



LIPCA

LIP Certification Authority

Certificate Policy and Certification Practice Statement (CP/CPS)

Version 5.3
15 January 2015

Contents

1. INTRODUCTION.....	8
1.1. Overview.....	8
1.2. Document name and identification.....	8
1.3. PKI participants.....	9
1.3.1. Certification authorities.....	9
1.3.2. Registration authorities	9
1.3.3. Subscribers	9
1.3.4. Relying parties	9
1.3.5. Other participants.....	9
1.4. Certificate usage.....	10
1.4.1. Appropriate certificate uses.....	10
1.4.2. Prohibited certificate uses	10
1.5. Policy administration.....	10
1.5.1. Organization administering the document.....	10
1.5.2. Contact person.....	10
1.5.3. Person determining CPS suitability for the policy	11
1.5.4. CPS approval procedures	11
1.6. Definitions and acronyms	11
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	12
2.1. Repositories.....	12
2.2. Publication of certification information	12
2.3. Time or frequency of publication.....	12
2.4. Access controls on repositories	12
3. IDENTIFICATION AND AUTHENTICATION.....	12
3.1. Naming	12
3.1.1. Types of names.....	12
3.1.2. Need for names to be meaningful	14
3.1.3. Anonymity or pseudonymity of subscribers.....	15
3.1.4. Rules for interpreting various name forms.....	15
3.1.5. Uniqueness of names	15
3.1.6. Recognition, authentication, and role of trademarks	15
3.2. Initial identity validation.....	15
3.2.1. Method to prove possession of private key	15
3.2.2. Authentication of organization identity.....	15
3.2.3. Authentication of individual identity	16
3.2.4. Non-verified subscriber information.....	17
3.2.5. Validation of authority.....	17
3.2.6. Criteria for interoperation.....	17
3.3. Identification and authentication for re-key requests.....	17
3.3.1. Identification and authentication for routine re-key	17
3.3.2. Identification and authentication for re-key after revocation	18
3.4. Identification and authentication for revocation request.....	18
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS.....	18
4.1. Certificate Application	18

4.1.1. Who can submit a certificate application	18
4.1.2. Enrollment process and responsibilities	18
4.2. Certificate application processing	19
4.2.1. Performing identification and authentication functions	19
4.2.2. Approval or rejection of certificate applications	19
4.2.3. Time to process certificate applications	20
4.3. Certificate issuance	20
4.3.1. CA actions during certificate issuance	20
4.3.2. Notification to subscriber by the CA of issuance of certificate	20
4.4. Certificate acceptance	20
4.4.1. Conduct constituting certificate acceptance	20
4.4.2. Publication of the certificate by the CA	20
4.4.3. Notification of certificate issuance by the CA to other entities	21
4.5. Key pair and certificate usage	21
4.5.1. Subscriber private key and certificate usage	21
4.5.2. Relying party public key and certificate usage	21
4.6. Certificate renewal	21
4.6.1. Circumstance for certificate renewal	21
4.6.2. Who may request renewal	21
4.6.3. Processing certificate renewal requests	21
4.6.4. Notification of new certificate issuance to subscriber	22
4.6.5. Conduct constituting acceptance of a renewal certificate	22
4.6.6. Publication of the renewal certificate by the CA	22
4.6.7. Notification of certificate issuance by the CA to other entities	22
4.7. Certificate re-key	22
4.7.1. Circumstance for certificate re-key	22
4.7.2. Who may request certification of a new public key	22
4.7.3. Processing certificate re-keying requests	23
4.7.4. Notification of new certificate issuance to subscriber	23
4.7.5. Conduct constituting acceptance of a re-keyed certificate	23
4.7.6. Publication of the re-keyed certificate by the CA	23
4.7.7. Notification of certificate issuance by the CA to other entities	23
4.8. Certificate modification	23
4.8.1. Circumstance for certificate modification	23
4.8.2. Who may request certificate modification	23
4.8.3. Processing certificate modification requests	24
4.8.4. Notification of new certificate issuance to subscriber	24
4.8.5. Conduct constituting acceptance of modified certificate	24
4.8.6. Publication of the modified certificate by the CA	24
4.8.7. Notification of certificate issuance by the CA to other entities	24
4.9. Certificate revocation and suspension	24
4.9.1. Circumstances for revocation	24
4.9.2. Who can request revocation	24
4.9.3. Procedure for revocation request	25
4.9.4. Revocation request grace period	25
4.9.5. Time within which CA must process the revocation request	25

4.9.6. Revocation checking requirement for relying parties.....	25
4.9.7. CRL issuance frequency (if applicable)	25
4.9.8. Maximum latency for CRLs (if applicable)	25
4.9.9. On-line revocation/status checking availability	26
4.9.10. On-line revocation checking requirements	26
4.9.11. Other forms of revocation advertisements available	26
4.9.12. Special requirements re key compromise	26
4.9.13. Circumstances for suspension	26
4.9.14. Who can request suspension	26
4.9.15. Procedure for suspension request	26
4.9.16. Limits on suspension period	26
4.10. Certificate status services	27
4.10.1. Operational characteristics	27
4.10.2. Service availability	27
4.10.3. Optional features	27
4.11. End of subscription	27
4.12. Key escrow and recovery	27
4.12.1. Key escrow and recovery policy and practices	27
4.12.2. Session key encapsulation and recovery policy and practices	27
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	28
5.1. Physical controls	28
5.1.1. Site location and construction	28
5.1.2. Physical access	28
5.1.3. Power and air conditioning	28
5.1.4. Water exposures	28
5.1.5. Fire prevention and protection	28
5.1.6. Media storage	28
5.1.7. Waste disposal	28
5.1.8. Off-site backup	29
5.2. Procedural controls	29
5.2.1. Trusted roles	29
5.2.2. Number of persons required per task	29
5.2.3. Identification and authentication for each role	29
5.2.4. Roles requiring separation of duties	29
5.3. Personnel controls	30
5.3.1. Qualifications, experience, and clearance requirements	30
5.3.2. Background check procedures	30
5.3.3. Training requirements	30
5.3.4. Retraining frequency and requirements	30
5.3.5. Job rotation frequency and sequence	30
5.3.6. Sanctions for unauthorized actions	30
5.3.7. Independent contractor requirements	30
5.3.8. Documentation supplied to personnel	30
5.4. Audit logging procedures	31
5.4.1. Types of events recorded	31
5.4.2. Frequency of processing log	31

5.4.3. Retention period for audit log	31
5.4.4. Protection of audit log	31
5.4.5. Audit log backup procedures.....	31
5.4.6. Audit collection system (internal vs. external)	31
5.4.7. Notification to event-causing subject.....	31
5.4.8. Vulnerability assessments.....	31
5.5. Records archival	32
5.5.1. Types of records archived	32
5.5.2. Retention period for archive	32
5.5.3. Protection of archive	32
5.5.4. Archive backup procedures.....	32
5.5.5. Requirements for time-stamping of records	32
5.5.6. Archive collection system (internal or external)	32
5.5.7. Procedures to obtain and verify archive information	32
5.6. Key changeover.....	33
5.7. Compromise and disaster recovery	33
5.7.1. Incident and compromise handling procedures.....	33
5.7.2. Computing resources, software, and/or data are corrupted	33
5.7.3. Entity private key compromise procedures.....	33
5.7.4. Business continuity capabilities after a disaster	34
5.8. CA or RA termination.....	34
6. TECHNICAL SECURITY CONTROLS	34
6.1. Key pair generation and installation.....	34
6.1.1. Key pair generation	34
6.1.2. Private key delivery to subscriber.....	34
6.1.3. Public key delivery to certificate issuer.....	35
6.1.4. CA public key delivery to relying parties.....	35
6.1.5. Key sizes.....	35
6.1.6. Public key parameters generation and quality checking	35
6.1.7. Key usage purposes (as per X.509 v3 key usage field)	35
6.2. Private Key Protection and Cryptographic Module Engineering Controls	36
6.2.1. Cryptographic module standards and controls.....	36
6.2.2. Private key (n out of m) multi-person control.....	36
6.2.3. Private key escrow	36
6.2.4. Private key backup	36
6.2.5. Private key archival	36
6.2.6. Private key transfer into or from a cryptographic module	36
6.2.7. Private key storage on cryptographic module	36
6.2.8. Method of activating private key	37
6.2.9. Method of deactivating private key.....	37
6.2.10. Method of destroying private key	37
6.2.11. Cryptographic Module Rating.....	37
6.3. Other aspects of key pair management.....	37
6.3.1. Public key archival	37
6.3.2. Certificate operational periods and key pair usage periods.....	37
6.4. Activation data	37

6.4.1. Activation data generation and installation	37
6.4.2. Activation data protection	38
6.4.3. Other aspects of activation data	38
6.5. Computer security controls	38
6.5.1. Specific computer security technical requirements	38
6.5.2. Computer security rating	38
6.6. Life cycle technical controls	38
6.6.1. System development controls	38
6.6.2. Security management controls	38
6.6.3. Life cycle security controls	39
6.7. Network security controls	39
6.8. Time-stamping	39
7. CERTIFICATE, CRL, AND OCSP PROFILES	39
7.1. Certificate profile	39
7.1.1. Version number(s)	39
7.1.2. Certificate extensions	39
7.1.3. Algorithm object identifiers	40
7.1.4. Name forms	40
7.1.5. Name constraints	40
7.1.6. Certificate policy object identifier	40
7.1.7. Usage of Policy Constraints extension	40
7.1.8. Policy qualifiers syntax and semantics	41
7.1.9. Processing semantics for the critical Certificate Policies extension	41
7.2. CRL profile	41
7.2.1. Version number(s)	41
7.2.2. CRL and CRL entry extensions	41
7.3. OCSP profile	41
7.3.1. Version number(s)	41
7.3.2. OCSP extensions	41
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS	42
8.1. Frequency or circumstances of assessment	42
8.2. Identity/qualifications of assessor	42
8.3. Assessor's relationship to assessed entity	42
8.4. Topics covered by assessment	42
8.5. Actions taken as a result of deficiency	42
8.6. Communication of results	42
9. OTHER BUSINESS AND LEGAL MATTERS	43
9.1. Fees	43
9.1.1. Certificate issuance or renewal fees	43
9.1.2. Certificate access fees	43
9.1.3. Revocation or status information access fees	43
9.1.4. Fees for other services	43
9.1.5. Refund policy	43
9.2. Financial responsibility	43
9.2.1. Insurance coverage	43
9.2.2. Other assets	43

9.2.3. Insurance or warranty coverage for end-entities	44
9.3. Confidentiality of business information	44
9.3.1. Scope of confidential information	44
9.3.2. Information not within the scope of confidential information	44
9.3.3. Responsibility to protect confidential information	44
9.4. Privacy of personal information.....	44
9.4.1. Privacy plan.....	44
9.4.2. Information treated as private.....	44
9.4.3. Information not deemed private.....	44
9.4.4. Responsibility to protect private information.....	44
9.4.5. Notice and consent to use private information	45
9.4.6. Disclosure pursuant to judicial or administrative process.....	45
9.4.7. Other information disclosure circumstances.....	45
9.5. Intellectual property rights.....	45
9.6. Representations and warranties	45
9.6.1. CA representations and warranties	45
9.6.2. RA representations and warranties	45
9.6.3. Subscriber representations and warranties	46
9.6.4. Relying party representations and warranties	46
9.6.5. Representations and warranties of other participants	46
9.7. Disclaimers of warranties.....	46
9.8. Limitations of liability.....	46
9.9. Indemnities	46
9.10. Term and termination.....	47
9.10.1. Term.....	47
9.10.2. Termination	47
9.10.3. Effect of termination and survival	47
9.11. Individual notices and communications with participants	47
9.12. Amendments.....	47
9.12.1. Procedure for amendment.....	47
9.12.2. Notification mechanism and period	47
9.12.3. Circumstances under which OID must be changed	48
9.13. Dispute resolution provisions	48
9.14. Governing law	48
9.15. Compliance with applicable law	48
9.16. Miscellaneous provisions	48
9.16.1. Entire agreement.....	48
9.16.2. Assignment	48
9.16.3. Severability.....	48
9.16.4. Enforcement (attorneys' fees and waiver of rights)	49
9.16.5. Force Majeure	49
9.17. Other provisions.....	49

1. INTRODUCTION

1.1. Overview

Laboratório de Instrumentação e Física Experimental de Partículas (LIP) is a Portuguese non-profit technical and scientific association for the research in the field of experimental High Energy Physics and associated computing and instrumentation.

LIPCA is a Portuguese Certification Authority maintained by LIP. The main objective of the LIPCA is to issue certificates to support Portuguese academic research activities in the Grid computing domain.

This document is a combined Certificate Policy (CP) and Certification Practice Statement (CPS). It describes the set of procedures followed by the LIPCA in issuing certificates, as well as the responsibilities of the involved parties.

The document is based on the structure suggested by the RFC 3647.

This document describes:

- ✓ Applicability of certificates signed by the LIPCA
- ✓ Operational practices used by the LIPCA

1.2. Document name and identification

Title: LIPCA Certificate Policy and Certification Practice Statement.
Version: 5.3
Date: 15 January 2015
Expiration: This document is valid until further notice.
ASN.1 OID: The following unique Object Identifier (OID) identifies this CP/CPS:
1.3.6.1.4.1.9846.10.1.1.5.3

The next table describes the meaning of the OID:

1.3.6.1.4.1	Prefix for IANA private enterprises
9846	LIP registered identifier
10	Certification Authorities
1	LIPCA
1	CP/CPS
5.3	Major and minor CP/CPS version number

1.3. PKI participants

1.3.1. Certification authorities

The LIPCA issues certificates to the Portuguese academic community and related entities. All certificates issued under this CP/CPS must be signed by the LIPCA.

1.3.2. Registration authorities

Registration authorities (RAs) will be created as needed to support the academic research activities in the country. RAs must be operated by organizations related with the Portuguese academic community. RAs must sign an agreement contract with the LIPCA where they assume the obligation of following the procedures imposed by the CA for their operation and authentication of requests.

A generic RA provides authentication services to any certificate requester (see 1.3.3).

The LIPCA operates the LIP-Lisbon RA.

1.3.3. Subscribers

The LIPCA issues certificates for entities related with the following organizations:

- ✓ Portuguese academic organizations (e.g. Universities and Education Institutes);
- ✓ Portuguese academic research centers (public and private non-profit).

The subject entities for certificates are of the following types:

- ✓ Employees, researchers and students related with the above organizations;
- ✓ Computer systems and services related with the above organizations;

1.3.4. Relying parties

Entities that need to verify the identity and validity of certificates issued by LIPCA.

1.3.5. Other participants

No stipulation

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Certificate issued by the LIPCA can be used for:

- ✓ Authentication
- ✓ Confidentiality
- ✓ Integrity

1.4.2. Prohibited certificate uses

No stipulation

1.5. Policy administration

1.5.1. Organization administering the document

The LIPCA is responsible to drafting, registering, maintaining and updating this CP/CPS.

The LIPCA contacts are:

LIP Certification Authority

LIP

Av. Elias Garcia 14, 1º

1000-149 Lisboa

Portugal

Phone: (+ 351) 217973880

Fax: (+ 351) 217934631

E-mail: ca@lip.pt

1.5.2. Contact person

Nuno Dias

LIP

Av. Elias Garcia 14, 1º

1000-149 Lisboa

Portugal

Phone: (+ 351) 217973880
Fax: (+ 351) 217934631
E-mail: ndias@lip.pt

1.5.3. Person determining CPS suitability for the policy

The LIPCA Manager is the person responsible to determining CPS suitability for this policy.

1.5.4. CPS approval procedures

Changes in CP/CPS will be submitted and approved internally by LIPCA, then will be submitted to EUGridPMA to approved to be used in the Trust domain of IGTF.

1.6. Definitions and acronyms

C	Country
CA	Certification Authority
CN	Common Name
CDROM	Compact Disc Read Only Memory
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
DN	Distinguish name
DNS	Domain Name System
EUGridPMA	European Policy Management Authority for Grid Authentication
LDAP	Lightweight Directory Access Protocol
LIP	Laboratório de Instrumentação e Física Experimental de Partículas
LIPCA	LIP Certification Authority
MIME	Multi-purpose Internet Mail Extensions
NTP	Network Time Protocol
O	Organization
OID	Object Identifier
OU	Organizational Unit
PKI	Public Key Infrastructure
RA	Registration Authority
RDN	Relative Distinguished Name
SSL	Secure Sockets Layer
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier
URL	Universal Resource Locator

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The LIPCA repository is available at <http://ca.lip.pt>

2.2. Publication of certification information

The LIPCA publishes the following information through its online repository:

- ✓ The CA root certificate;
- ✓ The latest CRL;
- ✓ The CP/CPS and other previous versions used to issue certificates;
- ✓ Other relevant information.

2.3. Time or frequency of publication

New information will be published as soon as available.

CRLs must be issued immediately after a certificate revocation or at least 7 days before CRL expiration. CRLs must be published immediately after issued.

2.4. Access controls on repositories

Currently the LIPCA does not impose any access control restrictions to the information available on its public web site.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

The certificate subject names used as unique certificate identifiers obey to the X.501 standard. Subject names have a fixed and a variable component. The certificate subject names start with the fixed component to which a variable component is appended to make it unique.

The fixed component is common to all certificates issued by the LIPCA and is used to identify the namespace that can be signed by the CA. The fixed component is as follows:

/C=PT/O=LIPCA

The variable component is as follows:

An optional Location (L) RDN identifies the location (City) of a RA, which provides authentication services to any certificate requester.

A mandatory organization (O) RDN identifies the subject affiliated Institution. The organization name must be meaningful and correspond to a real organization name as stated in section 3.1.2.

An optional organizational unit name (OU) may be specified when the certificate subject is related with:

- a) A sub-organization of the main organization with legal existence. This can be a University foundation, faculty or research institute with autonomy;
- b) A branch or department of the main organization;
- c) A non-academic organization related with the main academic organization. For instance if a company is working in collaboration with a University in a grid computing research project, certificates would be granted with the University as the organization and the company as the organizational unit.

A common name (CN) that uniquely identifies the subject name within the CA namespace must follow the organization names.

The CN must have one of the following formats:

- ✓ The common name must be obtainable from the subject real name as stated in section 3.1.2.
- ✓ For computer systems or services the common name is the full-qualified DNS name of the system, prefixed with an optional "host/" for a system or a mandatory "service/" for a service where the word service must be replaced by the name of the actual service eg. ldap, smtp etc.
- ✓ For robots the common name must be prefixed by the string "robot:" follow by the requester name.

The generic format for a person subject is as follows:

/C=PT/O=LIPCA/O=organization/OU=org-unit/CN=subject-name

The generic format for a system subject is as follows:

/C=PT/O=LIPCA/O=organization/OU=org-unit/CN=host-dns-name

The generic format for a service subject is as follows:

/C=PT/O=LIPCA/O=organization/OU=org-unit/CN=service/host-dns-name

The generic format for a robot is as follows:

/C=PT/O=LIPCA/O=organization/OU=org-unit/CN=robot:subject-name

The generic format of a certificate requested from a generic RA is as follow:

/C=PT/O=LIPCA/L=City/O=organization/OU=org-unit/CN=(see examples above)

The common names must be encoded as PrintableStrings according with RFC1778 and RFC2252. The characters allowed in the common names of personal certificates are as follows:

'0' – '9', 'a' – 'z', 'A' – 'Z', '-', ' ' ,

In addition the character '.' (period) and the character '/' (slash) are allowed in host and service certificates. The period must be used to separate the DNS host name components and the slash must be used to separate the service name from the DNS host name. The character ":" (colon) is allowed in robot names as a separator between the robot prefix and the requester name.

E-mail addresses must be structured according with RFC822.

3.1.2. Need for names to be meaningful

The names specified in the common name, in the organization name and in the organizational unit must be meaningful. The names must be related with the subject organization and with the subject real name.

For persons the common name must be obtainable from the legal person name as presented in an official governmental identity document such as a passport or identity card.

For server (machine) or service certificates the common name must be the full-qualified DNS name.

3.1.3. Anonymity or pseudonymity of subscribers

All certificates issued by the LIPCA must be associated to a person, and this person must have been authenticated through the procedures documented in this CPS/CPS. Anonymity or pseudonymity are not supported.

3.1.4. Rules for interpreting various name forms

Refer to section 3.1.1 and 3.1.2

3.1.5. Uniqueness of names

All certificate subject names must be unique. Since Portuguese person names are usually quite long it is not required that a subject name contains all the person real names. However for persons with three or more names at least three should be specified in the common name in order to avoid clashes. In cases where the person name is not sufficient to differentiate two certificates then numbers will be added to the end of the common name.

Certificate subject names can not be reused by a different person, even if the certificate has expired.

3.1.6. Recognition, authentication, and role of trademarks

The LIPCA does not guarantee that the subject names of the certificates issued will contain the requested trademarks.

Name disputes are managed according to the Portuguese law.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

The possession of private key is considered proven if the digital signature of the certificate signing request (CSR) is verified using the public key contained in the CSR.

3.2.2. Authentication of organization identity

The relation between the subscriber and the organization or organizational unit mentioned in the subject name must be proved through an organization identity card

or organization official document stamped and signed by an official representative of the organization. In case of doubt the RA may take any required steps to inquire about the relation of the subscriber with the organization. The request may optionally be authorized through the digital signature of an official representative of the organization in possession of a valid LIPCA issued certificate.

Organizations can provide to the RAs access to databases that can be used to verify the relation of the requester with the organizations. In this case the RA must produce and keep a written document where it declares that the relation of the requester with the organization was performed according with the data in the database provided by the organization. The accuracy of the databases contents is of the responsibility of the organizations. The access to the database information must be performed in a secure way.

The method used to verify the relation between the subscribers and the organization or organizational unit must be specified in the RA operation rules document.

3.2.3. Authentication of individual identity

Individuals are authenticated through the presentation of a valid official governmental identity document such as a passport or identity card containing a photograph. The individual must present himself (physically) to a LIPCA Registration Authority (RA) for the identity to be verified.

For generic RA's, authentication by videoconference is allowed when the requester location distance to the RA is not feasible to a physical presence.

For each authentication the RA will record:

- ✓ The type, identification number and name in the identification document presented by the subject to be authenticated;
- ✓ The document(s) used as proof of relation with the organization(s);
- ✓ The E-mail and phone number of the requester;
- ✓ The identification of the person that has performed the authentication;
- ✓ The date, time and place of the authentication;
- ✓ Whether the authentication was successful or not and why.

In special cases where the RA is inside the organization under which the certificate is being requested other forms of authentication can be acceptable such as personal acquaintance of the requester with the RA personnel. In this case physical presence may not be necessary and can be replaced by phone contact. However all other steps including the record of the above information must be performed. The certification record must still contain the identification document number and type and a proof of the relation of the individual with the organization. This kind of authentication is of the complete responsibility of the RA.

For host, service or robot certificates an email signed with a LIPCA issued certificate corresponding to the system administrator or system responsible could replace the face to face authentication.

The specific method(s) used to verify the identity must be specified in the RA operation rules document.

3.2.4. Non-verified subscriber information

No stipulation

3.2.5. Validation of authority

The RA corresponding to the organization mentioned in the distinguish name of the certificate sign request will verify whether the requester has the right to request a certificate for the intended host or service.

3.2.6. Criteria for interoperation

No stipulation

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

For re-key a new certificate with the same DN must be requested. Then an email signed with the old but still valid certificate must be sent to the CA (The personal certificate of the requester can be used to sign the mail in case of host, service or robot certificate request). The mail must contain the serial number of the new request.

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 distinguish name of the certificate sign request. Although a proof of relation is required the re-key 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/electronic mail.

Re-verification of the identity of the requester, for certificates re-keyed consecutively for more than 5 years is mandatory. The process is the same described in 3.2.3

3.3.2. Identification and authentication for re-key after revocation

Re-key requests for expired certificates are not accepted. In this case the procedure for obtaining a new certificate must be followed.

3.4. Identification and authentication for revocation request

Revocation requests from the subscriber must be authenticated by:

- ✓ The procedure in the section 3.2.3.
- ✓ A signed E-mail message to ca@lip.pt. The E-mail message must be signed with a valid non-expired certificate.
- ✓ Through the LIPCA online interface, using a PIN code (obtained in the online interface when requesting the certificate), or signing the request with a valid certificate.

The LIPCA 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. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

The LIPCA issues certificates to Portuguese academic organizations and related entities for:

- ✓ Persons from eligible organizations;
- ✓ Hosts administrated by eligible organizations;
- ✓ Services running on hosts administrated by eligible organizations.
- ✓ Robots running on hosts administrated by eligible organizations.

4.1.2. Enrollment process and responsibilities

The application for a LIPCA certificate is performed online at the LIPCA web site. The LIPCA provides the mechanisms through which the key generation and request submission must be performed.

The enrollment process is as follows:

- ✓ Fill in the form in the LIPCA web site;
- ✓ Generate a key pair performed in the requester browser, the encrypted private key is stored in the system of the requester;
- ✓ Send the CSR to the appropriate RA;
- ✓ Send the paper form to the RA;

The subscriber's obligations are as follows:

- ✓ Read and accept the policies and procedures published in the CP/CPS document;
- ✓ Keep the private key safe and protected. The subscribers are fully responsible for the private key confidentiality and integrity;
- ✓ Use a strong pass-phrase with a minimum of 16 characters to protect the private key of personal certificates;
- ✓ Notify the CA in case of possible private key compromise;
- ✓ Notify the CA in case of key destruction and loss;
- ✓ Notify the CA when the certificate is no longer required;
- ✓ Notify the CA when the information in the certificate becomes wrong or inaccurate;
- ✓ Use the certificates only for the purposes authorized by the CP/CPS document;
- ✓ Must accept the treatment and conservation of their personal data used in the request verification process.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

The RA must perform the following actions after receiving a certificate request:

- ✓ Authenticate the subject identity;
- ✓ Verify the relation of the subject with the organization;
- ✓ Verify the CSR signature;
- ✓ Verify that the request obeys to the LIPCA subject distinguish name scheme;
- ✓ Verify that the subject distinguish name is unique;
- ✓ Verify that the key has 1024 bits.

4.2.2. Approval or rejection of certificate applications

After successful authentication of the CSR, the RA will approve and sign the request with the personal certificate of the RA operator. An automatic process will inform the CA of a pending approved certificate request.

A certificate request will be rejected if it does not meet the CP/CPS requirements or if the RA fails to authenticate the requester within seven working days. The RA will do its best effort to inform the requester.

4.2.3. Time to process certificate applications

The time to process certification request depends mostly of authentication and identification process, but typical processing time will be ten working days.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

The actions performed by the LIPCA to issue the certificates are as follow:

- ✓ Transfer the CSR from the online machine to the offline machine, through a USB Pen;
- ✓ Verify the RA operator signature and the certificate request content;
- ✓ Verify the DN uniqueness;
- ✓ Issue the certificate;
- ✓ Transfer the certificate to the online machine through a USB Pen.

4.3.2. Notification to subscriber by the CA of issuance of certificate

The subscriber will be notified by e-mail about the certificate issuance. The e-mail includes information on how to download the certificate from the LIPCA web site.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

In the absence of mail delivery errors the certificate issuance notification is considered received by the subscriber. The reception of the e-mail notification implies the automatic acceptance of the issued certificate by the subscriber. If a user wants to reject a certificate it must submit a revocation request.

4.4.2. Publication of the certificate by the CA

The certificates will not be published by the LIPCA.

4.4.3. Notification of certificate issuance by the CA to other entities

No stipulation.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

Certificates issued by the LIPCA and corresponding private keys must be used in accordance with the terms established in session 1.4.

4.5.2. Relying party public key and certificate usage

The relying party obligations are as follows:

- ✓ Accept the policies and procedures published in the CP/CPS document;
- ✓ Use the certificates only for the purposes authorized by the CP/CPS document;
- ✓ Verify the digital signature of digital messages and verify the digital signature of the CA;
- ✓ Verify the certificate validity or revocation while performing the certificate authentication;
- ✓ Verify the authenticity of the LIPCA root certificate.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

The LIPCA does not perform renewal of certificates using the same key pair.

4.6.2. Who may request renewal

Not applicable

4.6.3. Processing certificate renewal requests

Not applicable

4.6.4. Notification of new certificate issuance to subscriber

Not applicable

4.6.5. Conduct constituting acceptance of a renewal certificate

Not applicable

4.6.6. Publication of the renewal certificate by the CA

Not applicable

4.6.7. Notification of certificate issuance by the CA to other entities

Not applicable

4.7. Certificate re-key**4.7.1. Circumstance for certificate re-key**

Certificate re-key can only be obtained for valid certificates. Requests can be performed during the last 30 days before the expiration date.

LIPCA Root Certificate can be re-key before the expiration date upon suspected of compromised private key, or when a requested for an one year validity End Entity Certificate, can't be approved because supersedes the validity of the LIPCA Root Certificate.

4.7.2. Who may request certification of a new public key

LIPCA Administrators are the only eligible persons to request a LIPCA Root Certificate re-key.

No restrictions are imposed to certification of a new public key by other entities, provided they comply with this CP-CPS.

4.7.3. Processing certificate re-keying requests

The procedures to process re-keying certificate requests are the same as the ones for initial certificate issuance. However the identification and authentication process can be avoided by sending to the RA a signed e-mail with the subscriber valid certificate, containing the CSR request number.

4.7.4. Notification of new certificate issuance to subscriber

see 4.3.2

4.7.5. Conduct constituting acceptance of a re-keyed certificate

see 4.4.1

4.7.6. Publication of the re-keyed certificate by the CA

End Entities certificates, see 4.4.2

The LIPCA Root Certificate will be published on the LIPCA website.

4.7.7. Notification of certificate issuance by the CA to other entities

End Entities certificates, see 4.4.3

Upon issuance of a new LIPCA Root Certificate, EugridPMA, TACAR and the relying parties will be informed.

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

Certificate modification is not permitted, if the information contained in the certificate is incorrect, the certificate must be revoked and a new one must be requested.

4.8.2. Who may request certificate modification

Not applicable

4.8.3. Processing certificate modification requests

Not applicable

4.8.4. Notification of new certificate issuance to subscriber

Not applicable

4.8.5. Conduct constituting acceptance of modified certificate

Not applicable

4.8.6. Publication of the modified certificate by the CA

Not applicable

4.8.7. Notification of certificate issuance by the CA to other entities

Not applicable

4.9. Certificate revocation and suspension**4.9.1. Circumstances for revocation**

Certificates must be revoked on termination of the subscriber relationship with the institution, violation of CP/CPS rules and obligations by the subscriber, loss or suspected compromise of the private key.

4.9.2. Who can request revocation

Revocation of a certificate can be requested by:

- ✓ The certificate subscriber;
- ✓ A host, service or robot certificate can be revoked by the related system administrator or system responsible;
- ✓ Any entity presenting proof of the certificate misuse;
- ✓ Any entity presenting proof of the private key compromise;
- ✓ Any entity presenting proof of the modification of the subscriber's data;

An entity can be a person, organization, an automatic process, etc ...

4.9.3. Procedure for revocation request

Revocation requests must be made using one of the following methods:

- ✓ Through the LIPCA online interface, using a PIN or signing the request with a LIPCA valid certificate;
- ✓ By signed e-mail with a valid LIPCA certificate;

In emergency cases the revocation request could be made via oral communication, by phone for example, in this case or when RA's are acting on their own the request could be made through the RA interface.

Independently from the method used to request the revocation, the source of the request must be authenticated using the procedures described in 3.2.3. It is considered authenticated when the request is signed with a valid LIPCA certificate.

4.9.4. Revocation request grace period

No grace period is defined, the subscriber must act as soon as possible upon raised the conditions to request the revocation.

4.9.5. Time within which CA must process the revocation request

The revocation request must be process with high priority.

4.9.6. Revocation checking requirement for relying parties

Relying parties must check the status of the certificates on which they wish to rely, against the last CRL issued by LIPCA.

4.9.7. CRL issuance frequency (if applicable)

CRLs are issued immediately after a certificate revocation or at least 7 days before expiration.

4.9.8. Maximum latency for CRLs (if applicable)

CRLs are published immediately after issuance.

4.9.9. On-line revocation/status checking availability

The CRL is published in the CA web site with a lifetime of 30 days, no other checking is available.

4.9.10. On-line revocation checking requirements

On-line checking mechanism is not available.

4.9.11. Other forms of revocation advertisements available

No other forms of revocation advertisements are available.

4.9.12. Special requirements re key compromise

No stipulation.

4.9.13. Circumstances for suspension

The LIPCA does not support certificate suspension.

4.9.14. Who can request suspension

No stipulation.

4.9.15. Procedure for suspension request

No stipulation.

4.9.16. Limits on suspension period

No stipulation.

4.10. Certificate status services

4.10.1. Operational characteristics

The LIPCA CA Root certificate and CRLs will be published in the online repository.

4.10.2. Service availability

The service is running continuously (24x7). Nevertheless downtime can happen due to maintenance or unforeseen problems.

4.10.3. Optional features

No stipulation.

4.11. End of subscription

The subscription ends when:

- ✓ The certificate expires;
- ✓ The affiliation of the subscriber with the organization ends. In this case a revocation request must be performed.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

All keys are generated in the subscriber browser and stored in its key store. It is a subscriber obligation to maintain a backup of the key. The LIPCA does not have access to the subscriber's private keys and thus does not provide backup for private keys.

4.12.2. Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical controls

5.1.1. Site location and construction

The LIPCA equipment is located at the LIP Computer Centre facilities in Lisbon.

5.1.2. Physical access

The access to the LIP Computer Centre has restricted access by physical key and access code, only authorized personal have access.

5.1.3. Power and air conditioning

The CA systems are protected by uninterrupted power supplies. Environment temperature in the room containing CA related equipment is maintained at appropriate levels by air conditioning systems.

5.1.4. Water exposures

The LIP Computer Centre has water flood probes.

5.1.5. Fire prevention and protection

The LIP Computer Centre has fire detection and extinguishing system.

5.1.6. Media storage

All media storage used in the operation of LIPCA (Backup Tapes, CD's, etc) are kept in a waterproof safe.

5.1.7. Waste disposal

Waste carrying potential confidential information is physically destroyed before sent to the trash.

5.1.8. Off-site backup

Off-site backups are made to a secondary Computer Center located in Lisbon, the backups are encrypted before sent.

5.2. Procedural controls

5.2.1. Trusted roles

The following roles are defined within the LIPCA:

- ✓ CA Administrator: is the overall responsible for the administration of the CA covering all administrative and technical aspects of the CA activities.
- ✓ CA Operator: issues certificates and CRLs, revokes certificates and performs backups.
- ✓ RA Administrator: is the responsible for a RA, appoints the RA Operator.
- ✓ RA Operator: identifies and authenticates requests.
- ✓ Auditor: verifies the procedures and ensures the proper compliance of the CA operation with the CP/CPS and operation documents.

5.2.2. Number of persons required per task

Ideally there should be at least one person per role in case of Administrators and two persons in case of Operators. However it is considered that one person can accumulate several roles within the same organization.

5.2.3. Identification and authentication for each role

All the roles are well identified by the CA Administrator, only the RA operators need to authenticate themselves when operating the RA interface.

5.2.4. Roles requiring separation of duties

No stipulation.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

CA personnel is recruited from the LIP Computer Centre team. RAs are responsible for the recruitment of their own personnel.

5.3.2. Background check procedures

No stipulation.

5.3.3. Training requirements

Training is given by LIPCA own staff when a new RA is created.

5.3.4. Retraining frequency and requirements

Additional training will be available if required or asked by RAs.

5.3.5. Job rotation frequency and sequence

No job rotation is performed.

5.3.6. Sanctions for unauthorized actions

Unauthorized actions will be analyzed on the light of organization statutes and Portuguese Law.

5.3.7. Independent contractor requirements

No Stipulation.

5.3.8. Documentation supplied to personnel

The LIPCA provides a copy of the CP/CPS document and the LIPCA Operations manual, other documentation could be provided as necessary.

5.4. Audit logging procedures

5.4.1. Types of events recorded

All operations in a lifecycle of a certificate are recorded. The operation of the machines is also recorded, as reboots, successful/unsuccessful logins, http requests, etc.

5.4.2. Frequency of processing log

The logs are archived weekly. Every day an automatic system checks the logs and makes a report.

5.4.3. Retention period for audit log

Logs are kept for a minimum of five years.

5.4.4. Protection of audit log

Only the CA Administrator has access to the logs. All the logs are protected against modification.

5.4.5. Audit log backup procedures

Backups of the logs are made regularly to tape.

5.4.6. Audit collection system (internal vs. external)

The audit collection system is internal to the LIPCA.

5.4.7. Notification to event-causing subject

Subjects causing audit events are not notified.

5.4.8. Vulnerability assessments

Audit data is run daily through a simple tool that can identify potential attempts to breach the security of the system, when necessary other tools can be used.

5.5. Records archival

5.5.1. Types of records archived

All audit data, certificate application information, and documentation supporting certificate applications are archived.

5.5.2. Retention period for archive

Archives are kept for a minimum of five years.

5.5.3. Protection of archive

Only the CA Administrator has access to the archive. The archive is protected against modification.

5.5.4. Archive backup procedures

Backups of the archives are made regularly to tape.

5.5.5. Requirements for time-stamping of records

Archive records are time-stamped. For online systems the clock is synchronized through NTP. For offline systems the clock is manually set and periodically verified.

5.5.6. Archive collection system (internal or external)

The archive collection system is internal to the LIPCA.

5.5.7. Procedures to obtain and verify archive information

When necessary a copy of the archive information will be made and verified.

5.6. Key changeover

All keys are generated in the subscriber browser, no keys will be provided to end users.

LIPCA Root keys are generated in the offline machine with a lifetime no longer than 20 years. Upon LIPCA Root key changeover, only the new key will be used for certificate signing purposes.

The older valid certificate will be available to verify old signatures, and issue CRLs, until all the certificates signed using the associated private key have expired.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

In case of incident or compromise the procedures described in 5.7.2 will be followed.

5.7.2. Computing resources, software, and/or data are corrupted

In case of corruption or hardware malfunction, the CA systems will be restored from the last good backup, and repaired.

If a good backup cannot be identified or in case of major disaster where critical CA information is completely lost the CA will cease operations. As in the case of CA private key compromise the systems will be reinstalled from scratch and new keys generated.

5.7.3. Entity private key compromise procedures

If an end entity private key is compromised, the revocation procedure must be followed.

If the LIPCA private key is compromised the following steps apply:

- ✓ Terminate the issuance of certificates and CRLs;
- ✓ Notify the subscribers and relaying parties;
- ✓ Generate a new CA key pair, a new CA certificate and new CRL.
- ✓ Publish the new information on the LIPCA site.

5.7.4. Business continuity capabilities after a disaster

No stipulation.

5.8. CA or RA termination

Upon a RA termination, the LIPCA will:

- ✓ Notify subscribers of certificates associated with the RA;
- ✓ Revoke all certificates still valid associated with the RA;
- ✓ Archive as possible the records related with the RA.

Upon termination of the CA, LIPCA will:

- ✓ Notify the LIPCA subordinate RAs;
- ✓ Notify subscribers;
- ✓ Terminate the issuance and distribution of certificates and CRLs;
- ✓ Notify relying parties as wide as possible;
- ✓ Destroy the private key associated with the public key of the CA;
- ✓ Archive the CA records, these will remain if possible under the custody of LIP.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

The key pair used by the CA is generated by the LIPCA manager on a machine not connected to the network.

Each subscriber must generate his own key pair which is done in the requester browser.

6.1.2. Private key delivery to subscriber

The LIPCA does not generate private keys to end entities.

6.1.3. Public key delivery to certificate issuer

At the moment of the generation of the key pair, a request containing the public key is created online in the RA server, this is done using an SSL session.

The transfer of the request to the CA is made internally to the server.

6.1.4. CA public key delivery to relying parties

The LIPCA certificate can be obtained at the LIPCA online repository.

6.1.5. Key sizes

The LIPCA root certificate must have a key size of 2048 bits. End entity certificates must have a key size of at least 1024 bit.

6.1.6. Public key parameters generation and quality checking

No stipulation.

6.1.7. Key usage purposes (as per X.509 v3 key usage field)

Digital Signature, Key Encipherment, Data Encipherment

The LIPCA end entity certificates may be used for:

- ✓ Authentication
- ✓ Data and Key Encipherment
- ✓ Messages integrity
- ✓ Session establishment and sign proxy certificates.

The LIPCA CA root certificate may be used for:

- ✓ Certificate signing
- ✓ CRLs signing

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

Keys for end entities are generated on the subscriber browser using the cryptographic module provided by the browser. The subscriber must protect the private key with a passphrase of at least 16 characters.

The CA private key is generated using OpenSSL and is protected by a passphrase of at least 16 characters.

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

Not supported.

6.2.3. Private key escrow

Not supported.

6.2.4. Private key backup

Backups of the LIPCA private key are kept encrypted in recordable media inside a safe. A hardcopy pass phrase of LIPCA private key, is kept in a different safe, accessible only to authorized personnel.

Subscribers are responsible for the backup of their private keys.

6.2.5. Private key archival

No stipulation.

6.2.6. Private key transfer into or from a cryptographic module

In order to use it the private key can be unlocked using the passphrase.

6.2.7. Private key storage on cryptographic module

The LIPCA private key is stored encrypted. The end entities private keys must be stored encrypted.

6.2.8. Method of activating private key

The private key is activated by entering a passphrase.

6.2.9. Method of deactivating private key

Upon the end of operations, the erase of the RAM is enough to deactivate the private key.

6.2.10. Method of destroying private key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other aspects of key pair management

6.3.1. Public key archival

All certificates issued by LIPCA are archived in recordable media on a safe.

6.3.2. Certificate operational periods and key pair usage periods

The lifetime of a subscriber certificate is 365 days, no restriction is imposed to the usage period of the subscriber key pair.

The lifetime of LIPCA Root certificate is 20 Years, after the expiration date, the certificate must not be used anymore.

6.4. Activation data

6.4.1. Activation data generation and installation

Private keys must be protected by a passphrase of at least 16 characters.

6.4.2. Activation data protection

The passphrase needed to activate the end entities private key must not be shared. The access to the passphrase of the CA private key is limited to the Administrator and Operadores of the LIPCA.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

The security technical requirements are as follows:

- ✓ The operating systems of CA/RA systems are maintained at a high level of security by applying all the relevant patches;
- ✓ Monitoring is performed to detect unauthorized software changes;
- ✓ The CA systems configuration is reduced to the base minimum;
- ✓ The signing machine is kept powered off between uses.
- ✓ All CA/RA operations are authenticated by certificate and username/password.
- ✓ All connections are made through a secure channel.

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

No stipulation.

6.6.3. Life cycle security controls

No stipulation.

6.7. Network security controls

The CA signing machine is kept offline.

The online machine is protected by a firewall and the network services reduced to the minimum necessary.

6.8. Time-stamping

The LIPCA online system has its time synchronized through the network time protocol, using as source the keeper of the Portuguese official time.

The offline machine has its time manually synchronized by the LIPCA operators.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

7.1.1. Version number(s)

The LIPCA issues X.509 v3 certificates.

7.1.2. Certificate extensions

The extensions present in LIPCA end entity certificates are as follow:

Basic Constraints:	critical, CA:FALSE
Key Usage:	critical, Digital Signature, Key Encipherment, Data Encipherment
Extended Key Usage:	<i>Personal, Robot:</i> TLS Web Client Authentication, E-mail Protection <i>Server:</i> TLS Web Server Authentication, TLS Web Client Authentication
Subject Key Identifier:	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey.
Authority Key Identifier:	keyid: 160-bit SHA-1 hash of the value of the BIT STRING authorityPublicKey.

Subject Alternative Name:	<i>Personal, Robot:</i> Subject e-mail Server: Server Fully Qualified Domain Name
Issuer Alternative Name:	CA e-mail
Certificate Policies:	OID of the CP/CPS in use at the time of the issuance of the certificate. OID of the policy used by EuGRIDPMA to approve the CP/CPS
CRL Distribution Points:	HTTP URI of the CRL

The extensions present in LIPCA self sign certificates are as follows:

Basic Constraints:	critical, CA:TRUE
Subject Key Identifier:	160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey.
Key Usage:	critical, Certificate Sign, CRL Sign

7.1.3. Algorithm object identifiers

The OIDs for algorithms used for signatures of end entities certificates issued by LIPCA Certification Authority are according to:

- ✓ hash function: sha512 2.16.840.1.101.3.4.2.3
- ✓ encryption: rsaEncryption 1.2.840.113549.1.1.1
- ✓ signature: sha512RSA 1.2.840.113549.1.1.13

7.1.4. Name forms

See 3.1.1

7.1.5. Name constraints

See 3.1.1 and 3.1.2

7.1.6. Certificate policy object identifier

Each LIP certificate policy has a unique associated object identifier (OID). The OID for this policy is described in 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 Policies extension

No Stipulation.

7.2. CRL profile

7.2.1. Version number(s)

The LIPCA issues X.509 v2 CRLs compliant with RFC 5280

7.2.2. CRL and CRL entry extensions

The extensions present in LIPCA CRL are as follow:

Authority Key Identifier: 160-bit SHA-1 hash of the value of the BIT STRING
subjectPublicKey.
DirName: Distinguish Name of LIPCA
serial: Serial number of the LIPCA ROOT Certificate

CRL Number: Incremental number

7.3. OCSP profile

The LIPCA do not support OCSP.

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or circumstances of assessment

The LIPCA may be audited by other trusted CAs or relying parties to verify its compliance with the rules and procedures specified in the CP/CPS.

The LIPCA 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 compliance audit the LIPCA will take the appropriate measures to correct these deficiencies as soon as possible.

8.2. Identity/qualifications of assessor

No stipulation.

8.3. Assessor's relationship to assessed entity

Assessments are made by LIPCA own personnel.

If other trusted CAs or relying parties request an external audit or assessment they must provide the means and pay the costs.

8.4. Topics covered by assessment

The assessment will verify that the LIPCA operation comply with the latest version of the LIPCA CP/CPS.

8.5. Actions taken as a result of deficiency

If as result of the assessment deficiencies are detected, the LIPCA will take all the steps to correct the problems.

8.6. Communication of results

The results of the assessment must be communicated to the LIPCA manager. Upon request the results can be available to trusted CAs and relying parties.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

No fees are charged for the services of LIPCA.

9.1.1. Certificate issuance or renewal fees

See 9.1

9.1.2. Certificate access fees

See 9.1

9.1.3. Revocation or status information access fees

See 9.1

9.1.4. Fees for other services

See 9.1

9.1.5. Refund policy

See 9.1

9.2. Financial responsibility

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

9.2.1. Insurance coverage

No stipulation.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

No stipulation.

9.3. Confidentiality of business information**9.3.1. Scope of confidential information**

No stipulation.

9.3.2. Information not within the scope of confidential information

No stipulation.

9.3.3. Responsibility to protect confidential information

No Stipulation.

9.4. Privacy of personal information**9.4.1. Privacy plan**

No stipulation.

9.4.2. Information treated as private

Information obtained in the verification of the identity of the subscriber that is not present in the certificate and is not public is considered confidential.

9.4.3. Information not deemed private

See 9.4.2

9.4.4. Responsibility to protect private information

The LIPCA and associated RAs are responsible for the protection of private information.

9.4.5. Notice and consent to use private information

Confidential information can be released upon owner's agreement.

9.4.6. Disclosure pursuant to judicial or administrative process

Confidential information can be released upon a Portuguese court order.

9.4.7. Other information disclosure circumstances

No stipulation.

9.5. Intellectual property rights

The LIPCA do not claim intellectual property rights on CP/CPS, certificates, names, and keys.

This document is partly based on the following documents:

- ✓ CP/CPS of LIPCA version 4.2
- ✓ CP/CPS of the AUSTRIANGRID CA version 1.2.0
- ✓ CP/CPS of UK eScience version 1.4

This document can be copied as a whole or partly provided acknowledgment is done about the source.

9.6. Representations and warranties

9.6.1. CA representations and warranties

For the best of LIPCA knowledge the information contained in the certificates and CRLs is accurate, no other warranties are accepted.

9.6.2. RA representations and warranties

RAs will follow the steps described in the CP/CPS to identify and authenticate the requesters at the best of their knowledge, no other warranties are accepted.

9.6.3. Subscriber representations and warranties

By requesting a certificate from LIPCA the subscriber are obliged to follow what is stipulated in the CP/CPS, in particular to protect the private key and inform without delay the LIPCA if the private key associated with the certificate is lost or compromised.

9.6.4. Relying party representations and warranties

Relying parties must check the validity of the certificates issued by LIPCA against the LIPCA Root Certificate and CRL.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7. Disclaimers of warranties

The LIPCA uses software and procedures that at its best knowledge do what is described in the CP/CPS, however no warranties are made about their full correctness. The LIPCA is not responsible for any problem or damage arising from the use of the certificates issued by LIPCA.

9.8. Limitations of liability

The LIPCA and associate RAs will not be held liable for any problems arising from its operation or use made of certificates it issues.

9.9. Indemnities

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

9.10. Term and termination

9.10.1. Term

This document becomes effective when published on the public LIPCA web site
No expiration date is set.

9.10.2. Termination

This document is effective until a new version is published.

9.10.3. Effect of termination and survival

This document remains available at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

9.11. Individual notices and communications with participants

Communications by e-mail with content that need to be confirmed must have the sender authenticated by a signed e-mail with a LIPCA certificate.

9.12. Amendments

9.12.1. Procedure for amendment

Amendments to this document must follow the some procedure describe in 1.5.4.
Minor changes like spelling corrections or layout format modifications are not considered amendments.

9.12.2. Notification mechanism and period

The LIPCA will inform relying parties and subscribers affected by the changes by e-mail.

9.12.3. Circumstances under which OID must be changed

Amendments to the document (see 9.12.1) will change the OID of the document. Minor changes will change the minor number, major changes will change the major number. The decisions regarding the OID changes are made by the LIPCA Administrator.

9.13. Dispute resolution provisions

Disputes arising out of the CP/CPS will be resolved by the LIPCA Administrator.

9.14. Governing law

The law governing the interpretation of this CP/CPS document is the Portuguese law.

Legal disputes arising from the operation of the LIPCA will be resolved according to the Portuguese law.

9.15. Compliance with applicable law

The operation of the LIPCA must comply with the Portuguese law.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

This CP/CPS document supersedes all prior understandings, written or oral, between the parties.

9.16.2. Assignment

No stipulation.

9.16.3. Severability

If some clause of this document is considered invalid by a Portuguese court, that clause will be removed from the document. However the remainder of the document will remain in force.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5. Force Majeure

Events outside of control of the LIPCA will be addressed as soon as possible.

9.17. Other provisions

No stipulation.