimus aprašytus CWA 14167-1 standarte [3]. Darbe nagrinėsime tik privalomas pagrindines sertifikatų centro funkcijas.

Sistemos saugumo reikalavimai skirstomi į dvi grupes: bendruosius ir pagrindinius.

1.4.1. Bendrieji sistemos saugumo reikalavimai

Bendrieji saugumo reikalavimai yra privalomi visoms Sistemos funkcijoms. Į reikalavimus taip pat įeina Sistemoje naudojamų elektroninio parašo algoritmų reikalavimai ir parametrai [13].

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

Sistemoje turi būti priemonės nustatyti ir kontroliuoti su Sistema dirbti galinčių asmenų teisėms ir pareigoms. Sistemą eksploatuoti ir prižiūrėti gali šie pareigūnai:

1) saugumo pareigūnai;
2) registracijos pareigūnai;
3) Sistemos administratoriai;
4) Sistemos operatoriai;
5) Sistemos auditoriai.

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

2. Sistemos veikimas (*Systems&Operations*).

a) *Sistemos priežiūra*. Sistema turi būti eksploatuojama teisingai, kad būtų minimizuota sutrikimų rizika, apsaugota nuo virusų, nuo nesankcionuotų pakeitimų.

b) Sertifikatų centro veiklos nenutrūkstamumas. Sertifikatų centro veikla neturi nutrūkti netgi įvykus Sistemos gedimams. Sertifikatų duomenų, CRL sąrašų teikimas bei prašymų nutraukti sertifikatų galiojimą aptarnavimas neturi nutrūkti ilgam. Sistemos atstatymas neturi turėti įtakos Sistemos patikimumui.

c) Sistemos veiksmų sinchronizavimas laike. 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*) vienos sekundės tikslumu.

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

Tik 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:

a) vartotojų autentifikavimas. Kiekvienas asmuo turi būti identifikuotas ir patikrinti jo įgaliojimai prieš leidžiant jam atlikti bet kokį veiksmą su Sistema.

b) autentiškumo nepripažinimas. Po nustatyto kiekio nesėkmingų autentifikavimo bandymų Sistema turi užblokuoti tolesnius vartotojo autentifikavimo bandymus ir užfiksuoti tokį faktą.

c) slaptųjų elementų tikrinimas. Sistemoje turi būti priemonės patikrinti, ar kiekvieno jos komponento slaptieji elementai atitinka nustatytus reikalavimus. Bet kuriuo atveju bandymo atspėti arba klaidingo kreipimosi tikimybė turi būti labai maža.

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

Kontrolės pagrindinis tikslas yra užtikrinti, kad Sistemos objektus naudotų tik identifikuoti ir atitinkamus įgaliojimus turintys asmenys. 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 kreipimosi į viešai neskelbtiną darbo procese išliekančią informaciją.

5. Raktų tvarkymas *(Key Managemet)*

Skiriamos trys sertifikatų centro raktų kategorijos:

- ✓ raktai kvalifikuotiems ar nekvalifikuotiems sertifikatams pasirašyti;
- ✓ infrastruktūriniai raktai saugiam duomenų perdavimui tarp atskirų Sistemos dalių arba saugomiems duomenims (pvz., audito duomenims) pasirašyti;
- ✓ Sistemos kontroliniai raktai, kuriuos naudoja sertifikatų centro darbuotojai, dirbantys su Sistema.

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

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

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

a) kopijų darymas. Sistemoje turi būti priemonės duomenų kopijoms daryti. Turi būti daromos kopijos tik tų duomenų, kurių reikia Sistemos stoviui atstatyti. Kopijas gali daryti tik įgalioti asmenys – Sistemos operatorius kartu su saugumo pareigūnu;

b) kopijų informacijos vientisumas ir konfidencialumas. Duomenų kopijos turi būti apsaugotos nuo pakeitimo, naudojant elektroninius parašus, duomenų santraukas (*hash)* ar autentifikavimo kodus;

c) Sistemos atstatymas. 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.

1.4.2. Pagrindiniai sistemos saugumo reikalavimai

Pagrindiniai saugumo reikalavimai skirstomi į tokias grupes:

***1. Bendrojo pobūdžio reikalavimai*.**

Visi sertifikatų centro tarnybų siuntinėjami pranešimai turi būti apsaugoti naudojant elektroninius parašus, duomenų santraukas (*hash*) ar autentifikavimo kodus. Pranešimuose turi būti jų sukūrimo laikas, taip pat atsitiktinis skaičius (*nonce*), padedantis apsisaugoti nuo klaidų.

2. Abonentų registravimo reikalavimai *(Registration Service).*

Į sertifikatų centro funkcijas įeina asmenų, prašančių sudaryti sertifikatą, tapatybės ir kitų jų duomenų patikrinimas bei pateiktų duomenų tvarkymas ir saugojimas. Registracijos pareigūnas įstatymų leistinomis priemonėmis turi patikrinti prašytojo tapatybę ir jo pateiktus duomenis sertifikatui sudaryti. Registravimo tarnybos siunčiamų prašymų sertifikatų sudarymo tarnybai konfidencialumas turi būti garantuotas, pasirašant juos infrastruktūriniu arba kontroliniu raktu.

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

Funkcijos ir reikalavimai:

a) sertifikatų sudarymas. Atėjus iš registravimo tarnybos prašymui sudaryti sertifikatą, Sistema sudaro sertifikatą, įtraukdama į jį pateiktą viešąjį raktą. Tokiu būdu abonentas susiejamas su jam priklausančiu viešuoju raktu.

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

Prieš sudarydama sertifikatą Sistema turi patikrinti pareigūno įgaliojimus.

Sertifikatų centro 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 nustatytos formos (profilio) sertifikatai. Visi Sistemos sudaryti kvalifikuoti sertifikatai turi atitikti Lietuvos Respublikos elektroninio parašo įstatymo reikalavimus. Taip pat turi atitikti saugumo reikalavimus, aprašytus CWA 14167-1 ir ETSI TS 101 456 standartuose [3,1].

b) sertifikatų atnaujinimas. 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.

Reikalaujama, kad Sistema garantuotų saugų sertifikatų atnaujinimą ir nebūtų neleistinų pakeitimų sertifikatuose. Atnaujinti privatūs raktai turi garantuoti ne mažesnį kaip buvusį saugumo lygį. Rekomenduojama abonentų sertifikatus keisti dar nesibaigus jų galiojimo terminui, kadangi

pranešimų siuntimo tarp abonento ir sertifikatų centro saugumui užtikrinti gali būti panaudoti senieji raktai/sertifikatai;

c) sertifikatų sudarymo auditas. Sertifikatų sudarymo tarnyba savo veiklos bėgyje turi registruoti tokius duomenis:

- visų sertifikatų centrų sertifikatų, naudojamų abonentams sudaromiems kvalifikuotiems sertifikatams pasirašyti, tvarkymo duomenis;
- visų sertifikatų centro raktų, naudojamų kvalifikuotiems sertifikatams pasirašyti, tvarkymo duomenis;
- visus abonentų sertifikatų tvarkymo duomenis.

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

Sistema turi teikti sertifikatų duomenis laikydamasi abonentų pateiktų apribojimų.

5. Sertifikatų galiojimo nutraukimo reikalavimai (*Certificate Revocation Management Service).*

a) prašymas pakeisti sertifikato statusą. Jei abonentas yra įsitikinęs, kad jo privatusis raktas yra atskleistas, turi būti siunčiamas prašymas nutraukti sertifikato galiojimą jį sudariusiam sertifikatų centrui.

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

Visi prašymai nutraukti sertifikato galiojimą turi būti tinkamai patikrinti (autentifikuoti) ir patvirtinti. Jei sertifikato galiojimas buvo nutrauktas, Sistema turi garantuoti, kad jis nebebus atstatytas.

Sertifikato statusas turi būti keičiamas tik dalyvaujant ir leidus:

- registracijos pareigūnui arba saugumo pareigūnui, keičiant abonentų sertifikatų statusą;
- turint abonento sutikimą dėl jo paties sertifikato statuso keitimo.

Sertifikato taisyklėse gali būti nustatyta, kad abonento sertifikato statusą gali pakeisti trečiasis asmuo (pvz., abonento darbdavys), nusiuntęs atitinkamą prašymą sertifikatų centrui.

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

b) sertifikato galiojimo stabdymas/nutraukimas. Sertifikatų centras yra atsakingas už sertifikatų statuso duomenų atnaujinimą ir perdavimą į nebegaliojančių sertifikatų sąrašų (CRL – *Certificate Revocation List*) teikimo tarnybą. Sistema gali siųsti pranešimus iš sertifikatų galiojimo nutraukimo 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 galiojimo nutraukimo tarnybos.

Sistema turi būti pajėgi nutraukti sertifikato galiojimą netgi po nelaimingų įvykių. Jei pranešimai (CRL sąrašai, CRL pokyčiai ar pavienių sertifikatų statuso informacija) tarp sertifikatų galiojimo nutraukimo 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 papildomai bent kartą per dieną;
- pranešime rekomenduojama kiekvienam CRL sąrašo sertifikatui nurodyti jo serijinį numerį ir statuso keitimo priežastį.

Jei pranešimai tarp sertifikatų galiojimo nutraukimo 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 galiojimo nutraukimo tarnyba iš savo CRL duomenų bazės turi pateikti duomenis apie to sertifikato einamąjį statusą;
- turi būti patikimas duomenų perdavimo kelias tarp sertifikatų galiojimo nutraukimo tarnybos ir CRL teikimo tarnybos;
- užklausos ir atsakymai dėl sertifikatų statuso turi būti apsaugoti nuo klastočių (panaudojant *nonce*);

c) nebegaliojančių sertifikatų tvarkymo. Sertifikatų galiojimo nutraukimo 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) sertifikato statuso duomenys. CRL teikimo tarnyba elektroninių parašų naudotojams teikia sertifikatų statuso (galioja ar nebegalioja) informaciją. CRL teikimo tarnyba duomenis apie sertifikatų statuso pakeitimus gauna iš sertifikatų centro sertifikatų galiojimo nutraukimo tarnybos. Tam yra tokie reikalavimai:

- pranešimus į CRL teikimo tarnybą realiu laiku (kai tik gaunama užklausa) arba periodiškai (nustatytais laiko tarpais) turi siųsti tik sertifikatų galiojimo nutraukimo tarnyba;
- Sistema, *on-line* režimu 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. Pasitikinti šalis (parašo tikrintojas), gavusi iš sertifikatų centro sertifikatų duomenų teikimo tarnybos reikiamą sertifikatą parašui patikrinti, turi patikrinti ir sertifikato statusą. Sertifikatų statuso informaciją teikia CRL teikimo tarnyba. Tai CRL tarnyba 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) režimu.

On-line režimo atveju pasitikinti šalis siunčia į CRL tarnybą užklausą dėl sertifikato statuso. CRL tarnyba realiu laiku kreipiasi į sertifikatų duomenų bazę einamajai informacijai apie sertifikatą gauti arba, jei naudojamas periodinis CRL sąrašų apsikeitimas tarp bazės ir CRL teikimo tarnybos, šią informaciją CRL tarnyba ima iš paskutinio periodiškai gauto CRL sąrašo. Klausėjui siunčiamas suformuotas atsakymas, kuriame yra informacija apie jį dominančio sertifikato statusą.

Off-line režimo atveju CRL teikimo tarnyba, turėdama paskutinę CRL sąrašo versiją, persiunčia ją pasitikinčiai šaliai, kad ji galėtų tikrintis sertifikatų statusus.

Reikalavimai CRL teikimo tarnybos atsakymams:

- *on-line* režimu išduotas atsakymas turi būti pasirašytas tarnybos skaitmeniniu parašu;
- atsakyme turi būti nurodytas laikas, kada CRL teikimo tarnyba pasirašė atsakymą.

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

1.4.3. Saugūs duomenų perdavimo protokolai

Sertifikatų centras su parašo tikrintojais bendrauja elektroninėje erdvėje. Sertifikatų centras turi užtikrinti perduodamų duomenų saugumą. Saugumui užtikrinti diegiamos įvairios technologijos pvz.. saugūs protokolai, ugniasienės (firewall). Saugūs protokolai - vienas efektyviausių ir populiariausių metodų elektroninių duomenų perdavimo saugumui užtikrinti. Šiuo metu yra sukurta daug ir įvairių duomenų perdavimo protokolų.

1.5 lentelė

Duomenų perdavimo protokolų palyginimas

Eil. Nr.	Protokolo pavadinimas	Trumpas aprašymas
1.	HTTP *(HyperText Transfer Protocol)*	Pranešimai neapsaugoti, visa informacija perduodama kaip ASCII tekstas, kurį nesąžiningi žmonės gali pakeisti.
2.	SSL *(Secure Sockets Layer)*	Apsaugo komunikacijos kanalą. Seanso tarp kliento ir tarnybinės stoties pradžioje nustatomas simetrinis raktas (*sesion key*), šifravimo algoritmas, patikrinama kliento ir tarnybinės stoties tapatybė. Simetrinį raktą sukuria kliento naršyklė ir užšifruoja tarnybinės stoties viešuoju raktu. Tarnybinė stotis iš kliento gautą simetrinį raktą atšifruoja savo privačiuoju raktu ir naudoja jį viso seanso metu. SSL protokolas numato galimybę autentifikuoti vartotoją. SSL protokolu, galima naudotis nemokamai. „Netscape‘ ir „Microsoft“ naršyklės „supranta“ SSL v.3.0.

1.5 lentelės tęsinys kitame puslapyje

1.5 lentelės tęsinys

Eil. Nr.	Protokolo pavadinimas	Trumpas aprašymas
3.	SET *(Secure Electronic Transaction)*	Protokolas skirtas atsiskaitymams kreditinėmis kortelėmis. SET pranešimus sudaro dvi dalys - užsakymo informacija (*Order Information*) ir mokėjimo informacija (*Payment Information*). Pirmoji informacija skirta pardavėjui, o antroji - bankui. SET protokolo licenzija mokama, todėl SSL už SET gerokai populiaresnis.
4.	S-HTTP *(Secure HTTP)*	Tai HTTP protokolo plėtinys, skirtas saugiai siųsti duomenis „Web“ tinklu. S-HTTP taikomojo lygio protokolas apsaugo siunčiamus pranešimus tarp tarnybinės stoties ir vartotojo. Jis leidžia tarnybinei stočiai ir naršyklei pasirašyti elektroniniu parašu, sudaryti ir šifruoti paketus. S-HTTP užšifruoja siunčiamus pranešimus, kuo ir skiriasi nuo SSL, sukuriančio saugų kanalą duomenims siųsti.
5.	IPSec *(IP Security)*	„IPSec“ protokolų rinkinys apsaugo duomenis IP paketų lygiu. Naudojami du IPv4 adresų plėtiniai: ESP (*Encapsulating Sesurity Payload*) antraštė ir autentifikavimo antraštė (*authentication header, AH*). „IPSec“ leidžia taikyti du duomenų siuntimo režimus: transporto ir tunelio. „IPSec“ dažniausiai naudojamas virtualiose privačiuose tinkluose. „IPSec“ saugumo galimybėmis galima naudotis tik turint IPv6 adresus.
6.	PCT *(Private Cummunications Technology)*	„Microsoft“ sukurtas protokolas, funkciškai labai panašus į SSL. PCT protokole ištaisytos klaidos, buvusios SSL v.1.0 ir SSL v.2.0 versijose. Kaip ir SSL protokole, seanso pradžioje „sutariamas“ seanso raktas ir simetrinis šifravimo algoritmas. Tačiau autentifikavimas atliekamas atskirai nuo šifravimo, todėl jo mechanizmas patikimesnis už SSL. PCT protokolo licenzija mokama.

Atlikus protokolų apžvalgą galima daryti išvadą, kad šiuo metu populiariausias ir pakankamai saugus protokolas yra SSL. Todėl darbe duomenų perdavimui naudosiu SSL protokolą.

1.5. SERTIFIKATŲ CENTRŲ ANALITINĖ APŽVALGA

Pagal galiojantį Lietuvos Respublikos elektroninio parašo įstatymą, Nr. VIII-1822, įsigaliojusį nuo 2000 07 26, mūsų šalyje gali veikti ne vienas sertifikatų centras. Abonentams išduodamame sertifikate turi būti jį sudariusio sertifikatų centro elektroninis parašas. Kad sertifikatų centras galėtų pasirašinėti elektroniniu parašu, jis savo ruožtu turi gauti sertifikatą iš aukštesnio lygmens sertifikatų centro. Aukščiausiasis (nacionalinis, valstybinis) sertifikatų centras sertifikatą pasidaro pats. JAV, Kanadoje, Australijoje, kitur nacionaliniai sertifikatų centrai yra valstybiniai. Nacionalinio sertifikatų centro vienas iš uždavinių yra koordinuoti visų kitų sertifikatų centrų veiklą, kad būtų laikomasi vieningų standartų ir taisyklių šioje veikloje.

Elektroninio parašo sertifikatų centrai veikia įvairiose pasaulio šalyse. Kai kurie plačiai žinomi visame pasaulyje. Magistriniame darbe, apžvelgsiu keleto šalių sertifikatų centrus ir jų teikiamas paslaugas ir veiklos principus. Sertifikatų teikimo veiklai analizuoti naudojausi informacija, pateikta interneto tinklalapiuose. 1.6 lentelėje išskyriau keletą kriterijų, pagal kuriuos vertinau sertifikatų centrų veiklą. Pateikta informacija daugiau skirta bendrajam palyginimui.

1.6 lentelė

Sertifikatų centro veiklos vertinimo kriterijai

Kriterijus	Galimi atsakymai
Sertifikatų centro (SC) vieta	Kur įsikūręs SC
Reikalavimai sertifikato prašymo pateikimui	Prašymas turi būti pateikiamas asmeniškai
	Prašymas turi būti pateiktas su įgaliojimu
	Prašymas gali būti pateikiamas per tinklą
Atsakomybė ir sutarčių sąlygos, nustatytos SC veiklos nuostatuose	Nuostatai apibrėžia ribotą turtinę SC atsakomybę
	SC prisiima visą atsakomybę
	Turtinė atsakomybė nurodoma ne tik SC veiklos nuostatuose, bet galima sudarant ir individualias sutartis
Sertifikatų naudojimo sritys	Sertifikatai fiziniams asmenims
	Sertifikatai juridiniams asmenims
	Sertifikatai serveriams
Teisinis pagrindas	Elektroninio parašo įstatymo pagrindu
	Pagrindiniu ginčų sprendimo įstatymu
	Licencijuojama veikla pagal įstatymą
Prieinama informacija	SC veiklos nuostatai (CPS)
	Nebegaliojančių sertifikatų sąrašas (CRL)
	Viešai prieinama sertifikatų duomenų bazė
Paslaugų kaina	Informacijos pateikimo kaina

„128i“ sertifikatų centras

„128i“ yra Naujojoje Zelandijoje veikiantis viešasis sertifikatų centras. Šis sertifikatų centras elektroninio tinklo vartotojams teikia identifikavimo ir autorizavimo paslaugas. „128i“ užtikrina visišką bendravimo internetu saugumą. Sertifikatų centro naudojami procesai yra visiškai suderinti su tarptautiniais procedūriniais ir saugumo standartais. „128i“ sertifikatų centras bendradarbiauja su pasaulyje žinomiausiais, saugius komunikavimo sertifikatus naudojančiais partneriais. „128i“ yra sertifikuotas ISO 9001 standartu. Išsamesnė „128i“ sertifikatų centro veikos analizė pateikta 1.7 lentelėje.

Hong Kong paštas

Hong Kong paštas yra įkūręs viešojo rakto infrastruktūrą ir veikia kaip pirmasis viešasis sertifikatų centras Hong Konge. Hong Kong pašto viešasis sertifikatų centras išduoda skaitmeninius sertifikatus privatiems ir juridiniams asmenims, įgalinančius identifikuoti abonentą. Hong Kong pašto išduodami skaitmeniniai sertifikatai vadinami e-CERT. Sertifikatų centras prižiūri sertifikatų duomenų bazę, kad visuomenė galėtų pasitikrinti viešojo rakto galiojimą, prieš atliekant pašto veiksmus.

VeriSign, Inc.

VeriSign **-** vienas seniausiai ir sėkmingiausiai veikiantis skaitmeninių sertifikatų (viešųjų raktų infrastruktūros) centras, ne tik USA, bet ir visame pasaulyje. Jų vartotojai yra stambios kompanijos. Šio sertifikatų centro teikiamos paslaugos užtikrina vartotojams saugų bendravimą internete ir kituose tinkluose. VeriSign turi ryšius su daugiau kaip 100 nepriklausomų programinės įrangos tiekėjų.

Kompanija yra užmezgusi strateginius bendravimo ryšius su garsiomis kompanijomis kaip Visa, Netscape, Microsoft, AT&T, Softbank, Oracle, American Onlain, Hewlett-Packard ir daugeliu kitų. Sertifikatų centro viešųjų raktų infrastruktūros spendimai veikia efektyviai su standartiniais tiekėjų produktais. VeriSign turi atstovybę Japonijoje. VeriSign integruota viešojo rakto platforma yra pasiekiama per VeriSign vietinius atstovus, perpardavėjus arba tiesiogiai per jų interneto puslapius. Saugaus serverio identifikatorius (ID) ir jo skaitmeninis identifikatorius (ID) pasiekiamas tiesiogiai per kompanijos tinklalapį.

Netrust

Bendra įmonė NCB (Nacional Omputer Bord) ir NETS (Network for Electronic Transaction Pte LTD) buvo sukurta 1997 metų gegužę tikslu sukurti saugią apsikeitimo duomenimis aplinką. Netrust pirmas sertifikatų centras Pietų Azijoje (Singapūre). Jis teikia skaitmeninius sertifikatus patvirtinančius rekvizitus šalių, dalyvaujančių elektroniniuose duomenų pasikeitimuose. Naudodamos Netrust paslaugas įmonės, įstaigos ir organizacijos gali elektroniniu būdu bendrauti saugiai ir konfidencialiai.

GlobalSign

GlobalSign sertifikatų centras yra vienas žinomiausių sertifikatų centrų Europoje. Jis įsikūręs Belgijoje. GlobalSign sertifikatai pripažįstami nepriklausomai nuo geografinės padėties, verslo šakos ar programos. Šio sertifikatų centro sąjunga su Microsoft, Netscape, RSA Security ir kitomis kompanijomis lėmė tai, kad GlobaSign viešasis pagrindinis raktas įtrauktas į visas pagrindines interneto naršykles ir kitas klientines programas.

Pagal 1.6 lentelėje pateiktus sertifikatų veiklos vertinimo kriterijus atlikta penkių sertifikatų centrų veiklos palyginamoji analizė. Analizės rezultatai pateikti 1.7 lentelėje.

1.7 lentelė

Informacija apie sertifikatų centrus

Kriterijus	128i	Hong Kong Post	Verisign, Inc.	Netrust	GlobalSign
Kur įsikūręs Sertifikatų centras	Naujoji Zelandija	Hong Konge	USA	Singapūre	Belgija
Prašymas turi būti pateikiamas asmeniškai	ne	taip	Tik 3 klasės sertifikatams	taip	taip
Prašymas turi būti pateiktas su įgaliojimu	taip	taip	2 ir 3 klasės sertifikatams	taip	taip
Prašymas gali būti pateikiamas per tinklą	Inicijuojama per operaciją	ne	taip	ne	ne
Nuostatai apibrėžia ribotą turtinę SC atsakomybę	taip	taip	taip	taip	taip
SC prisiima visą atsakomybę	taip	taip	taip	taip	ne
Turtinė atsakomybė nurodoma ne tik nuostatuose, bet apibrėžiama sudarant ir individualias sutartis	nenustatyta	nenustatyta	taip	nenustatyta	nenustatyta

1.7 lentelės tęsinys kitame puslapyje

1.7 lentelės tęsinys

Kriterijus	128i	Hong Kong Post	Verisign, Inc.	Netrust	GlobalSign
Sertifikatai išduodami fiziniams asmenims	taip	taip	taip	taip	taip
Sertifikatai išduodami juridiniams asmenims	taip	taip	taip	taip	taip
Sertifikatai išduodami serveriams	taip	taip	taip	taip	ne
Teisinis pagrindas - Elektroninio parašo įstatymas	nenustatyta	Elektroninių transakcijų potvarkiu	nenustatyta	nenustatyta	nenustatyta
Teisinis pagrindas - Pagrindinis ginčų sprendimo įstatymas	Naujosios Zelandijos	Hong Kongo specialaus administracinio regiono	USA, Kalifornijos valstijos	Singapūro Respublikos	nenustatyta
Licencijuojama veikla pagal įstatymą	nenustatyta	taip	nenustatyta	nenustatyta	nenustatyta
Ar yra SC veiklos nuostatai (CPS)	taip	taip	taip	taip	taip
Ar teikiamas nebegaliojančių sertifikatų sąrašas (CRL)	taip	taip	taip	taip	taip
Viešai prieinama sertifikatų duomenų bazė	Taip, bet abonentas gali atsisakyti	taip	taip	taip	taip
Informacijos pateikimo kaina	$NZ 150 $NZ 450	$HK 50 $HK 2,500	$US 20 ir daugiau.	$S 18 $S 1,000	16€ - 70€

Atlikus elektroninio parašo sertifikatų centrų veiklos analizę, nustatyta, kad visi centrai sudaro sertifikatus fiziniams ir juridiniams asmenis, visi centrai turi savo veiklos nuostatus, parašo tikrintojams teikia nebegaliojančių sertifikatų sąrašus ir teikia duomenis iš sertifikatų duomenų bazės.

Atsižvelgiant į analizės rezultatus magistrinio darbo projekte bus kuriami elektroninio parašo sertifikatai fiziniams ir juridiniams asmenims, bus sudaromas nebegaliojančių sertifikatų sąrašas ir duomenys parašo tikrintojams bus teikiami iš sertifikatų duomenų bazės.

1.6. ELEKTRONINIO PARAŠO SERTIFIKATŲ CENTRŲ PROGRAMINĖS ĮRANGOS APŽVALGA

Atliekant elektroninio parašo sertifikatų centrų apžvalgą pastebėjau, kad sertifikatų centrų tinklalapiuose dažnai deklaruojamas programinės įrangos atitikimas standartams ir įstatymams, tačiau programinės įrangos gamintojai ar diegimo subtilybės nėra skelbiamos. Manau, kad tai yra teisinga tendencija, nes išsami informacija apie saugumą tikrai nedidina pačios sistemos saugumo. Norint detaliau pažvelgti galimą bazinę elektroninio parašo infrastruktūros programinę įrangą reikia nagrinėti rinkos pasiūlą.

Tarp sertifikatų valdymo programinės įrangos gamintojų galima būtų išskirti tokias kompanijas arba produktus: Entrust, Baltimore Technologies, RSA Security Inc, iD2 technologies, IBM Vault Registry, Micrrosoft Certificate Server, Netscape Certificate Server, Entegrity.

Pagrindinė sertifikatų centrų programinės įrangos tiekėja yra kompanija „Baltimore Technologies“. Jos siūloma programinė įranga „UniCERT“ sudaryta iš atskirų komponentų, kurių kiekvienas gali būti įdiegtas ir palaikomas atskirai. Visi komponentai tarpusavyje keičiasi informacija arba per Oracle duomenų bazės duomenų perdavimo sistemą arba per saugius TCP/IP (PKIX) protokolo ryšius. Tai leidžia skirtingus UniCERT komponentus įdiegti skirtingose tarnybinėse stotyse ir tokiu būdu paskirstyti sistemos apkrovimą. UniCERT administravimas yra apsaugotas elektroninių kortelių (*smart cart*) naudojimo principais.

Ši programinė įranga veikia Windows ir Unix operacinėse sistemose; palaiko X.509 standarto sertifikatus; palaikoma RSA (iki 4096 bitų), DSA ir ECDSA kriptografija.

Rsa Security Inc. „RSA Keon“ produktų grupės programinė įranga „RSA Keon Certificate Authority“ atlieka sertifikatų centro sertifikatų valdymo sistemos funkciją. Ši programinė sistema veikia Solaris, Windows 2003 ir Windows NT operacinėse sistemose, palaiko X.509 v3 tipo sertifikatus, naudoja PKIX, SSL, S/MIME, IPSec ir SET protokolus, RSA, DSA ir ECDSA kriptografiją. Sertifikatų statuso informacija bei vidinė šios programinės įrangos informacija perduodama LDAP v2/v3 ir X.500 formatais, koduojama SSL technologija. Minimalūs reikalavimai serverio techninei įrangai – Pentium 4, 512MB operatyvios atminties, 300MB disko talpa.

Atlikus elektroninio parašo sertifikatų centruose naudojamos programinės įrangos analizę nustatyta, kad sertifikatų centruose naudojama Oracle duomenų bazės duomenų perdavimo sistema. Nors darbe būtų galima naudoti ir ORACLE 8i duomenų bazę, tačiau įsigyti tokios duomenų bazės programinę įrangą, paleisti ją yra labai brangu. Todėl darbe bus naudojama MySQL DBVS, kadangi ši priemonė platinama nemokamai, o su ja sukurtą programos prototipą galima nesunkia paleisti Oracle duomenų bazės sistemoje.

1.7. ELEKTRONINIO PARAŠO INFRASTRUKTŪROS VYSTYMO LIETUVOJE PROBLEMOS

Lietuva, siekdama neatsilikti nuo kitų Europos valstybių, pagal savo išgales diegia naujas informacijos technologijas. Elektroninio parašo technologijos naudojimą sąlygoja elektroninio verslo plėtra. Šios technologijos panaudojimas susietas su elektroninio parašo infrastruktūra, kurią būtina sukurti.

Elektroninio parašo elektroniniams duomenims teisinė galia turi būti tokia pati kaip ir ranka rašyto parašo rašytiniuose dokumentuose ir turi būti leidžiama naudoti jį kaip įrodinėjimo priemonę teisme. Tą patvirtina Lietuvos Respublikos elektroninio parašo įstatymas kuris įsigaliojo 2000-07-26. Įstatymas atitinka ES Direktyvos 1999/93/EC nuostatas. Šiam įstatymui įgyvendinti būtina

elektroninio parašo infrastruktūra – teisės aktų, normatyvinių dokumentų, standartų, organizacinių ir technologinių priemonių visuma.

Elektroninio parašo priežiūros institucijos funkcijas Lietuvoje atlieka Informacinės visuomenės plėtros komitetas prie Lietuvos Respublikos Vyriausybės. Jo funkcijos buvo apibrėžtos LR Vyriausybės nutarimais 2004-12-31 Nr.2106 „Dėl Lietuvos Respublikos Vyriausybės 2001 m. liepos 5 d. nutarimo Nr. 844 „Dėl Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės nuostatų patvirtinimo" pakeitimo“ ir 2002-04-23 Nr. 568 “ Dėl elektroninio parašo priežiūros institucijos”.

Kad vartotojai pasitikėtų elektroniniu parašu, reikia, kad sertifikatų centrai tinkamai atliktų savo funkcijas, laikytųsi saugumo reikalavimų. Todėl LR Vyriausybė (2002-12-31 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“) apibrėžė sertifikatų centrų funkcijas.

Informacinės visuomenės plėtros komitetas (IVPK) prie LRV 2003 metų pradžioje išleido įsakymus „Dėl minimalios draudiminės sumos kvalifikuotus sertifikatus sudarantiems sertifikavimo paslaugų teikėjams nustatymo“, „Dėl laiko žymos formavimo paslaugų“ teikimo tvarkos patvirtinimo“, „Dėl sertifikavimo paslaugų teikėjų akreditavimo reikalavimų ir tvarkos patvirtinimo“, reikalingus elektroninio parašo infrastruktūros plėtrai.

Lietuvoje elektroninio parašo teisinė bazė jau sukurta. Jos pakanka norintiems plėtoti elektroninio parašo infrastruktūrą, steigti sertifikatų centrus, atitinkančius Europos Sąjungos reikalavimams. Deja elektroninis parašas plačiau Lietuvoje dar nenaudojamas, kadangi iki šiol nėra nė vieno sertifikatų centro.

1.8. PROJEKTAVIMO METODAS IR PRIEMONĖS

Informacinės sistemos (IS) gali būti kuriamos vadovaujantis skirtingomis metodologijomis, pasirenkant skirtingas priemones. Kiekviena iš metodologijų reikalauja atitinkamo IS gyvavimo ciklo, turi savas galimybes. Gyvavimo ciklas - tai inžinerijos metodo realizavimo proceso modelis. Gyvavimo ciklo parinkimas yra tiesiogiai susijęs su turimos IS projektavimo programinės įrangos galimybėmis.

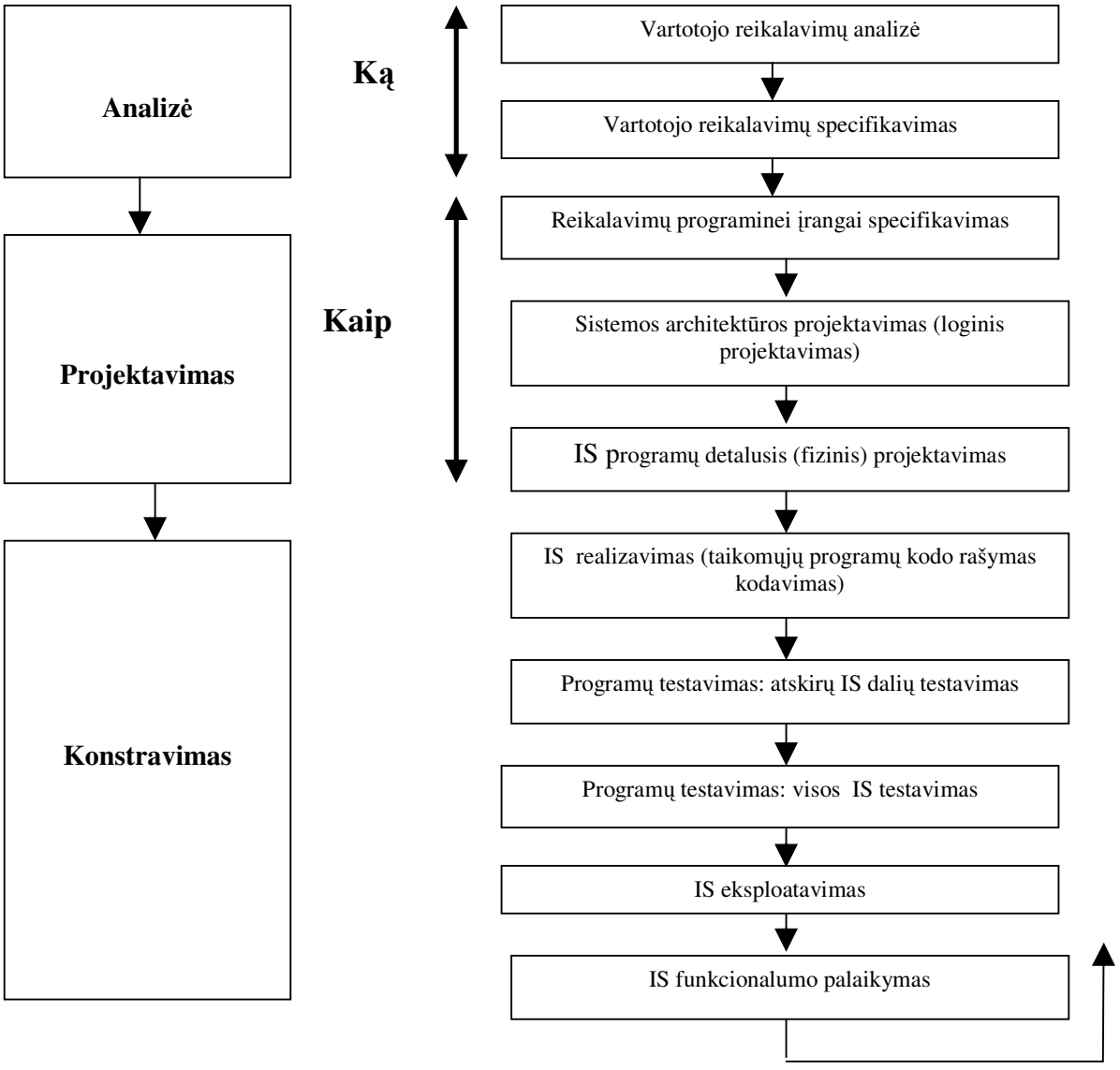
Žinomi keli klasikiniai IS kūrimo gyvavimo ciklo modeliai:

- Tradicinis arba „krioklio tipo“ gyvavimo ciklas, realizuojantis funkcinę dekompoziciją metodu „iš viršaus žemyn“ (*top-dow approach);*
- Objektinis arba „fontano tipo“ gyvavimo ciklas, skirtas realizuoti objektiškai orientuotą požiūrį metodu „iš apačios viršun“ (*bottom-up approach);*
- Iteracinis arba spiralės tipo gyvavimo ciklas, realizuojantis evoliucinį IS kūrimą;

× Lygiagretusis gyvavimo ciklas, taikomas dideliems projektams, kuriuos vykdo didelė projektavimo komanda.

Gyvavimo ciklo modelių yra ir daugiau. Šiuo metu pasaulyje yra daug CASE paketų, kiekvienas realizuoja savo gyvavimo ciklo modelį. Darbe naudosiu CASE sistemą ProVision Workbench^{TM}v.3.1, kuri grindžiama tradiciniu gyvavimo ciklu arba „krioklio tipo“ gyvavimo ciklu.

Tradicinis gyvavimo ciklas turi „krioklio tipo“ pavadinimą, nes jis aprašo IS inžinerijos eigą metodu „iš viršaus žemyn“. Trys apibendrinti IS inžinerijos etapai (analizė, projektavimas, realizavimas) skaidomi į smulkesnius žingsnius. Pagrindiniai IS gyvavimo ciklo etapai [25] pavaizduoti 1.4 paveiksle.



1.4 pav. Tradicinis (krioklio tipo) IS gyvavimo ciklas

Naudojant šį IS gyvavimo ciklą, IS kūrimo metu neatsižvelgiama į evoliucinius kompiuterizuotos sistemos pakitimus.

1.9. ANALITINĖS DALIES IŠVADOS IR PASIŪLYMAI

Visame pasaulyje pripažįstama, kad informacinės technologijos vystosi labai sparčiai ir yra neišvengiamas mūsų veiklos ir gyvenimo atributas. Kaip ir visame pasaulyje, taip ir Lietuvoje sparčiai vystosi elektroninė komercija. Elektroninės komercijos plėtra glaudžiai susijusi su elektroniniu parašu. Elektroninis parašas suteikia galimybę šiuolaikiniams verslo partneriams išlaikyti bendravimo konfidencialumą, taip pat, siunčiant svarbius dokumentus, identifikuoti autorių, nustatyti informacijos tikrumą, vientisumą. Viena problema: įgyvendinant Lietuvoje elektroninį parašą trūksta sertifikavimo institucijos, kuri išduotų kvalifikuotus sertifikatus. Tai turėtų būti Vyriausybės ar jos įgaliotos institucijos nustatytus reikalavimus atitinkantis sertifikavimo paslaugų teikėjas.

Pradžioje elektroninio parašo vartotojų būtų nedaug, o sertifikatų sudarymas, kaip ir visame pasaulyje, turėtų būti mokama paslauga. Manau, kad šia paslauga pirmiausiai pasinaudotų didelių komercinių firmų bei bankų atstovai. Reikia pripažinti, nemaža dalis gyventojų neturi pakankamo išsilavinimo ir žinių, kad galėtų pasinaudoti elektroniniu parašu. Šiuo metu vienu iš pagrindinių prioritetų turi būti švietimas, elektroninio raštingumo gerinimas. Tik gerai informuoti žmonės gali pradėti naudoti elektroninį parašą.

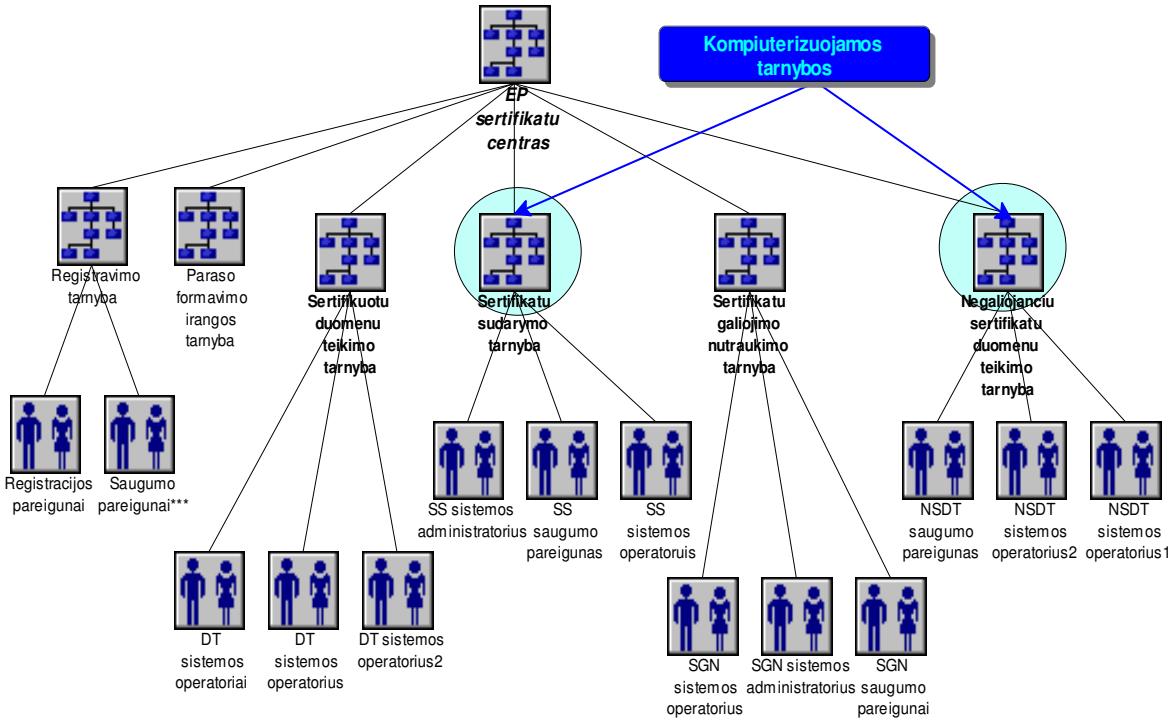
Pasaulyje egzistuoja daug sertifikatų centrų, kurie teikia kvalifikuotus ir nekvalifikuotus sertifikatus. Visų nagrinėtų sertifikatų centrų sudaromi sertifikatai atitinka IETF RFC 2459, IETF RFC 3039, ETSI TS 101 862 standartuose [9, 11, 2] nustatytą sertifikato struktūrą. Visos sertifikavimo paslaugos mokamos. Sertifikato kaina priklauso nuo sertifikato patikimumo. Daugumos sertifikatų centrų tinklalapiuose yra sukurtos demonstracinės versijos, leidžiančios iki įsigijimo sertifikatą pabandyti. Manau, kad tokiu būdu atliekama ir švietėjiška funkcija, nes kiekvienas susidomėjąs gali nemokamai išbandyti elektroninio parašo priemones. Taip pat visi nagrinėti sertifikatų centrai turi viešai prieinamą sertifikatų duomenų bazę ir pateikia negaliojančių sertifikatų sąrašą (CRL).

Siekiant užtikrinti sertifikatų centrų IS saugumą apie sertifikatų centruose naudojamą programinę įrangą pateikiama labai mažai informacijos. Norint detaliau apžvelgti bazinę elektroninio parašo infrastruktūros programinę įrangą, teko nagrinėti rinkos pasiūlą. Galima teigti, kad pagrindinė sertifikatų centrų programinės įrangos gamintoja yra „Baltimore Technologies“.

2. PROJEKTO DALIS

2.1. SERTIFIKATŲ CENTRO CHARAKTERISTIKA

Nagrinėjamasis objektas – elektroninio parašo sertifikatų centro informacinė sistema. Sertifikatų centrą sudaro 6 tarnybos: registravimo tarnyba, sertifikatų sudarymo tarnyba, parašo formavimo įrangos tarnyba, sertifikatų duomenų teikimo tarnyba, sertifikatų galiojimo nutraukimo tarnyba, nebegaliojančių sertifikatų sąrašo (CRL) teikimo tarnyba. Sertifikatų centre labai svarbią reikšmę turi auditas, tačiau tokios nedidelės įmonės organizacinėje schemoje audito skyrių išskirti kaip padalinį yra netikslinga. Parašo formavimo įrangos tarnybos sertifikatų centre gali ir nebūti. Raktų poras generuoti ir privačiuosius raktus rašyti į saugias laikmenas gali tuo besiverčiantys kiti paslaugų teikėjai (ne tik sertifikatų centras). Šiame darbe nagrinėsime sertifikatų sudarymo, sertifikatų duomenų teikimo, nebegaliojančių sertifikatų duomenų teikimo, sertifikatų galiojimo nutraukimo tarnybas.



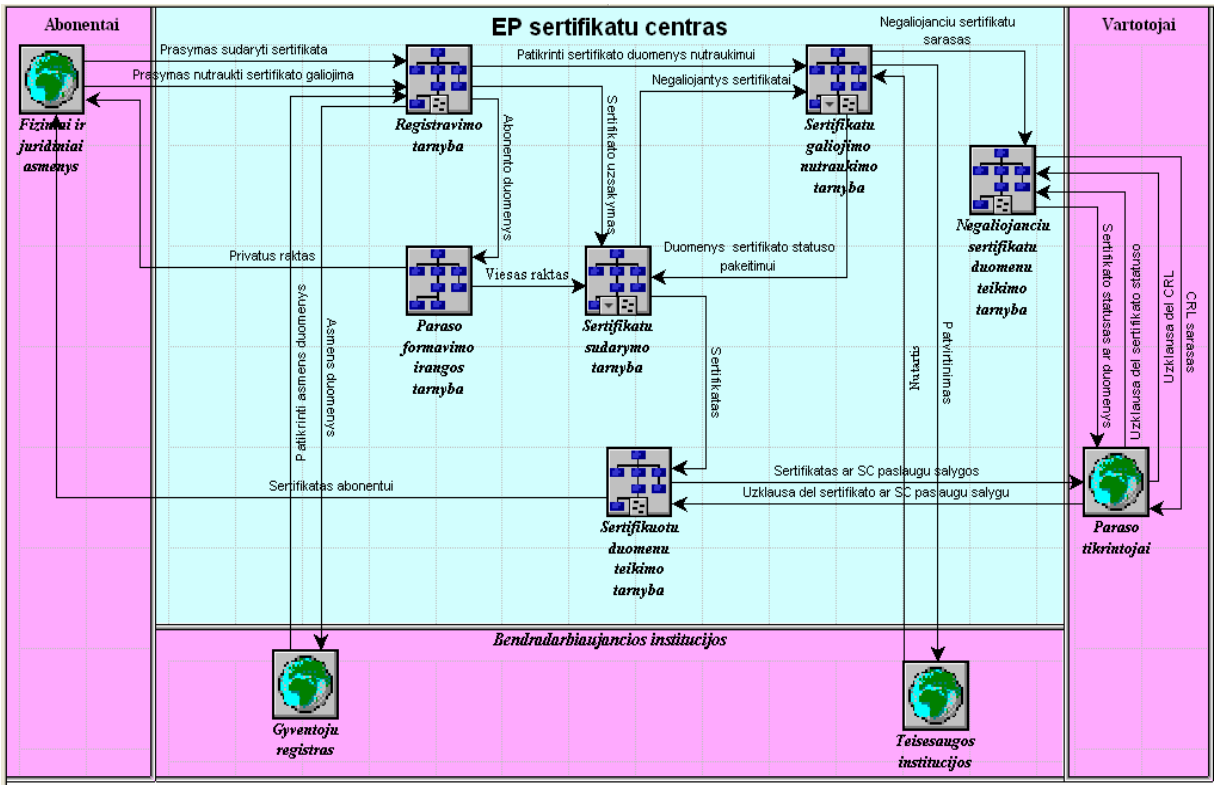
2.1 pav. Elektroninio parašo sertifikatų centro organizacinė struktūra

2.2. SERTIFIKATŲ CENTRO VEIKLOS MODELIS

Sertifikatų centro veiklos procesai ir naudojama įranga turi atitikti standartų ETSI TS 101 456, CWA 14167-1, CWA 14167-2 nustatytus reikalavimus [1, 3, 4]. Atsižvelgiant į šiuos reikalavimus sudarytas elektroninio parašo sertifikatų centro veiklos sąveikų modelis (2.2 pav.).

Veiklos sąveikų modelis parodo sąveiką tarp vidinių organizacijos objektų ir išorinių organizacijų. Šiame modelyje yra įvertinamos organizacijos objektų sąveikos ir ryšiai su vartotojais, abonentais ir bendradarbiaujančiomis institucijomis. Veiklos sąveikų modelis nėra orientuotas į organizacinių vienetų apibrėžimą, bet greičiau į ryšius ir informacijos siuntimus tarp organizacijų.

Modelyje svarbiausia yra vidinė sritis, atspindinti organizacijos veiklos sferą. Elektroninio parašo sertifikatų centro veiklos modelis pateiktas 2.2 paveiksle. Vidinė sritis - elektroninio parašo sertifikatų centro veikla, aplink kurią yra išsidėstę išoriniai objektai: abonentai, vartotojai ir bendradarbiaujančios institucijos.



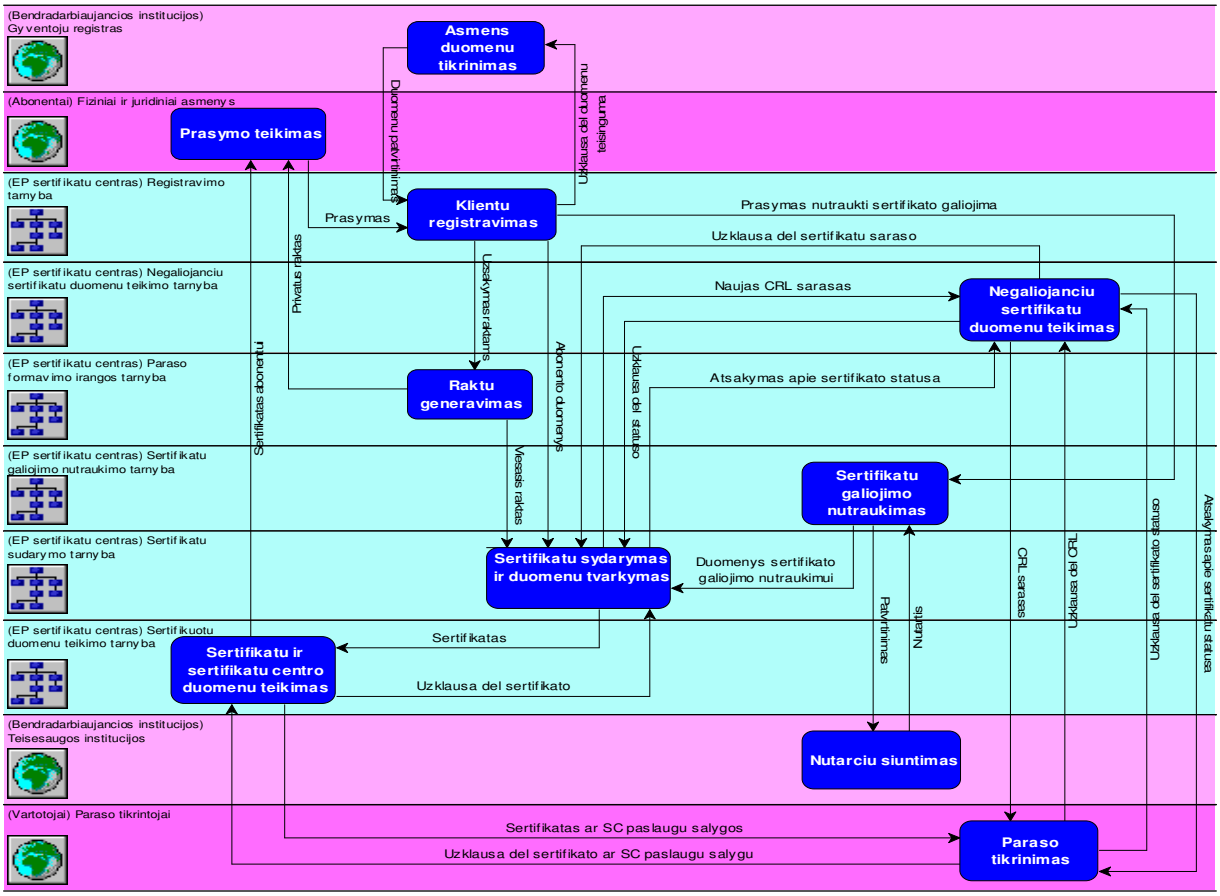
2.2 pav. Sertifikatų centro veiklos modelis

Abonentai sąveikauja su elektroninio parašo sertifikatų centru teikdami prašymus sudaryti sertifikatą ar nutraukti sertifikato galiojimą bei priimdami elektroninio parašo sertifikatus. Vartotojai (parašų tikrintojai) sąveikauja su šia organizacija gaudami informaciją apie sertifikatų centro abonentų sertifikatus. Bendradarbiaujančios institucijos - gyventojų registras, juridinių asmenų registras, teisėsaugos institucijos - taip pat sąveikauja su sertifikatų centru teikdamos informaciją apie sertifikatų centro būsimus abonentus ir siųsdami teisėsaugos institucijų nutartis nutraukti sertifikato galiojimą. Abonentai, vartotojai ir bendradarbiaujančios institucijos yra išoriniai objektai, šios rinkos dalyviai. Tiek tarp išorinių, tiek tarp vidinių esybių egzistuoja tarpusavio ryšiai-veiklos, kurie turi nurodytą duomenų srauto kryptį. Veiklos apibrėžiamos darbų sekos modeliu.

2.3. SERTIFIKAVIMO MODELIS

Sertifikatų centre vykstantiems procesams analizuoti yra sudarytas darbų sekų modelis. Kuriant jį panaudotas sertifikatų centro veiklos modelis (2.2 pav.), į kurį yra įtrauktos pagrindinės organizacinės struktūros, atliekančios tam tikrus darbus. Naudojant darbų sekos modeliavimą, sukurtas detalus veiklų modelis, kuris apima visą sertifikatų centro veiklos procesą.

Darbų sekos modelis atvaizduoja sertifikatų centro veiklos procesus, išreiškiant juos veiklos komponentais ir darbų seka tarp tų veiklų. Šis modelis atspindi darbų seką nuo veiklos pradžios iki galo (2.3 pav.), kuria siekiama bendro sertifikavimo tikslo.

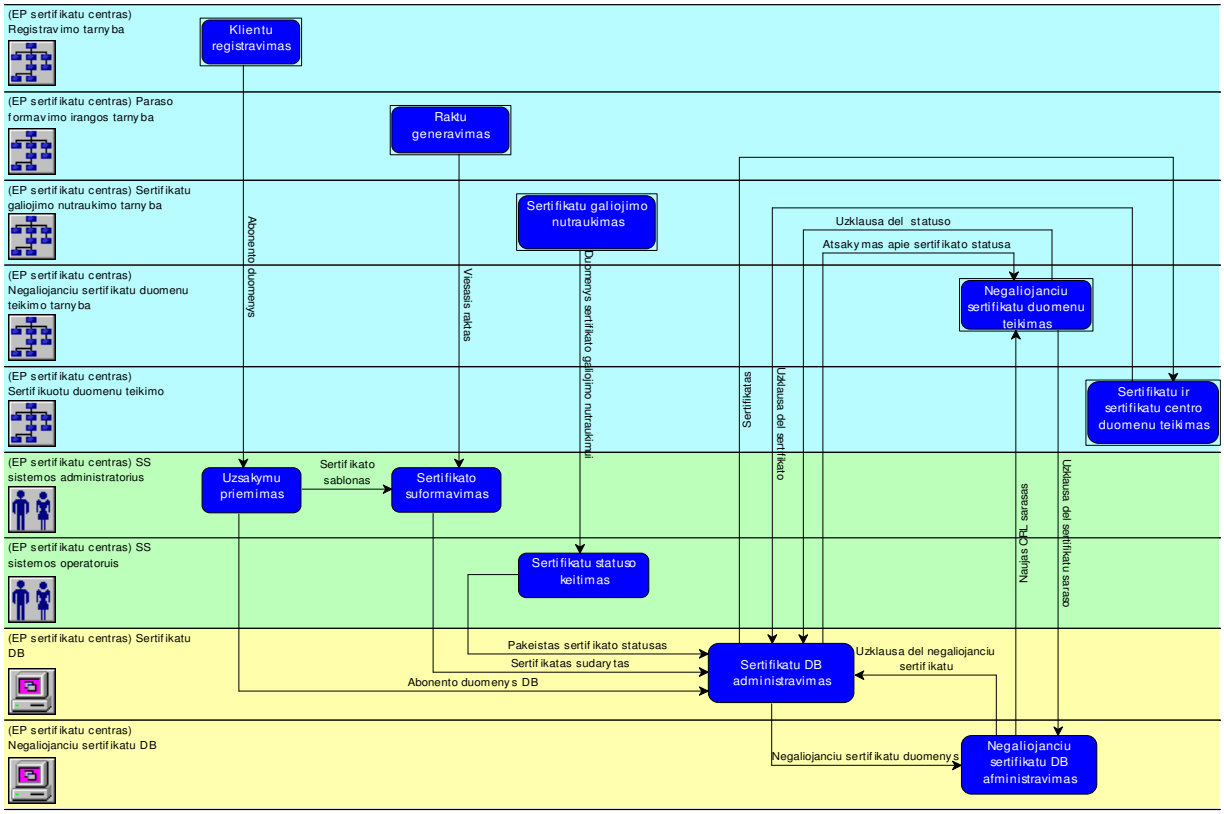


2.3 pav. Sertifikavimo darbų sekų modelis

Toliau darbe detaliau nagrinėjami sertifikatų ir sertifikatų centro duomenų teikimo, sertifikatų sudarymo ir duomenų tvarkymo, sertifikatų galiojimo nutraukimo, negaliojančių sertifikatų duomenų teikimo procesai. Kadangi visi ankščiau išvardinti procesai susideda iš eilės darbų, tai šiems procesams sukurti detalesni žemesnio lygio darbų sekų modeliai.

2.3.1. Sertifikatų sudarymo ir duomenų tvarkymo veiklos modelis

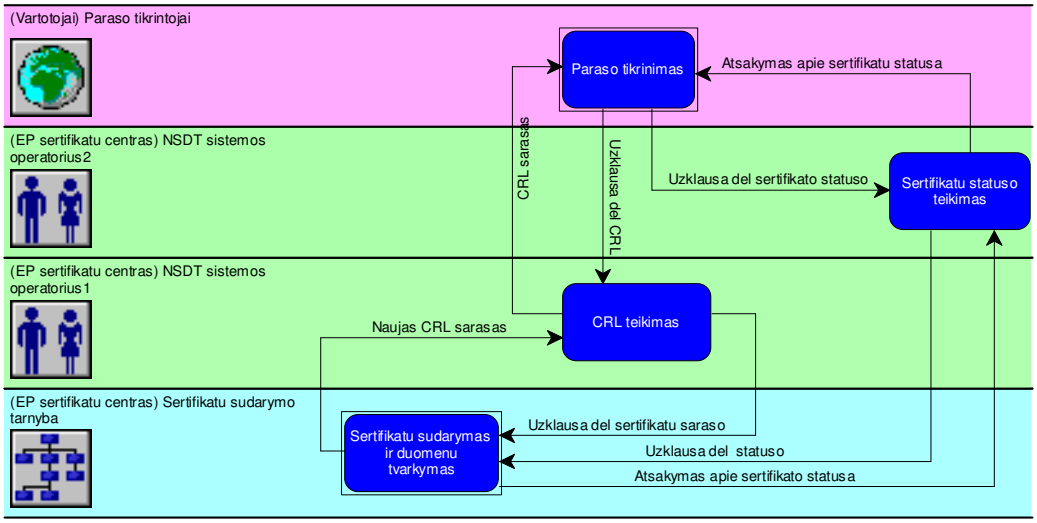
Sertifikatų sudarymo ir duomenų teikimo darbų sekų modelis aprašo atitinkamą sertifikatų centro funkciją. Sertifikatų sudarymo ir duomenų tvarkymo darbų sekos modelis (2.4 pav.) apima užsakymų priėmimo, sertifikatų suformavimo, sertifikatų statuso keitimo, sertifikatų duomenų bazės bei negaliojančių sertifikatų duomenų bazės administravimo procesus.



2.4 pav. Sertifikatų sudarymo ir duomenų tvarkymo darbų sekų modelis

2.3.2. Negaliojančių sertifikatų duomenų teikimo veiklos modelis

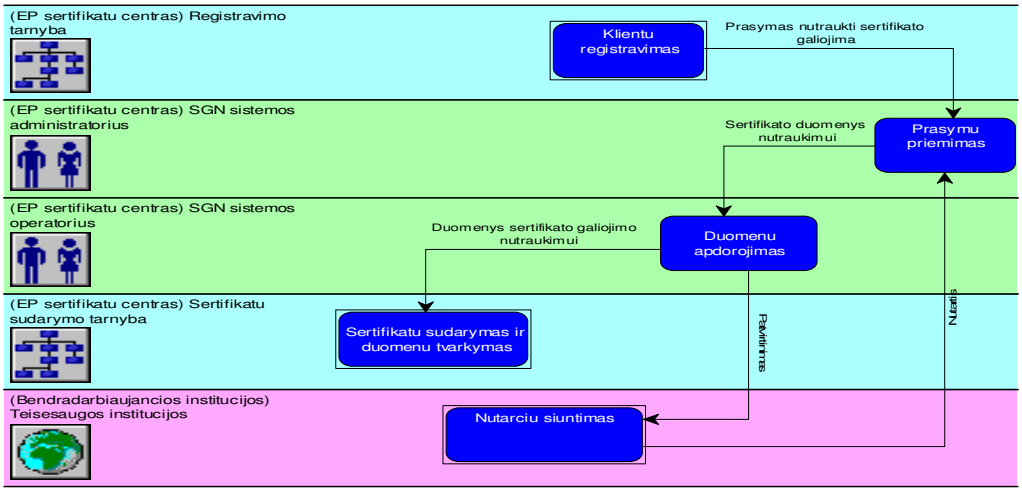
Negaliojančių sertifikatų duomenų (CRL) teikimo darbų sekų modelis (2.5 pav.) vaizduoja procesus, vykstančius teikiant CRL sąrašus elektroninio parašo tikrintojams. CRL teikimo tarnyba teikia informaciją vartotojams. Gavusi užklausą iš vartotojo, CRL teikimo tarnyba apdoroja ją ir siunčia į sertifikatų sudarymo tarnybą. Iš sertifikatų sudarymo tarnybos gauna naujausią CRL sąrašą, kurį pateikia vartotojams (parašo tikrintojams).



2.5 pav. Negaliojančių sertifikatų duomenų teikimo darbų sekų modelis

2.3.3. Sertifikatų galiojimo nutraukimo veiklos modelis

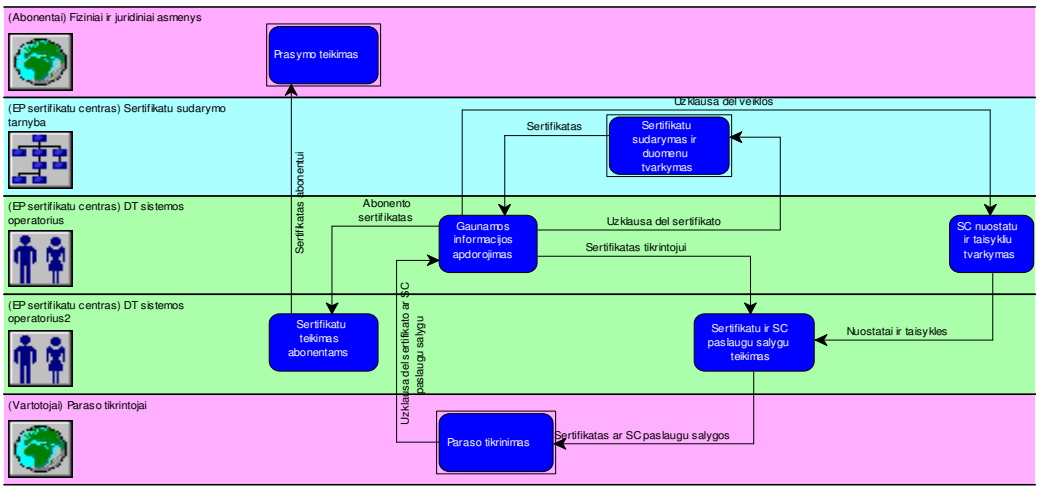
Sertifikatų galiojimo nutraukimo darbų sekų modelis aprašo sertifikatų galiojimo nutraukimo funkciją. Sertifikatų galiojimo nutraukimo darbų sekų modelis (2.6 pav.) apima prašymų priėmimo ir duomenų apdorojimo procesus.



2.6 pav. Sertifikatų galiojimo nutraukimo darbų sekų modelis

2.3.4. Sertifikatų ir sertifikatu centro duomenų teikimo veiklos modelis

Sertifikatų ir sertifikatų centro duomenis teikia sertifikatų duomenų teikimo tarnyba. Šios tarnybos funkciją aprašo sertifikatų ir sertifikatų centro duomenų teikimo darbų sekų modelis (2.7 pav.). Parašo tikrintojai siunčia užklausą dėl sertifikato statuso į sertifikatų duomenų teikimo tarnybą. Gauta užklausa apdorojama ir persiunčiama į sertifikatų sudarymo tarnybą sertifikato statusui gauti. Iš sertifikatų sudarymo tarnybos ateina atsakymas apie sertifikato statusą. Gauti duomenys teikiami parašo tikrintojams. Kai sudaromas naujas sertifikatas, jis patalpinamas į sertifikatų duomenų bazę. Iš jos sertifikatas gali būti perduotas abonentui.

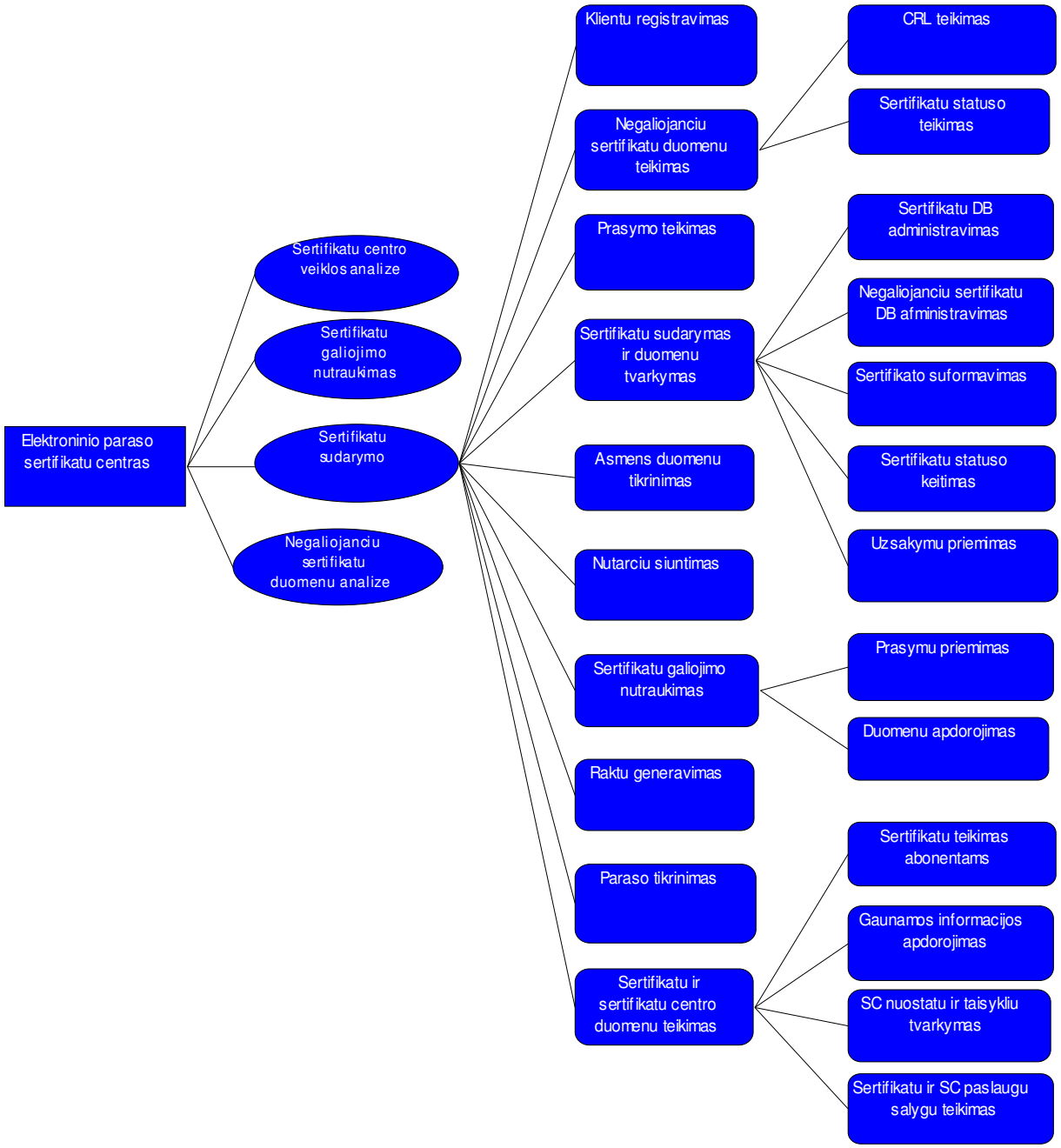


2.7 pav. Sertifikatų ir sertifikatu centro duomenų teikimo darbų sekų modelis

2.4. ELEKTRONINIO PARAŠO SERTIFIKATŲ CENTRO PROCESŲ MODELIS

Elektroninio parašo sertifikatų centro procesų modelis (2.8 pav.) yra sukurtas iš veiklos modelio (2.2 pav.) ir darbų sekų modelių (2.3-2.7 pav.). Procesų modelyje sudaroma veiklos procesų hierarchinė struktūra.

Kadangi procesų modelis yra kuriamas ir iš darbų sekų modelio, tai į jį yra įtraukiami darbų sekų modelio darbai kaip žemesnio lygio hierarchiniai procesai.



2.8 pav. Elektroninio parašo sertifikatų centro procesų modelis

2.5. VARTOTOJŲ POREIKIŲ ANALIZĖ IR SPECIFIKAVIMAS

Elektroninio parašo sertifikatų centro informacinė sistema aptarnauja sertifikatų sudarymo, sertifikatų duomenų teikimo, sertifikatų galiojimo nutraukimo ir negaliojančių sertifikatų duomenų teikimo tarnybas (žr. 1.3 pav.). Projekte nagrinėjami informaciniai procesai:

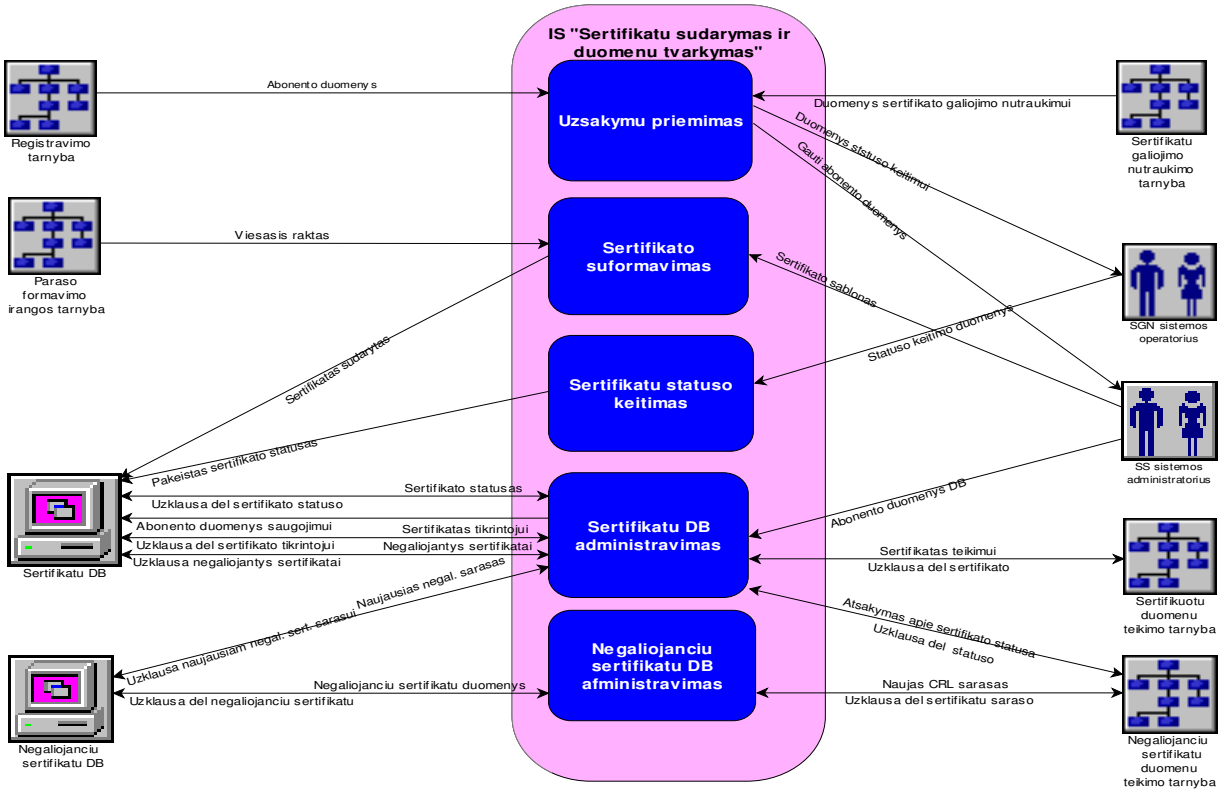
- sertifikatų sudarymas ir duomenų tvarkymo;
- negaliojančių sertifikatų duomenų teikimo;
- sertifikatų galiojimo nutraukimo;
- sertifikatų ir sertifikatų centro duomenų teikimo.

Turi būti kompiuterizuojami sertifikatų sudarymo, duomenų tvarkymo ir negaliojančių sertifikatų duomenų teikimo procesai, todėl jiems sudaromi taikomųjų uždavinių modeliai.

Taikomųjų uždavinių modelis detaliai aprašo ne tik informacijos srautus, bet ir kompiuterizuojamus uždavinius. Taikomųjų uždavinių modeliai sudaromi toliau tikslinant darbų sekų modelį, detaliai aprašant kompiuterizuojamus uždavinius.

2.5.1. Sertifikatų sudarymo ir duomenų tvarkymo taikomųjų uždavinių modelis

Sertifikatų sudarymo ir duomenų tvarkymo taikomųjų uždavinių modelis detaliai aprašo IS „Sertifikatų sudarymas ir duomenų tvarkymas“ informacijos srautus ir kompiuterizuojamus uždavinius (2.9 pav.). Sertifikatų sudarymo ir duomenų tvarkymo taikomųjų uždavinių modelis sudarytas smulkiau detalizuojant sertifikatų sudarymo ir duomenų tvarkymo darbų sekų modelį (2.4 pav.).



2.9 pav. Sertifikatų sudarymo ir duomenų tvarkymo taikomųjų uždavinių modelis

2.1 lentelė

Sertifikatų sudarymo ir duomenų tvarkymo taikomųjų uždavinių aprašymas

Uždavinys	Aprašymas
Užsakymų priėmimas	Registravimo tarnybų sertifikatų centras gali turėti ne vieną. Gavusi asmens prašymą registravimo tarnyba patikrina gautų duomenų teisingumą ir, jei duomenys teisingi, suformuoja užsakymą sertifikatui sudaryti ir siunčia į sertifikatų sudarymo tarnybą. Registravimo tarnyba į sertifikatų sudarymo tarnybos užsakymų priėmimą siunčia duomenis pasirašytus registravimo tarnybos elektroniniu parašu. Iš abonento duomenų suformuojamas sertifikato šablonas. Į sertifikatą talpinami duomenys priklausomai nuo abonento tipo. Visi abonento duomenys perkeliami į pagrindinę duomenų bazę. Užsakymų priėmimas atliekamas ir iš sertifikatų galiojimo nutraukimo tarnybos sertifikatų statusui pakeisti.
Sertifikato formavimas	Viena iš pagrindinių sertifikatų centro funkcijų - sudaryti sertifikatą. Visi sudaryti kvalifikuoti sertifikatai turi atitikti Lietuvos Respublikos elektroninio parašo įstatymo reikalavimus. Jie taip pat turi atitikti saugumo reikalavimus, aprašytus CWA 14167-1 ir ETSI TS 101 456 standartuose [3,1]. ETSI TS 101 456 standartas [1] reikalauja, kad sertifikate būtų nurodytas ir asmens vardas (arba slapyvardis), sertifikato leidėjas, o sertifikato išplėtimo laukuose (*extentions*) – asmens atributai, sertifikato taisyklės, rakto naudojimo paskirtis, biometriniai asmens duomenys, užrašas, kad tai kvalifikuotas sertifikatas. Atsižvelgiant į visus standartus, kvalifikuotame sertifikate turėtų būti tokie duomenys: × užrašas, kad tai yra kvalifikuotas sertifikatas; × sertifikavimo paslaugų teikėjo ir jo buveinės šalies identifikatoriai; × pasirašančio asmens vardas ir pavardė arba slapyvardis. Jei yra slapyvardis, tas turi būti aiškiai pabrėžta; × pasirašančio asmens specialūs atributai, jei tai reikalinga atsižvelgiant į numatomus sertifikato naudojimo tikslus; × parašo tikrinimo duomenys (viešasis raktas), atitinkantys pasirašančio asmens turimus parašo formavimo duomenis (privatųjį raktą); × sertifikato galiojimo pradžios ir pabaigos terminai; × Sistemos suteiktas unikalus sertifikato vardas ir serijos numeris. Tas unikalumas turi būti sertifikatų centro ribose; × sertifikatų centro saugus elektroninis parašas, sukurtas naudojant sertifikatų centro privatųjį raktą, skirtą pasirašyti kvalifikuotus sertifikatus; × Sistemos naudojamas algoritmas sertifikatams pasirašyti, atitinkantis standartų reikalavimus; × sertifikato naudojimo paskirties apribojimai, jei tai nustatyta; × leistina operacijų piniginė vertė, kada sertifikatas gali būti naudojamas, jei tai nustatyta. × sertifikato taisyklių nuoroda.
Sertifikatų statuso keitimas	Sertifikatų galiojimo nutraukimo tarnyba gavusi abonento prašymą pakeisti sertifikato statusą turi tinkamai tą prašymą patikrinti (autentifikuoti). Patikrinusi duomenis, sertifikatų galiojimo nutraukimo tarnyba kreipiasi į sertifikatų sudarymo tarnybą pakeisti sertifikato statusą. Maksimalus laiko tarpas tarp prašymo gavimo ir sertifikato galiojimo nutraukimo, įskaitant prašytojo autentiškumo nustatymą ir nutraukimo žinios paskelbimą, neturi būti didesnis kaip viena diena. Sertifikatų sudarymo tarnyba gauna sertifikato galiojimo nutraukimo priežasties aprašymą ir sertifikato numerį. IS, gavusi šiuos duomenis, pakeičia sertifikato statusą, įrašant sertifikato statuso pakeitimo laiką. IS privalo būti sinchronizuotas su UTC laiku vienos sekundės tikslumu. Duomenų bazė su sertifikatų statuso duomenimis pakoreguojama nedelsiant.
Negaliojančių sertifikatų duomenų bazės administravimas	Sertifikatų centro viena iš funkcijų teikti parašo tikrintojams negaliojančių sertifikatų sąrašus (CRL). CRL duomenų bazė apdoroja užklausas iš negaliojančių sertifikatų duomenų teikimo tarnybos. Periodiškai formuojama užklausa sertifikatų duomenų bazei naujausiam CRL sąrašui gauti.

2.1 lentelės tęsinys kitame puslapyje

2.1 lentelės tęsinys

Uždavinys	Aprašymas
Sertifikatų duomenų bazės administravimas	Visi sertifikatų centro abonentų duomenys saugomi sertifikatų duomenų bazėje. Į šią duomenų bazę talpinami sudaryti sertifikatai bei sertifikatai su pakeistu statusu. Šios duomenų bazės paskirtis apdoroti užklausas, ateinančias iš sertifikatų duomenų teikimo tarnybos, negaliojančių sertifikatų duomenų teikimo tarnybos, ir užklausas, ateinančias iš negaliojančių sertifikatų duomenų bazės. Parašo tikrintojas per sertifikatų duomenų teikimo tarnybą iš duomenų bazės parsisiunčia sertifikatą ir turi pasitikrinti sertifikato statusą. Kai *on-line* režimo atveju elektroninio parašo tikrintojas siunčia į negaliojančių sertifikatų duomenų (CRL) teikimo tarnybą užklausą dėl sertifikato statuso, CRL teikimo tarnyba realiu laiku kreipiasi į sertifikatų duomenų bazę einamajai informacijai apie sertifikatą gauti. Naudojamas periodinis CRL sąrašų apsikeitimas tarp sertifikatų duomenų bazės ir negaliojančių sertifikatų duomenų bazės.

2.2 lentelė

Sertifikatų sudarymo ir duomenų tvarkymo taikomųjų uždavinių modelio duomenų srautų aprašymas

Duomenų srautas	Aprašymas
Abonento duomenys	Registravimo tarnyba pateikia abonento duomenis. Nurodomas abonento tipas: fizinis ar juridinis asmuo. Jei abonentas yra fizinis asmuo pateikiami šie duomenys: vardas, pavardė arba slapyvardis, asmens kodas, adresas, telefonas, e-pašto adresas. Jei abonentas yra fizinis asmuo, atstovaujantis juridinį asmenį, pateikiami: vardas, pavardė, asmens kodas, adresas, telefonas, e-paštas, organizacijos pavadinimas, padalinio pavadinimas, organizacijos adresas, šalis kur įsikūrusi organizacija, organizacijos telefonas, organizacijos e-paštas, įstaigos kodas, įgaliojimo registracijos numeris, įgaliojimo fiziniam asmeniui išdavimo data ir vieta, asmens pareigos.
Gauti abonento duomenys	IS pateikia sertifikatų sudarymo tarnybos sistemos administratoriui abonento duomenis. Jei abonentas yra fizinis asmuo, pateikiami duomenys: vardas, pavardė arba slapyvardis, asmens kodas, adresas, telefonas, e-paštas. Jei abonentas yra fizinis asmuo, atstovaujantis juridinį asmenį, pateikiami duomenys: vardas, pavardė arba slapyvardis, asmens kodas, adresas, telefonas, e-paštas organizacijos pavadinimas, padalinio pavadinimas, organizacijos adresas, šalis kur įsikūrusi organizacija, organizacijos telefonas, organizacijos e-paštas, įstaigos kodas, įgaliojimo registracijos numeris, įgaliojimo asmeniui išdavimo data ir vieta, darbuotojo pareigos.
Viešasis raktas	Parašo formavimo įrangos tarnyba pateikia abonento viešąjį raktą. Viešasis raktas susideda iš dviejų dalių: modulio (*modulus*) ir eksponentės (*exponent*). Pagal EESSI reikalavimus modulio reikšmei užrašyti turi būti ne mažiau kaip 1024 bitų.
Sertifikato šablonas	Sertifikatų sudarymo tarnybos operatorius paruošia sertifikato šabloną, įveda duomenis. Jei abonentas yra fizinis asmuo, įvedami šie duomenys: vardas, pavardė arba slapyvardis, sertifikato versija, viešojo rakto algoritmas, rakto ilgis, sertifikatų centro duomenys, sertifikato naudojimo apribojimai, galiojimo pabaigos terminas. Jei abonentas - juridinis asmuo, įvedami duomenys: organizacijos pavadinimas, šalis kur įsikūrusi organizacija, sertifikato versija, viešojo rakto algoritmas, rakto ilgis, sertifikatų centro duomenys, apribojimai, galiojimo pabaigos terminas.
Duomenys sertifikato galiojimo nutraukimui	Sertifikatų galiojimo nutraukimo tarnyba pateikia užsakymą sertifikato galiojimo nutraukimui. Nurodomas sertifikato numeris, sertifikato galiojimo nutraukimo priežastis, abonento vardas, pavardė.
Duomenys statuso keitimui	IS pateikia abonento pavardę, vardą, sertifikato numerį ir sertifikato galiojimo nutraukimo priežastį.

2.2 lentelės tęsinys kitame puslapyje

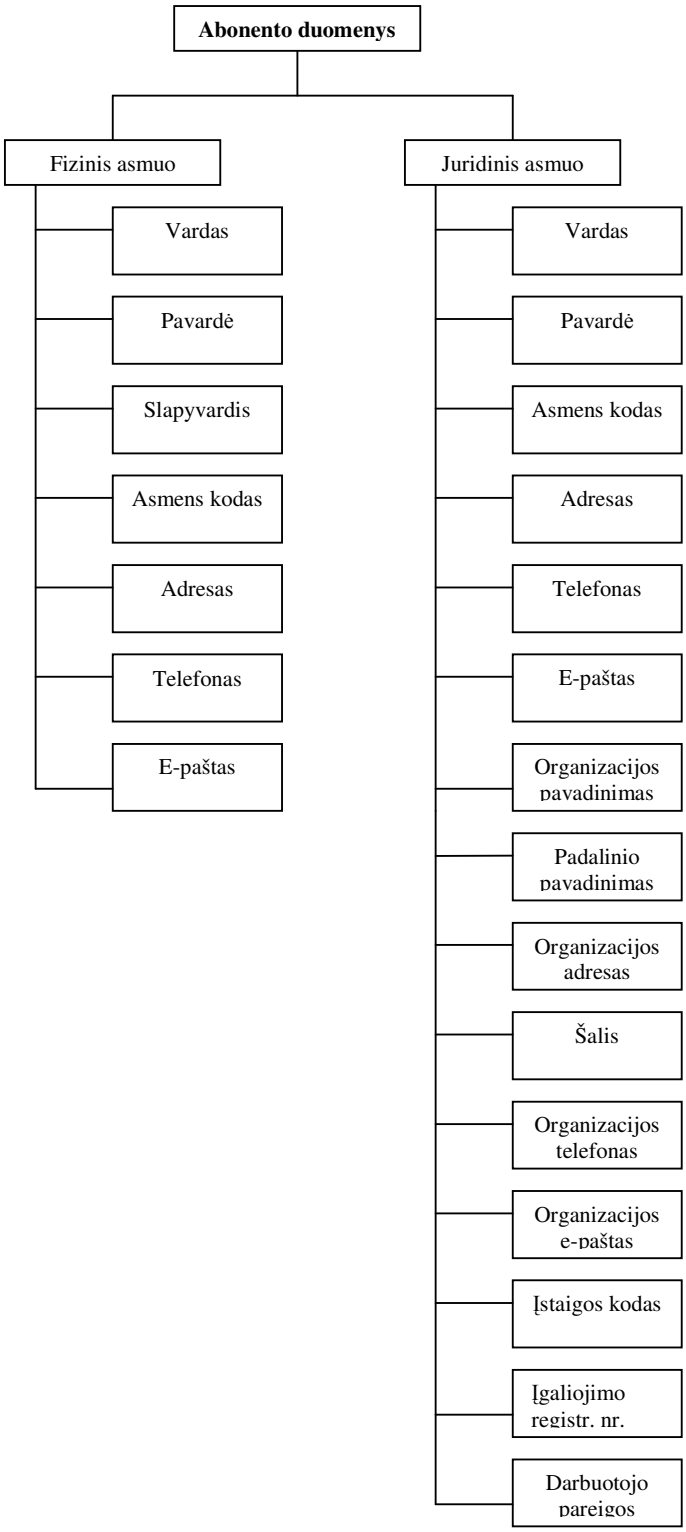
2.2 lentelės tęsinys

Suformuotas sertifikatas	IS pateikia DB sertifikatą, suformuotą pagal X.509 V3 standartą. Suformuotame sertifikate yra duomenys: sertifikato versija (šiuo metu V3 (0x2)), sertifikato serijinis numeris, parašo algoritmo identifikatorius, sertifikatų centro duomenys: C = LT, O = Vilnius University, OU = Info faculty, CN = LTVUSERT, e-mail = sert@ltvusert.lt, sertifikato galiojimo laikotarpis (nuo kada ir iki kada galioja sertifikatas), subjektas. Subjektas priklauso nuo abonento tipo. Jei tai fizinis asmuo, pateikiama vardas, pavardė arba slapyvardis, o jei juridinis asmuo- šalis kur įsikūrusi organizacija, organizacijos pavadinimas, padalinio pavadinimas, elektroninio pašto adresas. Taip pat pateikiamas viešojo rakto algoritmas, rakto ilgis, viešasis raktas (16-taine sistema). Pateikiami sertifikato išplėtimo laukai (X509v3 extentions) **Sertifikatų centro rakto identifikatorius** (Authority Key Identifier): **Identifikatorius** (Keyid): **EA:90:04:ED:9A:D1:47:26:46:94:5D:EA:09:31:C8:6D:31** **Išdavė sertifikatą** (DirName): **C=LT/ O=Vilnius University/ OU=Info faculty/ CN=LTVUSERT** **Serial: 00** **Sertifikato taisyklės** (Certificate policies): **Sertifikato taisyklių** (Policy) **identifikatorius: 1.2.440.43.2.1.1.1** **Sertifikatų centro veiklos nuostatai** (CPS): **http://www.ltvusert.lt/cps** **Nebegaliojančių sertifikatų sąrašo gavimo adresas** (CRL distribution points): **URI: http://www.ltvusert.lt/crl** **Pastaba vartotojams** (User notice): **Sertifikato taisyklės yra adresu http://www.ltvusert.lt/cp** **Kvalifikuotas sertifikatas** (qCStatements extension) **Sertifikatų centro parašo algoritmas** (signature algorithm) Pateikiamas sertifikatų centro parašo algoritmas.
Abonento duomenys duomenų bazei	Sertifikatų sudarymo tarnybos sistemos administratorius pateikia duomenis priklausomai nuo abonento tipo. Jei abonentas fizinis asmuo pateikiami duomenys: vardas, pavardė arba slapyvardis, asmens kodas, adresas, telefonas, e-paštas. Jei abonentas yra fizinis asmuo, atstovaujantis juridinį asmenį, pateikiami duomenys: vardas, pavardė arba slapyvardis, asmens kodas, adresas, telefonas, e-paštas organizacijos pavadinimas, padalinio pavadinimas, organizacijos adresas, šalis kur įsikūrusi organizacija, organizacijos telefonas, organizacijos e-paštas, įstaigos kodas, įgaliojimo registracijos numeris, įgaliojimo asmeniui išdavimo data ir vieta, darbuotojo pareigos.
Abonento duomenys saugojimui	IS pateikia sertifikatų duomenų bazei duomenis priklausomai nuo abonento tipo. Jei abonentas fizinis asmuo, pateikiami duomenys: vardas, pavardė arba slapyvardis, asmens kodas, adresas, telefonas, e-paštas. Jei abonentas yra fizinis asmuo, atstovaujantis juridinį asmenį, pateikiami duomenys: vardas, pavardė arba slapyvardis, asmens kodas, adresas, telefonas, e-paštas organizacijos pavadinimas, padalinio pavadinimas, organizacijos adresas, šalis kur įsikūrusi organizacija, organizacijos telefonas, organizacijos e-paštas, įstaigos kodas, įgaliojimo registracijos numeris, įgaliojimo asmeniui išdavimo data ir vieta, darbuotojo pareigos

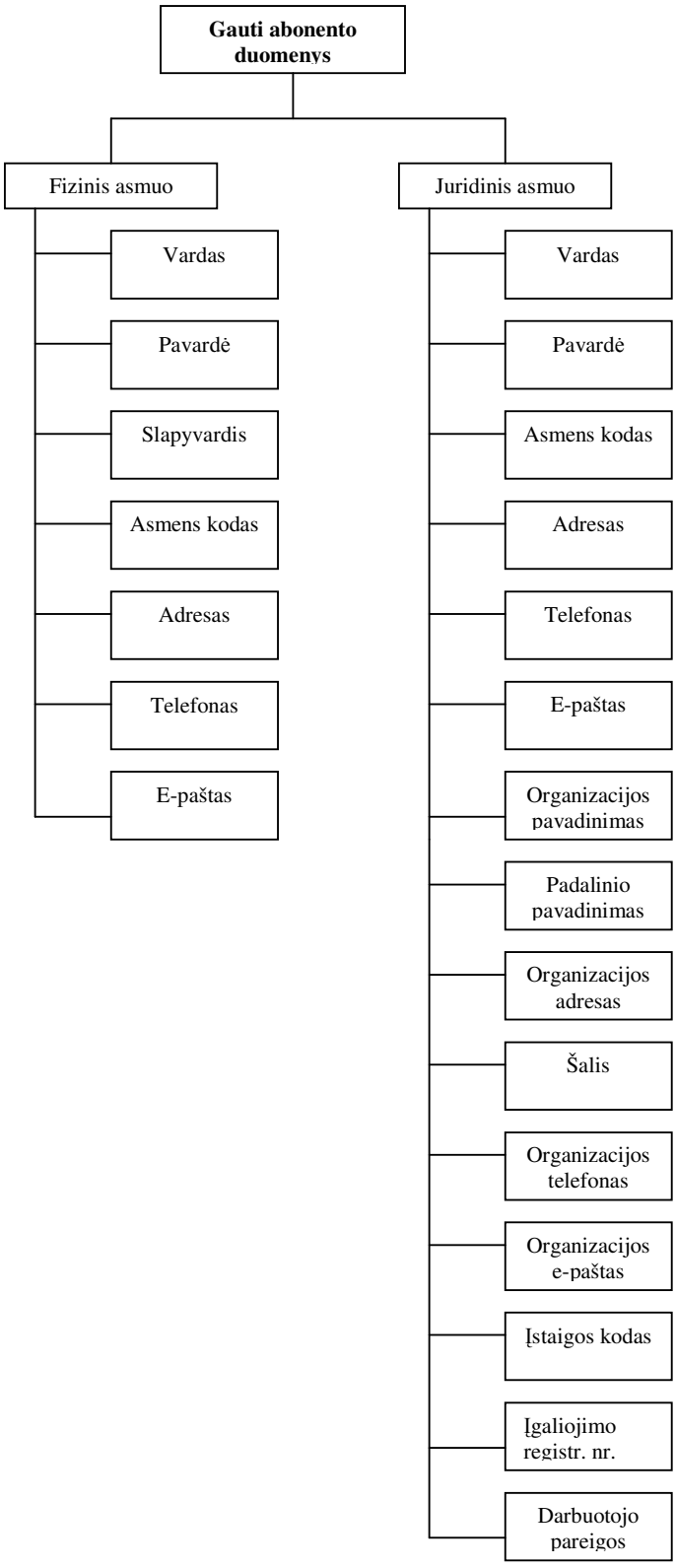
2.2 lentelės tęsinys kitame puslapyje

2.2 lentelės tęsinys

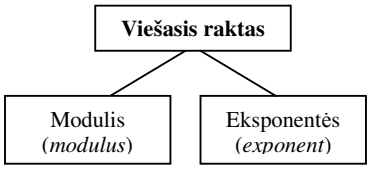
Statuso keitimo duomenys	Sertifikatų sudarymo tarnybos sistemos operatorius pateikia sistemai sertifikato numerį ir sertifikato galiojimo nutraukimo priežastį. Sistema automatiškai įveda sertifikato galiojimo nutraukimo datą ir laiką ir automatiškai pakeičia sertifikato statusą į „negalioja“.
Pakeisti sertifikato statusą	IS pateikia sertifikatų duomenų bazei sertifikato numerį ir sertifikato galiojimo nutraukimo priežastį.
Užklausa dėl sertifikato	Sertifikatų duomenų teikimo tarnyba suformuoja užklausą sertifikatui iš pagrindinės duomenų bazės gauti.
Sertifikatas teikimui	Iš sertifikatų duomenų bazės IS pateikiama duomenų bazėje saugomas sertifikatas pasirašytas sertifikatų centro elektroniniu parašu. Abonento sertifikatas pateikiamas pagal užklausoje pateiktą sertifikato numerį.
Užklausa dėl sertifikato tikrintojui	IS sertifikatų duomenų bazei suformuoja My SQL užklausą pagal sertifikato numerį sertifikatui iš pagrindinės duomenų bazės gauti.
Sertifikatas tikrintojui	IS pateikia sistemos sugeneruotą ir sertifikatų centro elektroniniu parašu pasirašytą abonento sertifikatą pagal užklausoje pateiktą sertifikato numerį.
Užklausa dėl statuso	Negaliojančių sertifikatų duomenų teikimo tarnyba gavusi užklausą iš parašo tikrintojo kreipiasi į IS.
Užklausa dėl sertifikato statuso	IS suformuojama My SQL užklausą pagal sertifikato numerį ir kreipiasi į sertifikatų duomenų bazę.
Sertifikato statusas	Duomenų bazė pateikia sistemai sertifikato numerį ir sertifikato statusą. Jei sertifikatas galioja pateikiamas “galioja“, jei negalioja pateikiama „negalioja“ ir galiojimo nutraukimo data.
Atsakymas apie sertifikato statusą	IS pateikia negaliojančių sertifikatų duomenų teikimo tarnybai pranešimą kuriame nurodoma sertifikato numeris ir sertifikato statusas. Jei sertifikato statusas „galioja“ tai pranešime nurodomas sertifikato numeris ir statusas „galioja“, jei sertifikatas negalioja tai pranešime nurodoma sertifikato numeris, statusas „negalioja“, sertifikato galiojimo laikotarpis.
Naujas CRL sąrašas	IS suformuoja negaliojančių sertifikatų sąrašą (CRL) kurį sudaro: sertifikato numerio, sertifikato galiojimo nutraukimo priežastis, sertifikato galiojimo nutraukimo data ir laikas. Negaliojančių sertifikatų sąrašas pasirašomas sertifikatų centro elektroniniu parašu.
Užklausa dėl sertifikatų sąrašo	Negaliojančių sertifikatų duomenų teikimo tarnyba gavusi užklausą iš parašo tikrintojo kreipiasi į IS.
Užklausa dėl negaliojančių sertifikatų	IS gavusi užklausą iš negaliojančių sertifikatų duomenų teikimo tarnyba kreipiasi į negaliojančių sertifikatų DB, suformuojant My SQL užklausą, negaliojančių sertifikatų sąrašui gauti.
Užklausa naujausiam negaliojančių sertifikatų sąrašui	Negaliojančių sertifikatų DB suformuoja My SQL užklausą, naujausiam negaliojančių sertifikatų sąrašui gauti.
Užklausa negaliojantys sertifikatai	IS kreipiasi į sertifikatų duomenų bazę suformuodama My SQL užklausą naujausiam negaliojančių sertifikatų sąrašui gauti.
Negaliojantys sertifikatai	Sertifikatų duomenų bazė pagal gautą užklausą suformuoja negaliojančių sertifikatų sąrašą kuriame pateikiama sąrašas kuriame yra negaliojančių sertifikatų numeriai, sertifikato galiojimo nutraukimo data ir priežastis.
Negaliojančių sertifikatų sąrašas	IS suformuoja negaliojančių sertifikatų sąrašą (CRL) kurį sudaro: sertifikato numerio, sertifikato galiojimo nutraukimo priežastis, sertifikato galiojimo nutraukimo data ir laikas. Ir perduoda negaliojančių sertifikatų duomenų bazei. Šioje duomenų bazėje visi sąrašai saugomi. Negaliojančių sertifikatų sąrašas pasirašomas sertifikatų centro elektroniniu parašu.
Negaliojančių sertifikatų duomenys	Negaliojančių sertifikatų duomenų bazė perduoda negaliojančių sertifikatų sąrašą kurį sudaro: sertifikato numerio, sertifikato galiojimo nutraukimo priežastis, sertifikato galiojimo nutraukimo data ir laikas.



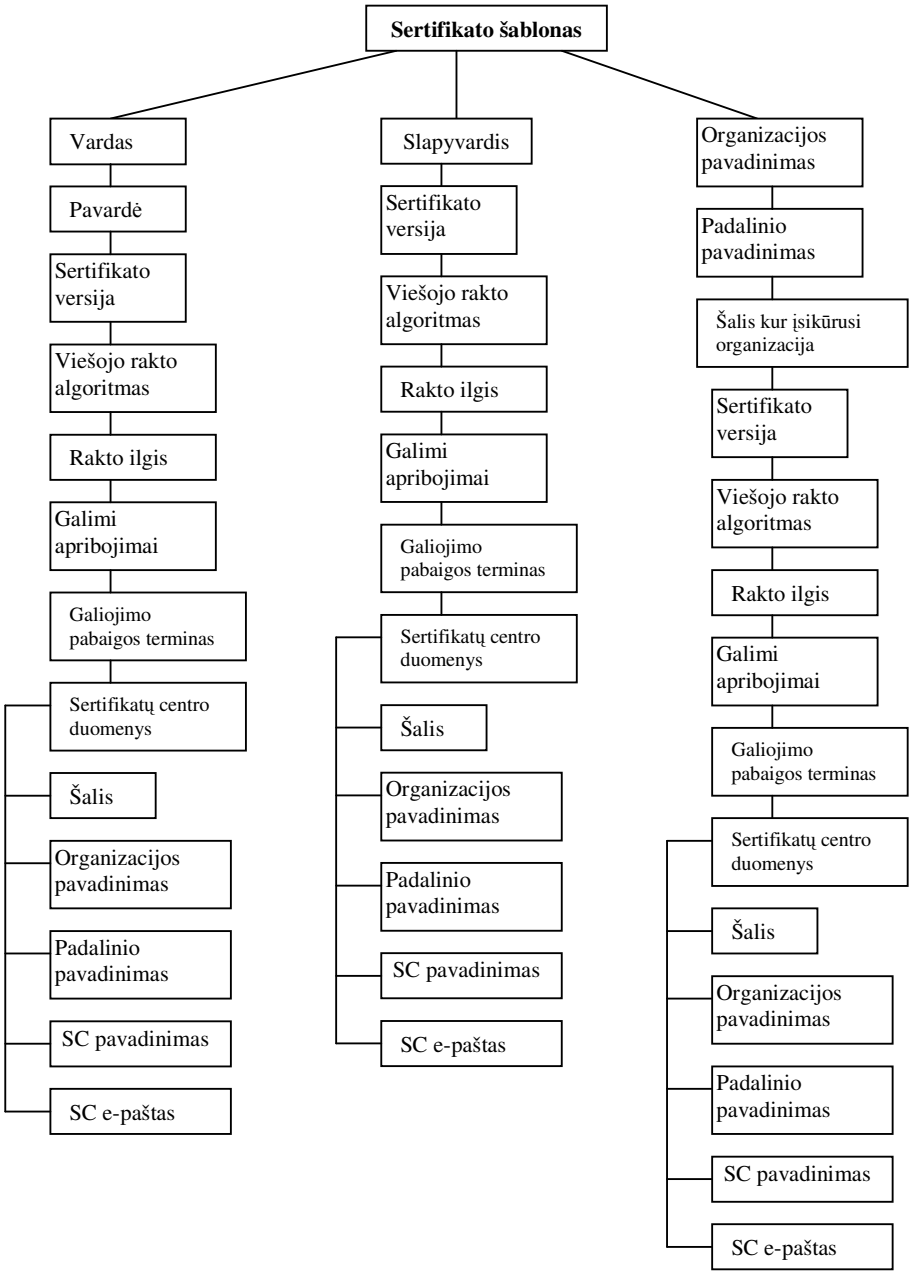
2.10 pav. Duomenų srauto „Abonento duomenys“ struktūros schema



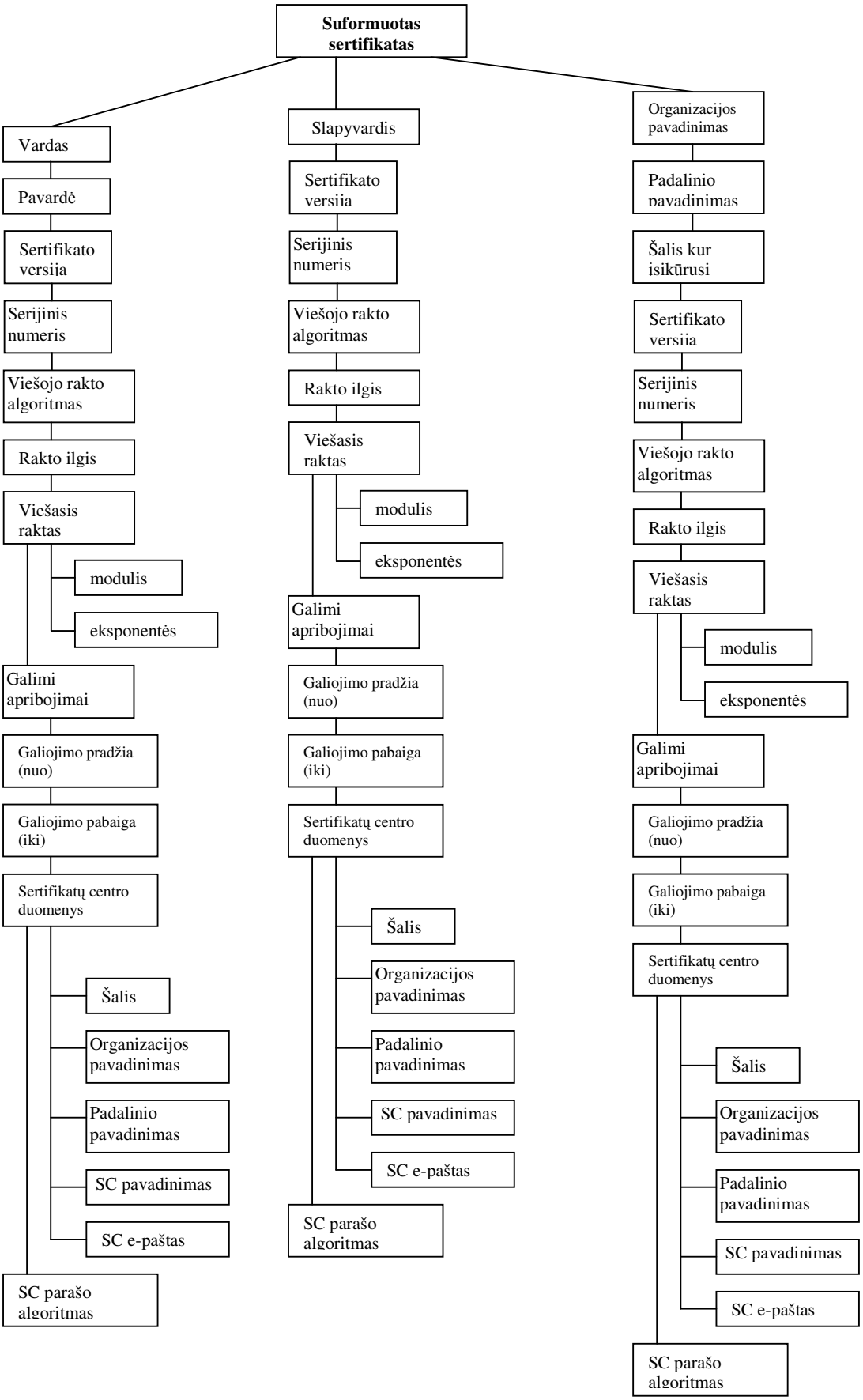
2.11pav. Duomenų srauto „Gauti abonento duomenys“struktūros schema



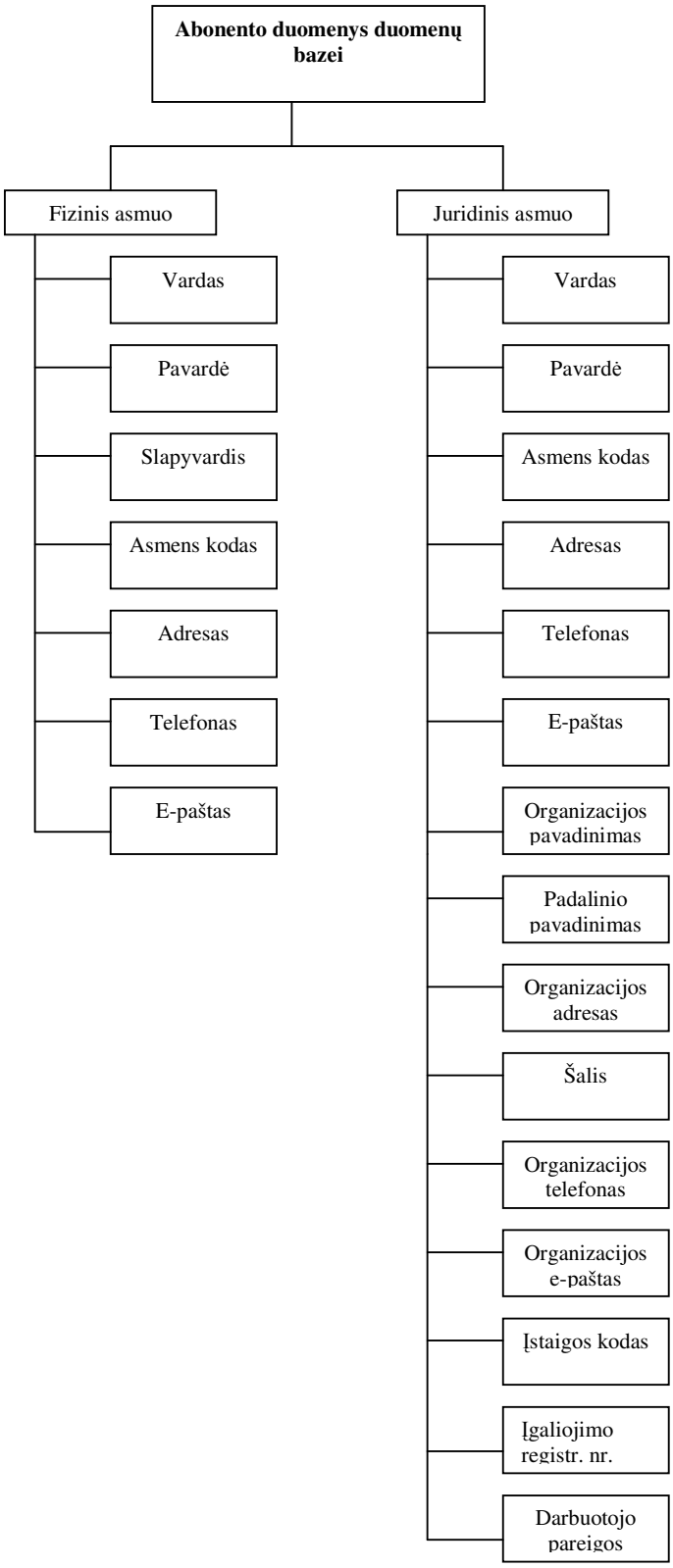
2.12 pav. Duomenų srauto „Viešasis raktas“ struktūros schema



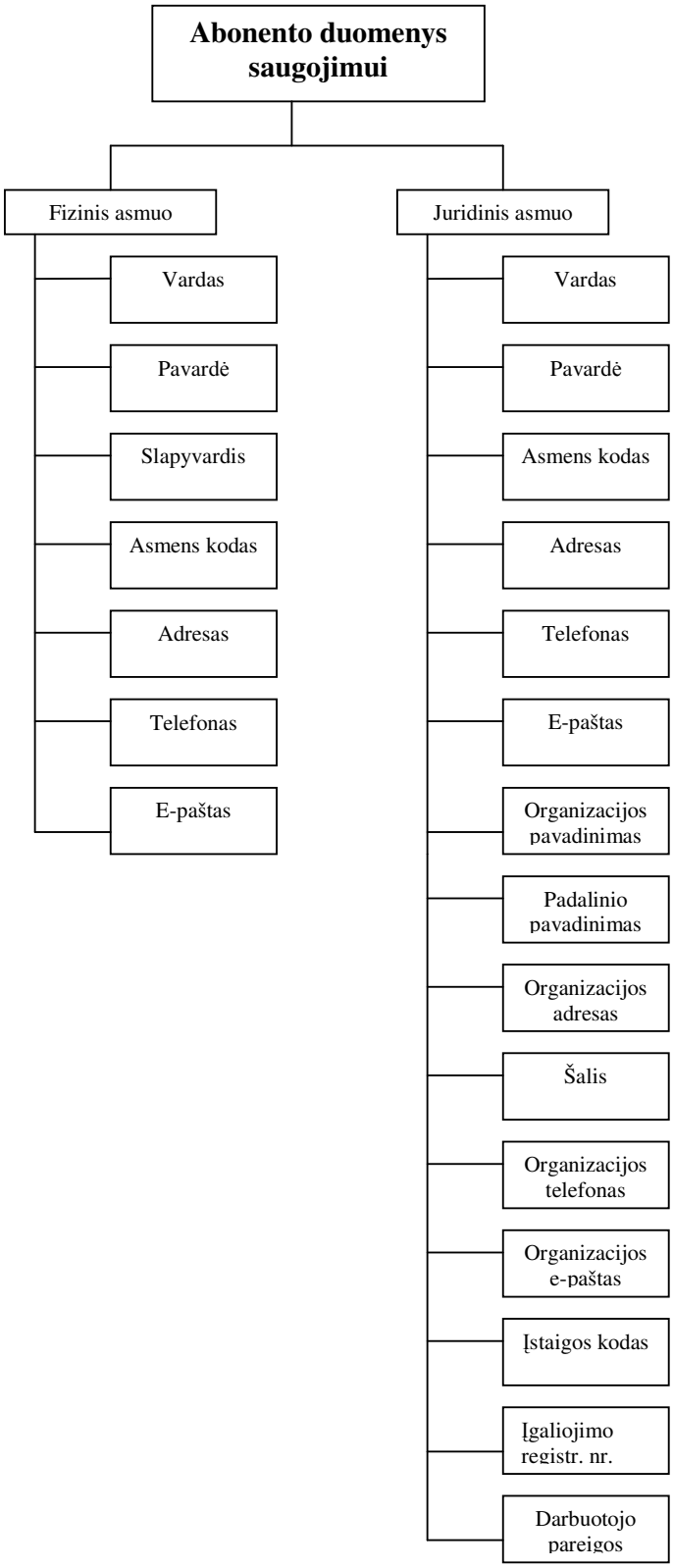
2.13 pav. Duomenų srauto „Sertifikato šablonas“ struktūros schema



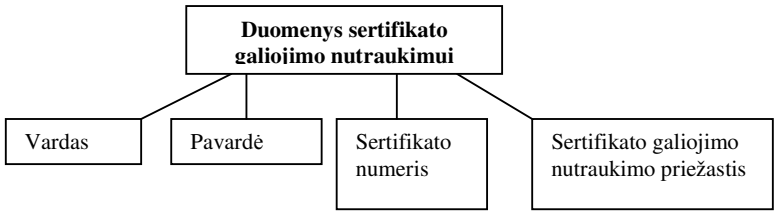
2.14 pav. Duomenų srauto „Suformuotas sertifikatas“ struktūros schema



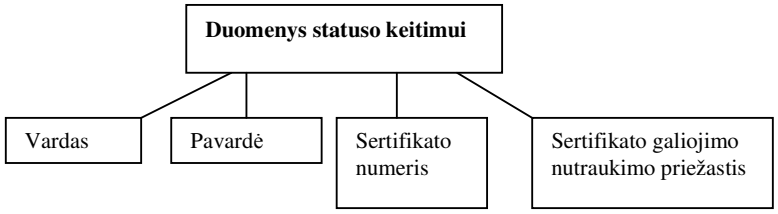
2.15 pav. Duomenų srauto „Abonento duomenys duomenų bazei“ struktūros schema



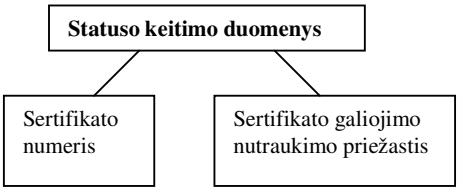
2.16 pav. Duomenų srauto „Abonento duomenys saugojimui“ struktūros schema



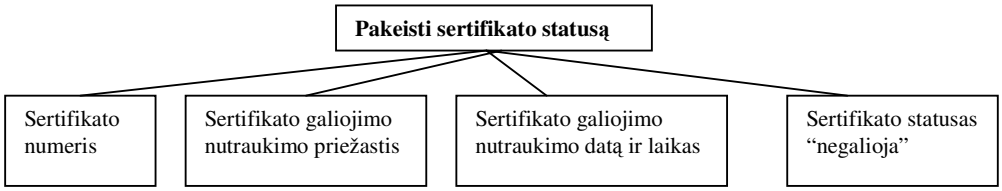
2.17 pav. Duomenų srauto „Duomenys sertifikato galiojimo nutraukimui“ struktūros schema



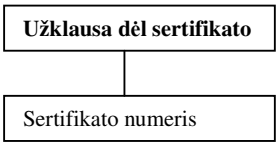
2.18 pav. Duomenų srauto „Duomenys statuso keitimui“ struktūros schema



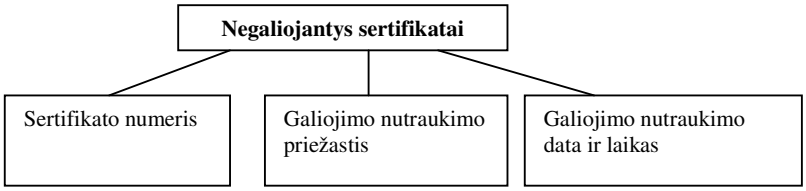
2.19 pav. Duomenų srauto „Statuso keitimo duomenys“ struktūros schema



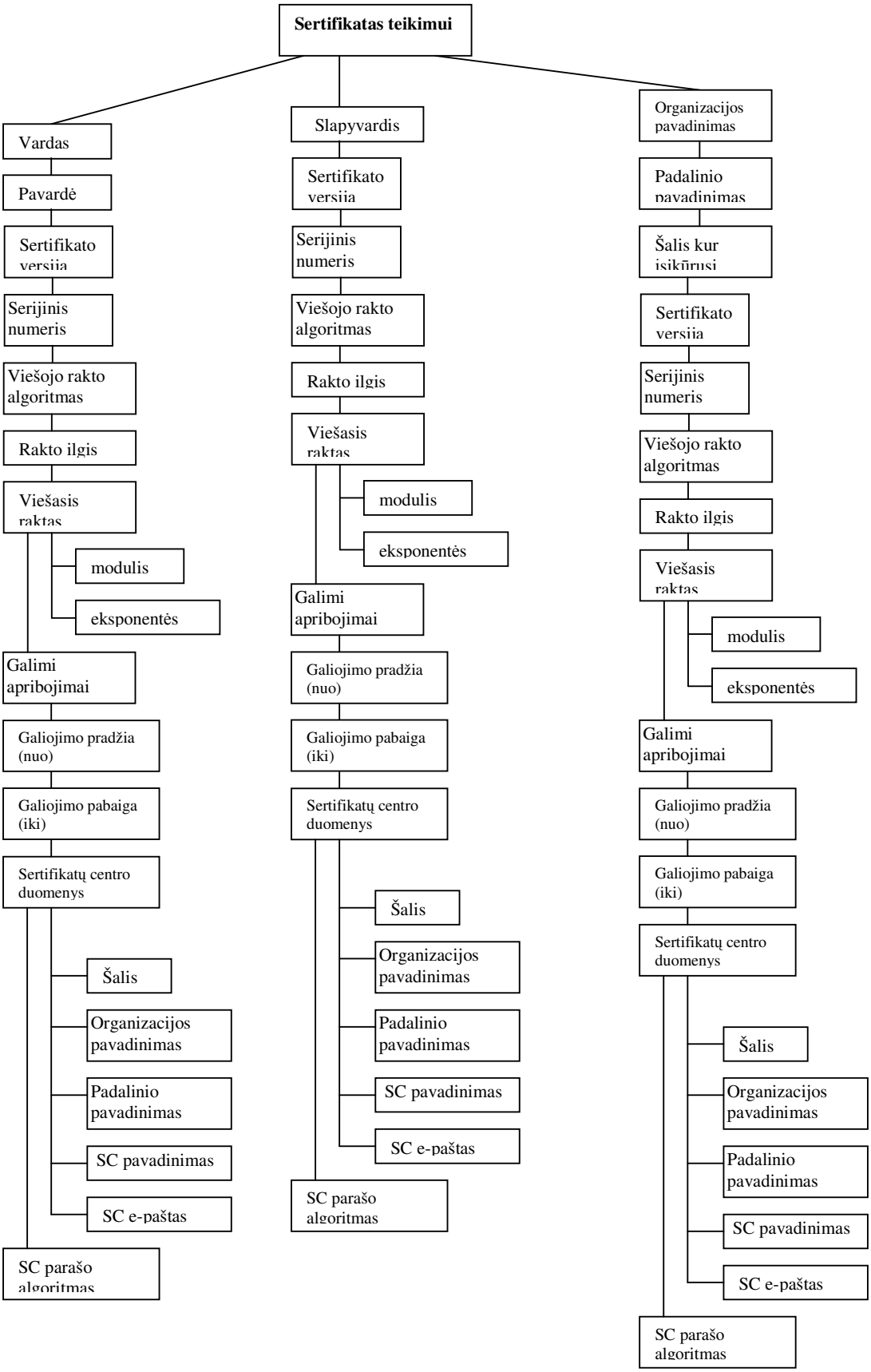
2.20 pav. Duomenų srauto „Pakeisti sertifikato statusą“ struktūros schema



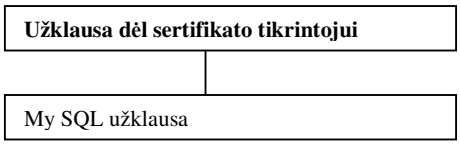
2.21 pav. Duomenų srauto „Užklausa dėl sertifikato“ struktūros schema



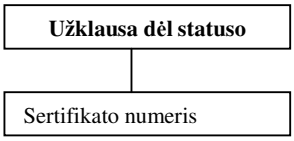
2.22 pav. Duomenų srauto „Negaliojantys sertifikatai“ struktūros schema



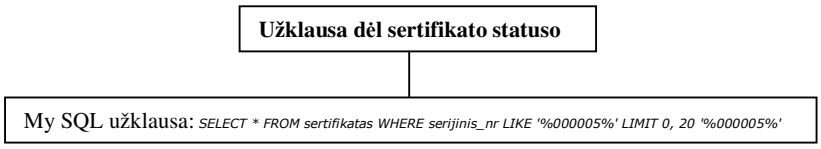
2.23 pav. Duomenų srauto „Sertifikatas teikimui“ struktūros schema



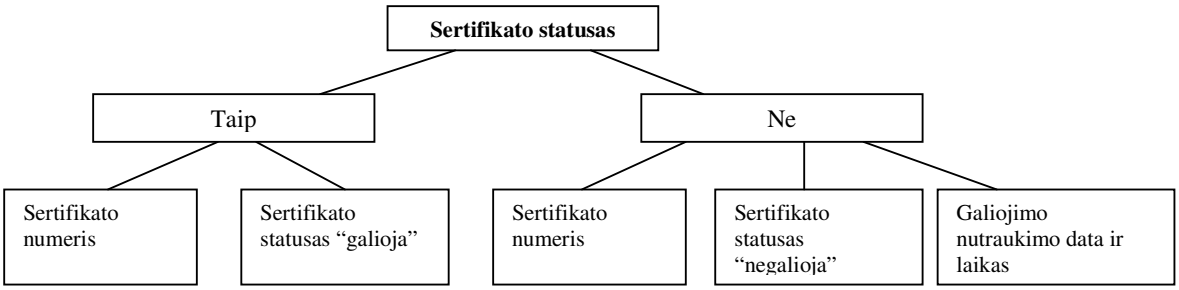
2.24 pav. Duomenų srauto „Užklausa dėl sertifikato tikrintojui“ struktūros schema



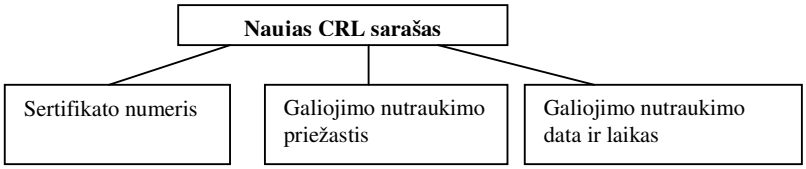
2.25 pav. Duomenų srauto „Užklausa dėl statuso“ struktūros schema



2.26 pav. Duomenų srauto „Užklausa dėl sertifikato statuso“ struktūros schema

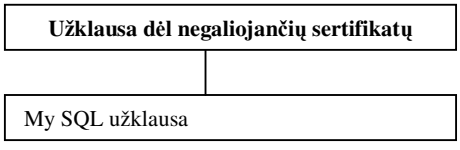


2.27 pav. Duomenų srauto „Sertifikato statusas“ struktūros schema

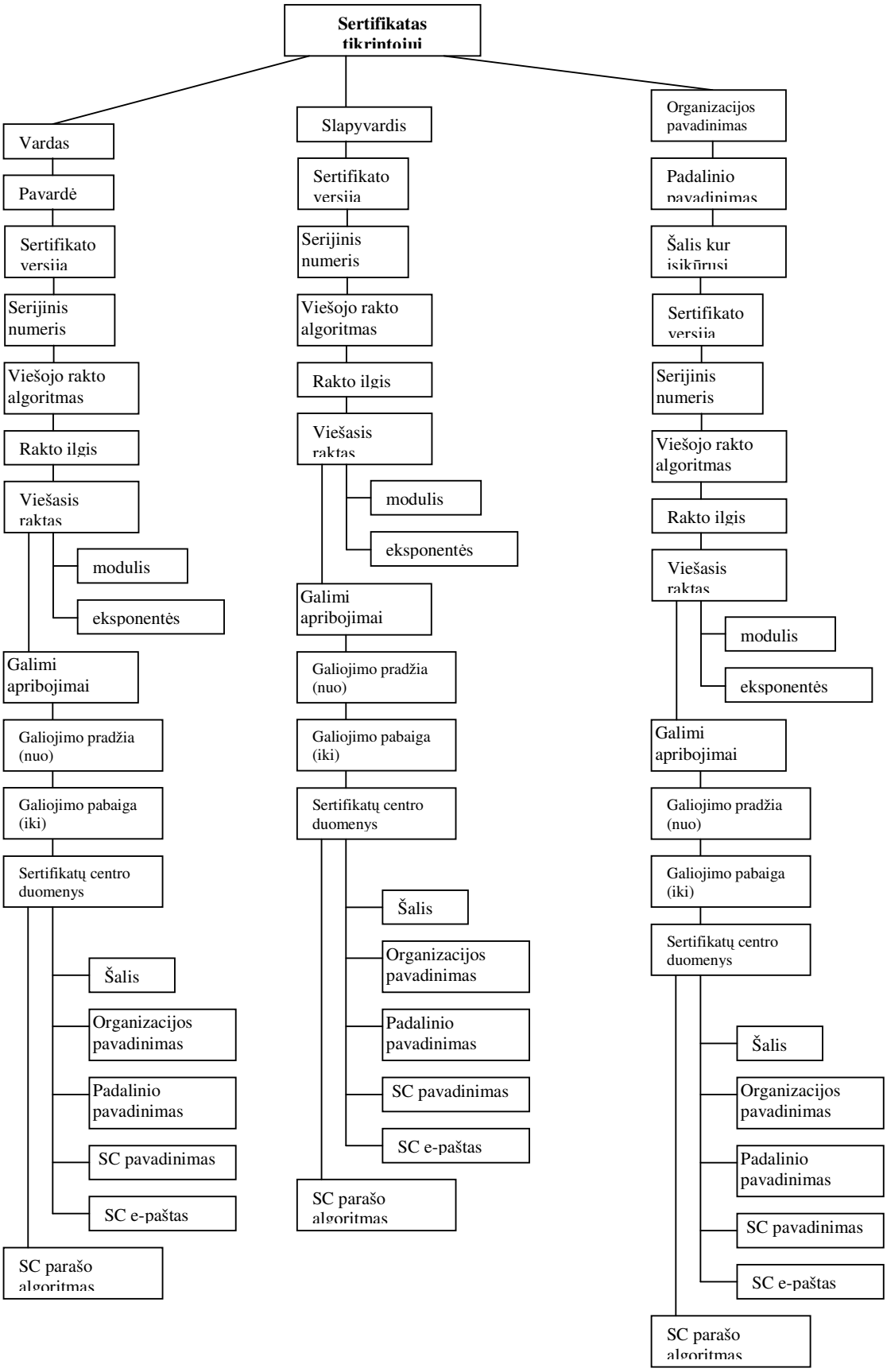


2.28 pav. Duomenų srauto „Naujas CRL sąrašas“ struktūros schema

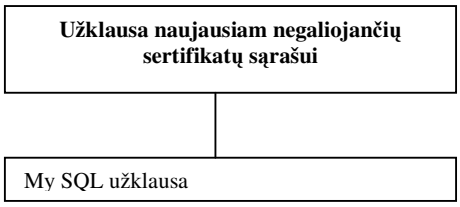
2.29 pav. Duomenų srauto „Užklausa dėl sertifikatų sąrašo“ struktūros schema



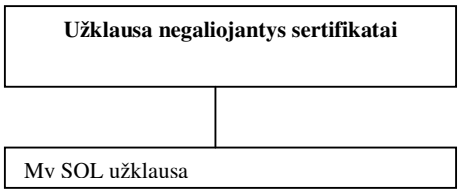
2.30 pav. Duomenų srauto „Užklausa dėl negaliojančių sertifikatų“ struktūros schema



2.31 pav. Duomenų srauto „Sertifikatas tikrintojui“ struktūros schema

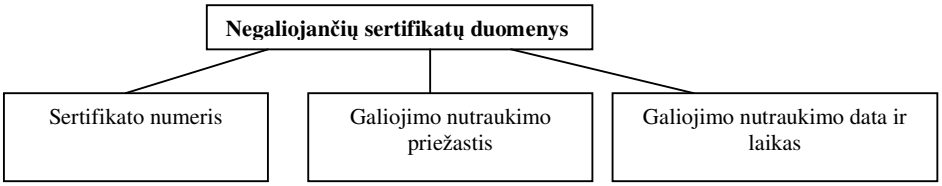


2.32 pav. Duomenų srauto „Užklausa naujausiam negaliojančių sertifikatų sąrašui“ struktūros schema

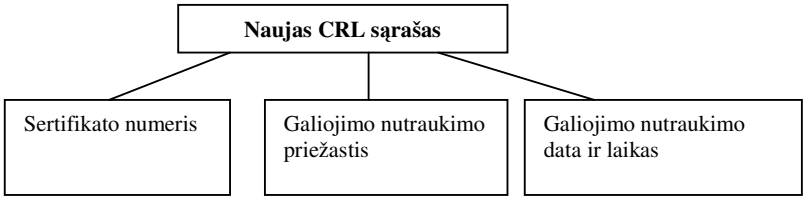


2.33 pav. Duomenų srauto „Užklausa negaliojantys sertifikatai“ struktūros schema

2.34 pav. Duomenų srauto „Negaliojančių sertifikatų sąrašas“ struktūros schema



2.35 pav. Duomenų srauto „Negaliojančių sertifikatų duomenys“ struktūros schema

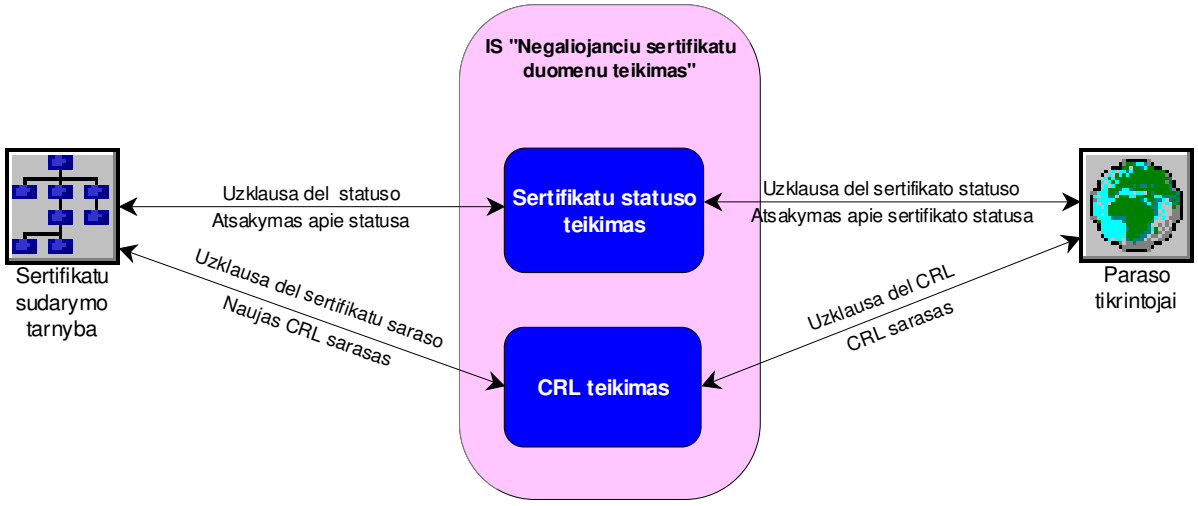


2.36 pav. Duomenų srauto „Naujas CRL sąrašas“ struktūros schema

2.37 pav. Duomenų srauto „Užklausa dėl sertifikatų sąrašo“ struktūros schema

2.5.2. Negaliojančių sertifikatų duomenų teikimo taikomųjų uždavinių modelis

Negaliojančių sertifikatų duomenų teikimo taikomųjų uždavinių modelis detaliai aprašo IS „Negaliojančių sertifikatų duomenų teikimas“ informacijos srautus ir kompiuterizuojamus uždavinius (2.38 pav.). Negaliojančių sertifikatų duomenų teikimo taikomųjų uždavinių modelis sudarytas detalizuojant negaliojančių sertifikatų duomenų teikimo darbų sekų modelį (2.5 pav.).



2.38 pav. Negaliojančių sertifikatų duomenų teikimo taikomųjų uždavinių modelis

2.3 lentelė

Negaliojančių sertifikatų duomenų teikimo taikomųjų uždavinių aprašymas

Uždavinys	Aprašymas
Sertifikatų statuso teikimas	CRL teikimo tarnyba elektroninių parašų naudotojams per internetą teikia informaciją apie sertifikatų statusą (galioja ar nebegalioja). CRL teikimo tarnyba duomenis apie sertifikatų statuso pakeitimus gauna iš sertifikatų centro sertifikatų duomenų bazės. Sertifikatų statuso informaciją CRL teikimo tarnyba gali teikti dviem būdais: *on-line* (sertifikato statuso informacija pateikiama realiu laiku) arba *off-line* (sertifikatų statuso informacija pateikiama periodiškai kas tam tikrą laiko tarpą) režimu. *On-line* režimo atveju elektroninio 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. Klausėjui siunčiamas suformuotas atsakymas, kuriame yra informacija apie jį dominančio sertifikato statusą.
CRL statuso teikimas	*Off-line* režimo atveju CRL teikimo tarnyba, turėdama paskutinę CRL sąrašo versiją, persiunčia ją elektroninio parašų tikrintojui, kad jis galėtų tikrintis sertifikatų statusus. Atsakyme turi būti nurodytas laikas, kada CRL teikimo tarnyba pasirašė atsakymą.

2.4 lentelė

Negaliojančių sertifikatų duomenų teikimo taikomųjų uždavinių modelio duomenų srautų aprašymas

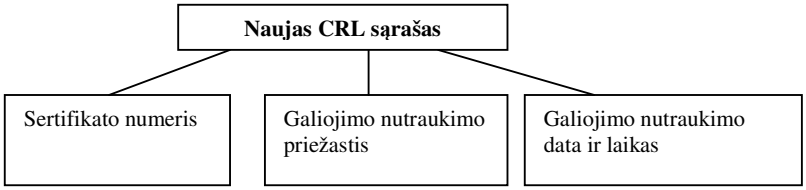
Duomenų srautas	Aprašymas
Užklausa dėl sertifikatų sąrašo	IS gavusi užklausą iš parašo tikrintojo kreipiasi į negaliojančių sertifikatų duomenų bazę, suformuojama My SQL užklausa.

2.4 lentelės tęsinys kitame puslapyje

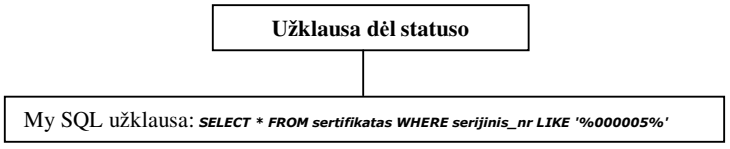
2.4 lentelės tęsinys

Duomenų srautas	Aprašymas
Naujas CRL sąrašas	Sertifikatų sudarymo tarnyba iš negaliojančių sertifikatų duomenų bazės siunčia naujausią negaliojančių sertifikatų sąrašą kurį sudaro: sertifikato numerio, sertifikato galiojimo nutraukimo priežastis, sertifikato galiojimo nutraukimo data ir laikas. Negaliojančių sertifikatų sąrašas pasirašomas sertifikatų centro elektroniniu parašu
Užklausa dėl statuso	IS gavusi užklausą iš parašo tikrintojo kreipiasi į pagrindinę sertifikatų duomenų bazę suformuodama My SQL užklausa sertifikato nurodytu numeriu statusui gauti.
Atsakymas apie statusą	Sertifikatų sudarymo tarnyba iš pagrindinės duomenų bazės pateikia pranešimą kuriame nurodoma sertifikato numeris ir sertifikato statusas. Jei sertifikato statusas „galioja“ tai pranešime nurodomas sertifikato numeris ir statusas „galioja“, jei sertifikatas negalioja tai pranešime nurodoma sertifikato numeris, statusas „negalioja“, sertifikato galiojimo laikotarpis.
Užklausa dėl sertifikato statuso	Parašo tikrintojas sertifikatų centro tinklalapyje pasirinkęs reikiamą komandą ir įvedęs sertifikato numerį suformuoja užklausą.
Atsakymas apie sertifikato statusą	IS gavusi pranešimą iš pagrindinės duomenų bazės pateikia pranešimą parašo tikrintojui kuriame nurodoma sertifikato numeris ir sertifikato statusas. Jei sertifikato statusas „galioja“ tai pranešime nurodomas sertifikato numeris ir statusas „galioja“, jei sertifikatas negalioja tai pranešime nurodoma sertifikato numeris, statusas „negalioja“, sertifikato galiojimo laikotarpis.
Užklausa dėl CRL	Parašo tikrintojas sertifikatų centro tinklalapyje pasirinkęs negaliojantys sertifikatai komandą suformuoja užklausą.
CRL sąrašas	IS parašo tikrintojams siunčia naujausią negaliojančių sertifikatų sąrašą kurį sudaro: sertifikato numerio, sertifikato galiojimo nutraukimo priežastis, sertifikato galiojimo nutraukimo data ir laikas. Negaliojančių sertifikatų sąrašas pasirašytas sertifikatų centro elektroniniu parašu

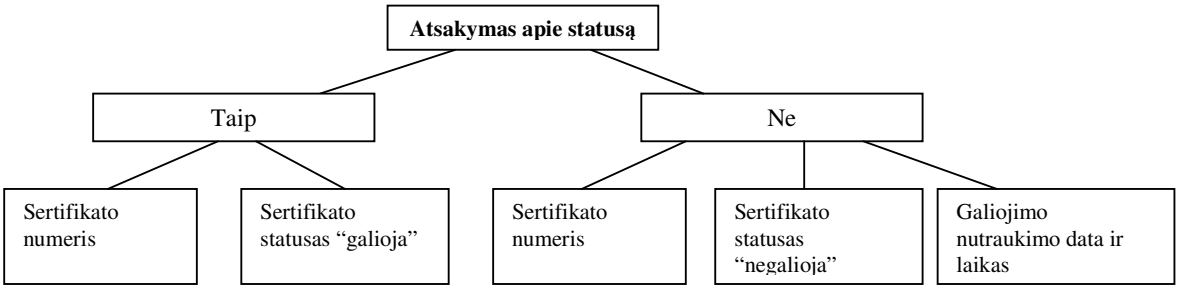
2.39 pav. Duomenų srauto „Užklausa dėl sertifikatų sąrašo“ struktūros schema



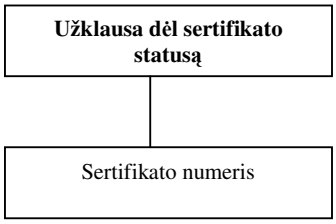
2.40 pav. Duomenų srauto „Naujas CRL sąrašas“ struktūros schema



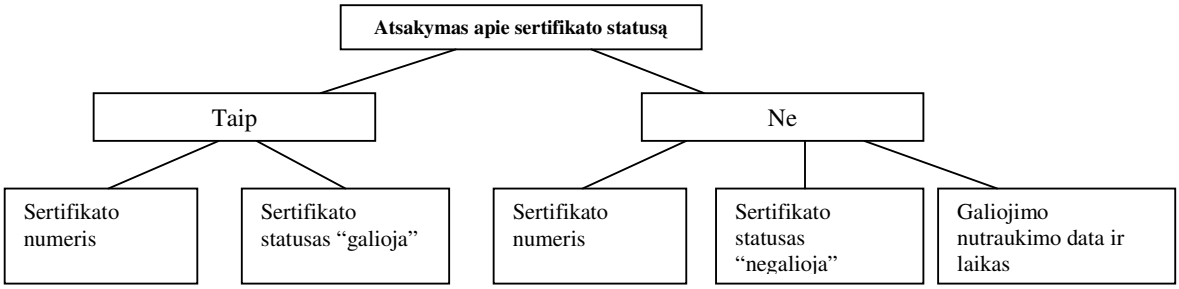
2.41 pav. Duomenų srauto „Užklausa dėl statuso“ struktūros schema



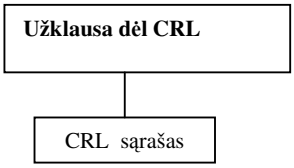
2.42 pav. Duomenų srauto „Atsakymas apie statusą“ struktūros schema



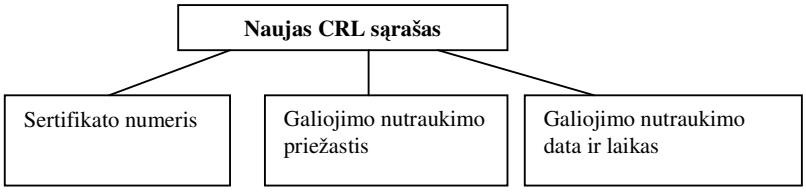
2.43 pav. Duomenų srauto „Užklausa dėl sertifikato statusą“ struktūros schema



2.44 pav. Duomenų srauto „Atsakymas apie sertifikato statusą“ struktūros schema



2.45 pav. Duomenų srauto „Užklausa dėl sertifikatų sąrašo“ struktūros schema



2.46 pav. Duomenų srauto „Naujas CRL sąrašas“ struktūros schema

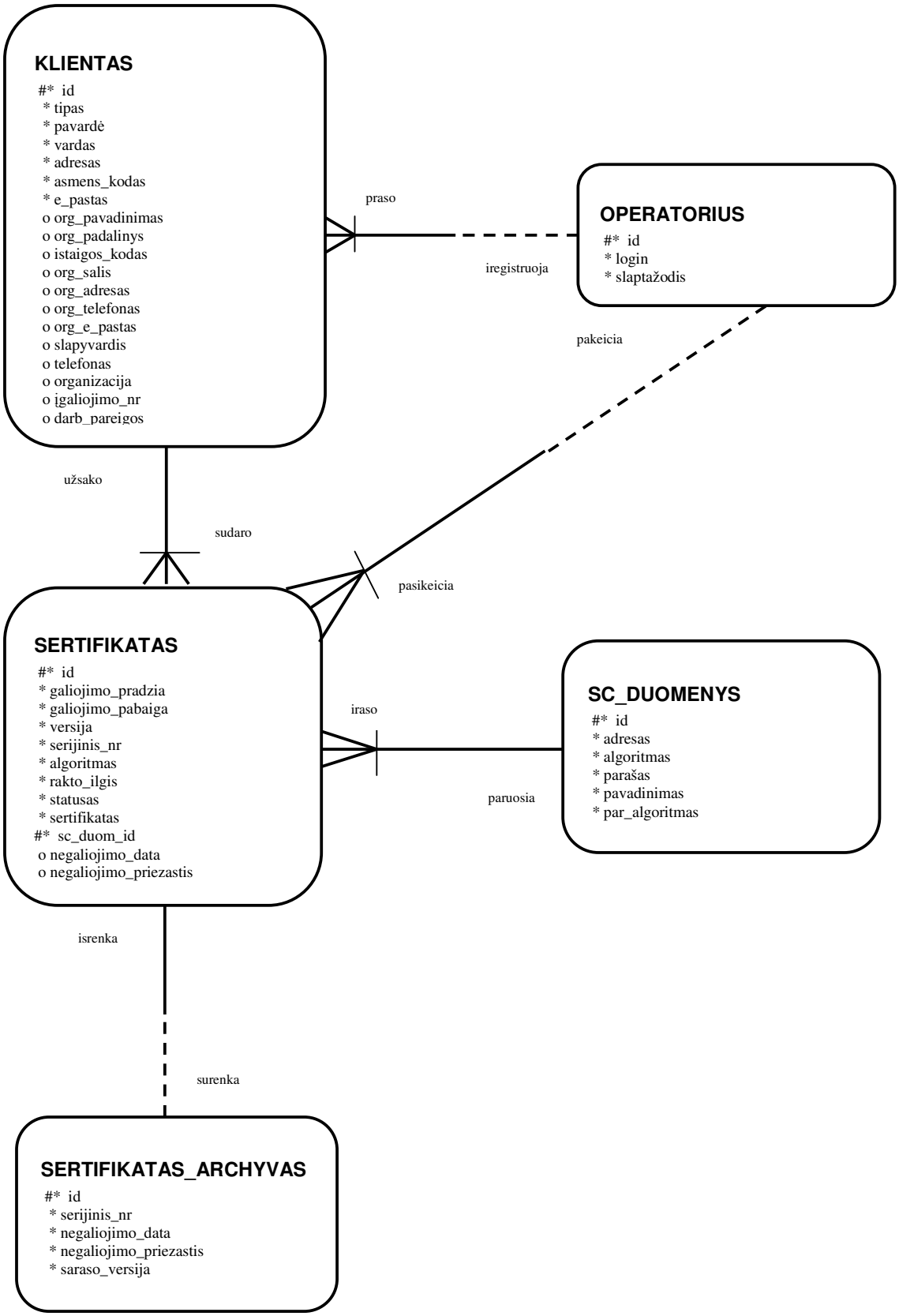
2.6. DUOMENŲ BAZĖS PROJEKTAVIMAS

2.6.1. Esybių - ryšių schema

Esybių-ryšių modeliavimo priemonėmis apibrėžiami elektroninio parašo sertifikatų centro informaciniai poreikiai. Sudaroma nagrinėjamos DB “Esign” esybių-ryšių schema, atitinkanti sukurtas lenteles.

Elektroninio parašo sertifikatų centras – organizacija sudaranti sertifikatus asmenims, norintiems savo veikloje naudoti elektroninį parašą, ir sertifikatų duomenis teikianti elektroninių parašų tikrintojams. Sistemos operatorius (vartotojas), gavęs užsakymą iš klientų registravimo tarnybos, surašo visus kliento (abonento) duomenis. Pirmiausiai nurodoma kliento tipas: fizinis ar juridinis. Jei fizinis asmuo pateikiama pavardė, vardas, adresas, asmens kodas, elektroninis paštas. Jei juridinis asmuo tai reikalingi papildomi duomenys: organizacijos pavadinimas, organizacijos padalinys, įstaigos kodas, organizacijos šalis, organizacijos adresas, organizacijos telefonas, organizacijos elektroninis paštas, telefonas, organizacijos suteiktas įgaliojimo numeris, darbuotojo pareigos. Užsakyme pateikiama sertifikato duomenys: galiojimo pradžia, galiojimo pabaiga, versija, algoritmas, rakto_ilgis. Sertifikato serijinis numeris sugeneruojamas sistemos. Jei iš klientų registravimo tarnybos pateikiama prašymas nutraukti sertifikato galiojimą tai pakeičiamas sertifikato statusas įvedant sertifikato galiojimo nutraukimo priežastį ir datą. Vartotojui kreipiantis į negaliojančių sertifikatų duomenų teikimo tarnybą iš Esign duomenų bazėje esančių negaliojančių sertifikatų suformuojamas negaliojančių sertifikatų sąrašas (CRL) kuriame yra sertifikato serijinis numeris, sertifikato galiojimo nutraukimo priežastis ir sertifikato galiojimo nutraukimo data ir šis sąrašas perkeliamas į negaliojančių sertifikatų duomenų bazę. Vartotojų kontrolei pateikiama slaptažodis ir vartotojo *id*.

Sudarant sertifikatą, klientas susiejamas su sertifikate esančias duomenimis. Sertifikate būtinai turi būti sertifikatų centro duomenys. Norint užtikrinti duomenų įvedimo kontrolę kiekvienas vartotojas susiejamas su kliento duomenimis. Kiekvienas vartotojas gali, bet nebūtinai būti užregistravęs bent vieną klientą nes vartotojas dar atlieka ir kitą funkciją- gavęs užsakymą keičia sertifikatų statusą. Pakeitus negaliojančių sertifikatų sąrašas perkeliami į negaliojančių sertifikatų duomenų bazę taigi į sertifikatų archyvą.



2.47 pav. Esybių - ryšių diagrama

2.6.2. Duomenų bazės loginės struktūros aprašymas

Duomenų bazė MySQL - reliacinė duomenų bazė. Ją sudaro tarpusavyje surištos reliacinės lentelės. Reliacinė lentelė tai dvimatė lentelė, susidedanti iš vienodo tipo eilučių (įrašų). Lentelės struktūrą apsprendžia kiekvieno stulpelio (lauko) duomenų tipas ir dydis. Be to, kiekvienai pagrindinei duomenų bazės lentelei rekomenduojama sudaryti pirminį raktą, kuris vienareikšmiškai identifikuoja jos įrašus ir padeda išvengti pasikartojančių įrašų.

Elektroninio parašo sertifikatų centro apdorojamos informacijos kiekis pakankamai didelis. Jeigu norėtume visą šią daugialypę informaciją laikyti viename objekte, tai jo atvaizdavimas būtų labai griozdiškas ir nepatogus, ypač esant didelės apimties informacijai. Todėl MySQL leidžia informaciją išskaidyti ir saugoti keliuose objektuose, - lentelėse, surištose tam tikrais ryšiais. Išskirkime informacinius objektus: **Klientas, Sertifikatai, SC duomenys ir Vartotojai.**

Pirmoji lentelė yra „klientas“, joje saugomi duomenys apie sertifikatų centro abonentus, kuriems sudaryti sertifikatai

2.5 lentelė

“Klientas” lentelės sudėtis

Lauko vardas	Pilnas pavadinimas	Raktas	Tipas	Ilgis
id	Kliento identifikatorius	Taip	Integer	10
tipas	Kliento tipas	-	character	1
vardas	Vardas	-	varchar	30
pavardė	Pavardė	-	varchar	40
slapyvardis	Slapyvardis	-	varchar	20
asmens_kodas	Asmens kodas	-	varchar	11
adresas	Adresas	-	varchar	255
telefonas	Telefonas	-	varchar	20
e_pastas	E- paštas	-	varchar	20
org_pavadinimas	Organizacijos pavadinimas	-	varchar	60
org_padalinys	Organizacijos padalinys	-	varchar	60
org_ adresas	Organizacijos adresas	-	varchar	255
org_salis	Organizacijos šalis	-	varchar	20
org_ telefonas	Organizacijos telefonas	-	varchar	20
org_e_pastas	Organizacijos e-paštas	-	varchar	20
istaigos_kodas	Įstaigos kodas	-	varchar	20
igaliojimo_nr	Įgaliojimo numeris	-	varchar	15
igaliojimo_vieta	Įgaliojimo išdavimo data ir vieta	-	varchar	200
darb_pareigos	Darbuotojo pareigos	-	varchar	40

Sertifikato sudarymui reikalingi duomenys ir sudarytas sertifikatas saugomi lentelėje „sertifikatai“.

2.6 lentelė

“Sertifikatai” lentelės sudėtis

Lauko vardas	Pilnas pavadinimas	Raktas	Tipas	Ilgis
id	Sertifikato identifikatorius	Taip	Integer	10
galiojimo_pradzia	Galiojimo pradžia	-	date time	14
galiojimo_pabaiga	Galiojimo pabaiga	-	date time	14

2.6 lentelės tęsinys kitame puslapyje

2.6 lentelės tęsinys

Lauko vardas	Pilnas pavadinimas	Raktas	Tipas	Ilgis
apribojimai	Apribojimai	-	varchar	255
versija	Versija	-	varchar	20
serijinis_nr	Serijinis numeris	-	varchar	20
algoritmas	Viešojo rakto algoritmas	-	varchar	30
rakto_ilgis	Rakto ilgis	-	integer	10
statusas	Sertifikato statusas	-	character	1
negaliojimo_priezastis	Sertifikato galiojimo nutraukimo priežastis	-	text	-
negaliojimo_data	Galiojimo nutraukimo data	-	date time	14
subjektas_vardas	Abonento vardas	-	varchar	30
Subjektas_pavarde	Abonento pavardė	-	varchar	40
Subjektas_slapyvardis	Abonento slapyvardis	-	varchar	20
subjektas_ organizacija	Juridinis asmuo kuriam sudaromas sertifikatas	-	varchar	255
sc_duom_id	SC duomenys	-	integer	10
sugeneruotas_sertifikatas	Išsaugotas sudarytas sertifikatas	-	text	-

Sudarant sertifikatą, sertifikatų centro duomenys įkeliami iš lentelė „sc_duomenys“ .

2.7 lentelė

“Sc_duomenys” lentelės sudėtis

Lauko vardas	Pilnas pavadinimas	Raktas	Tipas	Ilgis
id	Sertifikatų centro duomenų identifikatorius	Taip	Integer	10
adresas	Sertifikatų centro adresas	-	text	-
algoritmas	Algoritmas	-	varchar	30
pavadinimas	Sertifikatų centro pilnas pavadinimas	-	varchar	20
par_algoritmas	Parašo algoritmas	-	varchar	30

Norint užtikrinti duomenų saugumą ir teisinio ginčo atveju nesunkiai rasti sertifikatų centro darbuotoją sudariusį sertifikatą, prie duomenų bazės gali jungtis tik darbuotojai, turintys vartotojo teisę. Todėl vartotojo duomenys saugomi lentelėje „vartotojai“.

2.8 lentelė

“Vartotojai” lentelės sudėtis

Lauko vardas	Pilnas pavadinimas	Raktas	Tipas	Ilgis
id	Sertifikatų centro darbuotojo identifikatorius	Taip	Integer	10
login	Vartotojo prisijungimo vardas	-	tinytext	-
pw	Vartotojo prisijungimo slaptažodis	-	tinytext	-

Negaliojančių sertifikatų sąrašams tvarkyti reikia suprojektuoti reliacinę duomenų bazę „Esign_archyvas“. Ją sudaro viena reliacinės duomenų bazės lentelė sertifikatas_archyvas.

2.9 lentelė

“Sertifikatas_archyvas” lentelės sudėtis

Lauko vardas	Pilnas pavadinimas	Raktas	Tipas	Ilgis
id	Sertifikatų archyvo identifikatorius	Taip	Integer	10
serijinis_nr	Serijinis numeris	-	varchar	20
negaliojimo_priezastis	Sertifikato galiojimo nutraukimo priežastis	-	text	-
negaliojimo_data	Galiojimo nutraukimo data	-	date time	14
Saraso_versija	Negaliojančių sertifikatų versija	-	date time	14

Tokia duomenų bazės loginė struktūra užtikrina pakankamą jos informatyvumą bei lankstumą.

2.7. SERTIFIKATŲ CENTRO INFORMACIJOS SISTEMAI KELIAMI REIKALAVIMAI

Programinė ir techninė įranga, reikalinga sertifikatų centro veiklai užtikrinti:

× sertifikatų centro lokalusis tinklas turi turėti pastovų ir aukštos greitaveikos ryšį su internetu;

× ryšiui su internetu palaikyti ir apsaugai nuo išorinių įsilaužėlių turi būti naudojamas serveris, kartu atliekantis ugnies sienos (“firewall”) ir tarpininko (“proxy”) funkcijas;

× lokalaus tinklo palaikymo serverio funkcijos: darbuotojų registravimas, jų teisių nustatymas, tinklo resursų paskirstymas (galima kiekvienam SC darbuotojui nustatyti, prie kokios darbo stoties, programos ir kuriuo paros metu jis gali prisijungti);

× informacijos skelbimo internete WWW serveris. Jis turi tiesioginį ryšį su pagrindine duomenų baze, teikia informaciją apie galiojančius/nebegaliojančius sertifikatus el.parašų tikrintojams;

× pagrindinės duomenų bazės (duomenų bazė, kurioje laikoma visa informacija apie sertifikatus ir viešuosius raktus) serverio darbas yra informacijos tvarkymas, sertifikatų išdavimas ir tvarkymas, sertifikatų statuso keitimas, apsauga ir archyvavimas. Prie šios duomenų bazės tiesioginį priėjimą turi www serveris ir serveris šifravimo raktams generuoti, jei toks yra sertifikatų centre.

Techniniai ir programiniai reikalavimai kompiuteriams:

- **Firewall – proxy serveris:** P4 procesorius, 512MB RIMM, 10-20GB SCSI HDD, DVD-ROM, MS Windows2003 server, CheckPont firewall;
- **Vietinio tinklo palaikymo serveris:** P4 procesorius, 256MB RIMM, 80 GB SCSI HDD, DVD-ROM, MS Windows 2003 server;
- **WWW serveris:** P4 procesorius, 512MB RIMM, 80GB SCSI HDD, DVD-ROM, MS Windows 2003 server, MS IIS;
- **Pagrindinės duomenų bazės serveris:** 2-4 procesoriai P4, 2GB RIMM, 500GB RAID diskų masyvai, DVD-ROM, MS Windows 2003 server;
- **Sertifikatų išdavimo ir tvarkymo serveris:** P4 procesorius, 512MB RIMM, 20-30GB SCSI HDD, DVD-ROM, MS Windows 2003 server;
- **Darbo stotis:** P4 procesorius, 512MB RAM, 80 GB HDD, CD-ROM, 17” monitorius, klaviatūra su “smartcard” kortelių skaitliu, MS WindowsXP;

Reikalavimai programinei įrangai serverio išduodančio ir tvarknčio sertifikatus:

- Paskirtis: X.509V3 (RFC 1422) standarto sertifikatų sudarymas ir tvarkymas;
- Asimetrinio šifravimo algoritmai: RSA, DSA (naudojami sertifikatams pasirašinėti);
- Skaitmeninės santraukos algoritmai: SHA1, MD2, MD5 (naudojami sertifikatams pasirašinėti);
- Panaikintų sertifikatų sąrašo formavimas (X.509 CRL V2 standarto);
- Sertifikatų įrašymas įvairiose kompiuterinėse laikmenose;

- Turėtų būti galimybė ateityje nesunkiai įdiegti naujus šifravimo ir santraukos algoritmus

Reikalavimai pagrindinei duomenų bazei:

- Paskirtis: informacijai apie sertifikatus saugoti;
- Suderinama su ODBC;
- Galimybė išdėstyti duomenis keliuose diskuose;
- Indeksų naudojimas paieškai pagreitinti;
- Transakcijų auditas (užklausų siunčiamų į duomenų bazę ir duomenų bazės veiksmų fiksavimas).

Reikalavimai www serverio programinei įrangai:

- Paskirtis: viešosios informacijos skelbimas internete;
- Informacijos apie naujai sukurtus sertifikatus, ir viešuosius raktus paėmimas iš pagrindinės duomenų bazės;
- Negaliojančių sertifikatų sąrašo (CRL) paėmimas iš negaliojančių sertifikatų duomenų bazės;
- Informacijos apie sertifikatus patikrinimas pagal pasirašytų sertifikatų gavėjų užklausas pateiktas internetu.

2.8. PROJEKTINĖS DALIES REZULTATAI, IŠVADOS IR PASIŪLYMAI

Pagal LST ETSI TS 101 456 standartą sukurta elektroninio parašo sertifikatų centro organizacinė struktūra bei veiklos modelis. Veiklos modelyje yra įvertinta sąveika tarp organizacijos objektų ir ryšiai su vartotojais, abonentais ir bendradarbiaujančiomis institucijomis. Šis modelis nėra orientuotas į organizacinių vienetų apibrėžimą, bet daugiau atspindi ryšius ir informacijos siuntimą tarp organizacijų.

Naudojant darbų sekos modeliavimą, sukurti detalūs sertifikatų centro veiklų modeliai, kurie apima visą sertifikatų centro veiklos procesą. Darbų sekos modelis atvaizduoja sertifikatų centro veiklos procesus, išreiškiant juos veiklos komponentais ir darbų seka tarp tų veiklų. Šis modelis orientuotas į darbų seką nuo veiklos pradžios iki galo, skirtą bendram tikslui pasiekti.

Sukurti sertifikatų ir sertifikatų centro duomenų teikimo, sertifikatų sudarymo ir duomenų tvarkymo, sertifikatų galiojimo nutraukimo, negaliojančių sertifikatų duomenų teikimo darbų sekų modeliai. Toliau, tikslinant sertifikatų sudarymo ir duomenų tvarkymo proceso ir sertifikatų galiojimo nutraukimo proceso darbų sekų modelius sudaryti taikomųjų uždavinių modeliai. Taikomųjų uždavinių modeliai detaliai aprašo informacinius srautus ir kompiuterizuojamus uždavinius.

Suprojektuotos duomenų bazės. Panaudojant esybių-ryšių modeliavimo priemones, pagal duomenų srautų struktūrų schemas sudaryta esybių ryšių schema ir parengtas duomenų bazės loginės struktūros aprašymas. Suprojektuotos dvi tarpusavyje susietos reliacinė duomenų bazės MySQL. Duomenų bazę *esign* sudaro keturios lentelės, o *esign_archyvas* - viena lentelė.

3. SERTIFIKATŲ CENTRO IS REALIZACIJA

3.1. PROGRAMINĖS ĮRANGOS SUDĖTIS

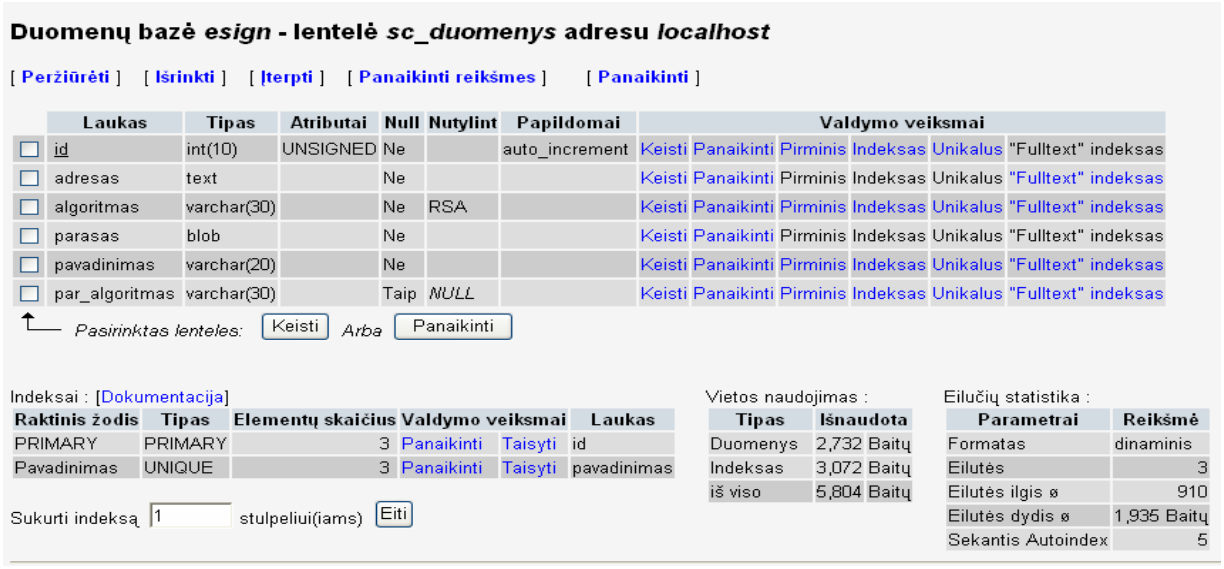
3.1.1. Programinės įrangos aprašymas

Visos naudotos priemonės – *MySQL4, PHP4.3*, *Web (Apache) server,* FrontPage 2002, Visio 2000 yra „draugiškos“ vartotojui, su jomis lengva kurti bei patogu tvarkyti sukurtus produktus. Programinės įrangos aprašymas yra skirtas trumpam duomenų bazių valdymo sistemų apibūdinimui.

MySQL4 - reliacinė duomenų bazių valdymo sistema. Tai programa, galinti saugoti didžiulį kiekį įvairios informacijos ir pateikti ją taip, kad tenkintų bet kokios organizacijos poreikius. Tai populiariausia atvirojo kodo duomenų bazė pasaulyje. *MySQL4* naudoja struktūrinę užklausų kalbą. Beveik visos DBVS naudoja SQL, nors kai kurios gali būti papildytos savaip. Su *MySQL4* sukurtą programos prototipą bus galima be problemų perkelti į kitas nuosavybės teisių saugomas reliacines duomenų bazes *Oracle, SQL Server, DB2, PostgreSQL, Sybase.* Dirbant su *MySQL4* , duomenų bazių taikomąsias programas galima kurti daugeliu šiuo metu naudojamų programavimo kalbų ir vykdyti jas daugelyje operacinių sistemų. *MySQL4* geriausiai integruojasi į *PHP, Perl, Java, C, C++ ir Python* programavimo aplinkas. Magistriniame darbe naudoju PHP programavimo aplinką.

3.1.2. Duomenų bazės realizacija

Naudojant reliacinę duomenų bazių valdymo sistemą MySQL, sukurta sertifikatų duomenų bazė „Esign“. Ją sudaro 4 reliacinės duomenų lentelės: klientas, sertifikatas, vartotojai ir sc_duomenys. Duomenų bazės lentelė „sc_duomenys“ pateikta 3.1 paveiksle. Lentelės: klientas, sertifikatas ir vartotojai pateiktos 2 priede.



Duomenų bazė *esign* - lentelė *sc_duomenys* adresu *localhost*

[Peržiūrėti] [Išrinkti] [Įterpti] [Panaikinti reikšmes] [Panaikinti]

	Laukas	Tipas	Atributai	Null	Nutylint	Papildomai	Valdymo veiksmai
☐	id	int(10)	UNSIGNED	Ne		auto_increment	Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	adresas	text		Ne			Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	algoritmas	varchar(30)		Ne	RSA		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	parasas	blob		Ne			Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	pavadinimas	varchar(20)		Ne			Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	par_algoritmas	varchar(30)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas

Pasirinktas lenteles: Keisti Arba Panaikinti

Indeksai : [Dokumentacija]

Raktinis žodis	Tipas	Elementų skaičius	Valdymo veiksmai		Laukas
PRIMARY	PRIMARY	3	Panaikinti	Taisyti	id
Pavadinimas	UNIQUE	3	Panaikinti	Taisyti	pavadinimas

Sukurti indeksą 1 stulpeliui(iams) Eiti

Vietos naudojimas :

Tipas	Išnaudota	
Duomenys	2,732	Baitų
Indeksas	3,072	Baitų
iš viso	5,804	Baitų

Eilučių statistika :

Parametrai	Reikšmė
Formatas	dinaminis
Eilutės	3
Eilutės ilgis ø	910
Eilutės dydis ø	1,935 Baitų
Sekantis Autoindex	5

3.1 pav. Duomenų bazės „esign“ lentelė “sc_duomenys”

Naudojant reliacinę duomenų bazių valdymo sistemą MySQL, sukurta sertifikatų duomenų bazė „Esign_archyvavimas“. Ją sudaro 1 reliacinės duomenų lentelė –sertifikatas_archyvas.

Duomenų bazė *esign_archyvas* - lentelė *sertifikatas_archyvas* adresu *localhost*

[Peržiūrėti] [Išrinkti] [Įterpti] [Panaikinti reikšmes] [Panaikinti]

	Laukas	Tipas	Atributai	Null	Nutylint	Papildomai	Valdymo veiksmai
☐	id	int(11)		Ne		auto_increment	Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	galiojimo_pradzia	datetime		Ne	0000-00-00 00:00:00		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	galiojimo_pabaiga	datetime		Ne	0000-00-00 00:00:00		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	serijinis_nr	varchar(20)		Ne			Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	saraso_versija	datetime		Ne	0000-00-00 00:00:00		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas

Pasirinktas lenteles: Keisti Arba Panaikinti

Indeksai : [Dokumentacija]

Raktinis žodis	Tipas	Elementų skaičius	Valdymo veiksmai		Laukas
PRIMARY	PRIMARY	1	Panaikinti	Taisyti	id

Sukurti indeksą 1 stulpeliui(iams) Eiti

Vietos naudojimas :

Tipas	Išnaudota
Duomenys	20 Baitų
Indeksas	2,048 Baitų
iš viso	2,068 Baitų

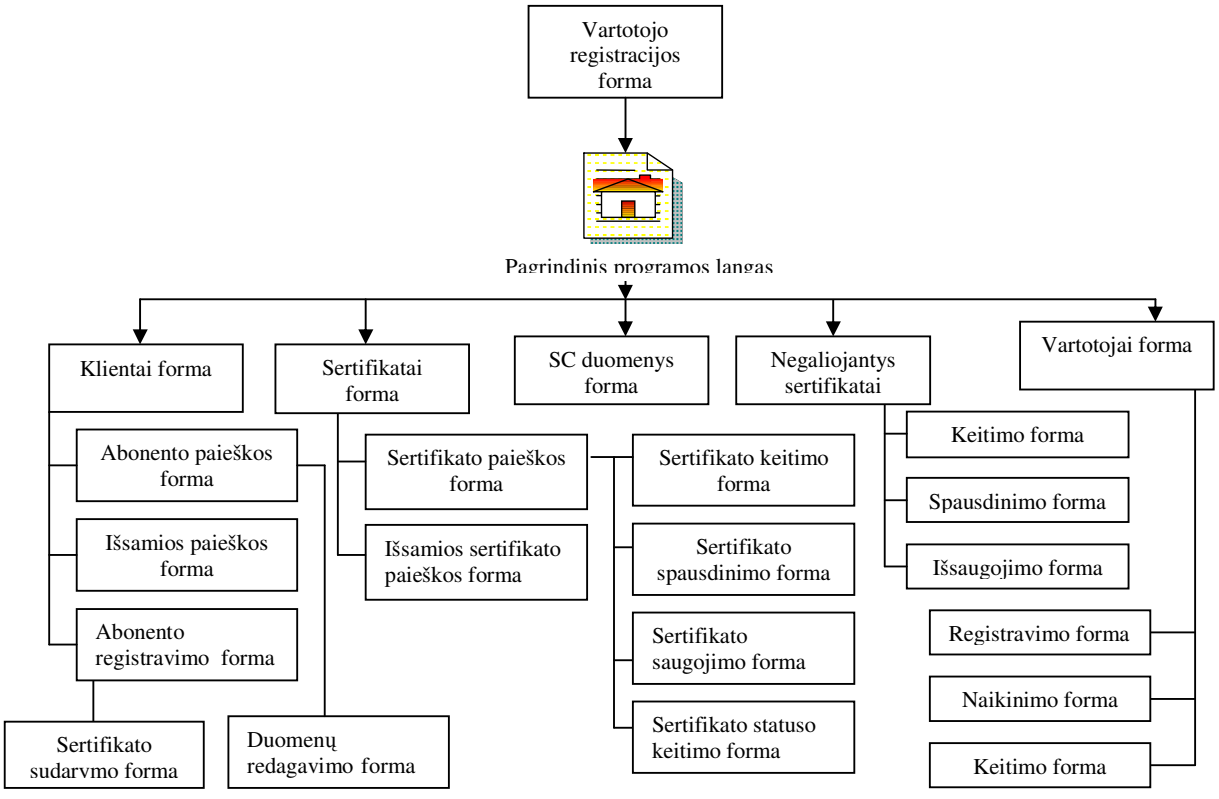
Eilučių statistika :

Parametrai	Reikšmė
Formatas	dinaminis
Eilutės	1
Eilutės ilgis ø	20
Eilutės dydis ø	2,068 Baitų
Sekantis Autoindex	2

3.2 pav. Duomenų bazės „esign_archyvas“ lentelė “sertifikatas_archyvas”

3.1.3. Programinių modulių specifikacijos

Visus programos modulius galima suskirstyti į sertifikatų centro administratoriaus ir kliento, todėl tokia tvarka jie pateikiami žemiau esančioje lentelėje. Sertifikatų duomenų bazė ir negaliojančių sertifikatų duomenų bazė - tai pagrindiniai informacinės sistemos elementai, į kurias informacija rašoma iš IS vartotojos (tarnybinės) dalies ir galima skaityti informaciją iš kliento aplinkos.



3.3 pav. Vartotojo sąsajos modelis (tarnybinės dalies architektūra)

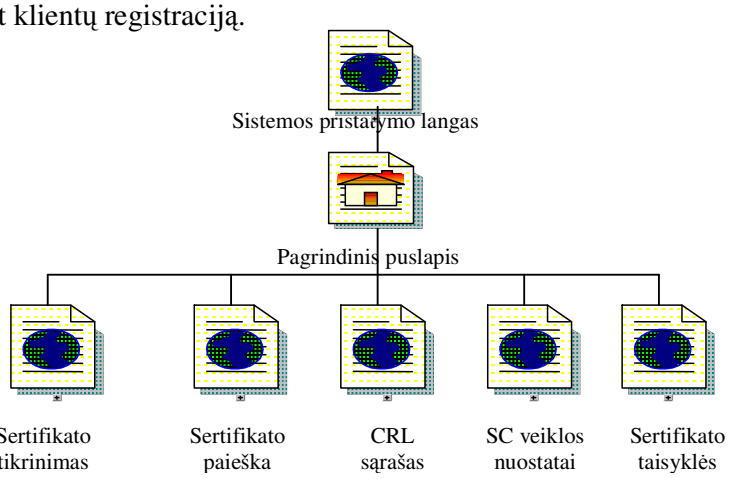
Visi tarnybinės stoties moduliai turi savo paskirtį. Mažas hierarchijos lygių skaičius rodo, kad navigacija sistemoje yra labai paprasta.

3.1 lentelė

Tarnybinės stoties moduliai

Fizinis modulio pavadinimas	Modulio paskirtis
index.php	Sukuria galimybę naudotis programa Internetu. Atidaromas pradinis puslapis.
setup.php	Šis modulis įkraunamas paleidus programą, skirtas vartotojų autorizacijai. Autorizacijai nepavykus, vienintelis aktyvus meniu punktas bus “Grįžti”.
op_klientai_add.php	Skirtas abonento duomenų įterpimui į duomenų bazę
op_klientai_edit	Skirtas abonento duomenų keitimui ir pakeistų duomenų išsaugojimui į duomenų bazę
op_sc_add.php	Skirtas sertifikatų centro duomenų pakeitimui ir išsaugojimui į duomenų bazę.
op_sc_delete.php	Skirtas sertifikatų centro duomenų trynimui
op_sc_edit.php	Modulis Skirtas redaguoti sertifikatų centro duomenis.
op_sert_add.php	Skirtas sertifikato suformavimui ir išsaugojimui į sertifikatų duomenų bazę.
print.php	Modulis skirtas sugeneruoto sertifikato peržiūrai
op_sert_disable.php	Skirtas suformuoti duomenims sertifikato statuso keitikui ir atlikti statuso keitimą
op_sert_edit.php	Modulis skirtas sertifikato duomenų keitimas kai norima pakeisti sertifikato viešąjį raktą.
save.php	Skirtas sertifikato išsaugoti į pasirinktą laikmeną.
op_users_add.php	Skirtas naujo vartotojo sukūrimui
op_users_delete.php	Skirtas vartotojo duomenų šalinimui
op_users_edit.php	Skirtas vartotojo duomenų redagavimui kai norima pakeisti slaptažodį
snip_sertifikatas.php	Sertifikato formavimas priklausomai nuo vartotojo tipo.
archyvuoti.php	Skirtas negaliojančių sertifikatų sąrašų archyvavimui
logaut.php	Atjungia nuo duomenų bazės
functions.php	Tarnybinis modulis, kuriame saugomos įvairios informacijos apdorojimo ir skaičiavimų funkcijos

Kliento dalies modulių struktūra (žr.3.4 pav.) yra paprastesnė. Norint naudotis šia dalimi, tereikia žinoti interneto naršyklės naudojimo pagrindus. Kol kas klientų registracija yra nenaudojama. Sistemos internetinis adresas bus viešai platinamas. Pradžioje sistemos klientų ratas bus nedidelis, todėl klientų registracijos atsisakyta. Norint užtikrinti sistemos saugumą ateityje, reikės sistemą tobulinti įvedant klientų registraciją.



3.4 pav. Kliento dalies architektūra

Kliento moduliai visada yra prienami, kai tik startuojamas pagrindinis puslapis. Hierarchijos lygių yra keturi, tačiau nuolat pasiekiami funkcijos pasirinkimo mygtukai padaro navigaciją labai nesudėtingą.

3.2 lentelė

Kliento dalies moduliai

Fizinis modulio pavadinimas	Modulio paskirtis
index.php	Sukuria galimybę naudotis programa internetu. Atidaromas pradinis puslapis.
area_main. php	Pagrindinis sistemos langas
area.negal. php	Suteikiama galimybė peržiūrėti ir parsisiųsti negaliojančių sertifikatų sąrašą
area_paieska_op. php	Atliekama sertifikato paieška pagal sertifikato numerį
area_tikrinti_op. php	Suteikia galimybę pasitikrinti sertifikato statusą arba parsisiųsti patį sertifikatą.
file.php	Suteikiama galimybė peržiūrėti sertifikato taisykles ir SC veiklos nuostatus.

Visų failų turinys pateiktas CD diske.

3.2. VARTOTOJO SĄSAJA

Informacinės sistemos vartotojai:

- Klientai – tai parašo tikrintojai, kurie jungiasi prie sistemos per internetą, norėdami pasitikrinti sertifikato statusą, o prireikus gali parsisiųsti ir sertifikatą ar CRL sąrašus.
- Vartotojai – sertifikatų centro darbuotojai kurie tvarko abonentų duomenis ir sudarinėja sertifikatus.

3.2.1. Kliento vadovas

LTVUSERT sertifikatų centro viešieji raktai platinami su pasirašytais sertifikatais ir bet kada prieinami patikrinimui operatyviuoju ryšiu (WWW serverio pagalba). Tai suteikia galimybę įsitikinti tam tikro sertifikato (pasirašyto SC privačiuoju raktu) autentiškumu ir sertifikato statusu.

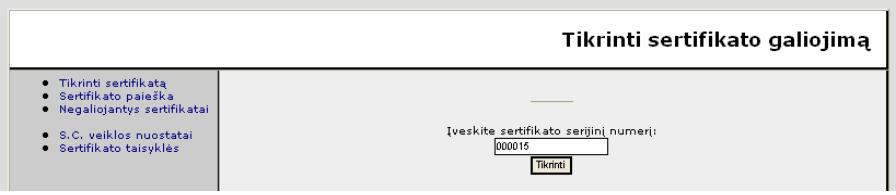
Tam reikia paleisti naršyklę “Internet Explorer”, parašyti sertifikatų centro adresą (pvz. **http://www.ltvusert.lt**). Tada pasileis pagrindinis kliento dalies langas (3.5 pav.) iš kurio bus galima pasirinkti reikiamas operacijas:

- tikrinti sertifikatą;
- atlikti sertifikato paiešką;
- peržiūrėti arba parsisiųsti negaliojančių sertifikatų sąrašą;
- peržiūrėti arba parsisiųsti sertifikatų centro veiklos nuostatus;
- peržiūrėti arba parsisiųsti sertifikato taisykles.

3.5 pav. LTVUSERT sertifikatų centro tinklalapio pagrindinis langas

Sertifikato tikrinimas.

Norint patikrinti sertifikato galiojimą, reikia pasirinkti komandą „Tikrinti sertifikatą“. Pateiktame lange (3.6 pav.) reikia įvesti sertifikato serijinį numerį ir paspausti komandų mygtuką „Tikrinti“. Priklausomai nuo paieškos rezultatų, pateikiama pranešimai (3.3 lentelė).



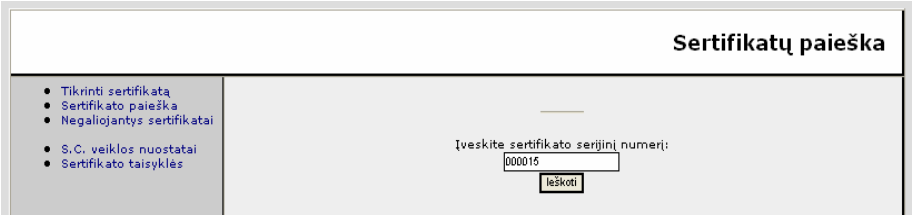
3.6 pav. LTVUSERT sertifikatų centro sertifikatų galiojimo tikrinimo langas

3.3 lentelė

“Sertifikato nurodytu numeriu paieškos sertifikatų centro duomenų bazėje rezultatai “

Paieškos rezultatas	Pranešimas
Sertifikatas yra sertifikatų centro duomenų bazėje	Sertifikatas 000000 galioja“
Sertifikato nėra sertifikatų centro duomenų bazėje	Sertifikatas su tokiu serijiniu Nr. nerastas
Sertifikatas su įrašytu numeriu negalioja	Sertifikatas 000000 negalioja. Jo galiojimo laikas yra: nuo YYYY-MM-DD; 00:00:00 GMT+02000 iki YYYY-MM-DD; 00:00:00 GMT+02000.

Sertifikato paieška



3.7 pav. LTVUSERT sertifikatų centro sertifikatų paieškos langas

Vartotojas sertifikatų centro tinklalapyje gali sužinoti ne tik sertifikato statusą, bet ir peržiūrėti, atsispausdinti ar išsisaugoti reikiamą sertifikatą savo kompiuteryje. Norint peržiūrėti sertifikatą, reikia išrinkti komandą „Sertifikato paieška“ ir pateiktame tinklalapio lange (3.7 pav.) įrašyti reikiamą sertifikato serijinį numerį.

Jei sertifikatas tokiu serijiniu numeriu yra surastas, ekrane pateikiama informacija „Sertifikatas 000000 surastas“. Galima pasirinkti komandas:

- spausdinti;
- saugoti.

Parinkus komandą „Spausdinti“, galima peržiūrėti sertifikatą ekrane (žr. 1 priedas). Parinkus komandą „Saugoti“, pateikiamas dialogo langas, kuriame galima nurodyti personalinio kompiuterio laikmeną sertifikatui išsaugoti.

Negaliojantys sertifikatai

Sertifikatų centro tinklalapyje pateikiamas „Negaliojančių sertifikatų sąrašas (CRL)“. Norint peržiūrėti negaliojančių sertifikatų sąrašą, reikia pasirinkti komandą „Negaliojantys sertifikatai“. Pateikiamas negaliojančių sertifikatų sąrašas (3.8 pav.), kuriame yra:

- sertifikato serijinis numeris,
- negaliojimo priežasties;
- sertifikato galiojimo nutraukimo datos.

Pasirinkę komandą „Išsaugoti sąrašą“, negaliojančių sertifikatų sąrašą galime išsaugoti personaliniame kompiuteryje.

Norint peržiūrėti reikiamą sertifikatą iš negaliojančių sertifikatų sąrašo, reikia nuvesti pelytės rodyklę ant reikiamo sertifikato numerio ir paspausti kairį pelės klavišą.

3.8 pav. LTVUSERT sertifikatų centro negaliojančių sertifikatų sąrašas (CRL)

Sertifikatų centro veiklos nuostatų ir sertifikato taisyklių peržiūra

Vartotojas, norintis peržiūrėti ar išsisaugoti savo kompiuteryje sertifikato taisykles, turi pasirinkti komandą „Sertifikato taisyklės“.

Vartotojas, norintis peržiūrėti ar išsisaugoti savo kompiuteryje sertifikatų centro veiklos nuostatus, turi pasirinkti komandą „SC veikos nuostatai“.

3.2.2. Vartotojo vadovas

Programos paleidimas

Paleisti naršyklę “Internet Explorer”, parašyti administratoriaus nurodytą adresą (pvz. http://www.marinet.lt/~vida/admin/).

Darbas su programa

Prisijungimas prie sistemos

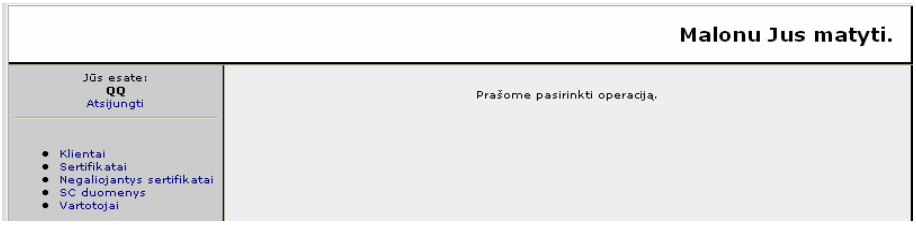
Sistemoje registruojamasi savo prisijungimo vardu ir slaptažodžiu, jei tai daroma ne pirmą kartą. Jei bandome registruotis pirmą kartą, prieš tai reikia susisiekti su sistemos administratoriumi ir jums bus paskirtas prisijungimo vardas ir slaptažodis. Vartotojo vardas ir teisės suteikiamos darbuotojui

pagal pareigybes ir sertifikatų centro nuostatus. Sertifikatų sudarymo tarnybos darbuotojas prisijungimo prie sistemos lange (3.9 pav.) įveda savo vartotojo vardą ir slaptažodį .

3.9 pav. Prisijungimo prie sistemos langas

Įvedęs vartotojo vardą ir slaptažodį ir sėkmingai prisijungęs prie duomenų bazės, sertifikatų sudarymo tarnybos darbuotojas gali pasirinkti reikiamas operacijas (3.10 pav.):

- Klientai;
- Sertifikatai;
- Negaliojantys sertifikatai;
- SC duomenys;
- Vartotojai.

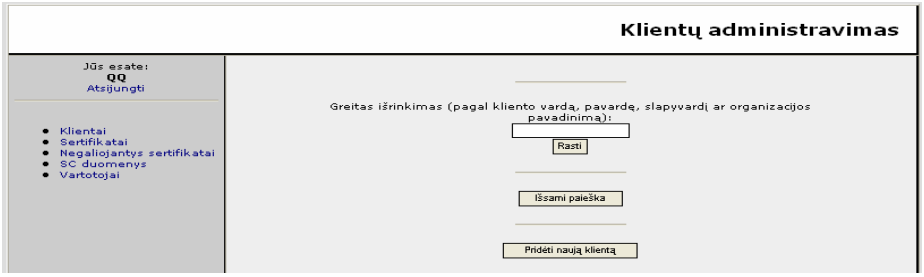


3.10 pav. Operacijų pasirinkimo langas

Sertifikatų centro klientų duomenų tvarkymas

Paspaudus mygtuką „Klientai“ (3.10 pav.), patenkame į darbalaukį (3.11 pav.), kuriame galime:

- pridėti naują klientą paspaudus mygtuką „Pridėti naują klientą“;
- atlikti kliento paiešką pagal vardą, pavardę, slapyvardį ar organizacijos pavadinimą paspaudus komandų mygtuką „Rasti“;
- atlikti išsamią paiešką komandų mygtuku „Išsami paieška“.

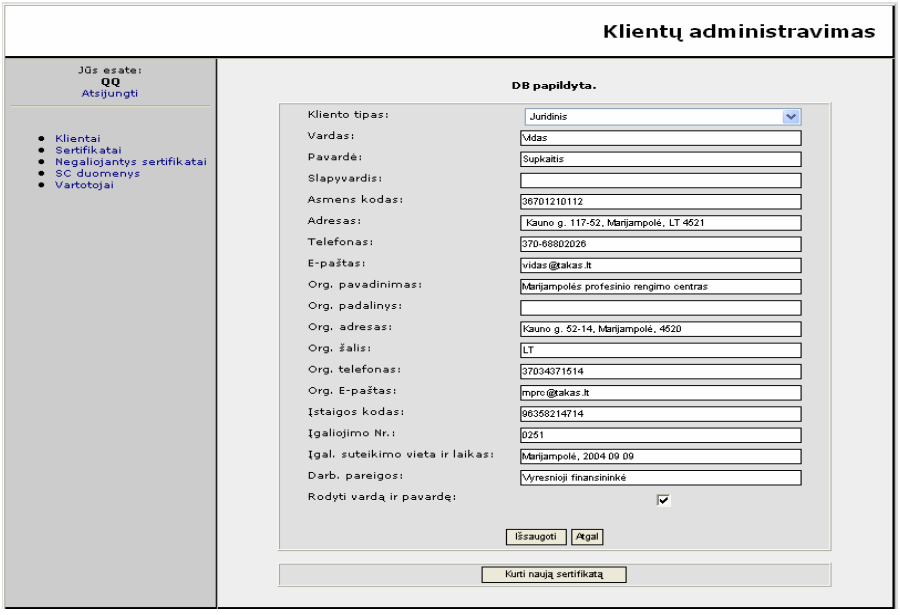


3.11 pav. Klientų administravimo langas

Naujo abonento registravimas

Paspaudus mygtuką „Pridėti naują klientą“ (3.12 pav.), pateiktoje formoje reikia pasirinkti kliento tipą ir įvesti sertifikatų centro abonento reikiamus duomenis. Suvedus duomenis paspauskite komandų mygtuką „Išsaugoti“.

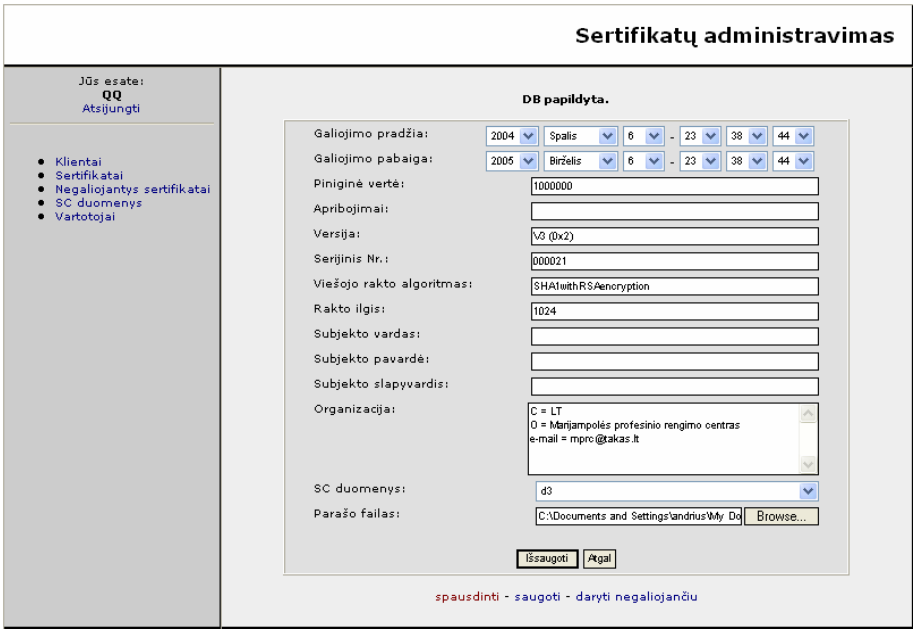
Norint sukurti sertifikatą reikia paspausti komandų mygtuką „Kurti naują sertifikatą“.



3.12 pav. Naujo abonento registravimas

Sertifikatų sudarymas

Vartotojui paspaudus komandų mygtuką „Kurti naują sertifikatą“, sistema pateikia formą „Sertifikatų administravimas“ (3.13 pav.), kurioje reikia įrašyti reikiamus sertifikato duomenis.



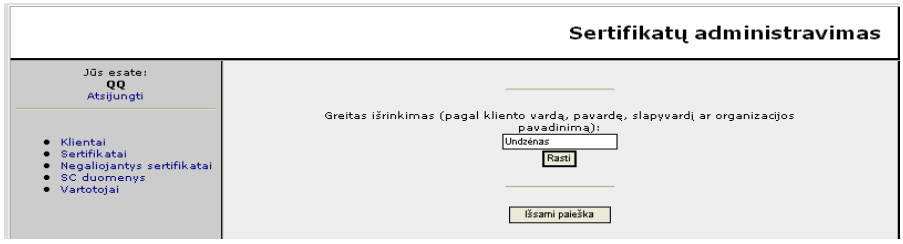
3.13 pav. Sertifikato sudarymas

Sistema reikiamus abonento duomenis įkelia iš duomenų bazėje išsaugotų abonento duomenų, o vartotojas turi nurodyti sertifikato galiojimo pabaigos datą, įvesti rakto ilgį, įkelti sertifikatų centro duomenis ir abonento viešąjį raktą. Abonento viešasis raktas įkeliamas iš failo kuris yra kataloge „Viešieji raktai“. Komandų mygtuku „Browse“. Suvedus reikiamus duomenis paspauskite komandų mygtuką „Išsaugoti“. Sertifikatas galiojimo pradžia laikoma tuomet, kai sertifikatas išsaugomas į sertifikatų duomenų bazę.

Sudarius ir išsaugojus sertifikatą duomenų bazėje komandų mygtuku „spausdinti“ galime peržiūrėti sudarytą sertifikatą (žr. 1priedas) arba išsaugoti į reikiamą informacijos laikmeną.

Sertifikatų administravimas

Paspaudus mygtuką „Sertifikatai“ (3.10 pav.), patenkame į darbalaukį (3.14 pav.) kuriame galime atlikti sertifikato paiešką pagal abonento vardą, pavardę, slapyvardį ar organizacijos pavadinimą. Galima atlikti ir greitą informacijos išrinkimą paspaudus komandų „Greitas išrinkimas“.



3.14 pav. Sertifikatų paieškos langas

Į paieškos langą įveskite abonento vardą, pavardę arba slapyvardį, o jei juridinis asmuo įveskite organizacijos pavadinimą ir paspauskite komandų mygtuką „Rasti“. Sistema pateiks paieškos rezultatą (3.15pav.).

3.15 pav. Sertifikatų paieškos pagal nurodytus kriterijus langas

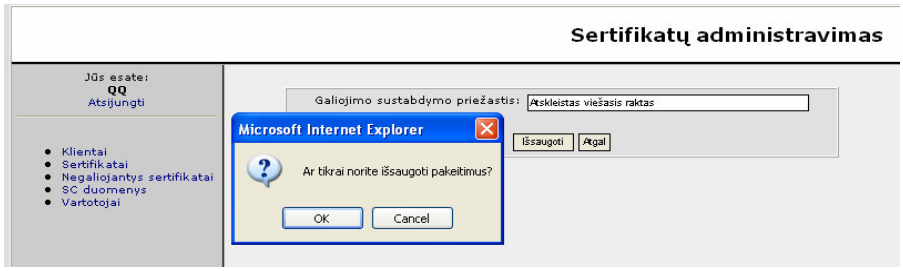
Pateiktame lange (3.15pav.) galima pasirinkti operacijas:

- keisti;
- spausdinti;
- saugoti;
- daryti negaliojančiu.

Operacija „keisti“ naudojama, kai abonentas nori sudaryti dar vieną sertifikatą kuris turėtų kitą raktą ar pakeistus apribojimus. Šiuo atveju sistema pateiks 3.13 paveiksle pateiktą formą kur reikės pakeisti reikiamus parametrus. Toliau vykdykite veiksmus aprašytus „Sertifikatų sudarymas“ dalyje. Šiuo atveju bus sudarytas naujas sertifikatas.

Pasirinkus operaciją „spausdinti“ bus pateiktas abonento sertifikatas (1 priedas).

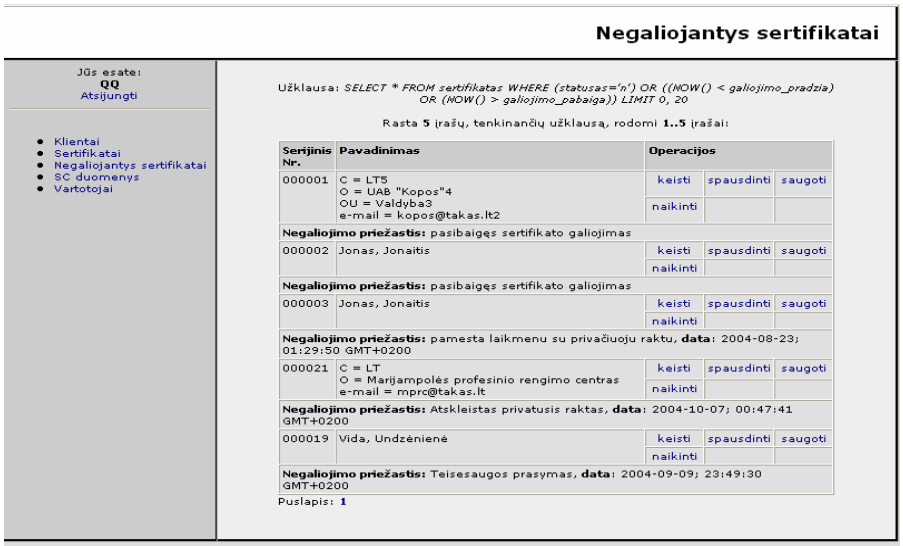
Kai reikia atlikti sertifikato statuso keitimą tuomet reikia pasirinkti operaciją „daryti negaliojančiu“. Sistema pateiks langą (3.16 pav.) kuriame reikia įrašyti sertifikato galiojimo sustabdymo priežastį ir paspausti komandų mygtuką „Išsaugoti“. Sistema visada pateikia pranešimą „Ar tikrai norite išsaugoti pakeitimus?“, kuriame reikia atlikti patvirtinimą paspaudus „OK“. Paspaudus „OK“ pateikiamas pranešimas „ Sertifikato galiojimas sustabdytas“. Sistema pakeičia sertifikato statusą iš „galioja“ į „negalioja“ ir įkeliama sistemos laikas nurodantis sertifikato galiojimo nutraukimą.



3.16 pav. Sertifikato statuso keitimas

Negaliojančių sertifikatų administravimas

Paspaudus mygtuką „Negaliojantys sertifikatai“ (3.10 pav.), darbalaukyje (3.17 pav.) pateikiama negaliojančių sertifikatų sąrašas kuriame nurodyta serijiniai numeriai, abonento pavadinimas, galiojimo nutraukimo priežastis ir jei sertifikato galiojimas buvo nutrauktas ankščiau sertifikate numatyto galiojimo pabaigos termino, tai nurodoma sertifikato galiojimo data ir laikas.



3.17 pav. Negaliojančių sertifikatų peržiūros langas

Pateiktame lange (3.17 pav.) galima pasirinkti operacijas:

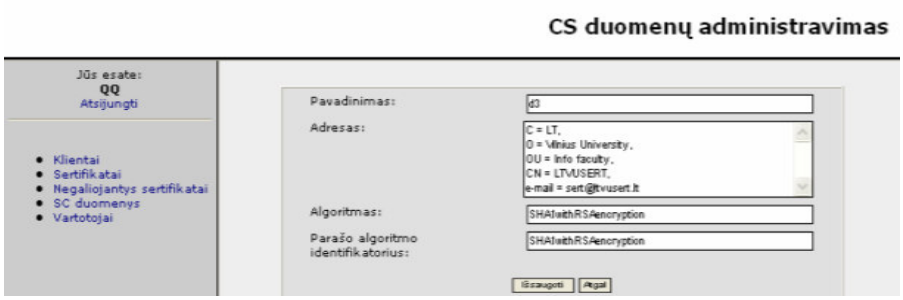
- keisti:
- spausdinti;
- saugoti.

Operacija „keisti“ naudojama, kai negaliojančio sertifikato savininkas nori sudaryti naują sertifikatą. Kadangi jo duomenys duomenų bazėje jau yra tai tam kad dar kartą nereikėtų įvedinėti abonento duomenų galima sudaryti sertifikatą. Toliau reikia atlikti veiksmus aprašytus „Sertifikatų sudarymas“ dalyje.

Pasirinkus operaciją „spausdinti“ bus pateiktas abonento sertifikatas (1 priedas).

SC duomenų administravimas

Kadangi elektroninio parašo sertifikatų centro duomenys sudarant sertifikatą keliami tie patys, tai vartotojo patogumui jie sudedami atskirai ir automatiškai įkeliami į reikiamas sertifikato vietas. Sertifikatų centro duomenis reikia keisti pakeitus sertifikatų centro adresui, elektroniniam paštui ar kitiems svarbiems duomenims kurie turi būti pareikti sertifikate. Tam reikia pasirinkti komandų mygtuką „SC duomenys“ (3.10 pav.) ir pateiktoje formoje (3.18 pav.) galime suvesti naują variantą arba pakeisti jau esamus, o nereikalingus ištrinti.



3.18 pav. SC duomenų keitimas

Naujų vartotojų sukūrimas

Teisė jungtis ir tvarkyti sistemos duomenis suteikiama darbuotojui pagal pareigybes kurios aprašytos sertifikatų centro nuostatuose. Vartotojo vardas suteikiamas sistemos administratoriaus. Slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių bei skaičių bei ne trumpesnis kaip aštuoni simboliai.

Paspaudys mygtuką „Vartotojai“, patenkame į darbalaukį kuriame matome visus vartotojus kurie gali prisijungti prie sistemos ir taip pat sukurti naują vartotoją. Pasirinkus komandų mygtuką „Pridėti naują“ pateikiamas langas kuriame reikia įrašyti vartotojo vardą ir slaptažodį.

Norint išeiti iš sistemos reikia paspausti komandų mygtuką „Atsijungti“.

Baigus darbą, uždarome naršylės langą, paspaudus viršutiniame dešiniajame kampe ant nedidelio kryžiuko.

3.3. PROGRAMUOTOJO VADOVAS

Administratoriaus dalis. Sistemai reikalinga veikianti MySQL duomenų bazė, veikiantis Web serveris ir PHP interpretatorius (versija vėlesnė nei 4.3).

- ***MySQL diegimas ir konfigūravimas***

1. Laikiname kataloge išarchyvuoti zip failiuką, paleisti Setup.exe.
2. Įdiegti MySQL kaip servisą. Komandinėje eilutėje surinkti:

   cd c:\mysql\bin
   mysqld-max-nt.exe –install

3. Paleisti MySQL serverį **"Control Panel->Administrative Tools**" pasirinkti "**Services**" sąraše MySQL ir paspausti "**start**".
4. Sutvarkyti MySQL saugumą. Komandinėje eilutėje surinkti:

mysqladmin –u root –p password jusu_pasirinktas_root_slaptazodis

Po to patikrinti ar galima prisijungti prie MySQL serverio, komandinėje eilutėje surinkti:

C:\mysql\bin>mysql –u root –p
Enter password:*****

5. Sukurti duomenų bazę "esign":

   c:\mysql\bin MORE esign.sql | mysql esign

- ***Web (Apache) serverio diegimas ir konfigūravimas***

1. Paleisti apache_1.3.31-Win32-x86-no_src.exe.
2. Pasirinkti standartinę *localhost* konfigūraciją:

   Network Domain: *localhost.lc*
   Server Name: *localhost.lc*
   Administrator's Email Address: *webmaster@localhost.lc*

3. Paleisti Apache **"Control Panel->Administrative Tools**" pasirinkti "**Services**" sąraše Apache ir paspausti "**start**".
4. Patikrinti ar veikia Apache: naršyklės adreso laukelyje surinkti *http://127.0.0.1/*.

- **PHP diegimas ir konfigūravimas**

1. Į laikinąjį katalogą c:\php išarchyvuoti php.zip.
2. Kataloge C:\Php esantį failą *php4ts.dll* perkelti į C\:Windows\System32
3. Kataloge C:\Php esantį failą php.ini-dist pervardinti į php.ini ir nukopijuoti į C:\Windows.
4. Sustabdyti Apache.
5. Redaguoti Apache konfigūracinį failą, esantį C:\Program File\Apache Group\Apache\conf\httpd.conf, kurioje nors vietoje įrašant tokias eilutes:

   # Load the PHP module and set up the .php extension
   LoadModule php4_module c:/PHP/sapi/php4apache.dll
   AddType application/x-httpd-php .php

6. Paleisti Apache.

7. Kataloge C:\Program File\Apache Group\Apache\htdocs sukurti savo projekto katalogą”esign” ir ten sudėti savo projektą.

8. Prieš naudojantis sistema reikia nurodyti prisijungimo prie duomenų bazės parametrus. Tam reikia functions.php faile nustatyti kintamuosius $mysql_databasename, $mysql_host, $mysql_username, $mysql_password.

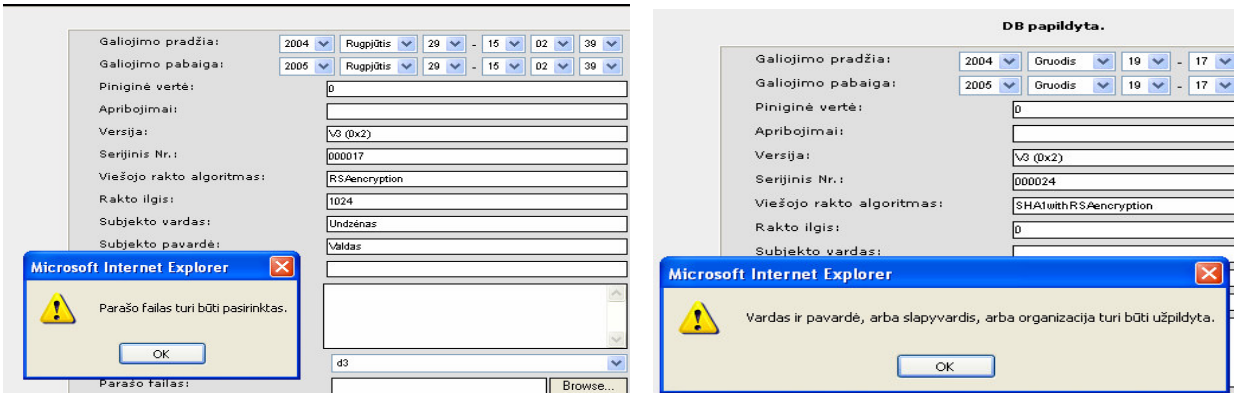
- **Sistemos konfigūravimas**

Paleisti programą atliekančią negaliojančių sertifikatų sąrašo sudarymą ir perkėlimą į negaliojančių sertifikatų duomenų bazę. **"Control Panel->Scheduled Tasks**" pasirinkti “**Add Scheduled Tasks** ” Atsidariusiame vedlio „**Scheduled Tasks** Wizard“ lange nurodykite kelią iki failo „*archyvuoti php*“ ir nurodykite programos paleidimo dažnumą 3 valandos.

Kliento dalis. Reikia užtikrinti ryšį su internetu ir instaliuoti naršyklę “Internet Explorer 4.0” arba aukštesnę versiją. Tada reikia pasirinkti naršyklės meniu punkte “Tools” papunktyje “Internet Options” kortelėje “Security” zoną “Internet”.

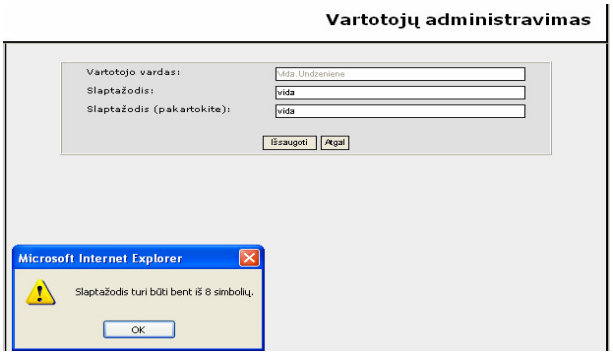
3.4. DUOMENŲ ĮVEDIMO KONTROLĖ

Kad išvengti duomenų įvedimo klaidų sistemoje veikia duomenų įvedimo kontrolė. Sistemos viena iš svarbiausių operacijų sertifikato generavimas, todėl labai svarbu, kad visi sertifikato laukai kuriuos nurodo IETF RFC 2459 standartas turi būti užpildyti. Jei pildant sertifikatų sudarymo formą neužpildoma kuris nors laukas, pvz. neparingtas viešojo rakto failas, neįvedus pavardės, vardo ar slapyvardžio, sistema pateikia pranešimą (3.19 pav.) ir neleidžia išsaugoti duomenų. Tik užpildžius visus laukus galima sudaruti sertifikatą.



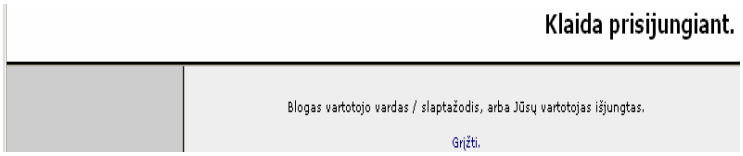
3.19 pav. Sertifikatų sudarymo formoje pateikiamas pranešimas pamiršus užpildyti lauką

Stengiantis užtikrinti sistemos saugumą vartotojo slaptažodį turi sudaryti ne mažiau kaip aštuoni simboliai. Tai gi registruojant naują vartotoją įvedus per trumpą slaptažodį sistema tokio slaptažodžio nepriima ir pateikiamas paaiškinimas, kad slaptažodį turi sudaryti bent aštuoni simboliai (3.20 pav.).



3.20 pav. Vartotojo slaptažodžio įvedimo kontrolė

Visi su sistema dirbantys vartotojai turi savo prisijungimo vardą ir slaptažodį. Jei sistemos vartotojas ne teisingai įveda vartotojo vardą ar slaptažodį jis prie sistemos duomenų neprileidžiamas, o sistema pateikia jam pranešimą. (3.21 pav.)



3.21 pav. Sistemos langas vartotojui klaidingai įvedus vartotojo vardą ar slaptažodį

3.5. TESTAVIMO APRAŠYMAS

„Krioklio“ modelis informacinės sistemos kūrimo eigoje apima visus etapus. Vienas iš etapų - tai sistemos testavimas. Testavimo tikslas yra ne ankstyvose fazėse paliktų defektų nustatymas, bet jų nebuvimo demonstravimas, validavimas ir patvirtinimas.

Kiekviena programos dalis buvo testuojama atskirai prieš ją integruojant į sistemą. Prieš apjungiant žemesnio lygio komponentus į vieną sistemą, buvo įsitikinama, kad jie individualiai dirba teisingai, o tik tada testuojama integruotai.

Zend kompiliatoriaus pagalba buvo atlikta komponentų automatinė statinė analizė. Čia buvo testuojama: sintaksės korektiškumas, kintamųjų panaudojimas, valdymo blokų teisingumas, įvedimo/išvedimo klaidų išankstinė analizė, programinė komponento sąsaja. Įsitikinus komponento veikimo teisingumu, jis buvo prijungiamas prie bendros programos sistemos.

Atliekant sistemos dalių testavimą buvo pastebėtos kelios nežymios klaidos. Sudarant sertifikatą (pagal IETF RFC 2459 standartą) sistema neįkeldavo slapyvardžio į sertifikatą, nors duomenų bazėje buvo užpildytas reikiamas laukas. Todėl teko koreguoti snip_sertifikatas.php failą. Taip pat testuojant sistemą buvo pastebėta, kad neatliekamas negaliojančių sertifikatų sąrašų archyvavimas. Klaidos buvo greitai surastos. Pataisytas *archyvuoti.php* failas.

Taip pat buvo atlikta vartotojo sąsajos testavimas. Testuotas vartotojo sąsajos suprantamumas, aiškumas bei patogumas naudotis. Tai buvo atlikta paprašius su šiuo projektu nieko bendro neturinčių žmonių, be jokių taisyklių ir apribojimų, pasinaudoti vartotojo sąsaja ir pateikti savo pastabas. Tai turėjo padėti surasti specifikacijos klaidas. Pritaikius šį metodą jokių grubių sutrikimų nepastebėta.

4. REZULTATAI IR IŠVADOS

Darbe išanalizuota:

- Elektroninio parašo sertifikato struktūrą nustatantys standartai IETF RFC 2459, IETF RFC 3039, IETF TS 101 862.
- Standartai ETSI TS 101 456, CWA 14167-1**,** CWA 14167-2, kuriuose nustatyti reikalavimai elektroninio parašo sertifikatų centro veiklos procesams ir naudojamai įrangai.
- Standartas CWA 14167-1, nustatantis saugumo reikalavimus patikimoms sertifikatų tvarkymo sistemoms.
- Elektroninio parašo infrastruktūros vystymo Lietuvoje problemos.
- Atlikta elektroninio parašo sertifikatų centrų analitinė apžvalga.
- Atlikta sertifikatų centruose naudojamos programinės įrangos ir saugių duomenų perdavimo protokolų apžvalga.

Pasirinktos elektroninio parašo sertifikatų centro IS sistemos projektavimui ir realizavimui reikalingos priemonės:

- organizacijų veiklos modeliavimo sistema *ProVision Workbench*^{TM}*v.3.1*,
- reliacinė duomenų bazių valdymo sistema *MySQL*,
- programavimo interpretatorius *PHP*,
- *Web* ***(Apache)*** serveris.

Suprojektuota:

- elektroninio parašo sertifikatų centro organizacinė struktūra;
- sudarytas sertifikatų centro veiklos modelis;
- sertifikavimo proceso analizei sudarytas darbų sekų modelis. Kadangi sertifikavimo procesą sudarantys sertifikatų ir sertifikatų centro duomenų teikimo, sertifikatų sudarymo ir duomenų tvarkymo, sertifikatų galiojimo nutraukimo, negaliojančių sertifikatų duomenų teikimo procesai yra sudėtiniai, tai šiems procesams sudaryta detalesni žemesnio lygio darbų sekų modeliai.
- sudaryti sertifikatų sudarymo ir duomenų tvarkymo bei negaliojančių sertifikatų duomenų teikimo taikomųjų uždavinių modeliai, kurie detaliai aprašo IS informacijos srautus ir kompiuterizuojamus uždavinius.
- Sudaryta visų IS informacijos srautų struktūrinės schemos.
- Pagal informacinius srautus sukurta esybių-ryšių schema, jos pagrindu parengta duomenų bazės loginė schema.

Sukurta:

- Naudojant reliacinę duomenų bazės valdymo sistemą sukurta dvi tarpusavyje sukurtos duomenų bazės *Esign* ir *Esign_archyvas*.

- Sukurtas programos modelis generuojantis elektroninio parašo sertifikatą kurio struktūra atitinka standartų IETF RFC 2459, IETF RFC 3039, IETF TS 101 862 reikalavimus.
- Sudarytas programinių modulių specifikacija.
- Sistemos vartotojams parengti trijų tipų vadovai – vadovas klientui, vadovas vartotojui (operatoriui) ir vadovas programuotojui,

Magistriniame darbe parengtas el.parašo sertifikatų centro informacinės sistemos projektas gali pasitarnauti kaip pradinis impulsas steigiant Lietuvoje pirmąjį sertifikatų centrą. Žinoma, kai kurios magistrinio darbo nuostatos turės būti tikslinamos ir papildomos pagal keliamus reikalavimus sertifikatams ir el.parašo naudotojų rato poreikius.

LITERATŪRA

1. European Telecommunication Standard Institute, Policy requirements for certification authorities issuing qualified certificates, ETSI TS 101 456, [žiūrėta 2003-12-12]. Prieiga per Internetą: http://portal.etsi.org/esi/el-sign.asp
2. European Telecommunication Standard Institute, Qualified Certificate Profile, ETSI TS 101 862, [žiūrėta 2003-12-13]. Prieiga per Internetą: http://portal.etsi.org/esi/el-sign.asp
3. CEN Workgroup Agreement Standard, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, CWA 14167-1, [žiūrėta 2003-12-13]. Prieiga per Internetą: http://www.cenorm.be/isss/CWAs/cwalist.htm#Electronic%20Signatures
4. CEN Workgroup Agreement Standard, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP), CWA14167-2, [žiūrėta 2003-12-18]. Prieiga per Internetą: http://www.cenorm.be/isss/CWAs/cwalist.htm#Electronic%20Signatures
5. CEN Workgroup Agreement Standard, Secure Signature-Creation Devices, version 'EAL 4', CWA 14168, [žiūrėta 2003-12-25]. Prieiga per Internetą: http://www.cenorm.be/isss/CWAs/cwalist.htm#Electronic%20Signatures
6. CEN Workgroup Agreement Standard, Secure Signature-Creation Devices, version 'EAL 4+', CWA 14169, [žiūrėta 2003-12-25]. Prieiga per Internetą: http://www.cenorm.be/isss/CWAs/cwalist.htm#Electronic%20Signatures
7. CEN Workgroup Agreement Standard, Procedures for Electronic Signature Verification, CWA 14171, [žiūrėta 2003-12-25]. Prieiga per Internetą: http://www.cenorm.be/isss/CWAs/cwalist.htm#Electronic%20Signatures
8. Internet Engineering Task Force and Request For Comments Standard, Internet X.509 Public Key Infrastructure. Certificate and CRL Profile, IETF RFC 1321, [žiūrėta 2001-01-25]. Prieiga per Internetą: http://www.ietf.org/rfc/rfc1321.txt
9. Internet Engineering Task Force and Request For Comments Standard, The MD5 message-digest algorithm, IETF RFC 2459, [žiūrėta 2001-01-25]. Prieiga per Internetą: http://www.ietf.org/rfc/rfc2459.txt
10. Internet Engineering Task Force and Request For Comments Standard, Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practice Statement, . IETF RFC 2527, [žiūrėta 2001-02-20]. Prieiga per Internetą: http://www.ietf.org/rfc/rfc2527.txt
11. Internet Engineering Task Force and Request For Comments Standard, Internet X.509 Public Key Infrastructure. Qualified Certificate Profile,IETF RFC 3039, [žiūrėta 2001-02-23]. Prieiga per Internetą: http://www.ietf.org/rfc/rfc3039.txt
12. Internet Engineering Task Force and Request For Comments Standard, US Secure Hash Algorithm (SHA-1), IETF RFC 3174, [žiūrėta 2001-03-23]. Prieiga per Internetą: http://www.ietf.org/rfc/rfc3174.txt
13. Electronic Signatures and Infrastructures (ESI), Algorithms and Parameters of Secure Electronic Signatures, ETSI SR 002 176, [žiūrėta 2001-03-20]. Prieiga per Internetą: http://portal.etsi.org/esi/el-sign.asp

14. NIST: Security Requirements for Cryptographic Modules, Federal Information Processing Standard FIPS PUB 140-2, 2001. [žiūrėta 2001-04-28]. Prieiga per Internetą: <http://www.nist.gov/cmvp >

15. Commission of the European Communities: Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, 1991.

16. **V.Stakėnas**. Kriptologija (paskaitų konspektai) [interaktyvus]. Vilnius: Matematinės informatikos katedra, Matematikos ir informatikos fakultetas, Vilniaus universitetas, 2001. [žiūrėta 2002-3-18]. Prieiga per internetą: http://www.mif.vu.lt/matinf/asm/vs/vs0.htm

17. Informacinės visuomenės plėtros komiteto prie LRV interneto puslapis. [žiūrėta 2002-3-18]. Prieiga per internetą: http://www.ivpk.lt

18**. Lietuvos Respublikos Seimas/**Elektroninio parašo įstatymas /VIII-1822/2000 07 11/Įsigalioja nuo 2000 07 26/Valstybės žinios'2000 Nr.61-1827.

19. **Lietuvos Respublikos Vyriausybė/** Nutarimas 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/2108/2002 12 31/Įsigalioja nuo 2003 01 09/Valstybės žinios'2003 Nr.2-47.

20. **Lietuvos Respublikos Vyriausybė/** Nutarimas dėl Lietuvos Respublikos Vyriausybės 2001 m. liepos 5 d. nutarimo Nr. 844 „Dėl Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės nuostatų patvirtinimo" pakeitimo/2106/2002 12 31/Įsigalioja nuo 2003 01 09/Valstybės žinios'2003 Nr.2-46.

21. **Lietuvos Respublikos Vyriausybė/** Nutarimas dėl elektroninio parašo priežiūros institucijos /568/2002 04 23/ Įsigalioja nuo 2002 04 27/ Valstybės žinios'2002 Nr.43-1634.

22. **J.Allen, Ch.Hernberger**. PHP4 vadovas. – K.: Smaltija, 2003. – 730p.

23. **I.Gilfillan**. MySQL4 vadovas. – K.: Smaltija, 2003. – 648p.

24. **R.Baronas**. Duomenų bazių sistemos (metodinė priemonė). – V.:TEV, 2002. 126p.

25. **L.Vrašinskaitė, S.Gudas**. Organizacijos veiklos modeliavimo sistemos ProVision Workbench ™ v.3.1 (vartotojo vadovas). – K.: KTU, 1999. - 48p.

26. **S.Gudas**. Objektinės CASE technologijos (paskaitų konspektai). – K.:, KTU, 2004.- 50p.

27. **S.Gudas**. Organizacijos veiklos integruotos sistemos informacinė architektūra. Konferencijų pranešimų medžiaga "Integruotos projektavimo ir gamybos sistemos", K.:, "Technologija", 1999, 4-16 p

SANTRUMPOS

ASN.1 - Abstract Syntax Notation 1, **Abstrakti žymėjimo sintaksė 1**
CA - Certification Authority, **Sertifikatų centras**
CPS - Certification Practice Statement, **Sertifikavimo veiklos nuostatai**
CRL - Certificate Revocation List, **Nebegaliojančių sertifikatų sąrašas**
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 inžinierinių uždavinių sprendėjai**
OCSP - Online Certificate Status Protocol, **Tiesioginės prieigos sertifikatų statuso protokolas**
PIN - Personal Identification Number, **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**
RSA - Rivest-Shamir-Adlemann algorithm, **RSA asimetrinio šifravimo algoritmas**
SHA1 - Secure Hash Algorithm 1, **Saugus santraukos algoritmas 1**
SCD - Signature Creation Device, **Parašo formavimo įranga**
SSCD - Secure Signature Creation Device, **Saugi parašo formavimo įranga**
UTC - Coordinated universal Time, **Universalusis laikas (Grinvičo laikas)**

PRIEDAI

1 PRIEDAS

LTVUSERT SERTIFIKATŲ CENTRO KVALIFIKUOTAS SERTIFIKATAS

VERSIJA (Version)			V3 (0x2)
SERTIFIKATO SERIJINIS NUMERIS (Serial Number)			000003
PARAŠO ALGORITMO IDENTIFIKATORIUS (Signature Algorithm)			SHA1withRSAencryption
SERTIFIKATĄ IŠDAVĘS SERTIFIKATŲ CENTRAS (Issuer)			C = LT, O = Vilnius University, OU = Info faculty, CN = LTVUSERT, e-mail = sert@ltvusert.lt
SERTIFIKATO GALIOJIMO LAIKAS (Validity)		**Nuo** (Not Before)	2004 8 23; 0:42:9 GMT+0300
		Iki (Not After)	2005 8 23; 0:42:9 GMT+0300
SUBJEKTAS (Subject)		**Vardas** (Name)	Jonas
		Pavardė (Surname)	Jonaitis
SUBJEKTO VIEŠASIS RAKTAS (Subject Public Key Info)	**Viešojo rakto algoritmas** (Public Key Algorithm)		SHA1with RSA
	RSA viešasis raktas (RSA Public Key)	**Rakto ilgis** (Key length)	2048 bit
		Modulis (Modulus)	1d:ac:5c:c9:f6:d3:08:03:19:ee:0a:fd:fd:af:b0:31:11:59:43:43:0e:2c:bd:c4:a2:de:fd:77:b1:f3:fb:b5:54:cc:da:68:c6:fe:92:38:a2:4c:3c:e8:0f:91:73:46:dc:0f:dc:f8:43:6a:a6:23:2b:20:ad:c5:2f:e1:eb:76:1c:05:9e:78:57:32:60:9c:1c:21:ba:b1:41:1c:f0:1f:b5:dd:83:a1:77:c3:bf:14:49:e4:ec:d4:13:19:d2:7f:34:d1:f3:8d:68:54:59:33:a4:67:08:64:43:10:7c:5d:68:44:57:97:62:9c:c7:64:ec:2f:9f:8c:64:18:e6:7d:e3:a5:1e:63:83:5d:96:e2:bb:5f:a1:70:02:52:72:0b:58:07:9e:91:59:53:50:17:6a:bb:83:3f:1a:7c:87:99:c4:22:06:ee:81:c0:12:7f:8c:2b:a0:98:c2:f0:6d:06:4c:b1:7e:38:17:af:4a:c0:9a:7c:a3:a5:53:b4:a3:d3:1b:de:d3:c1:bc:90:14:be:2a:64:7a:98:e5:d7:1c:7a:a3:f6:d4:4b:5f:f0:d7:05:7d:3c:84:af:69:32:95:d6:7a:89:2d:e7:a6:9b:4c:22:58:12:34:e0: d8: ba: 59: 99: cd: 62: 0b: 8e: d8: 9b: 65: b8: 41: f2: 3f: f5: 76: a2: cb: 5b
		Eksponentė (Exponent)	65537
SERTIFIKATO IŠPLĖTIMO LAUKAI (X509v3 extentions)			**Sertifikatų centro rakto identifikatorius** (Authority Key Identifier): **Identifikatorius** (Keyid): EA:90:04:ED:9A:D1:47:26:46:94:5D:EA:09:31:C8:6D:31 **Išdavė sertifikatą** (DirName): C=LT/ O=Vilnius University/ OU=Info faculty/ CN=LTVUSERT Serial: 00 **Sertifikato taisyklės** (Certificate policies): **Sertifikato taisyklių** (Policy) **identifikatorius**: 1.2.440.43.2.1.1.1 **Sertifikatų centro veiklos nuostatai** (CPS): http://www.ltvusert.lt/cps **Nebegaliojančių sertifikatų sąrašo gavimo adresas** (CRL distribution points): URI: http://www.ltvusert.lt/crl **Pastaba vartotojams** (User notice): **Sertifikato taisyklės yra adresu** http://www.ltvusert.lt/cp
SERTIFIKATŲ CENTRO PARAŠO ALGORITMAS (Signature Algorithm)			SHA1withRSAencryption
SERTIFIKATŲ CENTRO PARAŠAS (Signature Value)			8d:ac:5c:c9:f6:d3:08:03:19:ee:0a:fd:fd:af:b0:31:11:59:43:43:0e:2c:bd:c4:a2:de:fd:77:b1:f3:fb:b5:54:cc:da:68:c6:fe:92:38:a2:4c:3c:e8:0f:91:73:46:dc:0f:dc:f8:43:6a:a6:23:2b:20:ad:c5:2f:e1:eb:76:1c:05:9e:78:57:32:60:9c:1c:21:ba:b1:41:1c:f0:1f:b5:dd:83:a1:77:c3:bf:14:49:e4:ec:d4:13:19:d2:7f:34:d1:f3:8d:68:54:59:33:a4:67:08:64:43:10:7c:5d:68:44:57:97:62:9c:c7:64:ec:2f:9f:8c:64:18:e6:7d:e3:a5:1e:63:83:5d:96:e2:bb:5f:a1:70:02:52:72:0b:58:07:9e:91:59:53:50:17:6a:bb:83:3f:1a:7c:87:99:c4:22:06:ee:81:c0:12:7f:8c:2b:a0:98:c2:f0:6d:06:4c:b1:7e:38:17:af:4a:c0:9a:7c:a3:a5:53:b4:a3:d3:1b:de:d3:c1:bc:90:14:be:2a:64:7a:98:e5:d7:1c:7a:a3:f6:d4:4b:5f:f0:d7:05:7d:3c:84:af:69:32:95:d6:7a:89:2d:e7:a6:9b:4c:22:58:12:34: e0: d8: ba: 59: 99: cd: 62: 0b: 8e: d8: 9b: 65: b8: 41: f2: 3f: f5: 76: a2: cb: cb

2 PRIEDAS

DUOMENŲ BAZĖS „ESIGN“ LENTELĖS

Duomenų bazė *esign* - lentelė *klientas* adresu *localhost*

[Peržiūrėti] [Išrinkti] [Įterpti] [Panaikinti reikšmes] [Panaikinti]

	Laukas	Tipas	Atributai	Null	Nutylint	Papildomai	Valdymo veiksmai
☐	id	int(10)	UNSIGNED	Ne		auto_increment	Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	tipas	char(1)		Ne	f		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	slapyvardis	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	vardas	varchar(30)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	pavarde	varchar(40)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	asmens_kodas	varchar(11)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	adresas	varchar(255)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	telefonas	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	e_pastas	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	org_pavadinimas	varchar(60)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	org_padalinys	varchar(60)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	istaigos_kodas	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	org_salis	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	org_adresas	varchar(255)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	org_telefonas	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	org_e_pastas	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	igaliojimo_nr	varchar(15)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	igaliojimo_vieta	varchar(200)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	darb_pareigos	varchar(40)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	rodyti_pavarde	char(1)		Ne	t		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas

Pasirinktas lenteles: Keisti *Arba* Panaikinti

Indeksai : [Dokumentacija]

Raktinis žodis	Tipas	Elementų skaičius	Valdymo veiksmai		Laukas
PRIMARY	PRIMARY	16	Panaikinti	Taisyti	id

Sukurti indeksą 1 stulpeliui(iams) Eiti

Vietos naudojimas :

Tipas	Išnaudota
Duomenys	2,056 Baitų
Indeksas	2,048 Baitų
iš viso	4,104 Baitų

Eilučių statistika :

Parametrai	Reikšmė
Formatas	dinaminis
Eilutės	16
Eilutės ilgis ø	128
Eilutės dydis ø	257 Baitų
Sekantis Autoindex	21

1 pav. Duomenų bazės „esign“ lentelė “klientas”

Duomenų bazė *esign* - lentelė *sertifikatas* adresu *localhost*

[Peržiūrėti] [Išrinkti] [Įterpti] [Panaikinti reikšmes] [Panaikinti]

	Laukas	Tipas	Atributai	Null	Nutylint	Papildomai	Valdymo veiksmai
☐	id	int(11)		Ne		auto_increment	Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	galiojimo_pradzia	datetime		Ne	0000-00-00 00:00:00		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	galiojimo_pabaiga	datetime		Ne	0000-00-00 00:00:00		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	pinigine_verte	int(10)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	apribojimai	varchar(255)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	versija	varchar(20)		Ne	V3 versija (0x2)		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	serijinis_nr	varchar(20)		Ne			Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	algoritmas	varchar(30)		Ne	RSA		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	rakto_ilgis	int(10)	UNSIGNED	Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	eksponente	int(10)	UNSIGNED	Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	statusas	char(1)		Ne	g		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	negaliojimo_priezastis	text		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	negaliojimo_data	datetime		Taip	0000-00-00 00:00:00		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	subjektas_vardas	varchar(30)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	subjektas_pavarde	varchar(40)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	subjektas_slapyvardis	varchar(20)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	subjektas_organizacija	varchar(255)		Taip	*NULL*		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	sc_duom_id	int(10)	UNSIGNED	Ne	0		Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas
☐	sugeneruotas_sertifikatas	text		Ne			Keisti Panaikinti Pirminis Indeksas Unikalus "Fulltext" indeksas

Pasirinktas lenteles: Keisti *Arba* Panaikinti

Indeksai : [Dokumentacija]

Raktinis žodis	Tipas	Elementų skaičius	Valdymo veiksmai		Laukas
PRIMARY	PRIMARY	19	Panaikinti	Taisyti	id
Serijinis_Nr	UNIQUE	19	Panaikinti	Taisyti	serijinis_nr

Sukurti indeksą 1 stulpeliui(iams) Eiti

Vietos naudojimas :

Tipas	Išnaudota
Duomenys	105,716 Baitų
Indeksas	3,072 Baitų
Perteklinis	5,356 Baitų
Efektyvus	103,432 Baitų
iš viso	108,788 Baitų

[Optimizuoti lentelę]

Eilučių statistika :

Parametrai	Reikšmė
Formatas	dinaminis
Eilutės	19
Eilutės ilgis ø	5,282
Eilutės dydis ø	5,726 Baitų
Sekantis Autoindex	41

2 pav. Duomenų bazės „esign“ lentelė “sertifikatas”

Duomenų bazė *esign* - lentelė *vartotojai* adresu *localhost*

[Peržiūrėti] [Išrinkti] [Įterpti] [Panaikinti reikšmes] [Panaikinti]

	Laukas	Tipas	Atributai	Null	Nutylint	Papildomai	Valdymo veiksmai					
☐	id	int(10)	UNSIGNED	Ne		auto_increment	Keisti	Panaikinti	Pirminis	Indeksas	Unikalus	"Fulltext" indeksas
☐	login	tinytext		Taip	*NULL*		Keisti	Panaikinti	Pirminis	Indeksas	Unikalus	"Fulltext" indeksas
☐	pw	tinytext		Taip	*NULL*		Keisti	Panaikinti	Pirminis	Indeksas	Unikalus	"Fulltext" indeksas

Pasirinktas lenteles: Keisti *Arba* Panaikinti

Indeksai : [Dokumentacija]

Raktinis žodis	Tipas	Elementų skaičius	Valdymo veiksmai		Laukas
PRIMARY	PRIMARY	2	Panaikinti	Taisyti	id

Sukurti indeksą 1 stulpeliui(iams) Eiti

Vietos naudojimas :

Tipas	Išnaudota	
Duomenys	100	Baitų
Indeksas	2,048	Baitų
iš viso	2,148	Baitų

Eilučių statistika :

Parametrai	Reikšmė
Formatas	dinaminis
Eilutės	2
Eilutės ilgis ø	50
Eilutės dydis ø	1,074 Baitų
Sekantis Autoindex	4

2 pav. Duomenų bazės „esign“ lentelė “vartotojai”