**Laboratório de Instrumentação e Física Experimental de Partículas**

***COMPUTER CENTRE – LISBON – PORTUGAL***

# LIP CA

## Certificate Policy and Certification Practice Statement

**Version 4.0 (DRAFT-D)**

**15 May 2003**

# CONTENTS

# 1 INTRODUCTION

## 1.1 OVERVIEW

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

This document is a combined certification policy and certificate practice statement. It describes the set of procedures followed by the LIP CA in issuing certificates as well as the responsibilities of the involved parties. The document is based on the structure suggested by the RFC 2527.

This document describes:

a) Applicability of certificates signed by the LIP CA;
b) Operational practices used by the LIP CA.

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

## 1.2 IDENTIFICATION

Title:

LIP CA Certificate Policy and Certification Practice Statement.

Version:

Version 4.0 (DRAFT-D).

Date:

15 May 2003.

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. 4.0 (DRAFT-D)**

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 | LIP CA |
| 1 | CP/CPS |
| 4.0 (DRAFT-D) | Major and minor CP/CPS version number |

## 1.3 COMMUNITY AND APPLICABILITY

The LIP CA issues certificates to the Portuguese academic community.

### 1.3.1 Certification authorities

All certificates issued under this CP/CPS must be signed by the LIP CA.

### 1.3.2 Registration authorities

Registration authorities will be created as needed to support the academic research activities in the country. The LIP CA delegates the authentication to the following registration authorities:

1) LIP-Lisbon RA;
2) LIP-Coimbra RA;

Registration authorities must be operated by organizations related with the Portuguese academic community. RAs must sign an agreement with the LIP CA where they assume be obligation of following the procedures imposed by the CA for authentication.

### 1.3.3 End entities

The LIP CA issues certificates for entities related with the following organizations:

a) Portuguese academic organizations (e.g. Universities and education institutes);
b) Portuguese academic research centres (e.g. non-profit).

The subject entities for certificates are of the following types:

a) Employees, researchers and students related with the above organizations;
b) Computer systems and services related with the above organizations;
c) Legal entities related with the above organizations.

All subjects must be uniquely identified.

### 1.3.4 Applicability

Certificate issued by the LIP CA can be used for:

a) Authentication
b) Authorization
c) Confidentiality
d) Integrity
e) Non-repudiation

### 1.3.5 User restrictions

Certificates issued by the LIP CA are only valid in the context of academic research and educational activities, any other usage including financial transactions is strictly forbidden.

The ownership of a certificate issue by the LIP CA does not imply automatic access to any kind of computing resources.

Certificates issued by the LIP CA don't have any legal value.

### 1.3.6 Contact details

The LIP CA is managed by the LIP Computer Centre in Lisbon (Portugal).

The CA address for operational issues is:

LIP Certification Authority
Av. Elias Garcia 14, 1º
1000-149 Lisboa
Portugal

Phone: (+ 351) 217973880
Fax: (+ 351) 217934631
Email: ca@lip.pt

The contact person for questions related with this document or any other LIP CA related issues is:

Jorge Gomes
LIP
Av. Elias Garcia 14, 1º
1000-149 Lisboa
Portugal

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

The CA web server URL is:

http://www.lip.pt/ca

# 2 GENERAL PROVISIONS

## 2.1 OBLIGATIONS

### 2.1.1 CA and RA obligations

Certificate issuance obligations:

a) Accept certification requests for acceptable subjects (see section 1.3.3);
b) Authenticate subjects according with the procedures described in the CP/CPS document with the assistance of the recognized RAs;
c) Issue certificates based on the requests after successful authentication;
d) Notify the subscriber about the certificate issuance;
e) Publish the issued certificates;

Certificate revocation obligations:

a) Accept revocation requests from acceptable persons;
b) Authenticate revocation requests before performing revocations;
c) Issue and publish a CRL immediately after a revocation.

CRL issuance obligations:

a) Issue CRLs and publish them according with the rules described in the CP/CPS document;

Compliance obligations:

a) Publish the policies and procedures in a CP/CPS document.
b) Follow the policies and procedures described in the CP/CPS document.

Data privacy:

a) The CA only collects the personal data required to perform its function;
b) Information considered confidential is only accessible by the CA management personnel.

Private key protection and use:

a) The CA has the obligation of taking all appropriate measures to protect the integrity and confidentiality of the CA private key;
b) The CA private key can only be used to sign certificates, CRLs and information required for the proper CA operation.

### 2.1.2 RA obligations

RAs must adhere to the signed agreement conditions and follow the procedures described in the CP/CPS document while authenticating the subjects.

Each RA must:

a) Read and accept the policies and procedures published in the CP/CPS document;
b) Verify whether the certificate requesters and subjects obey to requirements expressed in the CP/CPS document;
c) Verify whether the certificate requests obey to requirements expressed in the CP/CPS document;
d) Authenticate the subjects according with the procedures described in the CP/CPS document;
e) Verify that the requesters are in the possession of the private key corresponding to the certificate request;
f) Notify the CA of the validation result through a secure and reliable mechanism;
g) The RA must keep a record on the authentications performed;
h) The RA must allow the CA to access the logs and documents related with the performed authentications.

Additionally the RA is responsible for:
a) Choosing their own staff and provide the conditions for the staff to operate the RA, always following the rules established in the CP/CPS;
b) Establish with the CA the community of subjects for which certificate requests can be authenticated.

### 2.1.3 Subscriber obligations

The subscriber's obligations are as follows:
a) Read and accept the policies and procedures published in the CP/CPS document;
b) Generate a key pair using a trustworthy method;
c) Keep the private key safe and protected. The subscribers are fully responsible for the private key confidentiality and integrity;
d) Use a strong pass-phrase with a minimum of 15 characters to protect the private key of personal certificates;
e) Notify the CA in case of possible private key compromise;
f) Notify the CA in case of key destruction and loss;
g) Notify the CA when the certificate is no longer required;
h) Notify the CA when the information in the certificate becomes wrong or inaccurate.
i) Use the certificates only for the purposes authorized by the Cp/CPS document;
j) Must allow the treatment and conservation of their personal data used in the authentication process.

### 2.1.4 Relaying party obligations

The relaying party obligations are as follows:
a) Read and accept the policies and procedures published in the CP/CPS document;
b) Use the certificates only for the purposes authorized by the CP/CPS document;

c) Verify the digital signature of digital messages and verify the digital signature of the CA;
d) Verify the certificate validity, revocation or suspension while performing the certificate authentication;
e) Verify the authenticity of the LIP CA root certificate.

#### 2.1.5 Repository obligations

The CA obligations regarding the repository are as follows:

a) LIP CA will publish on its web server the LIP CA public key;
b) LIP CA will publish on its web server the CRLs as soon as issued;
c) LIP CA will maintain a repository with the issued certificates.

### 2.2 LIABILITY

a) RAs guarantee to control the identity of the certification requests according to the procedures described in the CP/CPS document;
b) LIP CA and RAs guarantees to control the identity of the revocation requests according to the procedures described in the CP/CPS document;
c) LIP CA and RAs are run on a best effort basis and does not give any guarantees about the service security or suitability;
d) LIP CA and RAs will not be held liable for any problems arising from its operation or use made of certificates it issues;
e) LIP CA and RAs denies any kind of responsibilities for damages or impairments resulting from its operation.

### 2.3 FINANCIAL RESPONSIBILITY

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

### 2.4 INTERPRETATION AND ENFORCEMENT

#### 2.4.1 Governing law

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

#### 2.4.2 Dispute resolution procedures

Legal disputes arising from the operation of the LIP CA will be resolved according with the Portuguese law.

### 2.5 FEES

No fees are charged.

### 2.6 PUBLICATION AND REPOSITORIES

### 2.6.1 Publication of CA information

LIP CA publishes the following information through its online repository:

a) The CA certificate in “pem” format (http://www.lip.pt/ca/lipca.pem);
b) The latest CRL in “pem” format (http://www.lip.pt/ca/lip-crl.pem);
c) A copy of this CP/CPS document (http://www.lip.pt/ca/ca-policy.html);
d) The issued certificates (http://www.lip.pt/ca/ca-published-certs.html);
e) Other relevant information.

### 2.6.2 Frequency of publication

New information will be published as soon as available. CRLs will be issued according with section 4.4.8.

### 2.6.3 Access control

LIP CA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL, repository with public keys and a copy of the CP/CPS document.

LIP CA may impose a more restricted access control policy to the repository at its discretion.

The repository is maintained on a best effort basis.

### 2.6.4 Repositories

The LIP CA online repository is available at http://www.lip.pt/ca.

## 2.7 COMPLIANCE AUDIT

The LIP CA may be audited by other trusted CAs to verify its compliance with the rules and procedures specified in the CP/CPS.

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

In case deficiencies are found during a compliance audit the LIP CA will take the appropriate measures to correct these deficiencies as soon as possible.

## 2.8 CONFIDENTIALITY

### 2.8.1 Confidential Information kept by the CA/RA

The LIP CA keeps the following confidential information:

a) Subscriber full name;

b) Subscriber phone number;
c) Subscriber mail address;
d) Subscriber public key.

### 2.8.2 Types of Information not Considered Confidential

All information contained in the certificates and CRLs is not considered confidential. This includes among others the following:

a) The subscriber name in the certificate subject;
b) The Email address or DNS hostname;
c) The subscriber organization name.

### 2.8.3 Disclosure of certificate Revocation/Suspension information

Upon certificate revocation involving key compromise the CA may choose to notify and inform the following entities:

a) The subject of the personal certificate;
b) The requester of the server certificate;
c) Known relying parties.

The LIP CA does not suspend certificates.

### 2.8.4 Release of Information to Law Enforcement Officials

The information collect by the LIP CA will be made available to law enforcement officials upon request and exhibit of regular warrant.

### 2.8.5 Information that can be revealed as Part of Civil Discovery

Information considered confidential is not disclosed.

### 2.8.6 Conditions for Disclosure Upon Owner's Request

The LIP CA will release confidential information upon owner’s request.

### 2.8.7 Other Circumstances for Disclosure of Confidential Information

Not applicable.

## 2.9 INTELLECTUAL PROPERTY RIGHTS

This document is based on the following sources:

a) RFC 2527;
b) EuroPKI Certificate Policy;
c) TrustID Certificate Policy;
d) NCSA Certificate Policy;
e) FBCA Certificate Policy;
f) INFN Certificate Policy and Certificate Practice Statement;

g) NIKHEF Certificate Policy and Certificate Practice Statement;
h) CESNET CA Certificate Practice Statement;
i) DOE Grids Certificate Policy and Certification Practice Statement;
j) UK e-Science Certification Authority Certificate Policy and Certification Practice Statement.

# 3 IDENTIFICATION AND AUTHORIZATION

## 3.1 INITIAL REGISTRATION

### 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 name starts with the fixed component to which a variable component is added to make it unique.

The fixed component is common to all certificates issued by the LIP CA 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 contains an organization (O) RDN identifying the academic organization with which the subject is officially related. The organization name must be meaningful and correspond to a real organization name as stated in section 3.1.2.

A second 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 could be a University foundation 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 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 DNS full-qualified name of the system or service prefixed with the qualifier “host/” for a system, or the service name initials followed by a slash.

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/**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

Some examples of certificate subjects that obey to the LIP CA subject-naming scheme are as follows:

**/C=PT/O=LIPCA/O=FCTUNL/CN=Pedro Miguel Antunes**

**/C=PT/O=LIPCA/O=LIP/CN=host/ce02.lip.pt**

**/C=PT/O=LIPCA/O=LIP/CN=ldap/ca.lip.pt**

**/C=PT/O=LIPCA/O=LIP/OU=Coimbra/CN=Jose Pedro Tome**

**/C=PT/O=LIPCA/O=LIP/OU=COMPANYA/CN=John Smith**

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 or the keyword "host" from the DNS host name.

Email 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 password or identity card.

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

### 3.1.3 Rules for interpreting various name forms

Refer to sections 3.1.1 and 3.1.2.

### 3.1.4 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 at least three names 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.

### 3.1.5 Name claim dispute resolution procedure

Name disputes are managed according to the Portuguese law.

### 3.1.6 Recognition, authentication and role of trademarks

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

### 3.1.7 Method to prove possession of private key

Certificate requesters are required to prove the possession of the private key corresponding the public key in the certificate request.

For signature keys, this is done by the requester using its private key to sign a value and providing that value to the RA. The RA will validate the signature using the public key from the subscriber's certificate request.

For encryption keys, the requester is asked to decrypt a random challenge encrypted with the public key contained in the certificate request.

### 3.1.8 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 LIP CA certificate.

In special cases organizations can provide to the RAs access to databases that can be used to verify the relation of the requesters 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.

### 3.1.9 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 LIP CA Registration Authority (RA) for the identity to be verified. At that moment the individual should present the proof of relation with the organizations specified in the certificate subject distinguish name.

For each authentication the RA will record:

a) The type, identification number and name in the document presented by the subject to be authenticated;
b) The document used as proof of relation with the organization or organizations.
c) The identification of the person that has performed the authentication;
d) The date, time and place of the authentication;
e) 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 however all other steps including the record of the above information and the proof of private key possession must be performed.

For server or service certificates the requests must be signed with a LIP CA issued certificate corresponding to the system administrator or system responsible, which must have a certificate issued under the same organization name as the request.

## 3.2 ROUTINE REKEY

Rekey can be obtained by sending a request signed with the certificate before its expiration. However if the certificate subject is a person it must still provide a proof of relation with the organizations in the certificate subject name. This can be an organization identity card or organization official document stamped and signed by an official representative of the organization.

If the certificate expires the procedure for obtaining a new certificate must be followed.

## 3.3 REKEY AFTER REVOCATION

The LIP CA does not perform rekey of certificates after its revocation. A new certificate must be requested and the procedure for obtaining a new certificate must be followed.

## 3.4 REVOCATION REQUESTS

Revocation requests must be authenticated by:

a) The procedure in the section 3.1.9.

b) A signed Email message to ca@lip.pt. The Email message must be signed with a valid non-expired certificate.

The LIP CA can revoke certificates without authentication when it has proof of key compromise or violation of the rules and user obligations mentioned in the CP/CPS document by the certificate holder.

# 4 OPERATIONAL REQUIREMENTS

## 4.1 CERTIFICATE APPLICATION

The application for a LIP CA certificate is performed by:

a) Generating a key pair;
b) Sending the certificate request and other required information to a RA that accepts to authenticate the request.

Applications will be accepted only if the following requirements are meet:

a) The subject must be an acceptable end entity;
b) The request must obey to the LIP CA subject distinguish name scheme;
c) The subject distinguish name must be unique;
d) The key must have at least 1024 bits.

The LIP CA provides the mechanisms through which the key generation and request submission must be performed.

## 4.2 CERTIFICATE ISSUANCE

The certificate issuance process has the following steps:

a) The RA authenticates the subject identity;
b) The RA verifies the relation of the subject with the organization;
c) The RA checks for the possession of the private key;
d) The RA sends the request to the CA;
e) The CA verifies the RA signature and issues the certificate;
f) The CA publishes the certificate and notifies the subject;

The following requirements must be meet for a certificate to be issued:

a) The subject authentication performed by the RA must be successful;
b) The proof of relation of the subject with the organizations in the certificate distinguish name must be successful.

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

## 4.3 CERTIFICATE ACCEPTANCE

The LIP CA does not have a certification acceptance procedure. If a user wants to reject a certificate it must submit a revocation request.

## 4.4 CERTIFICATE SUSPENSION OR REVOCATION

### 4.4.1 Circumstances for Revocation

A certificate will be revoked in the following circumstances;

a) The subject of the certificate as ceased his relation with the organization;
b) The subject does not want the certificate any more;
c) The private key has been lost or compromised;
d) The information in the certificate is wrong or inaccurate;
e) The subject has failed to comply with the rules in the policy;
f) The system to which the certificate has been issued has been retired.

### 4.4.2 Who can request revocation

The revocation of a certificate can be requested by:

a) The certificate subscriber;
b) Any entity presenting proof of responsibility for a certified machine or service;
c) Any entity presenting proof of the certificate misuse;
d) Any entity presenting proof of the private key compromise;
e) Any entity presenting proof of the modification of the subscriber's data.

### 4.4.3 Procedure for Revocation Request

Revocation requests must be authenticated by:

a) The procedure in the section 3.1.9;
b) A signed Email message to ca@lip.pt. The Email message must be signed with a valid non-expired certificate.

The LIP CA will always try to notify the certificate subscriber before revoking the certificate.

The LIP CA can revoke certificates without authentication when it has proof of key compromise or violation of the rules and user obligations mentioned in the CP/CPS document by the certificate holder.

### 4.4.4 Revocation request grace period

The LIP CA will act promptly to revocation requests however the reaction can be delayed by weekends and public holidays.

### 4.4.5 Circumstances for Suspension

The LIP CA does not suspend certificates.

### 4.4.6 Who can request suspension

The LIP CA does not suspend certificates.

### 4.4.7 Procedure for suspension request

The LIP CA does not suspend certificates.

### 4.4.8 Limits on Suspension Period

The LIP CA does not suspend certificates.

### 4.4.9 CRL Issuance Frequency

The CRLs issuance frequency is as follows:

a) CRLs are issued at least once each 30 days;
b) CRLs are issued whenever certificates are revoked;
c) CRLs are published in the CA repository as soon as issued;
d) CRLs have a lifetime is 30 days;
e) CRLs are issued at least 7 days before expiration.

### 4.4.10 CRL Checking Requirements for Relaying Parties

Relying parties should download the CRL at least once a day and implement its restrictions while validating certificates.

### 4.4.11 Online Revocation/status Checking Availability

The LIP CA does not support this service.

### 4.4.12 Online Revocation Checking Requirements

The LIP CA does not support this service.

### 4.4.13 Other Forms of Revocation Advertisement

Subscribers are notified of the certificate revocation by Email or phone call.

### 4.4.14 Requirements for Relying Parties on Other Forms of Revocation Advertisement

None.

### 4.4.15 Special requirements for rekey compromise

None.

### 4.4.16 Variations of the Above in Case of Private Key Compromise

Upon private key compromise the LIP CA may choose to warn the known relying parties using any means seem fit.

## 4.5 SECURITY AUDIT PROCEDURES

### 4.5.1 Types of events recorded

The CA records the following events:

a) Certificate requests;
b) Revocation requests;
c) Issued certificates;
d) Issued CRLs.

The RA records the following events:

a) Certificate requests;
b) Identity authentication actions.

The following software/hardware related events are recorded:

a) System boots;
b) Login and logouts;
c) Use of the CA/RA software;
d) Unauthorized access attempts.

### 4.5.2 Frequency of processing log

Automatic processing of the logs is performed upon login and alarms are shown for relevant events. Periodic processing of the logs is not defined.

### 4.5.3 Retention period for audit logs

Logs are recorded and kept for a minimum of five years.

### 4.5.4 Protection of audit logs

#### *4.5.4.1 Access*

Audit logs may be consulted by:

a) LIP CA personnel;
b) External auditors authorized by the LIP CA.

#### *4.5.4.2 Protection Against Modification*

Audit logs are frequently copied to an off-line medium in encrypted format and stored in a safe place. While in the system the audit logs are protected by the file system security mechanisms.

#### *4.5.4.3 Protection Against Deletion*

Audit logs are frequently copied to an off-line medium in encrypted format and stored in a safe place. While in the system the audit logs are protected by the file system security mechanisms.

### 4.5.5 Audit log backup procedures

Logs are copied weekly to an off-line medium in encrypted format and stored in a safe place.

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

The audit collection system is internal to the LIP CA.

### 4.5.7 Notification to event-causing subject

Subjects causing audit events are not notified.

### 4.5.8 Vulnerability assessments

Assessments of the CA vulnerability are performed whenever necessary having in account all information and experience available and appropriate actions are taken to correct the identified vulnerabilities.

## 4.6 RECORDS ARCHIVAL

### 4.6.1 Types of events recorded

The following types of events are archived:

a) Certification requests;
b) Issued certificates;
c) Revocation requests;
d) Revoked certificates
e) Certificate rekey request;
f) Rekeyed certificates;
g) Issued CRLs;
h) Messages sent and received by the CA/RA;
i) Audit log events;
j) Implemented versions of the CP/CPS documents.

### 4.6.2 Retention period for the archive

The archive is kept for 5 years.

### 4.6.3 Protection of archive

#### *4.6.3.1 Access*

The archive may be consulted by:

a) LIP CA personnel;
b) External auditors authorized by the LIP CA.

#### *4.6.3.2 Protection Against Modification*

Archives are copied to a read only off-line medium in encrypted form and stored in a safe place. While in the system the audit logs are protected by the file system security mechanisms.

#### *4.6.3.3 Protection Against Deletion*

Archives are copied to a read only off-line medium in encrypted form and stored in a safe place. While in the system the audit logs are protected by the file system security mechanisms.

.

### 4.6.4 Archive backup procedures

The archives are copied weekly to an off-line medium in encrypted format and stored in a safe place. Paper documents are kept in a locked place with restricted access.

### 4.6.5 Requirements for time-stamping of records

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

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

The archive collection system is internal to the LIP CA.

### 4.6.7 Procedures to obtain and verify archive information

Information considered confidential is not made available to be public. Information considered non-confidential is available to the public only while kept on-line.

## 4.7 KEY CHANGEOVER

Issued certificates are distributed by signed E-mail, secure web server, floppy disk or CDROM.

## 4.8 COMPROMISE AND DISASTER RECOVERY

### 4.8.1 Private key compromise

If the CA private key is compromised or suspect of being compromised the CA will:

a) Notify the LIP CA subordinate RAs;
b) Notify subscribers;
c) Terminate the issuance and distribution of certificates and CRLs;
d) Notify relevant security contacts;
e) Notify relying parties as wide as possible.

#### 4.8.2 Computing resources, software, and/or data are corrupted

In case of corruption the CA systems are either repaired or rebuilt from the last good backup. If a good backup cannot be identified the systems will be reinstalled from scratch.

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.

If public certificates stored in the repository are lost or corrupted certificates will be revoked.

#### 4.8.3 Entity public key is revoked

If an entity public key needs to be revoked the procedure in section 4.4.3 will be followed. After revocation the user will have to request a new certificate.

#### 4.8.4 Entity key is compromised

If a private key is compromised the certificate will be revoked following the procedure in section 4.4.3. After revocation the user will have to request a new certificate.

#### 4.8.5 Secure facility after a natural or other type of disaster

The LIP CA will make its best efforts to keep the CA systems and materials secure in case of disaster. The recovery plan will be activated as soon as possible.

### 4.9 CA TERMINATION

Upon termination the LIP CA will:

a) Notify the LIP CA subordinate RAs;
b) Notify subscribers;
c) Terminate the issuance and distribution of certificates and CRLs;
d) Notify relevant security contacts;
e) Notify relying parties as wide as possible.

Notifications will be sent prior to the termination and as earlier as possible.

Upon termination the CA records will remain if possible under the custody of LIP.

# 5 PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

## 5.1 PHYSICAL SECURITY CONTROLS

### 5.1.1 Site Location

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

### 5.1.2 Physical Access

Physical access to the LIP CA is restricted to authorized personnel.

### 5.1.3 Power and Air Conditioning

The CA systems are protected by uninterruptible power supplies. Environment temperature in rooms containing CA related equipment is maintained at appropriate levels by dual air conditioning systems.

### 5.1.4 Water Exposures

Due to the location of the LIP CA facilities floods are not expected. The Computer Centre is situated in a first floor.

### 5.1.5 Fire Prevention and Protection

The LIP CA facilities obey to the Portuguese law regarding fire prevention and protection in buildings.

### 5.1.6 Media Storage

All media is kept in a safe place:

a) The LIP CA key is kept in several removable storage media;
b) Backup copies of CA related information are kept in magnetic tape cartridges, floppies and CDROM.

### 5.1.7 Waste Disposal

Waste carrying potential confidential information such as old floppy disks is physically destroyed before being trashed.

### 5.1.8 Off-site Backup

Off-site backups are planned but not currently performed.

## 5.2 PROCEDURAL CONTROLS

### 5.2.1 Trusted roles

The following roles are defined within the LIP CA:

a) CA manager: is the overall responsible for the administration of the CA covering all administrative and technical aspects of the CA activities.
b) System administrator: is responsible for the maintenance and security of the CA systems.
c) CA operator: issues certificates and CRLs, revokes certificates and performs backups.
d) RA manager: authenticates identities.
e) Auditor: verifies log files 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

All task require the presence of just one person.

### 5.2.3 Identification and authorization for each role

No stipulation.

## 5.3 PERSONNEL SECURITY CONTROLS

### 5.3.1 Background Checks and Clearance Procedures for CA Personnel

CA personnel is recruited from the LIP Computer Centre team.

### 5.3.2 Background Checks and Security Procedures for Other Personnel

No external persons are authorized to access the CA facilities without the physical presence of CA personnel.

### 5.3.3 Training Requirements and Procedures

Internal training is given to CA operators covering PKI principles, security, CA software and the CA operation procedures.

### 5.3.4 Training Period and Retraining Procedures

No stipulations.

### 5.3.5 Frequency and Sequence of Job Rotation

Job rotation is not performed.

### 5.3.6 Sanctions Against Personnel

No stipulations.

### 5.3.7 Controls on Contracting Personnel

No stipulations.

### 5.3.8 Documentation Supplied to Personnel

The following documentation is provided to the LIP CA personnel:

a) Copies of the CP/CPS document;
b) LIP CA Operations Manual;

Each RA will receive the following documentation:

c) Copies of the CP/CPS document;
d) LIP RA Operations Manual;

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 KEY PAIR GENERATION AND INSTALLATION

### 6.1.1 Key pair generation

Each subscriber must generate his own key pair. The LIP CA does not generate private keys for subjects.

The LIP CA root certificate key pair is generated by the LIP CA manager.

### 6.1.2 Private Key Delivery to Entity

The LIP CA does not generate private keys hence does not deliver private keys.

### 6.1.3 Public Key Delivery to Users

Public keys are delivered by signed E-mail, secure web server, floppy disk and CDROM.

### 6.1.4 CA public key delivery to users

The LIP CA certificate can be downloaded from the LIP CA web site.

### 6.1.5 Key sizes

The minimum key sizes are as follows:

a) The minimum key length for a personnel or server certificate is 1024 bits;
b) The CA key length is 2048 bits.

### 6.1.6 Public key parameters generation

No stipulations.

### 6.1.7 Parameter quality checking

No stipulations.

### 6.1.8 Hardware/software key generation

Currently the keys are generated by software.

### 6.1.9 Key usage purposes

The LIP CA certificates may be used for authentication, non-repudiation, data encipherment, message integrity, session establishment and sign proxy certificates. Certificates and CRLs can only be signed by the CA private key.

## 6.2 PRIVATE KEY PROTECTION

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

Not supported.

### 6.2.2 Private key escrow

Not supported.

### 6.2.3 Private key archival and backup

The LIP CA private key is kept encrypted in multiple copies in CDROMs stored in safe places.

## 6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

The LIP CA private key has a validity of five years.

## 6.4 ACTIVATION DATA

The LIP CA private key is protected by a pass-phrase with at least 15 characters.

## 6.5 COMPUTER SECURITY CONTROLS

### 6.5.1 Specific security technical requirements

The security technical requirements are as follows:

a) The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;
b) Monitoring is performed to detect unauthorized software changes;
c) CA systems configuration is reduced to the base minimum;
d) The signing machine is kept powered off between uses.

### 6.5.2 Computer security rating

No stipulations.

## 6.6 LIFE CYCLE SECURITY CONTROLS

No stipulations.

## 6.7 NETWORK SECURITY CONTROLS

The following network security measures have been taken:

a) The CA signing machine is kept off-line;
b) CA/RA machines other than the signing machine are protected by a firewall;
c) The network services in the on-line systems are reduced to the minimum;

### 6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

No stipulations.

# 7 CERTIFICATE AND CRL PROFILE

## 7.1 CERTIFICATE PROFILE

### 7.1.1 Version number

The LIP CA issues X.509 v3 certificates.

### 7.1.2 Certificate extensions

The certificate extensions are as follows :

a) Basic constraints (critical): **Not a CA**.
b) Key usage (critical): **Digital signature**, **non-repudiation**, **key encipherment**, **data encipherment**.
c) Subject key identifier: **unique identifier of the subject key (hash)**.
d) Authority key identifier: **unique identifier of the issuer (CA) key**.
e) Subject alternative name: **User Email address or server DNS host name**.
f) Issuer alternative name: **LIP CA Email address**.
g) CRL distribution points: **URI**.
h) Certificate policies: **The OID of the CP/CPS**.
i) Netscape base URL: **URI.**
j) Netscape cert type: **SSL server, SSL client, S/mime**.
k) Netscape comment: **CP/CPS version and CA name**.
l) Netscape CA policy URL: **URI**.
m) X509v3 CRL distribution points: **URI**.

### 7.1.3 Algorithm object identifiers

No stipulations.

### 7.1.4 Name forms

See section 3.1.1.

### 7.1.5 Name constraints

See section 3.1.1.

### 7.1.6 Certificate policy object identifier

The certificate policy object identifier (OID) is: **1.3.6.1.4.1.9846.10.1.1. 4.0 (DRAFT-D)**

### 7.1.7 Usage of policy constraints extensions

No stipulation.

### 7.1.8 Policy qualifier syntax and semantics

No stipulation.

## 7.2 CRL PROFILE

### 7.2.1 Version number(s)

The LIP CA issues x.509 v1 CRLs.

### 7.2.2 CRL and CRL entry extensions

No stipulations.

# 8 SPECIFICATION ADMINISTRATION

## 8.1 SPECIFICATION CHANGE PROCEDURES

Only the subscribers will be directly warned of changes to LIP CA's policy and CPS. Minor changes and corrections can be performed without notification.

## 8.2 PUBLICATION AND NOTIFICATION PROCEDURES

The LIP CA policy is available at the LIP CA repository.

## 8.3 CPS APPROVAL PROCEDURES

No stipulations.

# 9 DEFINITIONS

| | |
|---|---|
| Authentication | The process used to establish the authenticity of an individual, organization, computer system, service or software component. Authentication is used to ensure that the subject is really who or what it claims to be. In PKI there are two different authentications. The first occurs after a request for a certificate is made and has the objective of verifying that the certificate will be issued to the correct subject. The second is performed has the objective of verifying that data sent electronically was sent by the subject that claims to have sent it. |
| Certification Authority | A certification authority (CA) is a trusted authority that issues and manages public key certificates as part of a public key infrastructure (PKI). |
| Certificate Policy | A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. |
| Certification Practice Statement | A statement of the practices used by a certification authority while managing certificates (issuing, revoking etc.). |
| Certificate Revocation List | A time stamped list containing the index number of the revoked certificates, which is signed by a CA and made available in the CA public repository. |
| Certificate Subject | Who or what whose public key is certified in the certificate. |
| Identification | The process of establishing the identity of a |
| Issuing Certification Authority | For a given certificate is the Certification Authority that has issued it. |
| Registration Authority | An entity that is responsible for performing the identification and authentication of certificate subjects, but that does not issue certificates. |
| Relaying Party | |
| Repository | The on-line storage area where the CA stores issued certificates, CRLs, the root certificate etc. |
| Signed Email | An email message that has been check summed and signed by a valid certificate. |
| Strong pass-phrase | A characteristic of a password. The password used to protect the private key must be strong. That means difficult to guess. |
| Subscriber | The person to whom a certificate has been issued. |

# 10 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 |
| **LDAP** | Lightweight Directory Access Protocol |
| **LIP** | Laboratório de Instrumentação e Física Experimental de Partículas |
| **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 |
| **SSL** | Secure Sockets Layer |
| **UPS** | Uninterruptible Power Supply |
| **URI** | Universal Resource Identifier |
| **URL** | Universal Resource Locator |