LATVIJAS GRID SERTIFIKĀCIJAS AUTORITĀTES VEIDOŠANA

PROJEKTA OTRĀ GADA REZULTĀTI

Dokumenta faila vārds:	**LG-CA-v3.doc**
Aktivitāte:	**2.aktivitāte "Starpprogrammatūras rīku praktiskā realizācija"**
Projekta numurs:	**VPD1/ERAF/CFLA/05/APK/2.5.1./000055/027**
Organizācija:	**Latvijas Universitātes aģentūra ”Latvijas Universitātes Matemātikas un informātikas institūts”**
Autori:	**Baiba Kaškina, Dana Ludviga, Katrīna Sataki, Edgars Znots**

Anotācija:

Šis dokuments apraksta veiktos Latvijas Grid CA akreditācijas procesus organizācijas pievienošanai EuGridPMA, TACAR, kā arī nepieciešamos darbus Latvijas Grid CA dokumentu uzlabošanai. Šajā dokumentā tiek izklāstīti Projekta otrā gada laikā veiktie darbi, kas bija nepieciešami Debian Linux atklātās drošības kļūdas operētājsistēmas komplektā iekļaujamajā OpenSSL pakotnē novēršanai.

Saturs

1. IEVADS

Lai Latvijas Grid tīklā lietotāju identitāte un piešķirtās tiesības tiktu pārbaudītas, izmantojot īpašus Grid sertifikātus, bija nepieciešams turpināt projekta pirmā gadā aizsāktos Latvijas Grid Sertifikācijas autoritātes (turpmāk tekstā CA) veidošanas procesus.

Šajā dokumentā tiek aprakstīta Latvijas Grid CA pirmajā gadā iesākto akreditācijas procesu nobeigšanas, jaunu saknes sertifikātu ģenerēšanas, OpenSSL pakotnes kļūdu pārvarēšanas un dokumentāciju izveides un papildināšanas gaita. Tiek attēlota CA administratoru darbības atvieglošanai veidotā procesu instrukcija, kā arī pirmo lietotāju servera un servisa sertifikātu ģenerēšana un parakstīšana.

2. IEKĻAUŠANĀS STARPTAUTISKAJĀ VIDĒ

Lai jaunieviestās Latvijas Grid CA izsniegtie Grid lietošanas sertifikāti ļautu zinātniekiem izmantot un koplietot resursus, kas atrodas valstī, citur Eiropā vai pat pasaulē, tiem ir jākļūst atpazīstamiem un akceptējamiem arī ārpus Latvijas robežām.

Jau pirmajā projekta darbības gada laikā šim jautājumam tika pievērsta liela uzmanība, tika noskaidrotas visas nepieciešamās formalitātes un institūcijas, kuru sadarbība šī mērķa sasniegšanai ir nepieciešama (starptautiska uzticamības tīkla veidošanas organizācija EUGridPMA un Eiropas akadēmisko organizāciju CA saknes sertifikātu izplatītājs TACAR). Tika uzsākts Latvijas Grid CA akreditācijas process EUGridPMA.

Šajā nodaļā tiek izklāstīti Latvijas Grid CA veiktie akreditācijas un sadarbības procesi ar EUGridPMA organizāciju, kā arī TACAR (*Terena Academic CA Repository*).

2.1. CALG AKREDITĀCIJA EUGRIDPMA

Lai Latvijas Grid lietotāji varētu izmantot arī citus Grid resursus, vispār pieņemtā prakse Eiropā nosaka, ka konkrētajai Grid CA jāiziet akreditācijas process un jākļūst par EUGridPMA organizācijas biedru, kā arī jāievieto savas saknes sertifikāts TACAR sertifikātu repozitorijā.

Lai jauna CA tiktu akreditēta, tai jāveic šādi soļi:

1. jāpiesaka sava dalība akreditācijai, izsūtot pieteikumu pa e-pastu PMA katedrai;
2. EUGridPMA sanāksmē klātbūtnē jāprezentē savas valsts Grid iniciatīva, vēlme un iespējas izveidot un uzturēt savu CA;
3. jāizveido savas CA dokumentācija (CP/CPS);
4. klātbūtnē jāprezentē izveidotā dokumentācija un jānodod tā EUGridPMA dalībnieku recenzēšanai;
5. kad EUGridPMA ir atzinis CA dokumnetāciju par korektu, tiek organizēta akreditēšanas sanāksme, kurā tiek nolemts par CA akreditāciju.

Pirmie soļi Latvijas Grid CA akreditācijas uzsākšanai tika sperti 2007. gada maijā, kad Latvijas Grid CA pārstāve Baiba Kaškina piedalījās EUGridPMA sanāksmē un iepazīstināja citus dalībniekus ar Grid iniciatīvām Latvijā, to mērķiem un esošo situāciju. Pirmā projekta darbības gadā tika veikti arī Grid CA dokumentācijas izveidošanas darbi.

Turpinot jau iesāktos CA izveides darbus, projekta otrā gada laikā tika veikti CA dokumentācijas CP/CPS analīzes un uzlabošanas darbi. Lai uzsāktu akreditēšanas procesus un nepieciešamo dokumentāciju izveidotu pēc iespejas precīzāk un atbilstošāk EUGridPMA kritērijiem, tika apmeklētas vairākas EUGridPMA sanāksmes.

- 12(-tā) EUGridPMA sanāksme Amsterdamā (14.01.2008-16.01.2008);
- 13(-tā) EUGridPMA sanāksme Kopenhāgenā (26.05.2008-28.05.2008).

12(-to) EUGridPMA sanāksmi apmeklēja Baiba Kaškina un Dana Ludviga, tajā tika izklāstītas pašreizējās skaitļošanas Grid attīstības tendences valstī, tā potenciālie lietotāji, esošā situācija Latvijas Nacionālās izpētes un izglītības tīkla (NREN - National Research and Education Network) SigmaNet attīstībā un darbībā, kā arī pierādīta mūsu vēlme un spējas izveidot un uzturēt pašiem savu Grid sertifikātu izsniegšanas autoritāti (CA). Šajā sanāksmē

tika akceptēta Latvijas Grid CA akreditācijas uzsākšāna, rezervēts laiks nākamās sanāksmes prezentāciju kalendārā izveidotās CA dokumentācijas prezentēšanai un analīzei, kā arī piešķirti divi CP/CPS recenzenti – Dr. Jens G. Jensen no Apvienotās Karalistes CA un Hardi Teder kā BalticGrid CA pārstāvis.

Lai nodotu galveno Latvijas Grid CA procedūras aprakstošo dokumentu CP/CPS recenzijai, tika veikti tās uzlabošanas un papildināšanas darbi. Dokumenta papildināšanai par paraugu tika ņemti vairāku jau akreditētu CA CP/CPS. Tika uzlabotas un papildinātas sekojošas nodaļas:

1. Ievaddaļā tika precizēti CA sastāvdaļu un lietotāju definējumi.
2. Galveno noteikumu daļā tika papildināti Latvijas Grid CA saistības un atbildības apraksti, kā arī informācijas publicēšanas, konfidencialitātes un vairāki audita jautājumi.
3. Daļā „Identifikācija un autentifikācija" tika precizēta sertifikātu atsaukšanas pieprasījuma gadījumi, kā arī identitātes pārbaudes procedūras.
4. Operacionālo prasību daļā tika veikti vairāki labojumi, sertifikātu izsniegšanas, atsaukšanas, kā arī auditējamo rādītāju kritērijos. Tika precizētas arī CA darbības beigšanas procedūras.
5. Fiziskās, procedūru un personīgās drošības kontroles daļā tika precizēti fiziskās un personīgās drošības pielietojamie mēri, kas aizsargā CA.
6. Tehniskā drošība kontroles daļā, tika papildināti privātās un publiskās atslēgas piegādes procesi un paroles kritēriji;
7. Papildināta un precizētas izsniegtās CRL versijas un X509 sertifikātu izmantošanas iespējas;
8. Pēdējajā daļā tika precizēti CP/CPS OID maiņas nosacījumi.

Pēc minēto izmaiņu veikšanas 2008 gada 18. janvarī CP/CPS tika izsūtīts recenzentiem recenzijai. Recenzijas rezultāti tika izsūtīti īsi pirms nākamās 13(-tās) EUGridPMA sanāksmes (2008. gada 23. maijā). Jaunā pēc recenzijas pārveidotā CP/CPS 3. versija publiski pieejama Latvijas Grid portālā - http://grid.lumii.lv/section/show/38.

13(-to) EUGridPMA sanāksmi apmeklēja CA administrātore Dana Ludviga, prezentējot galvenās CA CP/CPS atrunātās procedūras. Pēc uzstāšanās EUGridPMA pārstāvji nolēma veikt atkārtotu jaunās CP/CPS versijas recenziju un pēc veiksmīgas recenzijas jau norunāt Latvijas Grid CA akreditēšanas sanāksmi.

Lai tiktu ievēroti visi CA dokumentā CP/CPS atrunātie procesi, bija nepieciešams ieviest arī CA administratoru darbu uzskaites un ģenerēto sertifikātu, pieprasījumu, CRL un citu nozīmīgo datu rezerves kopiju veikšanas iespējas. Šo rādītāju uzskaites dēļ tika izveidota speciāla audita klade, kurā tiek piefiskēti katra administratora veiktie darbi ar Latvijas Grid CA aparatūru (tādi kā sertifikāta, CRL u.c. datu ģenerēšana). Šie dati kalpo arī atskaitei un veikto procesu pārraudzībai, ik pēc pusgada dati tiek pārveidoti elektroniskā formā un to rezerves kopija uzglabāta atsevišķā veltītā zibatmiņas kartē.

2.2. CA AKREDITĀCIJA TACAR

Lai panāktu Latvijas Grid CA saknes sertifikāta publicešanu TACAR sertifikātu repozitorijā, nepieciešams:

- iepazīties ar TACAR akreditācijas politikas dokumentu (*Policy of the TERENA Academic CA Repository TACAR*);
- izveidot un klātienē TERENA pārstāvim piegādāt divas Reģistrācijas un Akreditācijas vēstuļu kopijas;
- piegādāt CA pārstāvju PGP atslēgas un jaunāko CP/CPS versiju.

Reģistrācijas vēstule (*Annex I: Template Letter of Registration*) ir pamata TACAR akreditācijas dokuments. Tas ir CA saknes sertifikāta iekļaušanas sākuma punkts, kas satur informāciju par CA, tā saknes sertifikātu, un politiku. Šis dokuments klātienē tika pasniegts TERENA pārstāvim 2008. gada 10. janvārī Amsterdamā, Nīderlandē, TERENA birojā. Reģistrācijas vēstules sagatave apskatāma pielikumā Nr.1.

Savukārt Akreditācijas vēstulē (*Annex II: Template Letter of Accreditation*) tiek atzīmētas visas CA akreditētās personas:

- administratīvās kontaktpersonas (*Administrative Contact Person*);
- tiešā atbildīgā persona (*Direct responsible Person*);
- CA administratori (*CA Administrators*).

Akreditācijas vēstules sagatave apskatāma pielikumā Nr.2.

Pēc veiksmīgas dokumentu iesniegšanas un savstarpējas informāciju apmaiņas šī gada 11. martā Latvijas Grid CA saknes sertifikāts tika publicēts TACAR sertifikātu repozitorijā. Repozitorijs publiskai apskatei pieejams saitā – https://www.tacar.org/repos/ .

3. TEHNISKAIS RISINĀJUMS

Latvijas Grid projekta 2. gadā nācās saskarties ar vairākām tehniskām problēmām, visbūtiskākās no tām - jauna Latvijas Grid CA saknes sertifikāta ģenerēšana, jo iepriekš ģenerētais sertifikāts izrādījās kriptogrāfiski vājš izmantotās programmatūras iekšējas kļūdas dēļ, kā arī OpenSSL CA konfigurācijas faila atribūtu aktualizēšana atbilstoši EuGridPMA prasībām, lai izsniegtie sertifikāti būtu atzīstami par derīgiem un lietojamiem.

3.1. LATVIJAS GRID CA SAKNES SERTIFIKĀTA PĀRĢENERĒŠANA

Sākotnējais Latvijas Grid CA saknes sertifikāts tika ģenerēts, izmantojot Knoppix LiveCD operētājsistēmas distributīvu ar tam līdzi nākošo OpenSSL programmatūru, kas paredzēta CA sertifikāta ģenerēšanai un lietotāju sertifikātu parakstīšanai. Katru reizi CA dators tika darbināts, izmantojot šīs operētājsistēmas LiveCD kompaktdisku. Knoppix operētājsistēmas distributīvs ir bāzēts uz Debian Linux.

2008. gada 13. maijā Debian Linux operētājsistēmas drošības komanda nāca klajā ar paziņojumu, ka atklāta kritiska drošības kļūda operētājsistēmas komplektā iekļaujamajai OpenSSL pakotnei, kuru šī distributīva vajadzībām bija modificējuši Debian Linux izstrādātāji (***Debian Security Advisory DSA-1571-1***, http://www.debian.org/security/). Kļūdas rezultātā visi Debian OpenSSL ģenerētie privātās un publiskās atslēgas pāri bija kriptogrāfiski vāji (viegli paredzami). Ņemot vērā to, ka Knoppix ir balstīts uz Debian Linux, tad arī Latvijas Grid CA atslēgu un sertifikāta ģenerēšanā izmantotais Knoppix LiveCD saturēja kļūdaino OpenSSL versiju, un Latvijas Grid CA privātās un publiskās atslēgas pāris vairs nebija uzskatāms par kriptogrāfiski drošu un izmantojamu. Apstiprinājums par Latvijas Grid CA atslēgas un sertifikāta vājumu tika arī saņemts no neatkarīga EuGridPMA pārstāvja, Reimer Karlsen-Masur no DFN-CERT Services GmbH:

```
---------- Forwarded message ----------
Date: Mon, 09 Jun 2008 10:47:50 +0200
From: "Reimer Karlsen-Masur, DFN-CERT" <karlsen-masur@dfn-cert.de>
To: baiba@latnet.lv, dana.ludviga@sigmanet.lv
Cc: guntis@latnet.lv, ca@grid.lumii.lv, katrina@latnet.lv,
    edgars.znots@lumii.lv, David Groep <davidg@nikhef.nl>
Subject: [CVE-2008-0166] Important Debian OpenSSL vulnerability

Hi Baiba, hi Dana,

I was running the "[CVE-2008-0166] Important Debian OpenSSL
vulnerability" check with the published tools on your LatGrid CA
certificate (as published on your website and on TACAR) and found that the
tools report it as affected. So the CA key seems to be generated with a
CVE-2008-0166 affected Debian openssl with a weak random generator. The
positive result of the test of your CA certificate was reconfirmed from a
local colleague and David Groep running their tests independently. Anyway
its key seems to be compromised.
```

```
    subject= /DC=LV/DC=latgrid/CN=Certification Authority for Latvian Grid
    serial=CB6EC9C522B8A3D7
    issuer= /DC=LV/DC=latgrid/CN=Certification Authority for Latvian Grid

    <http://grid.lumii.lv/ca-cert.txt>
    <http://grid.lumii.lv/ca-cert.pem>

    Latvian Grid CA provide PKI services for grid initiatives in Latvia.
    http://grid.lumii.lv/section/show/37

    ca-cert:
    MD5= DC:E5:0B:47:D1:C9:49:96:D0:0F:8C:F2:34:E4:BB:80
SHA1=6B:4D:BF:F4:1F:AB:08:24:CC:80:56:5C:A8:35:88:9D:C7:57:77:FD

    You should take immediate action to get that CA certificate replaced
with a new one. Before generating the new key, make sure you updated the
openssl programm and test the result again against the public
Debian/openssl-blacklists.

    You also want to make sure that all infrastructure that already rely on
the bad CA certificate/key is being secured with new certificates. And
services that implement TLS client authentication with this CA certificate
should be taken care of as well.

    Since your affected CA certificate is already published on TACAR you
must make sure that it vanishes from there as well. If you resubmit a new
replacement CA certificate to TACAR please make sure that is only listed
under IGTF Classic once your IGTF accreditation is officially assigned.

    --
    Kind Regards

    Reimer Karlsen-Masur
    --
    Dipl.-Inform. Reimer Karlsen-Masur (PKI Team),Phone +49 40 808077-615
    DFN-CERT Services GmbH, https://www.dfn-cert.de,Phone +49 40 808077-580
    Sitz / Register: Hamburg, AG Hamburg, HRB 88805,  Ust-IdNr.:DE
232129737
    Sachsenstr. 5,   20097 Hamburg/Germany,   CEO: Dr. Klaus-Peter
Kossakowski
```

Balstoties uz iekšēji veiktu pārbaudi un apstiprinājumu no ārēja eksperta, bija nepieciešams atsaukt esošo Latvijas Grid CA sertifikātu, izlemt par cita distributīva LiveCD

kompaktdiska lietošanu, kuram nebūtu šīs OpenSSL pakotnes kļūdas, kā arī no jauna izveidot Latvijas Grid CA privātās un publiskās atslēgas pāri un sertifikātu.

Sākotnēji tika veikta Latvijas Grid CA sertifikāta atsaukšana no TACAR CA sertifikātu repozitorija - www.tacar.org. Pēc tam, kad kļūdainais sertifikāts tika atsaukts no TACAR, tika uzsākti jauna atslēgu pāra un sertifikāta ģenerēšanas sagatavošanas darbi.

Pirms pārģenerēt Latvijas Grid CA atslēgu pāri un sertifikātu, bija nepieciešama izpēte par citu, drošu operētājsistēmas distributīvu un LiveCD kompaktdisku. Jaunais LiveCD distributīvs nedrīkstēja saturēt kļūdaino OpenSSL pakotni (pakotnes versiju noteiktā diapazonā), pretējā gadījumā arī no jauna noģenerētais atslēgu pāris un sertifikāts būtu kļūdains (kriptogrāfiski vājš). Veicot izpēti par esošajiem pieejamajiem LiveCD distributīviem, tika konstatēts, ka viens no retajiem LiveCD distributīviem, kurš iekļauj OpenSSL pakotni un nav balstīts uz Debian Linux, ir CentOS Linux distributīvs. Tika pieņemts lēmums izmantot CentOS distributīva LiveCD kompaktdisku (CentOS 5.1 i386), un 11.jūnijā tika noģenerēts jauns Latvijas Grid CA privātās, publiskās atslēgas pāris un sertifikāts. Noģenerētais atslēgu pāris un sertifikāts tika pārbaudīts, un tika secināts, ka nesatur Debian OpenSSL kriptogrāfisko vājību, līdz ar to derīgs sertifikātu parakstīšanai.

Pēc jaunās Latvijas Grid CA saknes sertifikāta ģenerēšanas tika veikti visi nepieciešamie darbi lai šis sertifikāts tiktu publicēts TACAR repozitorijā. Tajā pat dienā 11. jūnijā jaunais sertifikāts un tā dati tika pārsūtīti TERENA pārstāvei Licia Florio.

3.2. LATVIJAS GRID CA TEHNISKO PROCEDŪRU KONSULTĀCIJA

Pēc Latvijas Grid CA jaunā sertifikāta ģenerēšanas tika izlemts uzaicināt kādu EuGridPMA pārstāvi vai citas zem EuGridPMA ietilpstošas CA pārstāvi, kurš varētu ierasties un neformāli izvērtēt esošās Latvijas Grid CA tehniskās procedūras un veiktos pasākumus vecā sertifikāta anulēšanai un jaunā sertifikāta ģenerēšanai. Tika pieaicināts Hardi Teder, BalticGrid CA tehniskais speciālists no “EENet”, Tartu, Igaunijā kā viens no EuGridPMA akreditētajiem CA pārvaldniekiem (menedžeriem). Viņš 2008. gada 3. jūlijā ieradās LU MII, SigmaNetā, lai veiktu neformālu procedūru un pasākumu izvērtēšanu, kā arī sniegtu konsultācijas par CA darbības labo praksi.

Vizītes laikā tika veikts izklāsts par Latvijas Grid CA tapšanu, kļūdainā sertifikāta atcelšanu un procedūrām, kuras tika veiktas, lai no jauna noģenerētu drošu atslēgu pāri un sertifikātu. Tika arī apskatīta telpa, kurā notiek Latvijas Grid CA sertifikātu izsniegšana un tika demonstrēts CA vajadzībām izmantotais bezdisku (“*diskless*”) serveris ar CentOS LiveCD operētājsistēmu. Tika arī izklāstītas iepriekšējās tehniskās procedūras, pirms tika atklāta vājība vecajā Latvijas Grid CA sertifikātā. Pēc atbilstošo telpu, aparatūras un procedūru apskates EuGridPMA akreditētais CA pārvaldnieks un BalticGrid CA tehniskais speciālists Hardi Teder atzina, ka pieņemtie lēmumi saistībā ar vecā Latvijas Grid CA sertifikāta atcelšanu un visas turpmākās darbības jauna atslēgu pāra un sertifikāta izveidei esot bijušas pārdomātas un korektas, un pašreizējās Latvijas Grid CA tehniskās procedūras atbilst labajai praksei.

3.3. LATVIJAS GRID CA SERTIFIKĀTU IZSNIEGŠANA

3.3.1. OpenSSL konfigurācijas aktualizēšana

Pēc jaunā Latvijas Grid CA sertifikāta izveides bija iespējams uzsākt lietotāju un servisu sertifikātu izsniegšanu. Taču pirms tam bija nepieciešams aktualizēt vairākus OpenSSL programmatūras konfigurācijas parametrus, jo Latvijas Grid CA akreditācijas periodā niansēs mainījusies labā prakse attiecībā uz vairākiem X.509 PKI atribūtiem, kas tiek pievienoti izsniegtajos sertifikātos. Šajā nodaļā tiek aprakstītas izmaiņas OpenSSL konfigurācijā un izmainītie, jaunpievienotie vai dzēstie atribūti. Zemāk pievienots jaunais openssl.cnf konfigurācijas fails, kuru izmanto OpenSSL programmatūra darbā ar sertifikātiem.

Openssl.cnf:

```
HOME                    = .
RANDFILE                = $ENV::HOME/.rnd
[ ca ]
default_ca      = CA_default
[ CA_default ]
dir             = .
certs           = $dir/certs
new_certs_dir   = $dir/newcerts
crl_dir         = $dir/crl
database        = $dir/index
certificate     = $dir/ca-cert.pem
serial          = $dir/serial
crl             = $dir/ca-crl.pem
private_key     = $dir/private/ca-key.pem
RANDFILE        = $dir/private/.rand
x509_extensions = usr_cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt        = ca_default
cert_opt        = ca_default
default_crl_days= 30
default_days    = 365
default_md      = sha1
preserve        = no
policy          = policy_anything
```

```
[ policy_anything ]
countryName             = optional
stateOrProvinceName     = optional
localityName            = optional
organizationName        = optional
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits            = 2048
default_keyfile         = ./private/ca-key.pem
default_md              = sha1
prompt                  = no
distinguished_name      = root_ca_distinguished_name

x509_extensions = v3_ca
string_mask = nombstr

[ root_ca_distinguished_name ]
0.domainComponent = LV
1.domainComponent = latgrid
commonName = Certification Authority for Latvian Grid

[ usr_cert ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
basicConstraints=critical,CA:FALSE
keyUsage = critical, digitalSignature, keyEncipherment, dataEncipherment

issuerAltName         = URI:http://grid.lumii.lv/
crlDistributionPoints = URI:http://grid.lumii.lv/uploads/calg-crl.pem

certificatePolicies   = 1.3.6.1.4.1.28446.1.1.3.0

#subjectAltName          = @alt_names
[alt_names]
```

```
DNS.1                   = host.domain.zz

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment

[ v3_ca ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = critical, CA:true
keyUsage = critical,digitalSignature, keyCertSign, cRLSign
subjectAltName=URI:http://grid.lumii.lv/
crlDistributionPoints=URI:http://grid.lumii.lv/calg-crl.pem

[ crl_ext ]
# issuerAltName=issuer:copy
authorityKeyIdentifier=keyid:always,issuer:always
```

Redzamajā konfigurācijas failā atzīmēti izmainītie vai jaunpievienotie X.509 PKI atribūti:

- **keyUsage** - atbilstoši EuGridPMA jaunajām vadlīnijām, jaunajā Latvijas Grid CA versijā vairs nesatur "nonRepudiation" lietojumu, bet tikai "digitalSignature", "keyEncipherment", "dataEncipherment", kuri attiecīgi piešķir sertifikāta īpašniekam (lietotājam vai servisam/serverim) tiesības lietot savu sertifikātu digitālajam parakstam, šifrētai datu apmaiņai un datu šifrēšanai.
- **issuerAltName** - aizstāj novecojušo *nsBaseUrl* atribūtu
- **crlDistributionPoints** - aizstāj novecojušos nsCaRevocationUrl un *nsRevocationUrl*
- **certificatePolicies** - atbilstoši EuGridPMA vadlīnijām, satur atsauci uz konkrēto CP/CPS dokumentu, atbilstoši kuram konkrētais parakstītais sertifikāts izsniegts

- **subjectAltName = @alt_names**

  [alt_names]

  DNS.1 = host.domain.zz - atbilstoši EuGridPMA vadlīnijām, servisa/servera sertifikāta gadījumā satur servera pilno DNS domēnu (FQDN)

Atbilstoši jaunajām EuGridPMA vadlīnījām Grid CA izveidē, no konfigurācijas faila tika izņemti sekojoši atribūti, kas tiek uzskatīti par novecojušiem vai neieteicamiem:

nsCaRevocationUrl = http://grid.lumii.lv/ca-crl.pem

nsBaseUrl = http://grid.lumii.lv/

nsRevocationUrl = http://grid.lumii.lv/calg-crl.pem

3.3.2. Latvijas Grid CA administrēšanas instrukciju izveide

Lai padarītu Latvijas Grid CA administratoru darbu efektīvāku, un nodrošinātu viendabīgumu starp individuālu CA administratoru lietotajām komandām, tika izveidota dokumentācija Latvijas Grid CA administrēšanai. Tajā ietilpst biežāk lietotās komandas sertifikātu atcelšanai, parakstīšanai, sertifikātu atsaukumsarakstu (*CRL - Certificate Revocation List*) veidošanai, kā arī citas svarīgas CA administrēšanas komandas. Zemāk pievienots galvenais Latvijas Grid CA administrēšanas ceļvedis.

Latvijas Grid CA sertifikātu administrēšanas un izsniegšanas komandas

Lai radītu CRL priekš CA, vispirms jārada 'index' fails. Sākotnēji tas būs tikai tukšs fails, radīts ar 'touch' shell komandu. Visi atsauktie sertifikāti tiks glabāti šajā index failā, kas ir tekstveida datubāze. Tā kā šis index fails nav digitāli parakstīts, lai publicētu atsauktos sertifikātus, ir nepieciešams to digitāli parakstīt, izveidojot šī faila PEM un DER formātus.

Pirms darba pārliecināties, vai eksistē visi 'openssl.cnf' failā norādītie darba faili un direktorijas.

1) Ģenerēt jaunu CA

openssl req -config openssl.cnf -new -x509 -out cacert.pem -days 365

2) Nomainīt CA atslēgas paroli

openssl rsa -in <atslega.pem> -des3 -out <atslega.pem.new>

3) Atcelt eksistējošu sertifikātu

openssl ca -config openssl.cnf -revoke <sertifkats.pem>

4) Ģenerēt CRL

openssl ca -config openssl.cnf -gencrl

5) Ģenerēt CRL ar ilgāku derīguma termiņu

openssl ca -config openssl.cnf -gencrl -crldays <dienas>

6) Konvertēt CRL no PEM formāta uz DER formātu

openssl crl -inform PEM -outform DER -in <crl.pem> -out <crl.der>

7) Parakstīt sertifikāta pieprasījumu, izveidojot sertifikātu

openssl ca -config openssl.cnf -policy policy_anything -infiles <sert_piepras.pem>

8) Apskatīt eksistējošu sertifikātu

openssl x509 -in <sertifikats.pem> -text

9) Uztaisīt CA vai sertifikāta fingerprint

openssl x509 -noout -fingerprint -in <sertifikats.pem>

10) Pārbaudīt atsūtīta parakstīta servera/servisa sertifikāta pieprasījumu

openssl smime -verify -in signed_req.smime -signer usercert.pem -CAfile cacert.pem -out cert_request.pem

11) Parakstīt servera/servisa sertifikāta pieprasījumu ar eksistējošu lietotāja sertifikātu

openssl smime -sign -in request.pem -out sign_req.smime -signer cert.pem -inkey userkey.pem

3.3.3. Latvijas Grid CA izsniegtie sertifikāti

Pēc Latvijas Grid CA saknes sertifikāta pārģenerēšanas, tehnisko procedūru pārskatīšanas, ārēja eksperta konsultācijām un OpenSSL konfigurācijas aktualizēšanas pabeigšanas bija iespējams uzsākt Latvijas Grid CA lietotāju un servisu/serveru sertifikātu izsniegšanu atbilstoši CP/CPS dokumenta procedūrām. Sākotnēji tika parakstīts pirmais lietotāja sertifikāts. Pēc pirmā lietotāja sertifikāta izsniegšanas tika izveidoti parakstīti sertifikāta pieprasījumi serveru un servisu sertifikātu izsniegšanai - atbilstoši CP/CPS dokumentam, lietotāja sertifikāta pieprasījuma akceptēšanai nepieciešama lietotāja autentificēšana ar personu apliecinošiem dokumentiem, savukārt servera vai servisa sertifikāta pieprasījumu akceptēšanai nepieciešams, lai tos pirms tam ar savu lietotāja sertifikātu paraksta konkrēto serveru vai servisu administrators. Pēc paraugsertifikātu izsniegšanas tika atkārtoti pārbaudīts, vai izsniegtie paraugsertifikāti satur visus nepieciešamos X.509 PKI atribūtus, kā arī nesatur citus nevajadzīgus vai nekorektus atribūtus. Pārbaudē konstatēts, ka visi izsniegtie paraugsertifikāti ir korekti un turpmāk lietojami, līdz ar to iespējams uzsākt pilnvērtīgu Latvijas Grid CA darbību un izsniegt turpmākos sertifikātus. Pielikumos ir pievienotas izdrukas no paraugsertifikātiem.

- Lietotāja sertifikāta pieprasījums un izsniegtais sertifikāts (skatīt pielikumu Nr.3 un Nr.4);
- Servera sertifikāta pieprasījums un izsniegtais sertifikāts (skatīt pielikumu Nr.5 un Nr.6);
- Servisa sertifikāta pieprasījums un izsniegtais sertifikāts (skatīt pielikumu Nr.7 un Nr.8).

4. SECINĀJUMI UN CA TURPMĀKĀ ATTĪSTĪBA

Ņemot vērā ļoti operatīvu OpenSSL ievainojamības seku pārvarēšanu un atzīto precīzo darbību, var uzskatīt, ka Latvijas Grid CA ir izveidota kā operatīva, mūsdienīga, droša un kompetenta CA, kas balstīta uz pārbaudītām tehnoloģijām un jau drīz akreditētu politikas dokumentu (CP/CPS). CA ir jau izsniegusi vairākus Grid lietotāja, servera un servisa sertifikātus, kas pašlaik vēl lietojami tikai Latvijas Grid tīklā, taču tuvā nākotnē arī visā Eiropas Grid tīklā (*EGEE - Enabling Grids for E-sciencE)*.

Turpmāk ir ieplānots modernizēt pašreizējo Latvijas Grid CA lietotāja puses tiešsaistes saskarsmi, ar iespēju droši meklēt, atcelt, ielādēt un pārbaudīt sava lietotāja, servera vai servisa sertifikāta stāvokli. Tuvākā nākotnē ir arī gaidāma EUGridPMA recenzijas rezultātu un akreditācijas saņemšana. Pēc akreditācijas iegūšanas tiks veikti Latvijas Grid sertifikātu popularizēšanas pasākumi studentu un akadēmisko darbinieku vidū.

5. PIELIKUMI

5.1 PIELIKUMS NR.1 - ANNEX I: TEMPLATE LETTER OF REGISTRATION

This document is the core of the TACAR procedures. It is the starting point for the inclusion of a CA into the repository. For the first time, it must be delivered, validated, and signed by representatives of both parties (TERENA and the applicant) during a face-to-face meeting. Subsequent updates can be made electronically, as described by the TACAR in the policy.

If this document is accepted by TERENA, all formerly released Letters Of Registration issued by the applying CA are invalid.

If no accredited PGP key is used to sign the electronic versions of this and attached documents the printed paper versions of these documents are the relevant versions. In this case paper versions signed by an accredited signature of all related documents must be provided.

Once the initial *Letter Of Registration* is accepted by TERENA, updates can be send to TERENA via PGP signed e-mail or postal mail as long as the updated document is signed by any currently accredited person for the applying CA. TERENA will verify the signatures against the last received and accepted *Letter Of Accreditation.* TERENA will return signed copy of the received document.

Note: For TERENA's convenience a copy of this as word-processor source and PDF file should be provided on the CD-ROM and if accredited PGP keys are available a detached PGP signature should be placed on the CD-ROM as well.

Letter of Registration

The following institutional organisations, companies and persons hereby announce the following [updated] information to the TERENA Academic CA Repository by way of [electronically signed email | personal meeting with the TERENA Officer]:

Authorisation Information

a. TACAR Representative

TACAR representative can be either a TERENA Officer or one of the Trusted Introducer.

TACAR website: http://www.tacar.org

a.1 TERENA Officer Details

Name

Licia Florio

Affiliation

TERENA

PGP key fingerprint: C4EF BC37 9E0F 8A21 9B92 D473 1800 4F4A 2777 07CC

TERENA Address: Singel 468 D, 1017 AW Amsterdam

Phone number: +31 20 530 44 88

Fax number: +31 20 530 44 99

TERENA website: http://www.terena.nl

a.2 Trusted Introducer Details

Name: Baiba Kaškina

Affiliation: SigmaNet, IMCS UL

PGP key fingerprint: 4FD9 B1C9 494D 593C 4D06 6162 1336 98EC 99CC 83D3

b. CA Representative

Name

Dana Ludviga

Researcher and LatGrid CA administrator

Affiliation

LatGrid CA

Meeting Location and Date

Name

TNC PC 2008 meeting

Date

10 January 2008

Location

Amsterdam, the Netherlands, TERENA office

Organisation and Applying CA

Organisation Name

(The name of the organisation the CA belongs to or is managed by)

Institute of Mathematics and Computer Science, University of Latvia

Applying CA

(Legal name of the CA)

LatGrid CA

Name CA is known under

LatGrid CA

Address

SigmaNet

Matematikas un Informatikas instituts

Raina bulvaris 29

Riga, LV-1459

Latvia

Phone / Fax

Phone: <+37167211241>

Fax: <+37167225072>

Website

http://grid.lumii.lv/section/show/37

E-Mail Address

<ca@grid.lumii.lv>

Administrative Contact Person(s) (within the CA)

<Dana Ludviga, CA administrator>

<Edgars Znots, CA administrator>

<Solvita Rovīte, CA administrator>

Registered Root Certificates

The following list of certificates is a complete list of all X.509 root certificates belonging to the named applying CA that are presented in the TERENA Academic CA Repository. If this document is updated **all** certificates that are going to be listed in the root cert store have

to be listed in the sections below. [To add more than one root certificate duplicate the complete following section and change as needed.]

Root Certificate 1 – <Certification Authority for Latvian Grid>

Certificate Download Points

List of URLs to download certificate and related information.

Type: <X.509v3>

Mime-Type:

http://grid.lumii.lv/ca-cert.pem

1. Overview page for this certificate (optional)

http://grid.lumii.lv/ca-cert.txt

Subject (DN)

(add/remove components as needed)

C= LV

L=Riga

O=grid.lumii.lv

CN= Certification Authority for Latvian Grid

Email=ca@grid.lumii.lv

Validity

(e.g. date and time, timezone)

Valid not before: `Apr 11 19:49:41 2007 GMT`

Valid not after: `Apr 11 19:49:41 2017 GMT`

Fingerprint

SHA-1: 0531468567756ef445b284052d021b68c132850b

MD5: 2211bdb91fbf9705b9f18616958e2db5

Key Type

(e.g. RSA)

RSA

Key Size

(e.g. 1024 bit, 2048 bit)

2048 bit

CRL Distribution Points (optional)

CRL download URL:

Mime-Type: <application/pkix-crl>

`http://grid.lumii.lv/calg-crl.pem`

2.Overview page

isn't available

Policy (CP)

Certification Authority for Latvian Grid. Certificate Policy and Certification Practice Statement.

Document OID: 1.3.6.1.4.1.28446.1.1.2.0

- **URL (HTML)**

○http://grid.lumii.lv/section/show/38

URL (PDF)

- http://grid.lumii.lv/section/show/38
- **Fingerprint (of PDF)**

○ SHA-1:

- MD5:
- **Certification Practice Statement (CPS)**

Certification Authority for Latvian Grid. Certificate Policy and Certification Practice Statement.

Document OID: 1.3.6.1.4.1.28446.1.1.2.0

- **URL (HTML)**

- http://grid.lumii.lv/section/show/38
-

URL (PDF)

- http://grid.lumii.lv/section/show/38
-

Fingerprint (of PDF)

- SHA-1:
- MD5:

Final Statement

The information given above is correct and in conformance with the latest TERENA Academic CA Repository policy as of today. The representative of the applying CA is an accredited staff member as of the latest *Letter of Accreditation* issued by the applying CA.

The following items are attached to this document:

(all electronic versions of the documents are provided for TERENAs convenience)

1.1 CD-ROM medium with the following documents / files regarding this letter:

Root Certificate 1. **A**t least one of the following formats (and the corresponding dettached signature) shall be included, although including all of them is strongly recommended.

ca-cert.pem X.509 certificate file (PEM format)

ca-cert.pem.sig detached PGP signature for ca-cert.pem (if PGP keys are provided)

policy.pdf policy (CP)

policy.pdf.sig detached PGP signature for policy.pdf.sig (optional)

cps.pdf certification practice statement (CPS) (if available)

cps.pdf.sig detached PGP signature for cps.pdf.sig (optional)

○Letter-Of-Registration.doc

○Letter-Of-Registration.doc.sig detached PGP signature of Letter-Of-Registration.sxw (optional)

○Letter-Of-Registration.pdf (optional, recommended)

○Letter-Of-Registration.pdf.sig detached PGP signature of Letter-Of-Registration.pdf (optional)

For the applying CA:

Location:

Date:

Signatures:

<Baiba Kaškina CA Representative>

Applying CA Organisational crest:

For TERENA:

I, the TACAR representative checked the identity documents of the bearer of this letter, <Firstname Lastname>, the applying CA's representative. The identity documents and signature matches the ones stated in the most current *Letter Of Accreditation*.

Location:

Date:

Trusted Introducer Signature: TERENA Officer Signature:

<Baina Kaškina> <Firstname Lastname>

…… ……..

TERENA Organizational crest:

5.2 PIELIKUMS NR2. - ANNEX II: TEMPLATE LETTER OF ACCREDITATION

This document names the complete list of accredited persons for the applying CA. No other or formerly accredited person if not named in the this *Letter Of Accreditation* shall be accredited any longer for the applying CA.

If this document is accepted by TERENA, all formerly released Letters Of Registration issued by the applying CA are invalid.

If no accredited PGP key is used to sign the electronic versions of this and attached documents the printed paper versions of these documents are the relevant versions. In this case paper versions signed by an accredited signature of all related documents must be provided.

Once the initial *Letter Of Accreditation* is accepted by TERENA, updates of CA administrators must be send to TERENA via postal mail. The updated document shall be signed by any currently accredited person for the applying CA. TERENA will return signed copy of the received document.

Note: For TERENA's convenience a copy of this letter as word-processor source and PDF file should be provided on a CD-ROM and if accredited PGP keys are available a detached PGP signature should be placed on the CD-ROM as well.

Letter of Accreditation

The following institutional organisations, companies and persons are hereby accredited to the TERENA root certificate collection schema. The applying party is completely responsible for the accuracy of this information and for maintaining and updating this record with the responsible TERENA officer. The applying party is especially responsible to add or remove people from the list of accredited people in regards to the applying CA. If the applying party fails to these mandatory procedures, TERENA or TERENA’s officer shall not be responsible for any loss, damage or costs arising through this fact in any case to any individual or organisation.

Organisation and Applying CA

Organisation

Institute of Mathematics and Computer Science, University of Latvia (IMCS UL)

Name

SigmaNet, IMCS UL

Address

SigmaNet

Matematikas un Informatikas instituts

Raina bulvaris 29

Riga, LV-1459

Latvia

Phone / Fax

Phone: <+37167211241>

Fax: <+37167225072>

Website

<http://www.sigmanet.lv/>

Administrative Contact Person

(in e.g. the NREN)

Baiba Kaskina

Acting General Manager of SigmaNet

Applying CA

LatGrid CA

Name

LatGrid CA

Address

SigmaNet

Matematikas un Informatikas instituts

Raina bulvaris 29

Riga, LV-1459

Latvia

Phone / Fax

Phone: <+37167211241>

Fax: <+37167225072>

Website

http://grid.lumii.lv/section/show/37

E-Mail Address

<ca@lumii.lv>

Administrative Contact Person(s) (within the CA)

Dana Ludviga, CA administrator

Applying CA Host-Organisation

(The host organization of the applicant CA)

Name

SigmaNet, IMCS UL

Address

SigmaNet

Matematikas un Informatikas instituts

Raina bulvaris 29

Riga, LV-1459

Latvia

Phone / Fax

Phone: <+37167211241>

Fax: <+37167225072>

Website

<http://www.sigmanet.lv/>

Administrative Contact Person

(person the CA staff reports to, head of CA)

Baiba Kaskina, Acting General Manager of SigmaNet

Accreditational Body

(The person/people on whose order the CA staff are performing their jobs, e.g. teamlead, project leader, head of department etc, person the CA staff reports to)

Leading researcher, Latvian Grid project (Nr:VPD1/ERAF/CFLA/05/APK/2.5.1./000055/027) leader Guntis Bārzdiņš.

Name

SigmaNet, IMCS UL

Address

SigmaNet

Matematikas un Informatikas instituts

Raina bulvaris 29

Riga, LV-1459

Latvia

Phone / Fax

Phone: <+37167211241>

Fax: <+37167225072>

Website

<http://www.sigmanet.lv/>

Direct Responsible Person

(the person the head of CA reports to)

Name

Guntis Bārzdiņš

E-Mail address

<guntis.barzdins@lumii.lv>

PGP-Key (optional)

User-ID: Guntis Barzdins <guntis@latnet.lv>

Key-ID: AD297C07

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: ElGamal/2048

Fingerprint: 1D32 8456 D6F3 A541 E851 403A 48B2 36DE AD29 7C07

Preferred PGP-server URL (optional): http://pgp.mit.edu/

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: GnuPG

Accredited CA Staff

(people responsible for maintaining the information in the repository)

The following list is the complete and entire list of all accredited CA staff. The accreditational body is defined in Section *Accreditational Body*.

People

(all CA staff including head of CA if not already the direct responsible person, person who is meeting with the TERENA Officer)

CA Administrator 1 – Dana Ludviga

Name

Dana Ludviga, Researcher and LatGrid CA administrator

E-Mail address

dana.ludviga@lumii.lv

PGP-Key (optional)

User-ID: Dana Ludviga (LUMII) <dana@latnet.lv>

Key-ID: A1EADC43

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: ElGamal/2048

Fingerprint: 9AF3 098D B524 DBE0 C8D4 6C75 4958 6E5A A1EA DC43

Preferred PGP-server URL (optional): http://pgp.mit.edu/

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: GnuPG

CA Administrator 2 – Edgars Znots

Name

Edgars Znots, Researcher and LatGrid CA administrator

E-Mail address

edgars.znots@lumii.lv

PGP-Key (optional)

User-ID: Edgars Znots (BGCA RA in Latvia) <edgars.znots@sigmanet.lv>

Key-ID: 95139E69

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: ElGamal/2048

Fingerprint: B560 CAC6 59C1 4588 9D1A F600 59E8 27E1 9513 9E69

Preferred PGP-server URL (optional): http://pgp.mit.edu/

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: GnuPG

CA Administrator 3 – Solvita Rovīte

Name

Solvita Rovīte, Researcher and LatGrid CA administrator

E-Mail address

solvita.rovite@lumii.lv

PGP-Key (optional)

User-ID: Solvita Rovite (IMCS UL) <solvita@latnet.lv>

Key-ID: 2B47FF50

Algorithm, e.g. RSA, DSA, ElGamal / Length, e.g. 1024, 2048: ElGamal/2048

Fingerprint: `C20D 4727 40B5 BF26 0D0C  D2F4 856D 2AEC 2B47 FF50`

Preferred PGP-server URL (optional): http://pgp.mit.edu/

PGP Software preferably used, e.g. GnuPG, PGP.corp, PGP 2.6.x: GnuPG

Final Statement

The person named above, i.e. Dana Ludviga, Edgars Znots , Solvita Rovīte , Baiba Kaškina and Guntis Bārzdiņš are affiliated to the applying CA. They are commissioned, authorised and mandated to maintain and update the accreditation information as stated in this letter for the applying CA as well as register, maintain and update the root certificate information as stated in the *Letter Of Registration* presented to TERENA. Above named persons cross checked all information given in this letter, especially names, identity proof numbers, PGP-key IDs and fingerprints. We have read and understood the policies and procedures defined by TERENA's root certificate collection schema regarding the certificate store and we are adhering to them. The above information is correct as of signing date of this letter.

The following items are attached to this document:

1 CD-ROM with the following documents / files regarding this letter:

1.PGP keys (optional)

1.<file-name.asc> <Firstname Lastname> of all accredited persons

2.<file-name.asc> CA for above key(s)

1.1.<Letter-Of-Accreditation.doc>

1.2.<Letter-Of-Accreditation.sxw.sig> detached PGP signature of <Letter-Of-Accreditation.sxw> (optional)

1.3.<Letter-Of-Accreditation.pdf> <Letter-Of-Accreditation.pdf.sig> detached PGP signature of <Letter-Of-Accreditation.pdf> (optional)

For the applying CA:

Location: Amsterdam, the Netherlands, TERENA office

Date: 10 January 2008

Signatures:

<Guntis Bārzdiņš Direct Responsible Person> ……

<Dana Ludviga CA Administrator 1> ……

<Edgars Znots CA Administrator 2> ……

<Solvita Rovīte CA Administrator 3> ……

Organizational crest:

For TERENA:

I, the TACAR representative,checked the identity documents of the bearer of this letter, <Firstname Lastname>, the applying CA's accredited representative. The identity documents matches the ones stated above.

Location:

Date:

Trusted Introducer Signature: TERENA Officer Signature:

Baiba Kaškina <Firstname Lastname>

……..
……..

TERENA Organizational crest:

5.3 PIELIKUMS NR.3

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: DC=LV, DC=latgrid, OU=grid.lumii.lv, CN=Edgars Znots
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ad:33:94:07:46:9a:50:5c:87:4d:69:fd:99:67:
                    0d:47:e9:e3:86:4a:af:f8:17:c4:3d:80:03:a8:b9:
                    76:90:dd:21:70:db:0a:e5:c9:98:30:c7:3a:77:d8:
                    ac:2f:5b:76:80:4f:9b:22:d1:ae:34:66:af:3c:ae:
                    41:b5:23:f0:74:4e:06:3f:4f:e0:a2:bf:ad:b3:93:
                    4f:45:58:17:d3:be:55:4a:05:a0:e5:e1:ad:27:19:
                    18:75:cd:34:98:45:23:fa:4c:d6:cd:bc:6c:a8:e7:
                    77:47:bb:6d:95:30:8d:9c:4d:3f:35:43:9b:e8:e1:
                    28:21:92:9e:6f:33:85:c6:f7
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        1a:fb:ba:9f:23:5b:16:0b:79:25:13:67:20:23:ae:39:10:1e:
        af:bf:69:57:59:60:0a:30:78:61:a9:8b:f7:28:d4:2e:91:6f:
        f3:1a:a3:d7:ac:8b:a3:1f:ba:e1:be:13:b1:d7:7d:15:e4:80:
        4c:f1:2a:40:04:31:c5:18:4a:c6:70:d4:ff:fd:42:fc:36:45:
        29:78:3e:55:cf:c6:d1:08:ba:81:0d:12:e0:67:17:54:b7:aa:
        26:59:37:d8:66:f2:ad:1b:a9:53:a2:f1:f6:d1:e5:25:97:c1:
        b0:bc:cf:e1:00:12:2c:9e:59:72:c0:58:92:8d:4f:ad:31:31:
        a1:7f
-----BEGIN CERTIFICATE REQUEST-----
MIIBnDCCAQUCAQAwXDESMBAGCgmSJomT8ixkARkWAkxWMRcwFQYKCZImiZPyLGQB
GRYHbGF0Z3JpZDEWMBQGA1UECxMNZ3JpZC5sdW1paS5sdjEVMBMGA1UEAxMMRWRn
YXJzIFpub3RzMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCtM5QHRppQXIdN
```

```
af2ZZw1H6eOGSq/4F8Q9gAOouXaQ3SFw2wrlyZgwxzp32KwvW3aAT5si0a40Zq88
rkG1I/B0TgY/T+Civ62zk09FWBfTvlVKBaDl4a0nGRh1zTSYRSP6TNbNvGyo53dH
u22VMI2cTT81Q5vo4Sghkp5vM4XG9wIDAQABoAAwDQYJKoZIhvcNAQEFBQADgYEA
Gvu6nyNbFgt5JRNnICOuORAer79pV1lgCjB4YamL9yjULpFv8xqj16yLox+64b4T
sdd9FeSATPEqQAQxxRhKxnDU//1C/DZFKXg+Vc/G0Qi6gQ0S4GcXVLeqJlk32Gby
rRupU6Lx9tHlJZfBsLzP4QASLJ5ZcsBYko1PrTExoX8=
```

-----END CERTIFICATE REQUEST-----

5.4 PIELIKUMS NR.4

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: DC=LV, DC=latgrid, CN=Certification Authority for
Latvian Grid
        Validity
            Not Before: Jul 21 20:15:39 2008 GMT
            Not After : Jul 21 20:15:39 2009 GMT
        Subject: OU=grid.lumii.lv, CN=Edgars Znots
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ad:33:94:07:46:9a:50:5c:87:4d:69:fd:99:67:
                    0d:47:e9:e3:86:4a:af:f8:17:c4:3d:80:03:a8:b9:
                    76:90:dd:21:70:db:0a:e5:c9:98:30:c7:3a:77:d8:
                    ac:2f:5b:76:80:4f:9b:22:d1:ae:34:66:af:3c:ae:
                    41:b5:23:f0:74:4e:06:3f:4f:e0:a2:bf:ad:b3:93:
                    4f:45:58:17:d3:be:55:4a:05:a0:e5:e1:ad:27:19:
                    18:75:cd:34:98:45:23:fa:4c:d6:cd:bc:6c:a8:e7:
                    77:47:bb:6d:95:30:8d:9c:4d:3f:35:43:9b:e8:e1:
                    28:21:92:9e:6f:33:85:c6:f7
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
```

CA:FALSE
X509v3 Subject Key Identifier:
AB:37:8E:D3:C5:0F:41:C6:69:76:47:4F:C2:8E:05:17:C2:49:EB:C5
X509v3 Authority Key Identifier:
keyid:0B:7B:E1:B3:56:48:CC:8E:7B:13:31:75:E2:4B:D8:61:73:F8:44:59
DirName:/DC=LV/DC=latgrid/CN=Certification Authority for Latvian Grid
serial:99:EF:19:3F:2F:31:04:F0

X509v3 Key Usage: critical
Digital Signature, Key Encipherment, Data Encipherment
X509v3 Issuer Alternative Name:
URI:http://grid.lumii.lv/
X509v3 CRL Distribution Points:
URI:http://grid.lumii.lv/calg-crl.pem

X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.28446.1.3.0

Signature Algorithm: sha1WithRSAEncryption
e3:df:10:c9:e9:8d:a4:77:69:2b:21:09:e6:42:05:03:1c:58:
87:49:2f:90:12:19:cc:f5:97:e5:41:70:a5:16:f5:b2:6f:56:
90:54:77:2d:18:46:40:9a:56:10:84:31:59:41:f4:09:82:f5:
ba:42:0d:13:d8:c7:4f:70:73:23:b0:b3:b7:ea:15:28:bc:8b:
ac:36:2e:ce:15:98:af:34:6b:79:5f:b9:78:85:af:36:99:55:
9d:d6:e6:e8:0c:ba:4f:39:bf:7c:e9:db:05:fa:66:2e:40:4a:
c0:fc:c7:e1:6a:12:b0:7c:4b:bd:1d:6e:62:12:e9:22:47:dc:
0a:91:3e:78:2b:b4:4d:06:91:1a:99:06:58:5e:8a:4e:61:a4:
5d:cb:cd:87:cd:c6:d3:68:6e:b7:42:ce:62:17:ba:64:38:bb:
70:8d:5c:98:a6:9d:6d:dc:d6:9b:6a:9b:8a:e3:67:4e:f6:28:
26:4e:2a:8a:98:81:d0:d7:91:9b:f6:a9:86:9e:d0:03:dd:2f:
25:9b:a2:b2:62:cd:45:fd:ea:d0:b4:f0:22:77:d7:4c:33:ce:
c6:d6:71:4d:4a:84:a1:17:a4:9c:53:25:d7:fb:34:90:28:01:
91:65:34:50:0d:40:45:19:dd:7b:2d:4f:7f:b1:c5:ae:38:cc:
b0:8d:5a:c9

```
-----BEGIN CERTIFICATE-----
MIIDzjCCAragAwIBAgIBBDANBgkqhkiG9w0BAQUFADBgMRIwEAYKCZImiZPyLGQB
GRYCTFYxFzAVBgoJkiaJk/IsZAEZFgdsYXRncmlkMTEwLwYDVQQDEyhDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eSBmb3IgTGF0dmlhbiBHcmlkMB4XDTA4MDcyMTIwMTUz
OVoXDTA5MDcyMTIwMTUzOVowLzEWMBQGA1UECxMNZ3JpZC5sdW1paS5sdjEVMBMG
A1UEAxMMRWRnYXJzIFpub3RzMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCt
M5QHRppQXIdNaf2ZZw1H6eOGSq/4F8Q9gAOouXaQ3SFw2wrlyZgwxzp32KwvW3aA
T5si0a40Zq88rkG1I/B0TgY/T+Civ62zk09FWBfTvlVKBaDl4a0nGRh1zTSYRSP6
TNbNvGyo53dHu22VMI2cTT81Q5vo4Sghkp5vM4XG9wIDAQABo4IBRjCCAUIwDAYD
VR0TAQH/BAIwADAdBgNVHQ4EFgQUqzeO08UPQcZpdkdPwo4FF8JJ68UwgZIGA1Ud
IwSBijCBh4AUC3vhs1ZIzI57EzF14kvYYXP4RFmhZKRiMGAxEjAQBgoJkiaJk/Is
ZAEZFgJMVjEXMBUGCgmSJomT8ixkARkWB2xhdGdyaWQxMTAvBgNVBAMTKENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5IGZvciBMYXR2aWFuIEdyaWSCCQCZ7xk/LzEE8DAO
BgNVHQ8BAf8EBAMCBLAwIAYDVR0SBBkwF4YVaHR0cDovL2dyaWQubHVtaWkubHYv
MDIGA1UdHwQrMCkwJ6AloCOGIWh0dHA6Ly9ncmlkLmx1bWlpLmx2L2NhbGctY3Js
LnBlbTAYBgNVHSAEETAPMA0GCysGAQQBgd4eAQMAMA0GCSqGSIb3DQEBBQUAA4IB
AQDj3xDJ6Y2kd2krIQnmQgUDHFiHSS+QEhnM9ZflQXClFvWyb1aQVHctGEZAmlYQ
hDFZQfQJgvW6Qg0T2MdPcHMjsLO36hUovIusNi7OFZivNGt5X7l4ha82mVWd1ubo
DLpPOb986dsF+mYuQErA/MfhahKwfEu9HW5iEukiR9wKkT54K7RNBpEamQZYXopO
YaRdy82HzcbTaG63Qs5iF7pkOLtwjVyYpp1t3NabapuK42dO9igmTiqKmIHQ15Gb
9qmGntAD3S8lm6KyYs1F/erQtPAid9dMM87G1nFNSoShF6ScUyXX+zSQKAGRZTRQ
DUBFGd17LU9/scWuOMywjVrJ
-----END CERTIFICATE-----
```

5.5 PIELIKUMS NR.5

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject:       DC=LV,       DC=latgrid,       OU=grid.lumii.lv,
CN=host/birzs.latnet.lv
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:a6:f5:d7:b1:05:37:8f:ed:3a:59:fa:18:ce:e8:
                    1c:a3:f1:f5:2f:0c:79:e0:5f:be:3d:c3:60:93:fc:
```

```
                    33:5f:88:e4:fe:45:e7:ec:ca:1d:30:26:6e:eb:c0:
                    ca:7a:ed:d9:c3:0e:1c:52:47:66:6e:df:fe:d1:8a:
                    4a:a9:f4:4f:0b:c6:ce:e0:32:c1:e6:eb:3f:a0:f7:
                    5b:20:cb:1e:cb:16:f8:7c:3d:23:95:27:29:9c:70:
                    91:9b:3a:9c:52:fa:51:46:83:55:83:cb:d9:67:e7:
                    96:98:c0:60:bd:36:5c:cb:fd:e6:c5:1e:05:72:c2:
                    c7:7c:08:bb:3c:19:b7:6c:25
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha1WithRSAEncryption
        45:4c:72:43:fa:14:3e:49:f3:9b:c4:ae:83:3d:bd:16:0e:f8:
        ef:67:67:bf:e2:b8:ed:55:c2:2f:2f:4d:dc:c5:27:b4:5a:10:
        6e:69:74:86:17:12:75:a4:63:48:b2:ef:c1:03:1c:4d:ac:34:
        88:6b:a5:ee:14:7c:7d:ab:0c:3b:c9:3d:c0:e0:c3:54:a6:a2:
        dd:bd:78:12:bd:ab:c7:05:5b:40:f1:33:6f:fe:30:c1:b9:ce:
        cb:1f:32:26:84:5b:2c:c9:c7:b9:8c:c1:a1:37:56:32:58:64:
        79:ee:ed:d9:32:b5:b5:9c:a9:69:a5:ac:55:3c:5b:36:65:7c:
        2d:04
-----BEGIN CERTIFICATE REQUEST-----
MIIBpDCCAQ0CAQAwZDESMBAGCgmSJomT8ixkARkWAkxWMRcwFQYKCZImiZPyLGQB
GRYHbGF0Z3JpZDEWMBQGA1UECxMNZ3JpZC5sdW1paS5sdjEdMBsGA1UEAxMUaG9z
dC9iaXJ6cy5sYXRuZXQubHYwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKb1
17EFN4/tOln6GM7oHKPx9S8MeeBfvj3DYJP8M1+I5P5F5+zKHTAmbuvAynrt2cMO
HFJHZm7f/tGKSqn0TwvGzuAywebrP6D3WyDLHssW+Hw9I5UnKZxwkZs6nFL6UUaD
VYPL2WfnlpjAYL02XMv95sUeBXLCx3wIuzwZt2wlAgMBAAGgADANBgkqhkiG9w0B
AQUFAAOBgQBFTHJD+hQ+SfObxK6DPb0WDvjvZ2e/4rjtVcIvL03cxSe0WhBuaXSG
FxJ1pGNIsu/BAxxNrDSIa6XuFHx9qww7yT3A4MNUpqLdvXgSvavHBVtA8TNv/jDB
uc7LHzImhFssyce5jMGhN1YyWGR57u3ZMrW1nKlppaxVPFs2ZXwtBA==
-----END CERTIFICATE REQUEST-----
```

5.6 PIELIKUMS NR.6

```
Certificate:
    Data:
        Version: 3 (0x2)
```

```
            Serial Number: 5 (0x5)
            Signature Algorithm: sha1WithRSAEncryption
            Issuer: DC=LV, DC=latgrid, CN=Certification Authority for
Latvian Grid
            Validity
                Not Before: Jul 21 21:15:43 2008 GMT
                Not After : Jul 21 21:15:43 2009 GMT
            Subject: OU=grid.lumii.lv, CN=host/birzs.latnet.lv
            Subject Public Key Info:
                Public Key Algorithm: rsaEncryption
                RSA Public Key: (1024 bit)
                    Modulus (1024 bit):
                        00:a6:f5:d7:b1:05:37:8f:ed:3a:59:fa:18:ce:e8:
                        1c:a3:f1:f5:2f:0c:79:e0:5f:be:3d:c3:60:93:fc:
                        33:5f:88:e4:fe:45:e7:ec:ca:1d:30:26:6e:eb:c0:
                        ca:7a:ed:d9:c3:0e:1c:52:47:66:6e:df:fe:d1:8a:
                        4a:a9:f4:4f:0b:c6:ce:e0:32:c1:e6:eb:3f:a0:f7:
                        5b:20:cb:1e:cb:16:f8:7c:3d:23:95:27:29:9c:70:
                        91:9b:3a:9c:52:fa:51:46:83:55:83:cb:d9:67:e7:
                        96:98:c0:60:bd:36:5c:cb:fd:e6:c5:1e:05:72:c2:
                        c7:7c:08:bb:3c:19:b7:6c:25
                    Exponent: 65537 (0x10001)
            X509v3 extensions:
                X509v3 Basic Constraints: critical
                    CA:FALSE
                X509v3 Subject Key Identifier:

D4:EF:04:AE:6E:41:1B:0A:EC:F9:B2:B0:C4:0C:51:F4:6A:F7:9D:9B
                X509v3 Authority Key Identifier:

keyid:0B:7B:E1:B3:56:48:CC:8E:7B:13:31:75:E2:4B:D8:61:73:F8:44:59
                    DirName:/DC=LV/DC=latgrid/CN=Certification Authority
for Latvian Grid
                    serial:99:EF:19:3F:2F:31:04:F0

                X509v3 Key Usage: critical
                    Digital Signature, Key Encipherment, Data Encipherment
```

```
            X509v3 Issuer Alternative Name:
                URI:http://grid.lumii.lv/
            X509v3 CRL Distribution Points:
                URI:http://grid.lumii.lv/calg-crl.pem

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.28446.1.3.0

            X509v3 Subject Alternative Name:
                DNS:birzs.latnet.lv
    Signature Algorithm: sha1WithRSAEncryption
        c9:2a:52:32:89:9a:a0:50:a7:3d:d2:ae:54:06:96:9e:8d:39:
        9a:36:8d:89:51:7f:90:32:37:79:52:5c:1a:70:61:00:cb:4b:
        9d:f4:dc:4d:c0:a4:58:5d:9d:7a:2d:39:14:22:75:49:f8:24:
        18:42:4c:3e:3a:bf:ef:d4:a7:e5:c9:98:ac:19:56:1f:d2:55:
        fc:3e:9b:c3:f1:61:8b:a9:18:47:a9:25:d3:ab:a2:6d:73:26:
        a1:55:9b:1b:8f:34:ab:cb:bc:ff:11:f2:65:3f:b9:de:f7:04:
        4a:40:82:60:fe:56:56:b5:22:a3:3a:74:b2:4c:6e:43:b0:83:
        bd:e1:fc:90:8c:bc:e2:bd:b5:30:27:7a:49:af:e0:36:7e:f1:
        92:3d:a4:43:81:9a:c2:9f:f5:87:32:d2:c8:44:bb:4b:2f:9c:
        4a:2e:1a:2c:f4:3d:09:c5:7e:6b:9b:84:2d:20:15:55:f7:4e:
        c6:81:46:3e:db:73:27:4e:96:6a:35:a4:1b:de:cf:6b:9f:fd:
        8e:03:09:6c:5d:17:24:4f:b8:cb:79:b8:b1:e5:fb:8c:b0:a1:
        a3:42:3d:fd:44:bb:22:bc:4b:cc:11:a5:17:ba:30:d6:78:e9:
        58:55:d7:3c:ec:db:e1:62:56:83:b8:b0:5b:d6:5f:2a:28:c7:
        48:b0:4d:97
-----BEGIN CERTIFICATE-----
MIID8jCCAtqgAwIBAgIBBTANBgkqhkiG9w0BAQUFADBgMRIwEAYKCZImiZPyLGQB
GRYCTFYxFzAVBgoJkiaJk/IsZAEZFgdsYXRncmlkMTEwLwYDVQQDEyhDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eSBmb3IgTGF0dmlhbiBHcmlkMB4XDTA4MDcyMTIxMTU0
M1oXDTA5MDcyMTIxMTU0M1owNzEWMBQGA1UECxMNZ3JpZC5sdW1paS5sdjEdMBsG
A1UEAxMUaG9zdC9iaXJ6cy5sYXRuZXQubHYwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAKb117EFN4/tOln6GM7oHKPx9S8MeeBfvj3DYJP8M1+I5P5F5+zKHTAm
buvAynrt2cMOHFJHZm7f/tGKSqn0TwvGzuAywebrP6D3WyDLHssW+Hw9I5UnKZxw
kZs6nFL6UUaDVYPL2WfnlpjAYL02XMv95sUeBXLCx3wIuzwZt2wlAgMBAAGjggFi
MIIBXjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBTU7wSubkEbCuz5srDEDFH0aved
```

```
mzCBkgYDVR0jBIGKMIGHgBQLe+GzVkjMjnsTMXXiS9hhc/hEWaFkpGIwYDESMBAG
CgmSJomT8ixkARkWAkxWMRcwFQYKCZImiZPyLGQBGRYHbGF0Z3JpZDExMC8GA1UE
AxMoQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgZm9yIExhdHZpYW4gR3JpZIIJAJnv
GT8vMQTwMA4GA1UdDwEB/wQEAwIEsDAgBgNVHRIEGTAXhhVodHRwOi8vZ3JpZC5s
dW1paS5sdi8wMgYDVR0fBCswKTAnoCWgI4YhaHR0cDovL2dyaWQubHVtaWkubHYv
Y2FsZy1jcmwucGVtMBgGA1UdIAQRMA8wDQYLKwYBBAGB3h4BAwAwGgYDVR0RBBMw
EYIPYmlyenMubGF0bmV0Lmx2MA0GCSqGSIb3DQEBBQUAA4IBAQDJKlIyiZqgUKc9
0q5UBpaejTmaNo2JUX+QMjd5UlwacGEAy0ud9NxNwKRYXZ16LTkUInVJ+CQYQkw+
Or/v1KflyZisGVYf0lX8PpvD8WGLqRhHqSXTq6JtcyahVZsbjzSry7z/EfJlP7ne
9wRKQIJg/lZWtSKjOnSyTG5DsIO94fyQjLzivbUwJ3pJr+A2fvGSPaRDgZrCn/WH
MtLIRLtLL5xKLhos9D0JxX5rm4QtIBVV907GgUY+23MnTpZqNaQb3s9rn/2OAwls
XRckT7jLebix5fuMsKGjQj39RLsivEvMEaUXujDWeOlYVdc87NvhYlaDuLBb1l8q
KMdIsE2X
```

-----END CERTIFICATE-----

5.7 PIELIKUMS NR.7

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject:        DC=LV,        DC=latgrid,        OU=grid.lumii.lv,
CN=ldap/birzs.latnet.lv
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:dd:ec:26:e1:08:73:2e:89:9e:5c:d3:0b:56:48:
                    9d:25:ba:6c:1f:98:03:86:41:cc:75:d3:62:8f:2d:
                    a3:d7:60:b2:fb:bb:45:d9:3c:37:34:54:1e:f6:ce:
                    63:4d:88:4f:12:0f:ae:a3:a4:99:42:e9:42:68:df:
                    c9:56:2f:46:ca:aa:55:2d:ac:41:24:de:1f:ef:ca:
                    46:d4:8c:d3:72:93:5f:7c:2c:a5:69:d1:9c:f0:33:
                    11:7a:2a:d4:05:54:e0:c1:12:55:ee:ed:18:27:ad:
                    dd:5c:f3:a3:8e:3a:69:15:ed:fd:56:ab:1f:c5:57:
                    2e:35:42:f8:cc:f6:d0:cd:a9
                Exponent: 65537 (0x10001)
        Attributes:
```

```
            a0:00
        Signature Algorithm: sha1WithRSAEncryption
            89:e2:9f:d9:5d:ee:b3:eb:34:a1:b4:0b:7e:28:1d:9a:2d:bb:
            78:9a:b5:75:ba:76:2f:25:55:25:e4:ea:24:83:21:32:39:55:
            11:53:c6:6a:ef:f4:75:0f:50:b0:68:47:1a:a2:0d:82:b1:99:
            cd:b6:40:5d:c1:7c:d4:6b:fe:c2:fa:f4:a3:3c:36:fb:c5:46:
            07:56:51:2a:90:68:3b:e2:8c:89:53:a1:91:1e:54:95:f7:50:
            e2:4c:fa:6e:84:cd:be:1d:fa:4f:b2:c6:29:50:eb:f6:04:5b:
            0f:ed:44:cb:3d:10:1f:fa:2b:ad:71:ce:46:62:5e:9b:24:6d:
            c0:51
    -----BEGIN CERTIFICATE REQUEST-----
    MIIBpDCCAQ0CAQAwZDESMBAGCgmSJomT8ixkARkWAkxWMRcwFQYKCZImiZPyLGQB
    GRYHbGF0Z3JpZDEWMBQGA1UECxMNZ3JpZC5sdW1paS5sdjEdMBsGA1UEAxMUbGRh
    cC9iaXJ6cy5sYXRuZXQubHYwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAN3s
    JuEIcy6JnlzTC1ZInSW6bB+YA4ZBzHXTYo8to9dgsvu7Rdk8NzRUHvbOY02ITxIP
    rqOkmULpQmjfyVYvRsqqVS2sQSTeH+/KRtSM03KTX3wspWnRnPAzEXoq1AVU4MES
    Ve7tGCet3Vzzo446aRXt/VarH8VXLjVC+Mz20M2pAgMBAAGgADANBgkqhkiG9w0B
    AQUFAAOBgQCJ4p/ZXe6z6zShtAt+KB2aLbt4mrV1unYvJVUl5OokgyEyOVURU8Zq
    7/R1D1CwaEcaog2CsZnNtkBdwXzUa/7C+vSjPDb7xUYHVlEqkGg74oyJU6GRHlSV
    91DiTPpuhM2+HfpPssYpUOv2BFsP7UTLPRAf+iutcc5GYl6bJG3AUQ==
    -----END CERTIFICATE REQUEST-----
```

5.8 PIELIKUMS NR.8

```
    Certificate:
        Data:
            Version: 3 (0x2)
            Serial Number: 6 (0x6)
            Signature Algorithm: sha1WithRSAEncryption
            Issuer: DC=LV, DC=latgrid, CN=Certification Authority for
Latvian Grid
            Validity
                Not Before: Jul 21 21:25:47 2008 GMT
                Not After : Jul 21 21:25:47 2009 GMT
            Subject: OU=grid.lumii.lv, CN=ldap/birzs.latnet.lv
```

```
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:dd:ec:26:e1:08:73:2e:89:9e:5c:d3:0b:56:48:
                    9d:25:ba:6c:1f:98:03:86:41:cc:75:d3:62:8f:2d:
                    a3:d7:60:b2:fb:bb:45:d9:3c:37:34:54:1e:f6:ce:
                    63:4d:88:4f:12:0f:ae:a3:a4:99:42:e9:42:68:df:
                    c9:56:2f:46:ca:aa:55:2d:ac:41:24:de:1f:ef:ca:
                    46:d4:8c:d3:72:93:5f:7c:2c:a5:69:d1:9c:f0:33:
                    11:7a:2a:d4:05:54:e0:c1:12:55:ee:ed:18:27:ad:
                    dd:5c:f3:a3:8e:3a:69:15:ed:fd:56:ab:1f:c5:57:
                    2e:35:42:f8:cc:f6:d0:cd:a9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:

B0:59:B7:BF:1F:72:EE:B4:D6:B4:89:DE:15:59:86:EB:79:5F:31:C0
            X509v3 Authority Key Identifier:

keyid:0B:7B:E1:B3:56:48:CC:8E:7B:13:31:75:E2:4B:D8:61:73:F8:44:59
                DirName:/DC=LV/DC=latgrid/CN=Certification Authority
for Latvian Grid
                serial:99:EF:19:3F:2F:31:04:F0

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment, Data Encipherment
            X509v3 Issuer Alternative Name:
                URI:http://grid.lumii.lv/
            X509v3 CRL Distribution Points:
                URI:http://grid.lumii.lv/calg-crl.pem

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.28446.1.3.0
```

```
            X509v3 Subject Alternative Name:
                DNS:birzs.latnet.lv
    Signature Algorithm: sha1WithRSAEncryption
        9f:5d:ca:83:d5:44:98:89:3a:70:7f:da:2e:f0:bb:1d:05:d3:
        9e:a8:93:84:e9:e1:d5:78:91:76:ab:fa:35:c5:a3:ff:a1:3a:
        b5:b4:54:93:8e:e0:81:bb:7c:0f:19:eb:94:f9:70:3b:4b:1d:
        1a:9f:e4:4e:26:a8:34:52:5a:16:ce:ff:8c:d6:7e:37:09:cb:
        9d:65:07:44:de:8a:44:ab:c0:bc:71:79:4d:cf:e3:3b:e3:f6:
        7c:1a:12:8f:cd:fa:cc:18:4c:81:93:1e:96:9f:a7:28:61:45:
        5b:ce:66:b6:c5:ee:76:72:63:d0:05:94:86:5c:79:f7:1f:db:
        e7:4e:43:4b:c6:a8:2f:48:c1:fa:aa:ae:58:b2:18:22:6a:80:
        84:42:32:01:24:ee:0c:b5:73:3e:95:ab:b4:15:11:94:d8:1b:
        dc:22:2d:42:3e:10:4b:91:ef:d6:b1:29:3f:29:67:65:1c:5c:
        e1:2e:c8:0c:da:e6:e8:b0:c0:26:9c:0f:53:e1:3b:3d:6b:96:
        e2:a0:a0:a6:2b:10:77:c6:90:95:b4:47:a5:5d:8c:91:c9:65:
        f8:43:b1:85:c3:bc:f1:bd:ae:b5:a9:c6:b1:84:f2:93:9f:ab:
        6b:d4:1d:61:bd:4f:32:e6:27:75:d9:a7:87:fe:a5:6c:a0:f7:
        3a:dc:9f:ab
-----BEGIN CERTIFICATE-----
MIID8jCCAtqgAwIBAgIBBjANBgkqhkiG9w0BAQUFADBgMRIwEAYKCZImiZPyLGQB
GRYCTFYxFzAVBgoJkiaJk/IsZAEZFgdsYXRncmlkMTEwLwYDVQQDEyhDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eSBmb3IgTGF0dmlhbiBHcmlkMB4XDTA4MDcyMTIxMjU0
N1oXDTA5MDcyMTIxMjU0N1owNzEWMBQGA1UECxMNZ3JpZC5sdW1paS5sdjEdMBsG
A1UEAxMUbGRhcC9iaXJ6cy5sYXRuZXQubHYwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAN3sJuEIcy6JnlzTC1ZInSW6bB+YA4ZBzHXTYo8to9dgsvu7Rdk8NzRU
HvbOY02ITxIPrqOkmULpQmjfyVYvRsqqVS2sQSTeH+/KRtSM03KTX3wspWnRnPAz
EXoq1AVU4MESVe7tGCet3Vzzo446aRXt/VarH8VXLjVC+Mz20M2pAgMBAAGjggFi
MIIBXjAMBgNVHRMBAf8EAjAAMB0GA1UdDgQWBBSwWbe/H3LutNa0id4VWYbreV8x
wDCBkgYDVR0jBIGKMIGHgBQLe+GzVkjMjnsTMXXiS9hhc/hEWaFkpGIwYDESMBAG
CgmSJomT8ixkARkWAkxWMRcwFQYKCZImiZPyLGQBGRYHbGF0Z3JpZDExMC8GA1UE
AxMoQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkgZm9yIExhdHZpYW4gR3JpZIIJAJnv
GT8vMQTwMA4GA1UdDwEB/wQEAwIEsDAgBgNVHRIEGTAXhhVodHRwOi8vZ3JpZC5s
dW1paS5sdi8wMgYDVR0fBCswKTAnoCWgI4YhaHR0cDovL2dyaWQubHVtaWkubHYv
Y2FsZy1jcmwucGVtMBgGA1UdIAQRMA8wDQYLKwYBBAGB3h4BAwAwGgYDVR0RBBMw
EYIPYmlyenMubGF0bmV0Lmx2MA0GCSqGSIb3DQEBBQUAA4IBAQCfXcqD1USYiTpw
f9ou8LsdBdOeqJOE6eHVeJF2q/o1xaP/oTq1tFSTjuCBu3wPGeuU+XA7Sx0an+RO
```

Jqg0UloWzv+M1n43CcudZQdE3opEq8C8cXlNz+M74/Z8GhKPzfrMGEyBkx6Wn6co
YUVbzma2xe52cmPQBZSGXHn3H9vnTkNLxqgvSMH6qq5YshgiaoCEQjIBJO4MtXM+
lau0FRGU2BvcIi1CPhBLke/WsSk/KWdlHFzhLsgM2ubosMAmnA9T4Ts9a5bioKCm
KxB3xpCVtEelXYyRyWX4Q7GFw7zxva61qcaxhPKTn6tr1B1hvU8y5id12aeH/qVs
oPc63J+r