LATVIJAS GRID SERTIFIKĀCIJAS AUTORITĀTES VEIDOŠANA

PROJEKTA PIRMĀ GADA REZULTĀTI

Dokumenta faila vārds:	**LG-CA-v1**
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:	Mārtiņš Freivalds, Baiba Kaškina, Dana Ludviga, Bruno Martuzāns, Leo Trukšāns, Katrīna Sataki

Anotācija:

Šis dokuments apraksta Latvijas Grid CA pamatprincipus, izvēlētās tehnoloģijas un sagatavotos politikas dokumentus. Dokumentā sniegts ieskats pasākumos, kas veicami, lai panāktu Latvijas Grid CA atzīšanu starptautiski, kā arī iezīmē turpmākos sniegto pakalpojumu uzlabošanas pasākumus.

Saturs

1. IEVADS

Grid tīklos lietotāju identitāte un piešķirtās tiesības tiek pārbaudītas, izmantojot īpašus Grid sertifikātus (parasti X509 formātā), kurus izsniedz vietējās Grid infrastruktūras Sertifikācijas autoritāte. Latvijas Grid projekta ietvaros tika nolemts veidot Latvijas Grid Sertifikācijas autoritāti (turpmāk CA), kas izsniegs Grid sertifikātus Latvijas zinātniekiem, kā arī sertificēs vietējos Grid klasterus.

Šajā dokumentā aprakstīta Latvijas Grid CA veidošana, programmatūras izvēles kritēriji, instalācijas gaita un lietošana, kā arī izveidotā dokumentācija un sadarbība ar starptautiskām organizācijām.

2. TEHNOLOĢISKĀ RISINĀJUMA IZVĒLE

Viss, kas nepieciešams CA "sistēmas" darbam ir komplekts, kas sastāv no CA atslēgu un sertifikātu failiem, kā arī programmatūras, ar kuras palīdzību veic CA darbības, piemēram, paraksta lietotāju sertifikātus. Bieži var iztikt ar CA atslēgām, kas glabājas drošā vietā, un OpenSSL programmatūru.

Pastāv vairāki lielāki CA programmatūras projekti, kas ļauj ērtāk veikt nepieciešamos uzdevumus un piedāvā papildu CA funkcijas, kas nepieciešamas lielākām organizācijām. LU MII pētnieki veica CA programmatūras izpēti ar mērķi atrast un ieviest LatGrid projektā vispiemērotāko CA programmatūru.

Tika meklēti funkcionāli bagātākie atklātā pirmkoda CA programmatūras projekti, kuriem izvirzītas šādas obligātas prasības:

- CA un RA (reģistrācijas autoritāte) un publiskajām funkcijām jābūt atdalāmām un izvietojamām uz dažādiem datoriem;
- jābūt iespējai CA un RA funkcijas deleģēt dažādiem administratoriem ar nodalītām tiesībām;
- sertifikātiem kopā ar informāciju par to lietotājiem jābūt pieejamiem LDAP datubāzē;
- jābūt iespējai lietotājiem izmantot drošas viedkartes, tātad ģenerēt privātās atslēgas ārpus CA sistēmas;
- sistēmai jābūt veidotai tīmekļa vietnes veidā ar HTTPS atbalstu, lai ar to var strādāt no jebkuras vietas.

Tika apskatīti trīs projekti: OpenCA, OpenXPKI, CSP. Pirmie divi ir funkcionāli ļoti bagāti un piedāvā gandrīz visas (bez viedkartēm) nepieciešamās iespējas. OpenCA projekta attīstība ir apstājusies, bet OpenXPKI ir tā turpinājums ar būtiski papildinātām iespējām un nedaudz mainītu uzbūvi. Abi projekti atbalsta viedkaršu izmantošanu sertificēšanā. CSP projekts ir neliela programma skripta veidā, kas "aptver" openssl komandu un ļauj to lietot nedaudz ērtāk – ar īsākām un vienkāršākām komandām. Eksistē vairāki šādi projekti, bet tie neapmierina vairākas izvirzītās prasības. Līdz ar to nopietnāk tika pētīti tikai OpenCA un pēc tam arī OpenXPKI projekti.

OpenCA projekts likās vispiemērotākais, jo tas labi atbilst visām vēlmēm un nav pārblīvēts ar papildu funkcionalitāti. Tas, tāpat kā OpenXPKI, ir plaši konfigurējams, ļaujot to ieviest visdažādākajās situācijās. OpenCA trūkumi ir sarežģītā konfigurēšana un tā vecums. Tā attīstība ir beigusies pirms vairākiem gadiem, un tas izmanto vecas papildprogrammu (OpenLDAP u.c.) versijas, līdz ar ko tā ieviešana kļūst vēl sarežģītāka.

OpenXPKI ir aktīvs projekts, līdz ar to tam ir gatavas mūsdienīgas pakotnes populārākajiem Linux distributīviem un FreeBSD. OpenXPKI ir veidots vēl sarežģītāks par OpenCA, pievienojot tam vēl vienu abstrakcijas līmeni – informācijas plūsmas (*workflow*). Ir labi jāiepazīst tā uzbūve un jādefinē plūsmas, kādās pārvietosies kriptogrāfiskā informācija, lai tiktu pie pirmās sertificēšanas.

Izpētes gaitā tika atklāts, ka gan OpenCA, gan OpenXPKI ģenerē un saglabā lietotāju privātās atslēgas pārlūkprogrammā, no kuras, protams, tās var izeksportēt. Bet līdz ar to nav iespējams izmantot viedkartes, kas privāto atslēgu ģenerē savā atmiņā un nelaiž ārpus tās. OpenXPKI projekts tiek saukts par "trustcenter" veida sistēmu. Šādu sistēmu īpatnība ir tāda,

ka tās operē ar lietotāju privātajām un publiskajām atslēgām. Pēc sīkākiem pētījumiem radās iespaids, ka šajās sistēmās būtu iespējams pieprogrammēt papildu funkciju lietotājiem iesniegt sertifikātu pieprasījumus kopā ar savu publisko atslēgu, atstājot atslēgu ģenerēšanu lietotāju ziņā.

Pēc visu triju CA sistēmu salīdzināšanas tika izdarīts secinājums, ka OpenCA un OpenXPKI iespējas tikai nedaudz atsver to trūkumus. Tās ir lielas, pamatīgas un labi pielāgojamas sistēmas, bet tās neļauj lietotājiem pašiem ģenerēt atslēgas. Turklāt OpenCA ir pamests projekts, bet OpenXPKI šķiet pārāk sarežģīts. Bija jāpieņem lēmums, vai turpināt apgūt šos lielos projektus vai sākt uzreiz ar pieticīgo OpenSSL rīku, izveidot CA un vēlāk pāriet uz kādu no lielajām sistēmām. Tika izvēlēts otrais Latvijas Grid CA veidošanas ceļš.

3. LATVIJAS GRID CA IZVEIDE

Saknes sertifikāta ģenerēšanai un sertifikātu izsniegšanai un atcelšanai tiek izmantota programmatūra OpenSSL (www.openssl.org).

Latvijas Grid CA izveidošana nozīmē to, ka ir jāizveido x509 sertifikāts un privātā atslēga. Latvijas Grid CA izmanto pašparakstītu (*self signed*) sertifikātu, tas nozīmē, ka sertifikātu gan ģenerē, gan apstiprina Latvijas Grid CA, sertifikāts netiek apstiprināts no kādas citas starptautiskas drošas sertifikātu izsniegšanas organizācijas.

Drošības apsvērumu dēļ CA x509 sertifikāts tiek ģenerēts uz datora, kas atslēgts no tīkla un tiek startēts no Linux *boot*CD. Sertifikāta privātā atslēga tiek glabāta uz USB *flash* atmiņas slēgtā seifā. Sertifikāta privātā atslēga tāpat tiek glabāta izdrukātā formātā citā seifā gadījumam, ja USB *flash* atmiņa tiek bojāta vai nozaudēta. Sertifikātam ir 10 gadi derīguma termiņš. Privātā atslēga ir aizsargāta ar 15 simbolus garu paroli. Paroles veidošanā izmantota labākā prakse: parole satur gan lielos, gan mazos burtus, ciparus un speciālo simbolu.

Visu sertifikātu pieprasījumu apstrādāšana tiek veikta uz datora, kas ir atslēgts no tīkla, izmantojot *boot*CD un USB *flash* ar CA privāto atslēgu.

Lai atvieglotu darbu ar OpenSSL, tika izveidots šāds *make* fails, kas ļauj gan izveidot CA, gan parakstīti sertifikātu pieprasījumus, gan izveidot atcelto sertifikātu sarakstu:

```
requests = *.csr
sign: ${requests}
${requests}: FORCE
	@openssl ca -config openssl.cnf -in $@ -out ${@:.csr=.cert}
	@[ -f ${@:.csr=.cert} ] && rm $@
revoke:
	@test $${cert:?"usage: make revoke cert=certificate"}
	@openssl ca -config openssl.cnf -revoke $(cert)
	@$(MAKE) gencrl
gencrl:
	@openssl ca -config openssl.cnf -gencrl -out ca-crl.pem
clean:
	-rm ${requests}
# creates required supporting files, CA key and certificate
init:
	@test ! -f serial
	@mkdir crl newcerts private
	@chmod go-rwx private
	@echo '01' > serial
	@touch index
	@openssl req -config openssl.cnf -days 3650 -x509 -newkey rsa:2048 -out ca-cert.pem -
outform PEM

help:
	@echo make sign
	@echo '  - signs all *.csr files in this directory'
	@echo
```

```
	@echo make revoke cert=filename
	@echo '  - revokes certificate in named file and calls gencrl'
	@echo
	@echo make gencrl
	@echo '  - updates Certificate Revocation List (CRL)'
	@echo
	@echo make clean
	@echo '  - removes all *.csr files in this directory'
	@echo
	@echo make init
	@echo '  - required initial setup command for new CA'

# for legacy make support
FORCE:
```

Sertifikāts ir publiski pieejams adresē http://grid.lumii.lv/ca-cert.pem.

Atcelto sertifikātu saraksts (revocation lists) ir publiski pieejams adresē http://grid.lumii.lv/calg-crl.pem.

OpenSSL konfigurācijas fails:

```
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_match
[ policy_match ]
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

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

[ req ]
default_bits            = 1024
default_keyfile         = ./private/ca-key.pem
default_md              = sha1

prompt                  = no
distinguished_name      = root_ca_distinguished_name

x509_extensions = v3_ca
string_mask = nombstr

# req_extensions = v3_req

[ root_ca_distinguished_name ]
0.domainComponent = LV
1.domainComponent = latgrid
commonName = Certification Authority for Latvian Grid
#countryName = LV
#localityName = Riga
#0.organizationName = grid.lumii.lv
#emailAddress = ca@grid.lumii.lv

[ usr_cert ]

basicConstraints=critical,CA:FALSE

subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
```

```
#nsCaRevocationUrl              = http://grid.lumii.lv/ca-crl.pem
nsBaseUrl                      = http://grid.lumii.lv/
nsRevocationUrl                        = http://grid.lumii.lv/calg-crl.pem
#nsRenewalUrl
#nsCaPolicyUrl
#nsSslServerName

[ 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
```

4. LATVIJAS GRID CA DOKUMENTĀCIJA

Lai CA izsniegtajiem sertifikātiem resursu piedāvātāji varētu uzticēties, ļoti ir svarīgi nodrošināt, lai CA darbībā tiktu ievērotas stingras drošības procedūras, t.sk., lai vienmēr tiktu pārbaudīta cilvēku identitāte, lai CA privātā atslēga tiktu glabāta drošībā, lai CA galvenais dators nebūtu pieslēgts Internetam.

Tas, kā katra konkrēta CA īsteno un ievēro visas prasības, parasti tiek aprakstīts CA dokumentācijā.

Galvenais dokuments, kas apraksta Latvijas Grid CA procedūras, ir „Certificate Policy and Certification Practice Statement" (turpmāk CP/CPS). Šī dokumenta pirmā versija ir publicēta 2007.gada martā. Dokuments ir angļu valodā, jo ir ļoti svarīgi, lai ar visām procedūrām varētu iepazīties potenciālie starptautiskie partneri, kas varētu piedāvāt izmantot savus resursus Latvijas zinātniekiem. Arī vietējo Grid klasteru turētājiem būs nepieciešams iepazīties ar Latvijas Grid CA dokumentāciju. Šim nolūkam tiks izveidots „Certificate Policy and Certification Practice Statement" kopsavilkums latviešu valodā, bet par pamatdokumentu joprojām būs angliskā versija ar starptautiski atzīto terminoloģiju.

CP/CPS dokumentā 8 galvenās sadaļas, kas apraksta dažādas ar CA darbību saistītas procedūras un prasības:

1. Ievaddaļā ir aprakstīts Latvijas Grid CA darbības lauks, potenciālie lietotāji, attiecības ar citām CA, kā arī sniegta precīza kontaktinformācija.
2. Galveno noteikumu daļā ir apskatītas Latvijas Grid CA saistības un atbildība, informācijas publicēšanas kārtība un konfidencialitātes jautājumi.
3. Daļā „Identifikācija un autentifikācija" sniegta informācija par sertifikāta formātu, kādam jābūt sertifikāta vārdam, kā translēt latviešu burtus, kā pārbaudīt sertifikātu pieprasītāja un RA identitātes, kā atsaukt sertifikātus un publicēt atsaukto sertifikātu informāciju.
4. Operacionālās prasības nosaka, kādā veidā tiek pieprasīti, izsniegti un atsaukti sertifikāti, kādos gadījumos iespējama un nepieciešama sertifikātu atsaukšana, kādas CA darbības tiek logotas un auditētas, kā mainīt CA atslēgas, cik ilgi jāglabā žurnālfaili, kā atjaunot CA darbību dažādu risku iestāšanās gadījumā un kā beigt CA darbību nepieciešamības gadījumā.
5. Fiziskās, procedūru un personīgās drošības kontroles daļa apskata, kādi dažādu veidu drošības mēri tiek pielietoti, lai aizsargātu CA pret dažādiem riskiem un garantētu tās nepārtrauktu darbību.
6. Tehniskā drošība kontrole nosaka, kā tie ģenerēta CA atslēga, kas un kā ģenerē lietotāju atslēgas, atslēgu nepieciešamie parametri, privātās atslēgas aizsardzības mehānismi un citas ievērotās drošības metodes.
7. CP/CPS dokumenta septītajā daļā doti sertifikātu un CRL (*Certificate Revocation List*) profili ar visiem nepieciešamajiem parametriem.
8. Dokumenta pēdējā daļā definēts dokumenta versiju maiņas mehānisms un citas specifiskas procedūras.

CP/CPS dokumentam ir arī pielikumi ar terminu skaidrojumu un atsauces.

Ļoti svarīgi ir saskaņot CP/CPS dokumentu ar tādām starptautiskām organizācijām kā EUGridPMA un TACAR. Sīkāk par šīm organizācijām ir aprakstīts šīs atskaites 5.daļā.

CP/CPS dokumentam vienmēr jāatspoguļo spēkā esošās CA procedūras, tāpēc jaunas dokumenta versijas jāpublicē katru reizi, kad tiek kaut kas mainīts, piemēram, sertifikāta formāts vai kāda no drošības procedūrām.

Ar pilno CP/CPS dokumenta tekstu var iepazīties internetā:

http://grid.lumii.lv/uploads/CA/CA_for_LatvianGrid.pdf

5. IEKĻAUŠANĀS STARPTAUTISKAJĀ VIDĒ

Lai arī Grid tīkli bieži tiek veidoti nacionālo iniciatīvu vai reģionālu projektu ietvaros, Grid infrastruktūras mērķis ir veidot to pieejamu visiem zinātniekiem neatkarīgi no viņu atrašanās vietas. Ļoti svarīga Grid tīklos ir iespēja izmantot resursus, kas atrodas ne tikai savas universitātes datorcentrā, bet arī citur valstī, citur Eiropā un citur pasaulē. Lai Latvijas zinātnieki varētu risināt savus uzdevumus uz jebkuriem Grid klasteriem Eiropā, ļoti svarīgi ir panākt, lai Latvijas Grid projekta ietvaros izsniegtie Grid lietošanas sertifikāti tiktu pazīti un akceptēti citos Grid tīklos. 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.

Latvijas Grid CA ir uzsākusi akreditācijas procesu un plāno tuvākajā laikā uzsākt sadarbību ar TACAR repozitoriju. Šajā nodaļā ir aprakstīta sadarbība šo divu iniciatīvu ietvaros.

1.1. EUGRIDPMA

EUGridPMA ir starptautiska organizācija, kas koordinē uzticamības tīkla veidošanu Eiropas Grid infrastruktūrām. EUGridPMA sadarbojas arī ar iniciatīvām no citiem kontinentiem, piemēram, APGridPMA un Amerikas Grid PMA, tādējādi nodrošinot zinātniekiem iespēju izmantot Grid resursus arī citos reģionos. Katru valsti vai reģionu EUGridPMA var pārstāvēt tikai viena organizācija. Līdz šim Latvija nav pārstāvēta EUGridPMA, bet BalticGrid projekta ietvaros Igaunijā EENet (Igaunijas nacionālais izglītības un zinātnes tīkls) paspārnē izveidotā BalticGrid CA pārstāv visas trīs Baltijas valstis.

CA, kas vēlas kļūt par EUGridPMA biedriem, nepieciešams iziet akreditācijas procesu, kurā tiek pārbaudīta CA dokumentācija, pieņemtie drošības mēri, procedūras un to atbilstība reālajām darbībām. Akreditācijas process parasti aizņem 6 mēnešus līdz 1 gadam, kura laikā citi EUGridPMA organizācijas locekļi iepazīstas ar jaunās CA pārstāvjiem, pārskata viņu sagatavoto dokumentāciju, sniedz savus priekšlikumus procedūru uzlabošanai un optimizēšanai, kā arī iepazīstina potenciālos biedrus ar organizācijas iekšējiem noteikumiem un kultūru. Šī procesa laikā jaunās CA pārstāvju privātās atslēgas paraksta EUGridPMA vadītājs un citi biedri, tādējādi apliecinot atslēgu piederību un nodrošinot iespēju izmantot šīs atslēgas turpmākai drošai saziņai un sadarbībai.

Kad jaunā CA tiek akreditēta EUGridPMA organizācijā, tad CA saknes sertifikāts (atslēga) tiek pievienota EUGridPMA sertifikātu kopumam, kas tiek izsūtīts visiem Eiropas Grid klasteru uzturētājiem atjaunināšanai viņu serveros. Vēlāk, balstoties uz šiem CA saknes sertifikātiem, tiek pārbaudīta Grid lietotāju identitāte un tiesības. Ja Grid sertifikāta izsniedzējorganizācijas CA saknes sertifikāts ir iekļauts EUGridPMA izplatītajā akreditēto CA sertifikātu pakotnē, tad tiek pieņemts, ka lietotājs tiešām ir saņēmis savu sertifikātu šajā CA, ka CA atbilst zināmiem drošības kritērijiem, un lietotājs var saņemt pakalpojumus uz konkrētā Grid klastera. Protams, vēl tiek pārbaudīta lietotāja piederība uz katra klastera atļautajām virtuālajām organizācijām, bet tas jau skar citus Grid infrastruktūras jautājumus.

Lai nodrošinātu Latvijas Grid lietotājiem iespēju izmantot rēķināšanas un glabāšanas resursus citās valstīs, tika uzstādīts mērķis akreditēt Latvijas Grid CA EUGridPMA organizācijā. Maijā Latvijas Grid CA pārstāve Baiba Kaškina piedalījās kārtējā EUGridPMA sanāksmē un iepazīstināja citus dalībniekus ar Grid iniciatīvām Latvijā, to mērķiem un esošo situāciju.

EUGridPMA pārstāvji sākumā uzskatīja, ka Latviju organizācijā jau pārstāv igauņu izveidotā BalticGrid CA. Šī CA piedāvā vienkāršus, bet kvalitatīvus pakalpojumus un reģionā nav nepieciešamības veidot jaunu CA.

No Latvijas Grid lietotāju viedokļa, BalticGrid CA patiešām nodrošina iespēju saņemt sertifikātus, kas būtu derīgi arī citos Grid klasteros Eiropā, tomēr attālinātā sertifikātu izsniegšana un vairāku svarīgu iespēju iztrūkums liek uzskatīt, ka vietējā CA varētu piedāvāt ērtākus un kvalitatīvākus servisus. Piemēram, Latvijas Grid CA veidotāji plāno nodrošināt ērtu sertifikātu meklēšanu, pieprasīšanu un atsaukšanu *on-line*, kā arī visu nepieciešamo informāciju latviešu valodā.

Šī dokumenta rakstīšanas laikā (2007.gada augusts), Latvijas Grid CA ir iekļauts akreditācijas kandidātu sarakstā EUGridPMA organizācijā, tomēr prognozējams vēl garš process, kamēr EUGridPMA biedri tiks pilnībā pārliecināti par jaunas CA nepieciešamību, kamēr tiks nodemonstrēta spēja piedāvāt kvalitatīvus servisus un sadalīt ietekmes sfēras ar igauņu kolēģiem. EUGridPMA akreditāciju Latvijas Grid CA varētu saņemt 2008.gada vidū.

1.2. TACAR

TERENA organizācijas izveidotais TACAR repozitorijs risina nedaudz atšķirīgu problēmu. Visu akadēmiskās sabiedrības CA un PKI uzturētāju un lietotāju problēma vienmēr ir bijusi, kā nodrošināt savus serverus ar tādiem serveru sertifikātiem, kurus pārlūkprogrammas atzītu par pārbaudītiem un drošiem un neziņotu par iespējamu drošības pārkāpumu, atverot attiecīgo interneta vietni. Šādus sertifikātus ir iespējams nopirkt no komerciālajām organizācijām (piemēram, VeriSign), kuru saknes sertifikāti ir jau iestādīti pārlūkprogrammās pēc noklusēšanas un izsniegtie sertifikāti tiek atzīti par drošiem. Diemžēl šādu sertifikātu iegāde ne vienmēr iekļaujas akadēmisko organizāciju budžetā, tāpēc tika sākta iniciatīva, kas apkopotu Eiropas akadēmisko organizāciju CA saknes sertifikātus un izplatītu tos atsevišķā pakotnē, kuru pievienojot pārlūkprogrammai, visi attiecīgo CA izsniegtie sertifikāti tiktu uzskatīti par drošiem. Šī iniciatīva sākās TERENA darba grupu paspārnē un vēlāk tika nosaukta par TACAR (*TERENA Academic CA Repository*).

Pievienošanās šim repozitorijam iespējama visiem tiem CA, kas izsniedz vai plāno izsniegt serveru sertifikātus un kuri ir izveidoti Eiropas akadēmisko organizāciju paspārnē. Lai iesniegtu CA saknes sertifikātu TACAR repozitorijā, jātiekas personīgi ar TACAR pārstāvjiem, jāiesniedz pieteikuma vēstule, akreditācijas vēstule un CA saknes sertifikāts.

Lai arī sākotnēji Latvijas Grid CA neplāno izsniegt serveru sertifikātus mājas lapu uzturēšanai, tomēr pievienošanās TACAR repozitorijam tika uzstādīta par vienu no prioritātēm, jo tas veicinās Latvijas Grid CA atpazīstamību un atvieglos serveru sertifikātu izsniegšanu, ja radīsies tāda nepieciešamība nākotnē.

Līdz šim Latvijas Grid CA pārstāvji ir iepazinušies ar TACAR politikas dokumentiem, reģistrācijas un akreditācijas vēstulēm, kā arī ar citu TACAR dalībnieku politikas dokumentiem. Tā kā pievienošanās TACAR repozitorijam prasa dažu dokumentu rūpīgu aizpildīšanu un tikšanos klātienē ar TACAR pārstāvjiem, tad Latvijas Grid CA pievienošanās ir sagaidāma tuvāko mēnešu laikā (septembris – oktobris 2007).

6. SECINĀJUMI UN CA TURPMĀKĀ ATTĪSTĪBA

Latvijas Grid CA ir izveidota kā mūsdienīga CA, balstīta uz drošām tehnoloģijām un pārdomātu politikas dokumentu, ievērojot vairāku pakāpju aizsardzības principus. CA var sākt izsniegt Grid lietotāju sertifikātus, kas būtu lietojami Latvijas Grid tīklā. Lai Latvijas Grid lietotāji varētu izmantot citus Grid resursus, jāpanāk Latvijas Grid CA akreditācija EUGridPMA organizācijā.

Pagaidām Latvijas Grid CA ir izveidota, izmantojot maksimāli vienkāršu un drošu tehnoloģiju. Šis risinājums diemžēl nepiedāvā nekādu lietotāja puses saskarsmi, nav iespējams meklēt sertifikātus, tos pieprasīt un atsaukt tiešsaistes režīmā. Kā viens no pirmajiem Latvijas Grid CA uzlabojumiem ir plānota lietotāja puses saskarsmes izveide, kas būtu balstīta uz OpenCA/OpenXPKI programmatūru. Šī programmatūra nodrošina iespēju lietotājiem meklēt citu lietotāju sertifikātus (publiskās atslēgas), pieteikt jaunu sertifikātu, atsaukt esošo sertifikātu, ja tas ticis kaut kādu iemeslu dēļ kompromitēts un veikt citas līdzīgas darbības. Kad LU MII speciālisti būs izpētījuši un ieviesuši darbībā šos sarežģītos programmatūras produktus, sertifikācijas pakalpojumi varētu tikt piedāvāti arī citiem interesentiem – citiem Grid projektiem, Latvijas uzņēmumiem un iestādēm, kam nepieciešama droša sertifikātu izsniegšana un apkalpošana.

Nākotnē Latvijas Grid CA varētu paplašināt savu darbības sfēru, piedāvājot lietotājiem SLCS (*Short Lived Credential Service*) sertifikātus, kurus izsniedz, balstoties uz esošo akadēmisko autorizācijas un autentifikācijas hierarhiju, kuru darbības laiks ir ierobežots un līdz ar to drošības prasības ir samazinātas un vieglāk izpildāmas no lietotāju puses.