



**Institute of Mathematics and Computer Science**  
**Certification Authority for Latvian Grid**

# **Certificate Policy and Certification Practice Statement**

*Version 2.0*

*Document OID: 1.3.6.1.4.1.28446.1.1.2.0*

January 2008

# Table of Contents

<b>1. INTRODUCTION</b>	<b>7</b>
<b>1.1 OVERVIEW</b>	<b>7</b>
<b>1.2 IDENTIFICATION</b>	<b>7</b>
<b>1.3 COMMUNITY AND APPLICABILITY</b>	<b>7</b>
1.3.1 CERTIFICATION AUTHORITIES	7
1.3.2 REGISTRATION AUTHORITIES	7
1.3.3 END ENTITIES	8
1.3.4 APPLICABILITY	8
1.3.5 USER RESTRICTIONS	8
<b>1.4 CONTACT DETAILS</b>	<b>8</b>
1.4.1 SPECIFICATION ADMINISTRATION ORGANIZATION	8
1.4.2 CONTACT PERSON	9
1.4.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY	9
<b>2. GENERAL PROVISIONS</b>	<b>10</b>
<b>2.1 OBLIGATIONS</b>	<b>10</b>
2.1.1 CALG OBLIGATIONS	10
2.1.2 RA OBLIGATIONS	10
2.1.3 SUBSCRIBER OBLIGATIONS	11
2.1.4 RELYING PARTY OBLIGATIONS	11
2.1.5 REPOSITORY OBLIGATIONS	12
<b>2.2 LIABILITY</b>	<b>12</b>
2.2.1 CALG LIABILITY	12
2.2.2 RA LIABILITY	12
<b>2.3 FINANCIAL RESPONSIBILITY</b>	<b>12</b>
2.3.1 INDEMNIFICATION BY RELYING PARTIES	13
2.3.2 FIDUCIARY RELATIONSHIPS	13
2.3.3 ADMINISTRATIVE PROCESSES	13
<b>2.4 INTERPRETATION AND ENFORCEMENT</b>	<b>13</b>
2.4.1 GOVERNING LAW	13
2.4.2 SEVERABILITY, SURVIVAL, MERGER, NOTICE	13
2.4.3 DISPUTE RESOLUTION PROCEDURES	13
<b>2.5 FEES</b>	<b>13</b>
<b>2.6 PUBLICATION AND REPOSITORY</b>	<b>13</b>
2.6.1 PUBLICATION OF CA INFORMATION	13
2.6.2 FREQUENCY OF PUBLICATION	14
2.6.3 ACCESS CONTROLS	14
<b>2.7 COMPLIANCE AUDIT</b>	<b>14</b>
2.7.1 FREQUENCY OF ENTITY COMPLIANCE AUDIT	14
2.7.2 IDENTITY/QUALIFICATIONS OF AUDITOR	14
2.7.3 AUDITOR'S RELATIONSHIP TO AUDITED PARTY	14

2.7.4 TOPICS COVERED BY AUDIT.....	14
2.7.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY.....	15
2.7.6 COMMUNICATION OF RESULTS.....	15
<b>2.8 CONFIDENTIALITY .....</b>	<b>15</b>
2.8.1 TYPES OF INFORMATION TO BE KEPT CONFIDENTIAL .....	15
2.8.2 TYPES OF INFORMATION NOT CONSIDERED CONFIDENTIAL .....	15
2.8.3 DISCLOSURE OF CERTIFICATE REVOCATION/SUSPENSION INFORMATION .....	15
2.8.4 RELEASE TO LAW ENFORCEMENT OFFICIALS .....	15
2.8.5 RELEASE AS PART OF CIVIL DISCOVERY .....	15
2.8.6 DISCLOSURE UPON OWNER'S REQUEST .....	15
2.8.7 OTHER INFORMATION RELEASE CIRCUMSTANCES .....	15
2.9 INTELLECTUAL PROPERTY RIGHTS .....	15

### **3. IDENTIFICATION AND AUTHENTICATION .....17**

<b>3.1 INITIAL REGISTRATION .....</b>	<b>17</b>
3.1.1 TYPES OF NAMES .....	17
3.1.2 NEED FOR NAMES TO BE MEANINGFUL .....	17
3.1.3 RULES FOR INTERPRETING VARIOUS NAME FORMS .....	18
3.1.4 UNIQUENESS OF NAMES .....	18
3.1.5 NAME CLAIM DISPUTE RESOLUTION PROCEDURE .....	18
3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS .....	18
3.1.7 METHOD TO PROVE POSSESSION OF PRIVATE KEY .....	18
3.1.8 AUTHENTICATION OF ORGANISATION IDENTITY .....	18
3.1.9 AUTHENTICATION OF INDIVIDUAL IDENTITY .....	18
<b>3.2 ROUTINE REKEY .....</b>	<b>19</b>
<b>3.3 REKEY AFTER REVOCATION .....</b>	<b>19</b>
<b>3.4 REVOCATION REQUEST .....</b>	<b>19</b>

### **4. OPERATIONAL REQUIREMENTS .....21**

<b>4.1 CERTIFICATE APPLICATION .....</b>	<b>21</b>
<b>4.2 CERTIFICATE ISSUANCE .....</b>	<b>21</b>
<b>4.3 CERTIFICATE ACCEPTANCE .....</b>	<b>21</b>
<b>4.4 CERTIFICATE SUSPENSION AND REVOCATION .....</b>	<b>22</b>
4.4.1 CIRCUMSTANCES FOR REVOCATION .....	22
4.4.2 WHO CAN REQUEST REVOCATION .....	22
4.4.3 PROCEDURE FOR REVOCATION REQUEST .....	22
4.4.4 REVOCATION REQUEST GRACE PERIOD .....	22
4.4.5 CIRCUMSTANCES FOR SUSPENSION .....	22
4.4.6 WHO CAN REQUEST SUSPENSION .....	22
4.4.7 PROCEDURE FOR SUSPENSION REQUEST .....	23
4.4.8 LIMITS ON SUSPENSION PERIOD .....	23
4.4.9 CRL ISSUANCE FREQUENCY (IF APPLICABLE) .....	23
4.4.10 CRL CHECKING REQUIREMENTS .....	23
4.4.11 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY .....	23
4.4.12 ON-LINE REVOCATION CHECKING REQUIREMENTS .....	23
4.4.13 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE .....	23
4.4.14 CHECKING REQUIREMENTS FOR OTHER FORMS OF REVOCATION ADVERTISEMENTS .....	23
4.4.15 SPECIAL REQUIREMENTS RE KEY COMPROMISE .....	23

<b>4.5 SECURITY AUDIT PROCEDURES .....</b>	<b>23</b>
4.5.1 TYPES OF EVENT AUDITED .....	23
4.5.2 FREQUENCY OF PROCESSING LOG .....	23
4.5.3 RETENTION PERIOD FOR AUDIT LOG .....	24
4.5.4 PROTECTION OF AUDIT LOG .....	24
4.5.5 AUDIT LOG BACKUP PROCEDURES .....	24
4.5.6 AUDIT COLLECTION SYSTEM (INTERNAL VS EXTERNAL) .....	24
4.5.7 NOTIFICATION TO EVENT-CAUSING SUBJECT .....	24
4.5.8 VULNERABILITY ASSESSMENTS .....	24
<b>4.6 RECORDS ARCHIVAL .....</b>	<b>24</b>
4.6.1 TYPES OF EVENTS RECORDED .....	24
4.6.2 RETENTION PERIOD FOR ARCHIVE .....	24
4.6.3 PROTECTION OF ARCHIVE .....	24
4.6.4 ARCHIVE BACKUP PROCEDURES .....	25
4.6.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS .....	25
4.6.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL) .....	25
4.6.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION .....	25
<b>4.7 KEY CHANGEOVER .....</b>	<b>25</b>
<b>4.8 COMPROMISE AND DISASTER RECOVERY .....</b>	<b>25</b>
4.8.1 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED .....	25
4.8.2 ENTITY PUBLIC KEY IS REVOKED .....	26
4.8.3 ENTITY KEY IS COMPROMISED .....	26
4.8.4 SECURE FACILITY AFTER A NATURAL OR OTHER TYPE OF DISASTER .....	26
<b>4.9 CA TERMINATION .....</b>	<b>26</b>

**5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS .....27**

<b>5.1 PHYSICAL CONTROLS .....</b>	<b>27</b>
5.1.1 SITE LOCATION AND CONSTRUCTION .....	27
5.1.2 PHYSICAL ACCESS .....	27
5.1.3 POWER AND AIR CONDITIONING .....	27
5.1.4 WATER EXPOSURES .....	27
5.1.5 FIRE PREVENTION AND PROTECTION .....	27
5.1.6 MEDIA STORAGE .....	27
5.1.7 WASTE DISPOSAL .....	27
5.1.8 OFF-SITE BACKUP .....	27
<b>5.2 PROCEDURAL CONTROLS .....</b>	<b>27</b>
5.2.1 TRUSTED ROLES .....	27
5.2.2 NUMBER OF PERSONS REQUIRED PER TASK .....	28
5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE .....	28
<b>5.3 PERSONNEL CONTROLS .....</b>	<b>28</b>
5.3.1 BACKGROUND, QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS .....	28
5.3.2 BACKGROUND CHECK PROCEDURES .....	28
5.3.3 TRAINING REQUIREMENTS .....	28
5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS .....	28
5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE .....	28
5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS .....	28
5.3.7 CONTRACTING PERSONNEL REQUIREMENTS .....	28
5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL .....	28

**6. TECHNICAL SECURITY CONTROLS .....29**

**6.1 KEY PAIR GENERATION AND INSTALLATION .....29**

6.1.1 KEY PAIR GENERATION .....29

6.1.2 PRIVATE KEY DELIVERY TO ENTITY .....29

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER .....29

6.1.4 CA PUBLIC KEY DELIVERY TO USERS .....29

6.1.5 KEY SIZES .....29

6.1.6 PUBLIC KEY PARAMETERS GENERATION .....29

6.1.7 PARAMETER QUALITY CHECKING .....29

6.1.8 HARDWARE/SOFTWARE KEY GENERATION .....29

6.1.9 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD) .....29

**6.2 PRIVATE KEY PROTECTION .....30**

6.2.1 STANDARDS FOR CRYPTOGRAPHIC MODULE .....30

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL .....30

6.2.3 PRIVATE KEY ESCROW .....30

6.2.4 PRIVATE KEY BACKUP .....30

6.2.5 PRIVATE KEY ARCHIVAL .....30

6.2.6 PRIVATE KEY ENTRY INTO CRYPTOGRAPHIC MODULE .....30

6.2.7 METHOD OF ACTIVATING PRIVATE KEY .....30

6.2.8 METHOD OF DEACTIVATING PRIVATE KEY .....30

6.2.9 METHOD OF DESTROYING PRIVATE KEY .....30

**6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT .....30**

**6.4 ACTIVATION DATA .....30**

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION .....30

6.4.2 ACTIVATION DATA PROTECTION .....31

6.4.3 OTHER ASPECTS OF ACTIVATION DATA .....31

**6.5 COMPUTER SECURITY CONTROLS .....31**

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS .....31

6.5.2 COMPUTER SECURITY RATING .....31

**6.6 LIFE CYCLE TECHNICAL CONTROLS .....31**

6.6.1 SYSTEM DEVELOPMENT CONTROLS .....31

6.6.2 SECURITY MANAGEMENT CONTROLS .....31

6.6.3 LIFE CYCLE SECURITY RATINGS .....31

6.7 NETWORK SECURITY CONTROLS .....31

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....32

**7. CERTIFICATE AND CRL PROFILES .....33**

**7.1 CERTIFICATE PROFILE .....33**

7.1.1 VERSION NUMBER .....33

7.1.2 CERTIFICATE EXTENSIONS .....33

7.1.3 ALGORITHM OBJECT IDENTIFIERS .....33

7.1.4 NAME FORMS .....33

7.1.5 NAME CONSTRAINTS .....34

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER .....34

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION .....34

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS .....34

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION .....34

**7.2 CRL PROFILE .....34**

7.2.1 VERSION NUMBER .....34  
7.2.2. CRL AND CRL ENTRY EXTENSIONS .....34

**8. SPECIFICATION ADMINISTRATION .....35**

**8.1 SPECIFICATION CHANGE PROCEDURES .....35**

**8.2 PUBLICATION AND NOTIFICATION POLICIES .....35**

**8.3 CPS APPROVAL PROCEDURES .....35**

**APPENDIX 1: GLOSSARY .....36**

**APPENDIX 2: KEY WORDS FOR USE IN RFCs TO INDICATE REQUIREMENT LEVELS 38**

**REFERENCES .....39**

# 1. INTRODUCTION

## 1.1 Overview

The purpose of this document is to describe the procedure of certification of grid users for the usage of Grid resources within Latvian Grid.

The scope of the Certification Authority for Latvian Grid is to provide PKI services for grid initiatives in the country.

Institute of Mathematics and Computer Science, University of Latvia (hereinafter – IMCS UL) manages, coordinates and develops the Certification Authority for Latvian Grid (hereinafter – CALG).

This document is the combined Certificate Policy and Certification Practice Statement of the CALG. It describes the set of procedures followed by the CALG and is structured according to RFC 2527. The latter does not form part of this document and only the information provided in this document may be relied on.

## 1.2 Identification

1. Document title: "Certification Authority for Latvian Grid. Certificate Policy and Certification Practice Statement"

2. Version: 2.0.

3. Document Date: 20.01.2008

4. OID: 1.3.6.1.4.1.28446.1.1.2.0

IANA	1.3.6.1.4.1
IMCS UL	28446
CALG	.1
CP/CPS	.1
Major Version	.2
Minor Version	.0

5. Expiration: This document is valid until further notice.

## 1.3 Community and Applicability

CALG provides PKI services for the academic and research community of Latvia.

### 1.3.1 Certification authorities

The CALG is defined as a medium security CA. CALG does not issue certificates to subordinate Certification Authorities.

### 1.3.2 Registration authorities

The procedures of verification of the Subscribers identity and of approving their certificate requests are performed by trusted individuals – Registration Authorities (RA) – assigned by the CALG. RAs must be operated by organizations related with the Latvian academic community.

The CALG manages the functions of its Registration Authorities. Additional RAs MAY be created as required. The identities and contact details of the valid Registration Authorities are published in a public repository described in 2.1.5.

RAs do not issue certificates.

Each RA MUST sign an agreement with CALG, stating their-adherence to the procedures described in this CP/CPS.

### **1.3.3 End entities**

The CALG issues certificates to natural persons (user certificate), computer (server certificate) and service entities (service certificate). The entities eligible for certification from the CALG are all those related to organisations, formally based in and/or having offices in Latvia, that are involved in research or deployment of multidomain distributed computing infrastructure, intended for cross-organizational sharing of resources. The focus of these organizations SHOULD also be in research and/or education.

### **1.3.4 Applicability**

There will be three categories of certificates:

3. **Server certificates:** authentication, non-repudiation and communication encryption;
4. **User certificates:** authentication, non-repudiation, data encryption and communication encryption.
5. **Service certificates:** authentication, non-repudiation, data encryption and communication encryption.

### **1.3.5 User restrictions**

Certificates issued by CALG are only valid in the context of academic research and educational activities, any other usage is forbidden. Certificates issued by CALG MUST NOT be used for financial transactions nor purposes that violate Latvian or international laws.

The ownership of a CALG certificate does not imply automatic access to any kind of resources.

## **1.4 Contact Details**

### **1.4.1 Specification administration organization**

The CALG is created and managed by the Institute of Mathematics and Computer Science.

The CALG address for operational issues is:

Certification Authority for Latvian Grid  
Institute of Mathematics and Computer Science  
Raina bulv. 29  
Riga LV-1459  
Latvia  
Tel: +371 67 211 241  
Fax: +371 67 225 072  
Email: ca@grid.lumii.lv

### **1.4.2 Contact person**

The CALG contact person is:

Dana Ludviga  
Institute of Mathematics and Computer Science  
Raina bulv. 29  
Riga LV-1459



Latvia  
Tel: +371 67 211 241  
Fax: +371 67 225 072  
Email: dana.ludviga@sigmanet.lv

CA (public repository) web server URL is: <http://grid.lumii.lv>

### **1.4.3 Person determining CPS suitability for the policy**

See Section 1.4.2

## **2. GENERAL PROVISIONS**

### **2.1 Obligations**

#### **2.1.1 CALG obligations**

The CALG is responsible for all aspects of the issuance and management of a certificate referencing this policy, including:

1. Development of a detailed statement of practices and procedures (the CPS) by which the CALG implements the requirements of this policy;
2. Publication of CALG contact information;
3. Certificate application/enrolment process;
4. Verification of the identity of the applicant;
5. Certificate signing process;
6. Provide a public repository with reference to Repository obligations described in 2.1.5.
7. Revocation of the certificate;
8. Certificate renewals;
9. Issuing certificate revocation lists;
10. Ensuring that all aspects of the CA services and CA operations and CA infrastructure related to certificates issued under this policy are performed in accordance with the requirements, representations, and warranties of this policy;
11. Define and publish a dispute resolution procedure;
12. Keep a record of all the operations performed;
13. Collect only the personal data required to perform its function.

By issuing a certificate that references this policy, the CA certifies to the subscriber, and to all relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period, that:

1. The CA has issued, and will manage, the certificate in accordance with this policy.
2. There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS.
3. The certificate meets all requirements of this policy and the CA's CPS.

#### **2.1.2 RA obligations**

The RA is responsible for the following aspects:

1. Authenticate entities requesting a certificate according to the procedures described in this document;
2. Send validated certificate requests to CALG;
3. Create and send validated revocation requests to the CALG;
4. Communicate with CALG using secure channels and methods;
5. Follow the policies and procedures described in this document;
6. Keep a record of all request validation operations performed;
7. Allow the CALG to access the logs and documents related with the performed validations;
8. Collect only the personal data required to perform its function (users e-mail address, telephone number, a copy of some kind of identification document (passport or drivers license), a proof of affiliation with the academic institution mentioned in the DN, and the printed certificate request).

### **2.1.3 Subscriber obligations**

In all cases, the CALG SHALL require that:

1. Subscribers MUST accurately represent the information required from them in a certificate request. The requirements are detailed in 3.1.1 and 3.1.2;
2. Subscribers MUST properly protect their private key at all times, against loss, disclosure to any other party, modification and unauthorized use, in accordance with this CP /CPS. From the creation of their private and public key pair, subscribers are personally and solely responsible of the confidentiality and integrity of their private keys. Every usage of their private key is assumed to be the act of its owner. The private key MUST NOT be shared to other parties;
3. Upon suspicion that their private keys are compromised subscribers MUST notify the CA that issued their certificates by sending a certificate revocation request;
4. Upon any change of information in their certificates subscribers MUST notify the CA that issued their certificates by sending a certificate revocation request;
5. Subscribers MUST use the keys and certificates only for the purposes authorized by the CA;
6. On submitting the certificate requests, subscribers MUST authorize the treatment and conservation of their personal data;
7. The pass phrase used for protection of subscribers private key MUST be at least 12 characters long;
8. Use the certificates only for the purposes authorized by the CP/CPS document.

### **2.1.4 Relying party obligations**

A relying party MUST be familiar with this CP/CPS before drawing any conclusion on how much trust it can put in the use of a certificate issued by the CA.

The relying party MUST only use the certificate for the prescribed applications and MUST NOT use the certificates for forbidden applications.

Relying parties MUST verify the digital signature of a received digitally signed message and to verify the digital signature of the CA who issued the certificate used for the verification purpose.

When validating a certificate a relying party SHOULD check it for its validity, revocation, or suspension.

## **2.1.5 Repository obligations**

The CALG obligations regarding the public repository are as follows:

1. Publish on its web server the CALG public key;
2. Publish on its web server the CRL as soon as issued;
3. Publish on its web server the the current and all the previous versions of the CP/CPS;
4. Publish on its web server CALG contact information as described in 1.4.1;
5. Publish on its web server a list with the current operational RAs;
6. Publish on its web server issued certificate search engine;
7. Publish on its web server oher relevant information relating to certificates that refer to this document.

## **2.2 Liability**

### **2.2.1 CALG liability**

1. CALG guarantees to control the identity of the certification requests according to the procedures described in this document;
2. CALG guarantees to control the identity of the revocation requests according to the procedures described in this document;
3. CALG is managed on a best effort basis and does not give any guarantees about the service security or suitability;
4. CALG SHALL NOT be held liable for any problems arising from its operations or improper use of the issued certificates or CRLs;
5. CALG denies any kind of responsibilities for damages or impairments resulting from its operation.

### **2.2.2 RA liability**

Provisions given in 2.2.1 apply *mutatis mutandis* to the liability of RAs.

## **2.3 Financial responsibility**

CALG denies any financial responsibilities for damages or impairments resulting from its operation.

### **2.3.1 Indemnification by relying parties**

CALG denies any financial responsibilities for damages or impairments resulting from improperly used certificates.

### **2.3.2 Fiduciary relationships**

No stipulation.

### **2.3.3 Administrative processes**

No stipulation.

## **2.4 Interpretation and Enforcement**

### **2.4.1 Governing law**

The enforceability, construction, interpretation and validity of this policy shall be governed by the Law

of the Republic of Latvia. Legal disputes arising from the operation of the CALG will be treated according to Latvian laws.

#### **2.4.2 Severability, survival, merger, notice**

CALG shall be entitled to terminate the certification services at any time. CALG will make all reasonable efforts to notify all its subscribers and relying parties known to CALG to be currently and actively relying on certificates issued by CALG on such termination. All certificates issued by CALG that reference this document will be revoked no later than the time of termination.

#### **2.4.3 Dispute resolution procedures**

The head of academic network laboratory SigmaNet at the IMCS UL resolves all disputes related to interpretation and enforcement of conditions and rules described in this document.

#### **2.5 Fees**

Fees SHALL NOT be charged.

#### **2.6 Publication and Repository**

##### **2.6.1 Publication of CA information**

The CALG is obligated to maintain a secure on-line repository that is available through a web interface at <http://grid.lumii.lv/section/show/38> and it contains:

1. The CALG certificate for its signing key;
1. The latest CRL signed by CALG;
2. The current and all the previous versions of the CP/CPS;
3. CALG contact information as described in 1.4.1;
4. A list with the current operational RAs;
5. An issued certificate search engine;
6. Other relevant information relating to certificates that refer to this document.

##### **2.6.2 Frequency of publication**

All information to be published in the repository SHALL be published promptly after such information is available to the CA. CRLs issued by CALG are renewed whenever any certificate is revoked, and at least 7 days before expiration of the previously issued CRL.

##### **2.6.3 Access controls**

CALG does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS. CALG may impose a more restricted access control policy to the repository at its discretion. The CALG web site is maintained on a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site SHOULD be available at all times.

#### **2.7 Compliance audit**

The CALG may be audited by members of EUGridPMA and other Relaying Parties to verify its compliance with the rules and procedures specified in this document. Any costs associated with such an audit MUST be covered by the requesting party.

CALG will be internally audited once per year. Extraordinary audits will be carried out upon suspicion of violation of the rules and procedures specified in the CP/CPS.

If deficiencies are found during a compliance audit the CALG will take the appropriate measures to correct these deficiencies as soon as possible.

#### **2.7.1 Frequency of entity compliance audit**

No stipulation.

#### **2.7.2 Identity/qualifications of auditor**

No stipulation.

#### **2.7.3 Auditor's relationship to audited party**

No stipulation.

#### **2.7.4 Topics covered by audit**

No stipulation.

#### **2.7.5 Actions taken as a result of deficiency**

No stipulation.

#### **2.7.6 Communication of results**

No stipulation.

### ***2.8 Confidentiality***

#### **2.8.1 Types of information to be kept confidential**

All subscribers information that is not present in the certificate and CRLs issued by CALG is considered confidential and SHALL NOT be released to third parties without explicit subscribers authorization except as described in 2.8.4.

#### **2.8.2 Types of information not considered confidential**

Information included in public certificates and CRLs issued by the CALG are not considered confidential.

#### **2.8.3 Disclosure of certificate revocation information**

When a certificate is revoked, the reason is not considered confidential and MAY be shared with all other users and relying parties. However, no other details concerning the revocation are normally disclosed.

#### **2.8.4 Release to law enforcement officials**

CALG MUST NOT disclose confidential information to any third party, except when required by law enforcement officials that exhibit regular warrant.

#### **2.8.5 Release as part of civil discovery**

No stipulation.

### **2.8.6 Disclosure upon owner's request**

The CA SHALL release information if authorised by the subscriber.

### **2.8.7 Other information release circumstances**

No stipulation.

### **2.9 Intellectual Property Rights**

The use of the following documents for drafting this document is acknowledged:

- RFC 2527;
- RFC 3280;
- BalticGrid CA and CPS;
- Croatian SRCE Certification Authority, CP/CPS.

## **3. IDENTIFICATION AND AUTHENTICATION**

### ***3.1 Initial Registration***

#### **3.1.1 Types of names**

The subject names for the certificate applicants SHALL follow the X.509 standard. Any name under this CP/CPS starts with DC=org, DC=latgrid.

1. In case of personal certificate:
  - Common Name MUST include the persons full name.
  - Organizational Unit MUST include the organization domain name.
2. In case of server certificate
  - Common Name MUST include the "host/" prefix, followed by the server DNS name (FQDN).
  - Organizational Unit MUST include the organization domain name.
3. In case of grid service certificate
  - Common Name MUST include the "servicename/" prefix, followed by the server DNS name (FQDN).
  - Organisational Unit MUST include the organization domain name.

#### **3.1.2 Need for names to be meaningful**

The Subject and Issuer names contained in a certificate MUST be meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong.

For personal certificates, the Common Name attribute contains the legal name as presented in a government issued photo-identification.

If the legal name includes letters which are not present among letters present in PrintableString as defined in RFC1778, then those letters MUST be substituted with PrintableString letters according to following conversion table:

Non-PrintableString letters	PrintableString letters
ā	a
č	c
ē	e
ġ	g
ī	i
ķ	k
ļ	l
ņ	n
ŗ	r
š	s
ū	u
ž	z

For server certificates, the CN DN attribute contains the fully qualified domain name of the server.

For service certificates, the CN MUST be related to the type of service the certificate is identifying.

### **3.1.3 Rules for interpreting various name forms**

See Section 3.1.1 and Section 3.1.2.

### **3.1.4 Uniqueness of names**

The Common Name MUST be unique for each subject entity certified by the CALG. In case of name collision when more than one person uses the same name, a number is appended to the Common Name to make the name unique.

### **3.1.5 Name claim dispute resolution procedure**

The person named in 1.4.2 will resolve any name claim dispute.

### **3.1.6 Recognition, authentication and role of trademarks**

No stipulation.

### **3.1.7 Method to prove possession of private key**

No stipulation.

### **3.1.8 Authentication of organisation identity**

CALG does not issue certificates to organisations.

### **3.1.9 Authentication of individual identity**

1. Person requesting a certificate:

- A request sent to RA SHALL be considered authenticated when it is cryptographically signed by requestors valid certificate issued for the requestor by the CALG or VAS Latvijas Pasts.
  - Otherwise, a user requesting a certificate MUST meet in person with the RA and show his/her personal photo-id (passport or Driver License). If the photo-id is valid and the photo image corresponds to the bearer, the RA SHALL consider the user correctly identified.
  - RA MUST take steps to ascertain that the organisation, which name is requested to be the part of a subject name, consents to such use.
  - The certificate request and other required information must be delivered to RA by e-mail.
2. Server or service certificate:
- Requests MUST be signed by the personal certificate of the corresponding system administrator issued by CALG.
3. Person not requesting a certificate (revocation):
- Individual identity may be authenticated by personal acquaintance with RA staff;
  - By physical presence and proof of identity through a photo-id (passport or Driver License);
  - By consulting a public directory and verifying whether the person made the request.
  - RA SHALL send authenticated requests to the CALG. Any information exchanged between the requestor, the RA and the CA shall be either signed by strong cryptographic means, or shall be verified by out-of-band methods in a phone conversation with firm positive identification by parties involved.

If authentication is not completed within seven days of receipt of the certificate request by the RA the request will be deemed to have expired and any authentication of identity must then be preceded by a new certificate request.

By obtaining certificate the person accepts conditions and adhere to the procedures described in this document.

### **3.2 Routine Rekey**

Expiration warnings will be issued to subscribers when rekey time arrives. Rekey before expiration can be accomplished by sending a rekey request signed with the certificate before its expiration. However if the certificate subject is a person it must still provide to the RA a proof of relation with the organizations mentioned in the certificate subject name. Although a proof of relation is required the rekey process does not require the identity verification by the RA and therefore does not require the physical presence of the subject. If the proof of relation is performed through paper documents they can be sent to the RA by surface mail.

### **3.3 Rekey after Revocation**

Rekey after revocation follows the same rules as an initial registration.

### **3.4 Revocation Request**

A proper authentication method is required in order to accept revocation request. CALG MUST accept as a revocation request a message digitally signed with a not expired and not previously revoked certificate issued under this policy. The same procedures adopted for the authentication during initial registration are also considered suitable.



CALG can revoke certificates without authentication upon proof of key compromise or violation of the CP/CPS rules and user obligations by the certificate holder.

## **4. OPERATIONAL REQUIREMENTS**

### ***4.1 Certificate Application***

The application for a CALG certificate is performed by:

1. Generating a key pair. The key pair generation must be performed by the requester;
2. Sending the certificate request to RA that is authorized to authenticate the request, if the e-mail is not cryptographically signed by requestors valid certificate issued for the requestor by the CALG or VAS Latvijas Pasts, the requestor **MUST** arrange a face to face meeting (see section 3.1.9).

The necessary provisions that **MUST** be followed in any certificate application request to the CALG are:

1. The subject **MUST** be an acceptable end user entity, as defined by this Policy;
2. The request **MUST** obey the CALG distinguished name scheme;
3. The distinguished name **MUST** be unambiguous and unique;
4. The key **MUST** have at least 1024 bits.

### ***4.2 Certificate Issuance***

When the applicant submits the request, appropriate RA performs identity vetting as described in 3.1.9.

If the request is valid, RA sends a signed request and other required information (see section 2.1.2.) to CA by e-mail.

CALG issues certificate if, and only if:

1. The authentication of the subject is successful according to 3.1.9.
2. The appropriate RA approves, signs and sends the request to the CA.
3. The CA has verified the RA signature and the certificate request content.

After the certificate is issued it is published and can be accessed through the public repository search engine, CA also notifies the applicant and the RA.

The subject will be notified by e-mail about the certificate issuance or rejection. In the case of rejection the e-mail will state the reason.

### ***4.3 Certificate Acceptance***

The certificate is assumed to be accepted unless its requester explicitly rejects it in an authenticated communication with the CA.

### ***4.4 Certificate Suspension and Revocation***

#### **4.4.1 Circumstances for revocation**

A certificate will be revoked when the information in the certificate is known to be suspected or compromised or at the request of the authorized entity. It includes following situations:

1. The associated private key is known to be compromised or misused;
2. The associated private key is suspected to be compromised or misused;
3. The subscriber's information in the certificate has changed;
4. The subscriber is known to have violated his obligations;
5. The authenticated requester requested the certificate revocation;
6. The subject of the certificate has ceased his relation with the organization;
7. The system to which the certificate has been issued has been retired.

#### **4.4.2 Who can request revocation**

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting proof of knowledge of the private key compromise or of the variation of the subscriber's data.

#### **4.4.3 Procedure for revocation request**

In case where the CA can independently confirm that the certificate has been compromised or misused, the CA SHALL revoke the certificate, even if the request to do so comes from an unauthenticated source and/or the holder of the certificate is unreachable.

In all other cases the CA SHALL authenticate the revocation request and try to contact the subscriber before revoking the certificate.

If the revoked certificate is the CA certificate then the CA SHALL in addition inform the subscribers and cross-certifying CAs and it SHALL terminate the certificate and CRLs distribution service for certificates/CRLs issued using the compromised private key.

#### **4.4.4 Revocation request grace period**

The CALG has a maximum response time of one day (excluding weekends and public holidays in Latvia) for revocations; it will however handle revocation requests with priority as soon as the request is recognised as such.

#### **4.4.5 Circumstances for suspension**

No stipulation.

#### **4.4.6 Who can request suspension**

No stipulation.

#### **4.4.7 Procedure for suspension request**

No stipulation.

#### **4.4.8 Limits on suspension period**

No stipulation.

#### **4.4.9 CRL issuance frequency (if applicable)**

CRLs issued by CALG are renewed whenever any certificate is revoked, and at least 7 days before expiration of the previously issued CRL. The maximum CRL lifetime MUST be at most 90 days.

#### **4.4.10 CRL checking requirements**

Before use of a certificate, a relying party SHOULD validate it against a recently issued CRL.

#### **4.4.11 On-line revocation/status checking availability**

The on-line revocation/status checking service is not currently available.

#### **4.4.12 On-line revocation checking requirements**

No stipulation.

#### **4.4.13 Other forms of revocation advertisements available**

The subscriber is notified of the revocation of his certificate by email.

#### **4.4.14 Checking requirements for other forms of revocation advertisements**

No stipulation.

#### **4.4.15 Special requirements re key compromise**

No stipulation.

### ***4.5 Security Audit Procedures***

#### **4.5.1 Types of event audited**

1. Boot and shutdown of CA machine;
2. Interactive system logins and logouts;
3. Certification requests;
4. Revocation requests;
5. Issued certificates;
6. Issued CRLs.

#### **4.5.2 Frequency of processing log**

Audit logs are processed on a weekly basis.

#### **4.5.3 Retention period for audit log**

Logs will be kept for a minimum of three years. After termination of CALG or a RA, the logs will be kept for a minimum of three years by CALG's host organization.

#### **4.5.4 Protection of audit log**

Audit logs may be consulted by:

1. CA personnel;
2. Authorised external auditors.

#### **4.5.5 Audit log backup procedures**

A backup of the audit logs **MUST** be performed on removable media at the time of audit log processing (see 4.5.2). The minimal retention period of backup copies of the audit logs is defined in 4.5.3. The backup media is kept in safe.

#### **4.5.6 Audit collection system (internal vs external)**

The audit collection system **SHALL** be running separately from the CA software in a secure environment. The audit collection system is internal to CALG.

#### **4.5.7 Notification to event-causing subject**

Operations personnel notifies security administrator when a process or action causes a critical security event or discrepancy.

#### **4.5.8 Vulnerability assessments**

A security risk assessment **MUST** be regularly repeated for CALG's host organisation. This assessment **MUST** cover the overarching risks and threats that may impact the PKI.

### **4.6 Records Archival**

#### **4.6.1 Types of events recorded**

The CA records the following:

1. Certificate requests;
2. Approved certificate requests;
3. Issued certificates;
4. Revocation requests;
5. Issued CRLs.

The RA records the following events:

1. Certificate requests;
2. Identity authentication actions
  - The name and surname of the RA representative and date and time of the face to face meeting
  - All personal data documents mentioned in section 2.1.2.

The following software/hardware related events are recorded:

1. System boots;
2. Login and logouts;
3. Unauthorized access attempts.

#### **4.6.2 Retention period for archive**

The minimum retention period is three years. After termination of CALG or a RA, the archive will be kept for a minimum of three years by CALG's host organization.

#### **4.6.3 Protection of archive**

Records are backed up on removable media, which are stored in a room with restricted access.

#### **4.6.4 Archive backup procedures**

See section 4.6.3.

#### **4.6.5 Requirements for time-stamping of records**

No stipulation.

#### **4.6.6 Archive collection system (internal or external)**

The archive collection system is internal to the CALG.

#### **4.6.7 Procedures to obtain and verify archive information**

No stipulation.

### **4.7 Key changeover**

CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA key is generated one year before the old one loses validity and, from that point

onwards, new certificates are signed with the new key. The new key is posted in the repository.

## **4.8 Compromise and Disaster Recovery**

If the private key of the CALG is compromised or suspected to be compromised, the CALG will:

1. Inform subscribers, relevant relying parties, security contacts and all cross-certifying CAs,
2. Terminate the issuance and distribution of certificates and CRLs,

If an entity's private key is compromised or suspected to be compromised, the entity or its administrator or responsible person **MUST** request revocation of the certificate and inform any relevant relying parties.

### **4.8.1 Computing resources, software, and/or data are corrupted**

The private keys of the CALG are only available in encrypted form on media stored in a secure location. The computer used to activate the private key is not accessible via any network. If the computer and/or the media are lost, this will be handled as a major compromise that implies generating a new key pair and terminating all services associated with the lost key pair.

If the hardware or software of the CA signing computer become corrupt, the status will be diagnosed and suitably repaired. If there is any doubt about the extent of the damage involved, this will imply rebuilding the machine from scratch, using original supplied parts and software distributions.

If data becomes corrupted, the cause will be diagnosed and the data restored from the latest backup.

### **4.8.2 Entity public key is revoked**

See section 4.8.

### **4.8.3 Entity key is compromised**

See section 4.8.

### **4.8.4 Secure facility after a natural or other type of disaster**

In case of (natural) disaster, the CALG administrator(s) will as soon as physically possible confirm that all CA activation materials are at the intended locations. Depending on the situation, disaster recovery will start.

## **4.9 CA Termination**

Before the CALG terminates its services, the CALG shall:

1. Make all reasonable efforts to inform subscribers, RAs and cross-certifying CAs;
2. Make knowledge of its termination widely available;
3. Cease issuing certificates and CRLs;
4. Destroy all copies of private keys.

Notifications will be sent prior the termination and as early as possible.

## **5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS**

### ***5.1 Physical Controls***

#### **5.1.1 Site location and construction**

The CALG is located at the IMCS UL office.

#### **5.1.2 Physical access**

Physical access to the CALG is restricted to authorized personnel of the IMCS UL.

CALG private key is not stored on the CA equipment but is kept locked in a safe equipped with electronic lock. Lock codes are known only to CA administrators. Change of staff will imply a change of all codes.

#### **5.1.3 Power and air conditioning**

The critical CALG equipment is connected to uninterrupted power supply units.

#### **5.1.4 Water exposures**

Due to the location of the CALG facilities floods are not expected. The CALG secure operating room is reasonably waterproof, no water exposure is expected to occur.

#### **5.1.5 Fire prevention and protection**

The CALG secure operating room is provided with smoke detectors.

#### **5.1.6 Media storage**

1. The CALG key is kept in several removable storage media;
2. Backup copies of CA related information are kept in USB storage devices and on CDROMs.

#### **5.1.7 Waste disposal**

All CALG paper waste **MUST** be shredded. Electronic media **MUST** be physically/mechanically destroyed before disposal.

#### **5.1.8 Off-site backup**

No off-site backups are currently performed.

### ***5.2 Procedural Controls***

#### **5.2.1 Trusted roles**

No stipulation.

#### **5.2.2 Number of persons required per task**

There are no requirements within the CALG to act within any role in the presence of more than one person.

#### **5.2.3 Identification and authentication for each role**

No stipulation.

## **5.3 Personnel Controls**

### **5.3.1 Background, qualifications, experience, and clearance requirements**

The role of the CA requires a suitably trained person that is familiar with the importance of a PKI, and who is technically and professionally competent. There are no background checks of clearance procedures for trusted or other roles.

### **5.3.2 Background check procedures**

No stipulation.

### **5.3.3 Training requirements**

Internal training is given to CA and RA operators.

### **5.3.4 Retraining frequency and requirements**

No stipulation.

### **5.3.5 Job rotation frequency and sequence**

No stipulation.

### **5.3.6 Sanctions for unauthorized actions**

No stipulation.

### **5.3.7 Contracting personnel requirements**

No stipulation.

### **5.3.8 Documentation supplied to personnel**

Copies of this document **MUST** be given to personnel of CA and RAs.

## **6. TECHNICAL SECURITY CONTROLS**

### **6.1 Key Pair Generation and Installation**

#### **6.1.1 Key pair generation**

Key pairs for the CALG are generated exclusively by authorized CALG personnel acting in the role of CA.

End entities' key pairs are always generated by their application during the requesting process. They are never generated or stored by the CALG.

#### **6.1.2 Private key delivery to entity**

CALG does not generate private keys hence does not deliver private keys . End entities are required to generate their own key pairs.

#### **6.1.3 Public key delivery to certificate issuer**

1. The entity **MUST** submit a certificate request with the public key according to the requirements detailed in section 4.1.
2. The entity **MUST** be authenticated according to the procedures described in 3.1.9 and 3.1.8.
3. The entity **SHOULD** submit a cryptographically signed certification request via e-mail to

ca@grid.lumii.lv or SHOULD deliver a certification request to the RA during face-to-face meeting.

#### **6.1.4 CA public key delivery to users**

The CA's root certificate can be downloaded from CALG website.

#### **6.1.5 Key sizes**

The RSA key length for the CALG is 2048 bits. Keys submitted for certification MUST be at least 1024 bits.

#### **6.1.6 Public key parameters generation**

No stipulation.

#### **6.1.7 Parameter quality checking**

No stipulation.

#### **6.1.8 Hardware/software key generation**

No stipulation.

#### **6.1.9 Key usage purposes (as per X.509 v3 key usage field)**

Keys may be used for authentication, non-repudiation, data encipherment, message integrity and session establishment. Certificates and CRLs are signed by the CA private key.

### ***6.2 Private Key Protection***

#### **6.2.1 Standards for cryptographic module**

No stipulation.

#### **6.2.2 Private key (n out of m) multi-person control**

No stipulation.

#### **6.2.3 Private key escrow**

No stipulation.

#### **6.2.4 Private key backup**

The CALG private key is kept encrypted in multiple copies on USB storage devices and CDROMs according to 5.1.2. The pass phrase is in a sealed envelope kept in a safe according to 5.1.2.

#### **6.2.5 Private key archival**

No stipulation.

#### **6.2.6 Private key entry into cryptographic module**

No stipulation.

#### **6.2.7 Method of activating private key**

Every activation of a CALG private key MUST require entering of pass phrase. Pass phrase MUST meet conditions described in 6.4.

Every activation of end entity's private key MUST require entering of pass phrase. Pass phrase SHOULD be suitably strong.



## **6.2.8 Method of deactivating private key**

No stipulation.

## **6.2.9 Method of destroying private key**

After termination of the CA and after the archival period for archives has expired, all media that contain the private key of the CA will be securely and permanently destroyed, according to the best current practice.

## **6.3 Other Aspects of Key Pair Management**

The CALG private key has a validity of ten years.

## **6.4 Activation Data**

### **6.4.1 Activation data generation and installation**

All pass phrases used by the CA have a length of at least 15 characters, and are suitably strong according to current best practice.

### **6.4.2 Activation data protection**

All pass phrases are known to CALG administrators. Change of staff will imply change of pass phrases.

### **6.4.3 Other aspects of activation data**

No stipulation.

## **6.5 Computer Security Controls**

### **6.5.1 Specific computer security technical requirements**

The secure environment for CA operations are provided by bootable Knoppix Linux CDROM, which is used for CA machines working environment. Unauthorised access to that Knoppix Linux CDROM and USB storage devices are prohibited.

The CA machine is a computer with no network connection. Keys and necessary scripts are kept on USB storage device, which is held in safe. Unauthorised physical access to CA machine or USB storage device is prohibited.

Copy of keys is printed out and held also in a safe.

The systems used by the CA to hold on-line repositories are maintained at a high level of security by applying all recommended and applicable security patches. The machine(s) are protected by a suitable firewall.

### **6.5.2 Computer security rating**

No stipulation.

## **6.6 Life Cycle Technical Controls**

### **6.6.1 System development controls**

No stipulation.

## 6.6.2 Security management controls

Software installed on the CA signing system is periodically checked for integrity by comparing strong cryptographic message digests. Firmware and hardware are not explicitly checked for correct operations.

## 6.6.3 Life cycle security ratings

No stipulation.

## 6.7 Network Security Controls

Certificates are issued on a machine that is not connected to any kind of network.

The public web interface equipment is protected by firewalls.

## 6.8 Cryptographic Module Engineering Controls

No stipulation.

# 7. CERTIFICATE AND CRL PROFILES

## 7.1 Certificate Profile

The certificates issued in accordance with this CPS SHOULD follow the RFC 2459 [3] and the PKIX profiles.

### 7.1.1 Version number

X.509 v3.

### 7.1.2 Certificate extensions

The following extensions are set in root certificates:

1. X509v3 Basic Constraints: CRITICAL, CA:TRUE
2. X509v3 Subject Key Identifier
3. X509v3 Authority Key Identifier
4. X509v3 Key Usage: CRITICAL, Digital Signature, Certificate Sign, CRL Sign
5. X509v3 Subject Alternative Name: URI:http://grid.lumii.lv/
6. X509v3 CRL Distribution Points: URI:http://grid.lumii.lv/ca-cert.pem

The following extensions are set in user certificates:

1. X509v3 Basic Constraints: CRITICAL, CA:FALSE
2. X509v3 Key Usage: CRITICAL
3. X509v3 Subject Key Identifier
4. X509v3 Authority Key Identifier
5. X509v3 Certificate Policies Identifier: 1.3.6.1.4.1.19974.11.1.1.1
6. X509v3 Issuer Alternative Name: URI:http://grid.lumii.lv/
7. X509v3 CRL Distribution Points: URI:http://grid.lumii.lv/ca-cert.pem

The following extensions are set in host and service certificates:

1. X509v3 Basic Constraints: CRITICAL, CA:FALSE
2. X509v3 Key Usage: CRITICAL
3. X509v3 Subject Key Identifier
4. X509v3 Authority Key Identifier
5. X509v3 Certificate Policies Identifier: 1.3.6.1.4.1.19974.11.1.1.1

6. X509v3 Issuer Alternative Name: URI:http://grid.lumii.lv/
7. X509v3 CRL Distribution Points: URI:http://grid.lumii.lv/ca-cert.pem
8. X509v3 Subject Alternative Name: dnsName: FQDN of the host

### **7.1.3 Algorithm object identifiers**

No stipulation.

### **7.1.4 Name forms**

Issuer: DC=org, DC=latgrid, OU=domain.zz, CN=Baltic Grid Certification Authority

Natural persons: DC=org, DC=latgrid, OU=domain.zz, CN=Firstname Lastname

Hosts: DC=org, DC= latgrid, OU=domain.zz, CN=host/fully.qualified.domain.name

Services: DC=org, DC= latgrid, OU=domain.zz,

CN=servicename/fully.qualified.domain.name

### **7.1.5 Name constraints**

See section 3.1.2.

### **7.1.6 Certificate policy Object Identifier**

See section 1.2.

### **7.1.7 Usage of Policy Constraints extension**

No stipulation.

### **7.1.8 Policy qualifiers syntax and semantics**

No stipulation.

### **7.1.9 Processing semantics for the critical certificate policy extension**

No stipulation.

## **7.2 CRL Profile**

### **7.2.1 Version number**

X.509 v1.

### **7.2.2. CRL and CRL entry extensions**

Digest and signature algorithms used for CRLs are the same as for certificates (see 7.1.3).

The following extensions are set in CRLs:

- X509v3 Issuer Alternative Name
- X509v3 Authority Key Identifier.

## **8. SPECIFICATION ADMINISTRATION**

### **8.1 Specification change procedures**

The significance of the change is evaluated by the CALG. If the change is determined to influence the trust procedures of relying parties and/or cooperating CAs, the CALG MUST assign a new OID to the modified CPS.

Minor editorial or typographical changes to the policy and CPS MAY be made without approval.

All changes MUST be communicated to the interested parties.

### **8.2 Publication and notification policies**

The policy is available on [http://grid.lumii.lv/uploads/CA/CA\\_for\\_LatvianGrid.pdf](http://grid.lumii.lv/uploads/CA/CA_for_LatvianGrid.pdf)

### **8.3 CPS approval procedures**

No stipulation.

## APPENDIX 1: Glossary

**Certification Authority (CA)** - An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

**CA-certificate** - A certificate for one CA's public key issued by another CA.

**CALG** – Certification Authority for Latvian Grid.

**Certificate policy (CP)** - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

**Certification path** - An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

**Certification Practice Statement (CPS)** - A statement of the practices which a certification authority employs in issuing certificates.

**Certificate revocation list (CRL)** - A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

**IMCS UL** – Institute of Mathematics and Computer Science.

**IPR** - Intellectual Property Rights

**Issuing certification authority (issuing CA)** - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

**Public Key Certificate (PKC)** - A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.

**Public Key Infrastructure (PKI)** - The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography.

**Registration authority (RA)** - An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is used elsewhere for the same concept.]

**Relying party (RP)** - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

**Subject certification authority (subject CA)** - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate.

## **APPENDIX 2: Key words for use in RFCs to Indicate Requirement Levels**

According to RFC 2119 [2] Key words for use in RFCs to Indicate Requirement Levels , we specify how the main keywords used in RFCs should be interpreted.

Authors who follow these guidelines should incorporate this phrase near the beginning of their document:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHAL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1. **MUST** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
2. **MUST NOT** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
5. **MAY** This word, or the adjective "OPTIONAL", mean that an item is truly optional.

## REFERENCES

- [1] EuroPKI Certificate Policy : VERSION 1.1 January 2004 [<http://www.europki.org/ca/root/>]
- [2] RFC 2119 Key words for use in RFCs to Indicate Requirement Levels March 1997  
[<ftp://ftp.isi.edu/in-notes/rfc2119.txt>]
- [3] RFC 2459 Internet X.509 Public Key Infrastructure: Certificate and CRL Profile January 1999  
[<ftp://ftp.isi.edu/in-notes/rfc2459.txt>]
- [4] BalticGrid CA and CSP