Universidad Nacional de La Plata

UNLP PKIGrid CA

Certificate Policy and Certification Practice Statement

OID Document 1.2.840.113612.5.4.2.3.1.0.2.7.

October 30, 2007

Contents

1 Introduction

This document is structured according to RFC 3647 and describes the set of rules and procedures established by UNLP for the operations of the UNLP PKIGrid CA service.

This document will include both the Certificate Policy and the Certification Practice Statement for the UNLP PKIGrid CA. The general architecture is a single certificate authority and several registration authorities. The certificate authority is a stand-alone self signed CA.

1.1 Overview

UNLP Grid is the infrastructure to support e-science activities of the Argentine academic community.

This document describes the set of rules and operational practices that shall be used by the UNLP PKIGrid CA, the Certification Authority (CA) for UNLP Grid, for issuing certificates. This and any subsequent CP/CPS document can be found on its web site

https://www.pkigrid.unlp.edu.ar

1.2 Document name and identification

Document title	UNLP PKIGrid CA Certificate Policy (CP) and Certification Practice Statement (CPS)
Document version	Version 2.7
Document date	30 October 2007
Document OID structure	
assigned by IGTF	1.2.840.113612.5.4.2.3
Document type (CP/CPS)	1
Document subtype	0
Version	2
Sub -Version	7

The Document OID structure is indicated in the document "Documents descriptions & Specifications" published in the site.

This document is valid until further notice.

1.3 PKI participants

1.3.1 Certification authorities

The UNLP PKIGrid CA does not issue certificates to subordinate Certification Authorities.

1.3.2 Registration authorities

Registration authorities (RA) will be created as needed to support the academic research activities in the country. Initially the UNLP PKIGrid CA delegates the authentication to CESPI RA.

CESPI - "Centro Superior para el Procesamiento de la Información" of the National University of La Plata is the center for computing services at UNLP. The CESPI was created in 1969 and provides services to all the University (with more than 95.000 student, over 140 university grade degrees and over 200 postgraduate degrees) and supporting 20% of the scientific & technical research done in Argentina.

The RA is responsible for enforcing the identity vetting rules on behalf of the CA during the process of issuing certificates to end identities (EEs).

Registration authorities must be operated by organizations related with the Argentine academic community. They assume the obligation of following the procedures imposed by the CA for their operation and authentication of certificate requests.

The RA operador must be a member of staff appointed by the organization.

The RAs are required to declare their understanding of and adherence to this CP/CPS, and to perform their functions in accordance with this CP/CPS and the current best practices as defined by the site of the UNLP PKIGrid.

The UNLP PKIGrid CA operates a network of distributed Registration Authorities (RAs). A list of registration authorities is maintained and published in the on-line repository. The list of RAs will contain at least the name of the RA, the contact information for the RA, and the home domain of registration for the RA.

The list of RAs for the UNLP PKIGrid CA is available from the PKIGrid website

https://www.pkigrid.unlp.edu.ar

1.3.3 Subscribers

The UNLP PKIGrid CA issues certificates for e-Science activities performed within the UNLP Grid constituency. The CA will issue personal, server and service certificates.

Requesters of certificates should be from Argentina academic community and MUST provide evidence of their need to work with the international Grid Community (i.e being presented by one project leader related to grid research).

Host or service certificate requesters MUST present a signed e-mail or letter countersigned by the project leader to prove that the requester is related to the host administration.

1.3.4 Relying parties

Relying parties may be:

- natural persons receiving signed e-mails, or accessing hosts or services
- host to which certificate owners login or send processes or jobs
- services called by owners of a certificate

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

CA certificates may only be used to issue certificates and for checking certificates that claim to be issued by the UNLP PKIGrid CA (see 1.3.3).

RA certificates may only be used by the RA agent for RA related activities, not for other activities of that natural person; these must be undertaken using an end-entity certificate.

The end-entity certificate may be used for any application that is suitable for X.509 certificates, in particular:

- authentication of users, hosts and services
- authentication and encryption of communications
- authentication of signed e-mails
- authentication of signed objects

The certificates may only be used or accepted for actions that support e-science activities.

1.4.2 Prohibited certificate uses

The certificates issued by UNLP PKIGrid CA must only be used for e-Science activities, and should not be used for others activities such us financial transactions.

They must not be used for purposes that violate any law of Argentina or the law of the country in which the target entity (i.e. application or host to use, addressee of an e-mail) is located.

1.5 Policy administration

1.5.1 Organization administering the document

The UNLP PKIGrid CA is managed by the CESPI Computer Centre in La Plata (Argentina).

The CA address for operational issues is:

UNLP Certification Authority

Calle 115 y 50 S/N

B1900AYB La Plata

Buenos Aires

Argentina

Phone: 542214257240

Fax: 542214236610

E-mail: ca@cespi.unlp.edu.ar

The CA web server URL is https://www.pkigrid.unlp.edu.ar

1.5.2 Contact person

The CA manager (contact person for questions related to this policy document) is:

Díaz, Francisco Javier

CESPI - UNLP

Calle 115 y 50 S/N

B1900AYB La Plata

Argentina

Phone: 542214236609

Fax: 542214236610

E-mail: jdiaz@unlp.edu.ar

1.5.3 Person determining CPS suitability for the policy

The manager of the UNLP PKIGrid CA (see 1.5.2) is responsible for determining the CPS suitability for the policy.

1.5.4 CPS approval procedures

The approved document shall be submitted to TAGPMA for acceptance and accreditation.

1.6 Definitions and acronyms

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

The definitions are organized by alphabetical order.

Activation Data

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (i.e., a PIN, a passphrase, or a manually-held key share).

Analyst

The analyst is a person that has experience in all the phases of project management and helps to make decisions or solve problems.

Authentication

The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This process corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the messages sender.

Certification Authority (CA)

An authority trusted by one or more subscribers to create and assign public key certificates. That entity/system issues X.509 identity certificates.

Certificate Policy (CP)

A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions.

Certification Practice Statement (CPS)

A statement of the practices, which a certification authority employs in issuing certificates.

Certificate Rekey

The process for re-key after revocation or expiration of a Subscriber certificate is complete re-enrollment, which requires the generation of a new Subscriber key pair. The certificate's

subscriber can request routine rekeying of a certificate by signed electronic mail, with the same subject name as the previous certificate **but with a new key pair**.

Certificate renewal

Certificate renewal is the process whereby a new certificate with an extended validity period is created for an existing key pair.

Users can renew their certificate as long as they haven´t expired or been revoked. They can reuse the private key (if the RA ascertain that there are no risks).

Certificate Revocation List (CRL)

A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

End Entity

Or sometimes called Subscriber, is a person or server to whom a digital certificate is issued.

Host Certificate

A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine.

Identification

The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization.

A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing Certification Authority (Issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Key changeover

Key changeover is the process to provide a new public key to a CA's users.

Person Certificate

A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person.

Policy Qualifier

The Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Project Leader

The person who is the responsible manager for a related GRID project. He is the point of contact with the RA, and has been chosen to handle all communications about policy matters with the UNLP PKIGrid manager.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relying Party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Repository

A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.

Service Certificate

A certificate for a particular service running on a host. It will represent a single service on a single host.

Subscriber

Or sometimes called End Entity is a person or server or service to whom a digital certificate is issued.

Virtual Organization (VO)

An organization that has been created to represent a particular research or development effort independent of the physical sites that the Scientist or Engineers work at.

2 Publication and repository responsibilities

2.1 Repositories

The online repository of information from the UNLP PKIGrid CA is accessible at the CA web server URL https://www.pkigrid.unlp.edu.ar

2.2 Publication of CA information

The UNLP PKIGrid CA will operate a secure online repository that contains:

- The UNLP PKIGrid CA' s certificate (available in PEM, CRT and DER formats), and all previous ones necessary to check still valid certificates,
- The certificates issued by the CA,
- A Certificate Revocation List (available in PEM or DER formats),
- A copy of the most recent version of this CP/CPS and all previous versions,
- Other information deemed relevant to the UNLP PKIGrid CA service.
- A link to the TAGPMA trust anchor repository (TACAR, www.tacar.org) where the CA root of trust has been previously published.

2.3 Time of frequency of publication

- All information published shall be up-to-date.
- Certificates will be published to the UNLP PKIGrid CA repository as soon as issued.
- The certificate revocation list (CRL) shall have a lifetime of at most 30 days.
- The UNLP PKIGrid CA MUST issue a new CRL at least 7 days before expiration or immediately after having processed a revocation, whichever comes first. A new CRL MUST be published immediately after its issuance.
- This CP/CPS will be published whenever it is updated.

2.4 Access Controls on repositories

The online repository is maintained on a best effort basis and is available substantially on a 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance. Outside the period 08:00-17:00 GMT- 03:00 on working days it may run unattended " at risk".

The UNLP PKIGrid CA does not impose any access control on its CP/CPS, its certificate, issued certificates or CRLs.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The Subject Name is of the X.500 name type. The CN component has one of the following forms:

- For people the name and surname or a text directly derived from their name (lower and upper case allowed) CN=JavierDiaz
- For Server the server fully qualified domain name (FQDN). The name MUST be in lower case. IP address are not accepted
- For Services the name of the service, the character "/" and the FQDN of the server. The name MUST be in lower case.

  Common Names (CNs) MUST be encoded as PrintableStrings. The maximal length of the CN is 128 characters for all types of certificates.
- For service certificates, the character "/" is also allowed in the Common Name and the text left to the "/" MUST be related to the type of service the certificate is identifying.

3.1.2 Need for names to be meaningful

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber. Subscribers must choose a representation of their names in the permitted character set (see 3.1.1). The name must not refer to a role.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers can neither be anonymous nor pseudonymous. No natural person certificates shall be issued to roles or functions, only to named and identified persons.

3.1.4 Rules for interpreting various name forms

- The CN component of the subject name in a certificate for a natural personal should contain the first and the family name (can be separated by a dot) as it appears in the

authentication document proving the name of the subscriber. It's also possible to use a text directly derived from the full name.

CN=JavierDiaz CN=Javier.Diaz

- The CN entry for a host shall be the fully qualified domain name (FQDN) that can be universally used to access that host.

CN=pkigrid.unlp.edu.ar

- The CN entry for a service shall be the name of the application followed by a slash "/" followed by the FQDN of the host on which the application is executed.

CN=ldap/pkigrid.unlp.edu.ar

3.1.5 Uniqueness of names

The Distinguished Name MUST be unique for each subject name certified by the UNLP PKIGrid CA service over the lifetime of the CA. The UNLP PKIGrid does this task before request is generated.

In this policy two names are considered identical if they differ only in case. In other words, case must not be used to distinguish names.

Certificates MUST apply to unique individuals or resources.

3.1.6 Recognition, authentication and role of trademarks

No stipulation

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The RA confirms the possession of the private key by verifying the signature of the certificate signing request (CSR).

3.2.2 Authentication of organization identity

The CA shall verify that the requesting party's organization or a unit of an organization is entitled (see 1.3.3) to get a certificate from the UNLP PKIGrid CA and that it consents to the request.

The first time an organization/unit wants to get a certificate for a natural person, a server or a service, or wants to install an RA, it has to announce this officially to the UNLP PKIGrid CA. The CA has to ascertain that the organization or organizational unit exists and is entitled to request an UNLP Grid certificate. It must also get competent information on who is entitled to sign on behalf of the institution.

3.2.3 Authentication of individual identity

In order to enable the RA to authenticate the individual's identity the latter MUST meet in person with the RA and present an officially recognized document proving the requesting party's identity. Only documents accepted by Argentine law (argentinian national identity document, valid passport) will be accepted.

The host certificate can only be requested by the administrator responsible for the particular host. The RA will request a signed mail or letter from the project leader confirming that the person who requested the certificate is the administrator responsible for the host to be identified by the certificate

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Not yet defined

3.2.6 Criteria for interoperability

No stipulation.

3.3 Identification and authentication of re-key request

3.3.1 Identification and authentication for routine re-key

The process for re-key after revocation or expiration of a Subscriber certificate is complete re-enrollment, which requires the generation of a new Subscriber key pair and the performance of the initial registration identification and authentication procedures specified in the current CP/CPS.

The certificate's subscriber can request routine rekeying of a certificate by signed electronic mail. This e-mail MUST contain a new certificate request, with the same subject name as the previous certificate **but with a new key pair**. Note: This is different than to update a certificate: a new certificate is being created

Rekey before the certificate expires can be done using a secure web interface. After expiration of the certificate no rekey is possible; a new application for initial registration must be made instead.

3.3.2 Identification and authentication for re-key after revocation

After revocation of a certificate, no re-key is possible. A new application for initial registration MUST be made.

3.4 Identification and authentication for revocation request

Unless the revocation request originates from the UNLP Grid because it has independently verified that a key compromise has occurred, the revocation request has to be verified and the requesting party has to be authenticated.

Such a request coming from an RA MUST be made in a signed transfer sent to the CA. The CA only need to authenticate the revocation's requester if the CA don´t have a full proof of key compromise or of inaccuracy of the certificate content.

In case of emergency the revocation can be initiated via oral communication with the appropriate RA or the UNLP PKIGrid CA. The RA or the UNLP PKIGrid CA have to use their best effort to authenticate the request, unless full proof of key compromise exists.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The UNLP PKIGrid CA issues certificates to members of the Argentinian academic community for:

- natural persons, and
- hosts administered by the requesting organization, and
- services provided on a host that is administered by an eligible organization.

It's recommended that certificate's requesters know and adhere to the current obligations as defined in the document "Subscriber obligations". This document is published on the UNLP PKIGrid site.

4.1.2 Enrollment process and responsibilities

The requesting party generates the key pair with a size of at least 1024 bit on their system through the form provided at the UNLP PKIGrid website. After the form has been completed the encrypted private key will be stored on the system where the browser runs in a file only accessible to the requester (if the operating system allows such a restriction), and the CSR will be stored in the LDAP system.

Subscribers must:

- Read and adhere to the procedures published in this document
- Use the certificate for the permitted purposes only
- Authorize the processing and conservation of personal data (as required under the data protection regulations)
- Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:
  - (Personal certificates) selecting a strong passphrase of at least 15 characters;

- (Personal certificates) protecting the passphrase from others;

- Notifying immediately the UNLP Grid CA and any relying parties if the private key is lost or compromised;

- Requesting revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

RA operator uses UNLP PKIGrid administration module to show all validate pending CSRs. In the case of a server/service request it must also check that the requestor is responsible for that host within the organization or unit that owns the host.

4.2.2 Approval or rejection of certificate applications

Upon successful authentication, a scanned copy of the requesting party's identification document and the certification request shall be stored. The specifications about scan format are indicated in the document "RA Structure and Operations" published on the CA Web site.

If the authentication information proves to be inaccurate or if a requesting party fails to meet the authentication requirements within 9 days after the request has been received by the RA, the request shall be rejected. If the requesting party insists on getting a certificate it has to initiate a new request.

4.2.3 Time to process certificate applications

The turn-around time from request to issuance depends mostly on the authentication process, but must issue the certificate within three days of receiving the request.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CSR shall be transferred to the computer which holds the private key of UNLP PKIGrid CA and which is not connected to any network. On this system the certificate is created and signed. The signed certificate shall then be transferred back to the UNLP PKIGrid online server.

The certificate MUST be issued based in the last approved CP/CPS by TAGPMA.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The UNLP PKIGrid system shall then send a mail to the requesting party with the URL of the certificate download page. It shall also send an acknowledgment of the issuance to the appropriate RA.

A certificate (personal, service or host) will be valid for 13 months from the date of issuance or less than one year in specific cases (i.e. if the applicant's affiliation to the organization/unit is known to be less than one year).

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The requesting party shall notify the UNLP PKIGrid CA of the rejection of a certificate, explaining the UNLP PKIGrid CA and the RA the reasons for the rejection. Certificates whose rejection have not been received by the UNLP PKIGrid CA within a week shall be considered accepted.

4.4.2 Publication of the certificate by the CA

The UNLP PKIGrid CA will publish on its web server certificates as soon as they are issued.

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 UNLP PKIGrid CA and their associated private keys must only be used according to the permissions and prohibition stated in section 1.4. They must only be used according to the key usage fields of the certificate. When a certificate is revoked or has expired the associated private key shall not be used anymore.

Subscribers MUST not share certificates.

4.5.2 Relying party public key and certificate usage

A relying party must, upon being presented with a certificate issued by the UNLP PKIGrid CA, check its validity by:

- checking that it trusts the CA that issued the certificate,
- checking that the certificate hasn't expired
- the appropriate usage as outlined in the CP pointed to by the certificate and in the usage keys included in the certificate
- consulting the UNLP PKIGrid CA CRL in effect at the time of use of the certificate.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Certificate renewal is the process whereby a new certificate with an extended validity period is created for an existing key pair.

Users can renew their certificate as long as they haven´t expired or been revoked.

Certificate renewal MUST be endorsed by the appropriate RA, that shall ascertain that there are no risks in the reuse of the private key. The information contained in the certificate must be without change or modification, and there must be no suspicion of compromise to the private key.

The UNLP PKIGrid CA may decide to reject such a renewal for security reasons, to avoid risks derived from long exposures of private keys.

4.6.2 Who may request renewal

The owner of a certificate may request the renewal of a certificate before it expires using a secure web interface.

4.6.3 Processing certificate renewal requests

Users can make new request for certificates, but they MUST prove their identity using their current certificate. The request MUST have the same DN as the certificate used to prove identity.

Upon receipt of the request endorsed by the appropriate RA, the UNLP PKIGrid CA shall process the renewal as it processes an initial certification request. The RA must validate that the requester is still working in the original project. The renewal requester must ask the project leader that originally confirmed the user's need for a certificate to inform the RA whether the user still is entitled to a certificate..

4.6.4 Notification of new certificate issuance to subscriber

The UNLP PKIGrid CA shall notify the subscriber of the issuance as described for the initial certificate issuance in 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

The same procedure shall be followed as described in 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See 4.4.2

4.6.7 Notification of certificate issuance by the CA to other entities

See 4.4.3

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

For security reasons, the certificate re-key is the preferred method for issuing a new certificate to a subscriber whose certificate is about to expire or who wants a change in the certificate parameters.

4.7.2 Who may request certification of a new public key

The owner of a valid certificate may request the certification of a new public key in a CSR also signed with his/her still valid private key.

If the certificate has already expired a certificate request procedure as described for an initial certification request must be followed.

4.7.3 Processing certificate re-keying requests

Users can use the UNLP PKIGrid web interface to request a certificate re-key. Upon receipt of the request endorsed by the appropriate RA, the UNLP PKIGrid CA shall process the renewal as it processes an initial certification request.

4.7.4 Notification of new certificate issuance to subscriber

The UNLP PKIGrid CA shall notify the subscriber of the issuance as described for the initial certificate issuance in 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The same procedure shall be followed as described in 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.4.3

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

Certificates MUST not be modified. The old certificate must be revoked, and a new key pair must be generated and a request for the modified certificate contents submitted with the new

public key. The revocation may be conditional on the issuance and acceptance of the new certificate, and thus the old certificate will only be revoked after the new one is accepted.

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

A certificate will be revoked when the information it contains or the implied assertions it carries are known or suspected to be incorrect or compromised. This includes situations where:

- The CA is informed that the subscriber has ceased to be a member of or associated with a UNLP PKIGrid program or activity,
- the subscriber's private key is lost or suspected to be compromised,
- it is not needed any more,
- the information in the subscriber's certificate is wrong or inaccurate, or suspected to be wrong or inaccurate
- the private key of the UNLP PKIGrid CA have been compromised or lost.

4.9.2 Who can request revocation

A certificate revocation can be requested by:

- the owner of the certified key;
- the UNLP PKIGrid CA or any RA that has proof of a compromise;
- the organization that wants to revoke its consent to its inclusion in the certificate;
- the Registration Authority which authenticated the holder of the certificate;
- the holder of the certificate;
- any person presenting proof of knowledge that the subscriber' s private key has been compromised or that the subscriber's data have changed.

4.9.3 Procedure for revocation request

Unless the UNLP PKIGrid CA acts on its own a revocation request must be made:

- by the owner of the certificate, properly authenticated, using the online revocation facilities. In case of compromise, the owner of the certificate must go to the RA as soon as possible and ask the appropriate RA to request revocation.
- by the RA administrator using a secure web interface

Before revoking a certificate the UNLP PKIGrid CA shall authenticate the source of the request according procedures as used for the initial registration.

4.9.4 Revocation request grace period

No grace period is defined for a revocation request.

4.9.5 Time within which CA must process the revocation request

The UNLP PKIGrid CA shall process the authenticated request with priority and publish the revocation within two working days of the CA determining the need for revocation.

4.9.6 Revocation checking requirement for relying parties

It's recommend relying parties verify a certificate against the most recent CRL issued from the CA in order to validate the use of the certificate.

4.9.7 CRL issuance frequency (if applicable)

CRLs are updated and re-issued after every certificate revocation or at least seven days before the expiration of the previous CRL.

4.9.8 Maximum latency for CRLs (if applicable)

The CRL shall be copied to a removable device immediately after creation on the offline CA system and transfered without delay to the on-line repository.

4.9.9 On-line revocation/status checking availability

The latest CRL is always available from the UNLP PKIGrid website. The UNLP PKIGrid CA shall publish the CRL in effect in its repository (see 2.1). No other on-line checking is available now.

4.9.10 On-line revocation checking requirements

No stipulations.

4.9.11 Other forms of revocation advertisements available

Except for informing the owner of a newly revoked certificate and the appropriate RA of the issued revocation no advertisement of a new CRL other than its publication in the UNLP PKIGrid CA repository will be made.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

No stipulation.

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 UNLP PKIGrid CA shall store in its public repository and make them available via its web site:

- the root CA certificate
- all issues certificates

- and the most up-to-date CRL

4.10.2 Service availability

The UNLP PKIGrid CA shall run this service available continuously, in the reasonable effort, except for unavoidable activities. Due to the nature of the Internet this service can not be guaranteed to be always accessible. Scheduled downtime will be announced on the CA's web page at least 48 hours in advance.

4.10.3 Optional features

No stipulation

4.11 End of subscription

The subscription ends with the expiry of the certificate if it is not renewed or rekeyed before that date. A subscription may end earlier if the subscriber requests a revocation of its certificate.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No key escrow or recovery services are provided. The key owner must take all steps to prevent a loss.

4.12.2 Session key encapsulation and recovery policy and practices

See 4.12.1

5 Facility, management and operational controls

5.1 Physical controls

The signing machine of the UNLP PKIGrid CA is offline at all times and in a safe when not in use. It is located at CESPI headquarters in La Plata. UNLP PKIGrid CA maintains a limited with an access control procedure to the system. All accesses to the server are limited to the UNLP PKIGrid CA staff of UNLP PKIGrid CA. The UNLP PKIGrid CA is run on a derivative of Debian Linux system.

5.1.1 Site location and construction

The UNLP PKIGrid CA is located at the following address: UNLP PKIGrid CA

Calle 115 y 50 S/N

B1900AYB La Plata

Argentina

Phone: 542214236609

Fax: 542214236610

5.1.2 Physical access

The CA operates in a controlled environment, where access is restricted to authorized people and logged. The machine hosting the CA private key is kept locked in a safe and the private key is locked in a different safe.

5.1.3 Power and air conditioning

The online machine(s) operates in an air conditioned environment and is(are) not rebooted or power-cycled except for essential maintenance.

The off line machine is switched off between signing operations. The machine operates in an air conditioned environment.

5.1.4 Water exposures

The building is in a zone not subject to floods.

5.1.5 Fire prevention and protection

The CA is stored in a non-flammable security box

5.1.6 Media storage

Removable media (USB sticks and disks) are stored in locked safe places to which only authorized personnel have access.

5.1.7 Waste disposal

Waste containing data to be protected (cryptographically relevant data like private keys or passphrases, or personal data) shall be disposed off in a way to guarantee that the information may not be re-used.

5.1.8 Off-site backup

A monthly backup will be stored in a different building of the University. The backup medium shall be stored in a fire proof safe room with restricted access.

5.2 Procedural controls

5.2.1 Trusted roles

No stipulations.

5.2.2 Number of persons required per task

At least 2 people shall be able to perform CA operator tasks in a non exclusive way.

5.2.3 Identification and authentication for each role

No stipulations.

5.2.4 Roles requiring separation of duties

Except for the management, no roles at the UNLP PKIGrid CA require separation of duties.

Information about a subscriber stored at the site of the UNLP PKIGrid CA and that is to be considered as private (see 9.4.2) shall only be accessible to the operators of the RA that administers that subscriber's requests.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All UNLP PKIGrid CA personnel shall have system administrator or analyst experience.

5.3.2 Background check procedures

- All access to the servers and applications that comprise the UNLP PKIGrid service is limited to UNLP PKIGrid CA system support staff.
- The RA Manager must be a paid employee of the Physical Organization hosting that Registration Authority and must be appointed by an Authority responsible for a Department within that physical organization.
- The RA Manager must be a member of that Department. The Authority will make a declaration to the CA Manager in writing on the organization's headed note paper. The information that must be contained in this letter is defined by the CA Manager.
- The RA Operator must be a paid employee of the site hosting that Registration Authority and will be appointed by the RA Manager concerned.
- The RA Manager will make a declaration to the CA Manager in writing on the organization's headed note paper. If the RA Operator is appointed in a different department from the RA Manager then the letter must be countersigned by an authority for the department in which the Operator is appointed. The information that must be contained in this letter is defined by the CA Manager. RA Operators must have certificates and must adhere also to the subscribers' Obligations.
- An RA Manager may appoint himself/herself as an RA Operator.
- An RA Manager may appoint any number of RA Operators.

5.3.3 Training requirements

All people acting as CA operator shall be trained on the job by the UNLP PKIGrid CA staff that have developed the CA interface.

5.3.4 Retraining frequency and requirements

Retraining shall be mandatory when new software or features, as well as new organizational procedures are introduced.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the event of unauthorized actions, abuse of authority or unauthorized use of entity systems by the CA or RA Operators, the CA manager may revoke the privileges concerned.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

All UNLP PKIGrid CA personnel shall be provided with all documentation required for successfully performing their task.

- It is the responsibility of the CA Manager to provide the CA Operators with a copy of the UNLP PKIGrid CA Operator's Procedure.
- It is the responsibility of the CA Manager to provide the RA Manager with a copy of the UNLP PKIGrid RA Manager's Procedure.
- It is the responsibility of the RA Manager to provide the RA Operator with a copy of the UNLP PKIGrid RA Operator's Procedure.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events shall be recorded:

UNLP PKIGrid CA host

- login / logout / reboot
- creation and signing of certificates
- revocation of certificates
- CRL issues

UNLP PKIGrid web/LDAP online server

- receipt of certificate revocation request
- validation of certificate request from RA
- export of CSR from RA
- issue and import of certificate to LDAP
- revocation of certificate
- CRL issues

5.4.2 Frequency of processing log

The log files shall be analyzed once a month or after a potential security breach is suspected or known; whichever comes first.

5.4.3 Retention period for audit log

The minimal retention period for the audit logs is 3 years for log files and LDAP data.

5.4.4 Protection of audit log

The audit logs shall only be accessible to the UNLP PKIGrid CA operators and managers and to authorized audit staff. The CA shall make best efforts to protect the logs.

5.4.5 Audit log backup procedures

The audit logs shall be backed-up on a removable medium no-rewriteble (WORM) every night.

The backup medium shall be stored in a fire proof safe room with restricted access.

The procedure of audit log backup is detailed in the document "CA_Obligations&Structure&Operations" published on the CA site.

5.4.6 Audit collection system (internal vs. external)

Internal

5.4.7 Notification to event-causing subject

No stipulations

5.4.8 Vulnerability assessments

No stipulations

5.5 Records archival

5.5.1 Types of records archived

See 5.4.1

5.5.2 Retention period of archive

The minimum retention period is 3 years.

5.5.3 Protection of archive

The archive shall be accessible to the UNLP PKIGrid CA operation and management personnel only.

5.5.4 Archive backup procedures

Records shall be backed up on removable media, which shall be stored in a fire proof safe room with restricted access.

5.5.5 Requirements for time-stamping of records

All event records shall bear a time-stamp.

5.5.6 Archive collection system (internal or external)

Internal.

5.5.7 Procedures to obtain and verify archive information

No stipulations.

5.6 Key changeover

Key changeover is the process to provide a new public key to a CA's users. When the CA's cryptographic data needs to be changed, such a transition shall be managed; from the time of distribution of the new cryptographic data, only the new key will be used for certificate signing purposes. The overlap of the old and new key must be at least the longest time an end-entity certificate can be valid. The older but still valid certificate must be available to verify old signatures – and the secret key to sign CRLs – until all the certificates signed using the associated private key have also expired.

The CA will generate a new root key pair at least one year before the expiry of the CA certificate. In the final year the CA's old certificate will be available for validation purposes only, whereas new certificates and CRLs will be signed with the new CA key.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

- If an RA Operator s private key is compromised or suspected to be compromised, the RA Operator or Manager must inform the CA and request the revocation of the RA Operator s certificate.
- If the CA's private key is (or suspected to be) compromised, the CA will:
  - ✓ make every reasonable effort to notify subscribers and RAs,
  - ✓ terminate issuing and distributing certificates and CRLs,
  - ✓ request revocation of the compromised certificate,
  - ✓ generate a new CA key pair and certificate and publish the certificate in the repository,
  - ✓ revoke all certificates signed using the compromised key, and publish the new CRL on the UNLP PKIGrid CA repository.

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

The CA will take best effort precautions to enable recovery.

In order to be able to resume operation as fast as possible after the compute basis of the CA is corrupted the following steps shall be performed:

- All CA software shall be backed-up on removable media after a new release of any of its components is installed.
- All data files of the offline CA shall be backed-up on a removable medium after each change, before the session is closed.

In case of corruption of any part of the running system, a functioning hardware shall be loaded with the latest state of the software and data backed-up on a readonly medium and estimated to be uncorrupted. If not all encrypted copies of the UNLP PKIGrid CA private key are destroyed or lost, and are not compromised, the operation shall be re-established as soon as possible without need to revoke all issued certificates.

5.7.3 Entity private key compromise procedures

In case the key of an end entity is compromised, the corresponding certificate MUST be revoked. All relying parties known to accept the key should be informed by the owner of the key.

5.7.4 Business continuity capabilities after a disaster

The UNLP PKIGrid CA is located inside a building that is part of governmental facilities for research and higher education. The plans for business continuity and disaster recovery for governmental activities related to research and education are applicable.

5.8 CA or RA termination

Before UNLP PKIGrid CA terminates its services, it will:

- Inform the Registration Authorities, subscribers and relying parties the CA is aware;
- Make information of its termination widely available;
- Stop issuing certificates;
- Revoke all certificates;
- Issue and publish CRL ;
- Destroy its private keys and all copies;
- Inform the TAGPMA

In the case of normal (scheduled) termination, the minimum notification time of the advance notice must be of 90 days.

The CA Manager at the time of termination shall be responsible for the subsequent archival of all records as required in section 5.5.2.

The CA Manager may decide to let the CA issue CRLs only during the last year (i.e. the maximal lifetime of a subscriber certificate) before the actual termination; this will allow subscribers' certificates to be used until they expire. In that case notice of termination is given no less than one year and 60 days prior to the actual termination, i.e. no less than 60 days before the CA ceases to issue new certificates.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

The key pair for the UNLP PKIGrid CA is generated by authorized CA staff on a computer which is not connected to the network. The keys are generated by trustworthy software using OpenSSL. The key pairs for natural-person (including RA agents), host or service certificates are generated by the requesting parties themselves on their system (web interface).

6.1.2 Private key delivery to subscriber

Each subscriber MUST generate his/her own key pair using the UNLP PKIGrid web interface. The CA does not generate private keys for its subscribers.

6.1.3 Public key delivery to certificate issuer

Subscribers' public keys are delivered to the issuing CA by the HTTPS protocol via the UNLP PKIGrid s web interface.

6.1.4 CA public key delivery to relying parties

The CA certificate (containing its public key) is delivered to subscribers by online transaction from the UNLP PKIGrid online web server. It can be downloaded form the repository (see 2.1).

6.1.5 Key sizes

Keys of length less than 1024 bits are not accepted. The UNLP PKIGrid CA key is of length 2048 bits.

6.1.6 Public key parameters generation and quality checking

No stipulations.

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

The keys may be used according to the type of certificate:

With an end-entity certificate for

- authentication
- non-repudiation
- data and key encipherment
- message integrity
- session establishment
- proxy creation

With the self-signed CA certificate

- certificate signing
- CRL signing

The CA s private key is the only key that can be used for signing certificates and CRLs.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

End entities shall use the web form available on the UNLP PKIGrid website for key and CSR generation.

The UNLP PKIGrid CA private key is generated using OpenSSL.

An extra instance of the private key encrypted with a randomly generated passphrase of at least 15 characters shall be stored on removable media which must be deposited in a safe and locked up place; the passphrase shall be stored on a different removable media or

written down, and the media or paper shall be placed in a sealed envelope and stored in a secure place.

No instance of the private CA key (plain or encrypted) shall reside on the permanent disc of any computer that is online.

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

This type of control is no yet installed

6.2.3 Private key escrow

Private keys must not be escrowed.

6.2.4 Private key backup

All backup copies of the CA private key are kept at least as secure as the one used for signing (i.e. encrypted, and on media locked in a safe). The passphrase for activating the backup is locked in a different safe from the one containing the encrypted key.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

The CA private key is activated by a passphrase which, for emergencies, is kept in a sealed envelope in a safe. The safe which contains the passphrase does not contain any copy of the private key.

6.2.8 Method of activating private key

The CA private key is activated by having the CA operator enter his/her personal passphrase and after the CA private key passphrase .

6.2.9 Method of deactivating private key

The plain private key shall only be stored in RAM and erased when the activity for which it is needed is finished.

6.2.10 Method of destroying private key

See 6.2.9.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

The CA archives all issued certificates on removable media that is stored offline in a secure vault.

6.3.2 Certificate operational periods and key pair usage periods

There is no stipulation as to the validity of the generated key pair. Only the validity of the certificate issued by the UNLP PKIGrid CA is defined by this CP/CPS document.

Subscribers' certificates have a validity period of 13 months (one year and one month) or less if the affiliation of the requesting party to the group participating in UNLP Grid is less than one year.

The CA certificate has a lifetime of 10 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The CA private key is protected by a strong passphrase which consist of at least 15 characters.

6.4.2 Activation data protection

All UNLP PKIGrid CA Operators know the activation data for the CA private key. No other person knows the activation data. However, the activation data for the CA private key is also kept in a sealed envelope in a safe in a separate location from the safes containing the private key and its backup copies.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The server hosting the CA product is run on a (Debian-based) Linux system with reasonable provenance.

No other services or software are loaded or operated on the CA server. The server will receive occasional patches and other adjustments if the security risk warrants, in the judgment of UNLP PKIGrid CA staff.

6.5.2 Computer security rating

No stipulations.

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 signing machine of the CA will never be connected to a computer network under any circumstances (it does not have a network adapter). Certificates are signed on a machine not connected to any kind of network, located in a secure environment and managed by a suitably trained person.

The public machine is protected by a suitably configured firewall.

6.8 Time-stamping

All time stamping of entries created on the online servers at the UNLP PKIGrid CA is based on the network time provided by the time server of UNLP PKIGrid CA, synchronized with the official time provided by the Astronomical Observatory of the Faculty of Astronomical and Geophysical Sciences of the U.N.L.P.

The hardware clock of the offline system for the certificate and CRL signing, which determines the time stamping of the certificates and the CRLs, will be synchronized by the operator whenever the host starts.

7 Certificate, CRL and OSCP profiles

7.1 Certificate profile

All certificates issued by the UNLP PKIGrid CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280.

7.1.1 Version number(s)

Only X.509 version 3 certificates are issued by the UNLP Grid CA.

7.1.2 Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in the UNLP Grid CA certificates are:

For natural person certificates:

▪ Basic Constraints:	critical, ca: false
▪ Subject Key Identifier:	hash
▪ Authority Key Identifier:	keyid
▪ Subject Alternative Name:	Email
▪ Key Usage:	critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
▪ Extended Key Usage	clientAuth, emailProtection, codeSigning timeStamping
▪ Netscape Cert Type:	SSL Client, S/MIME, Object Signing
▪ Netscape Comment:	STRING
▪ CRL Distribution Points:	URI
▪ Certificate Policies:	OID
▪ Issuer alternative Name:	Email
▪ nsRevocationUrl	URI
▪ nsCaPolicyUrl	URI

For server/services certificates:

▪ Basic Constraints:	critical, ca: false
▪ Subject Key Identifier:	Hash
▪ Authority Key Identifier:	Keyid
▪ Subject Alternative Name:	DNS, Email
▪ Key Usage:	critical, digitalSignature, KeyEncipherment, dataEncipherment
▪ Extended Key Usage	serverAuth, clientAuth, timeStamping
▪ Netscape Cert Type:	SSL Server, SSL Client
▪ Netscape Comment:	STRING
▪ CRL Distribution Points:	URI (CRL)
▪ Certificate Policies:	OID
▪ Issuer alternative Name:	Email
▪ nsRevocationUrl	URI
▪ NsCaPolicyUrl	URI

For CA certificates:

▪ Basic Constraints:	critical, ca: true
▪ Subject Key Identifier:	hash
▪ Authority Key Identifier:	keyid
▪ Key Usage:	Critical, KeyCertSign, CRLSign
▪ Netscape Comment:	STRING
▪ CRL Distribution Points:	URI
▪ nsRevocationUrl	URI
▪ NsCaPolicyUrl	URI

7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by the UNLP Grid CA are according to:

- hash function: id-sha1 1.3.14.3.2.26
- encryption: rsaEncryption 1.2.840.113612.1.1.1
- signature: sha1WithRSAEncryption 1.2.840.113612.1.1.5

7.1.4 Name forms

Each entity has a unique and unambiguous Distinguished Name (DN) in all the certificates issued to the same entity by the UNLP PKIGrid CA. The DN shall be structured as defined in ITUT Standards Recommendation X.501.

Issuer:

C=AR, O=e-Ciencia, OU=UNLP, L=CeSPI, CN=PKIGrid,

Subject EE:

C=AR, O=e-Ciencia, OU=UNLP CN=Javier Diaz

L will indicate the RA name. The valid RAs list will be publish in the public site.

7.1.5 Name constraints

There are no other name constraints than those that are to be derived from the stipulations in 7.1.4, 3.1.2 and 3.1.1.

7.1.6 Certificate policy object identifier

The OID of this CP/CPS is 1.2.840.113612.5.4.2.3.1.0.2.7.

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 UNLP PKIGrid CA creates and publishes X.509 v2 CRLs.

7.2.2 CRL and CRL entry extensions

The UNLP PKIGrid CA shall issue complete CRLs for all certificates issued by itself independently of the reason for the revocation. The reason for the revocation shall not be included in the individual CRL entries.

The CRL shall include the date by which the next CRL shall be issued. A new CRL shall be issued before this date if new revocations are issued.

The CRL extensions that shall be included are:

- The Authority Key Identifier
- The CRL Number

No CRL entry extensions will be used.

7.3 OCSP profile

Not used.

7.3.1 Version number(s)

No stipulations.

7.3.2 OCSP extensions

No stipulations.

7.3.3 Name constraints

There are no other name constraints than those that are to be derived from the stipulations in 7.1.4, 3.1.2 and 3.1.1.

7.3.4 Certificate policy object identifier

The OID of this CP is 1.2.840.113612.5.4.2.3.1.0.2.7.

7.3.5 Usage of Policy Constraints extension

No stipulation.

7.3.6 Policy qualifiers syntax and semantics

No stipulation.

7.3.7 Processing semantics for the critical Certificate Policies extension

No stipulation.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

The UNLP PKIGrid CA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.

The CA shall at least once a year assess the compliance of the procedures of each RA with the CP/CPS document in effect.

The internal operational audits must be carried by people not related to the CA/RA staff. The internal audits must be performed at least once per year.

8.2 Identity/qualifications of assessor

No stipulations

8.3 Assessor's relationship to assessed entity

The assessments are made by personnel of the UNLP PKIGrid CA or members of the UNLP Grid community.

An external audit can be performed by any Argentine government department or academic institution.

If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of UNLP PKIGrid CA's personnel and infrastructure.

8.4 Topics covered by assessment

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

8.5 Actions taken as a result of deficiency

In case of a deficiency, the UNLP PKIGrid CA Manager will announce the steps that will be taken to remedy the deficiency. This announcement will include a timetable.

If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

8.6 Communication of results

The CA Manager will make the result publicly available on the CA web site with as many details of any deficiency as (s)he considers necessary.

9 Other business and legal matters

9.1 Fees

No fees are charged for the certification service for the UNLP PKIGrid CA constituency and therefore there are no financial encumbrances.

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

No fees are charged for access to CP and CPS or other CA status information.

9.1.5 Refund policy

See 9.1.

9.2 Financial responsibility

No Financial responsibility is accepted for certificates issued under this policy.

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

The UNLP PKIGrid CA service collects information about the subscribers. Information included in issued certificates and CRLs is not considered confidential.

The UNLP PKIGrid CA collects a subscriber's name, work telephone numbers and e-mail address. Additionally, for RA Managers and Operators, personal contact information is kept by the CA (work telephone number, work address).

Under no circumstances will the UNLP PKIGrid CA have access to the private keys of any subscriber to whom it issues a certificate.

9.4.1 Privacy plan

Not yet defined.

9.4.2 Information treated as private

The information provided by the subscriber to verify his/her identity will be kept confidential except those included in the certificate.

9.4.3 Information not deemed private

Information included in issued certificates and CRLs is not considered confidential. RA contact information is not considered confidential since this information is generally available from the web pages of the RA s employer.

Statistics regarding certificates issuance and revocation contain no personal information and is not considered confidential.

9.4.4 Responsibility to protect private information

The responsibility to protect private information rests with the UNLP PKIGrid CA and all its accredited RAs.

9.4.5 Notice and consent to use private information

In case the UNLP PKIGrid CA or any of its accredited RAs wants to use private information it must ask the subscriber for a written consent. No subscriber shall be under the impression that he/she has an obligation to agree.

9.4.6 Disclosure pursuant to judicial or administrative process

The CA will not disclose confidential information to any third party unless authorized to do so by the subscriber or when required by law enforcement officials who exhibit the appropriate legal documentation.

9.4.7 Other information disclosure circumstances

Disclosure upon owner's request is done according to the Data Protection Law. Specifically, information is released to the subscriber if the CA has received a signed e-mail from the subscriber requesting the information. The CA charges no fee for this.

The CA will recognize requests in writing for the release of personal information from a subscriber provided the subscriber can be properly authenticated.

9.5 Intellectual property rights

The UNLP PKIGrid CA does not claim any IPR on certificates which it has issued.

Parts if this document are inspired or even copied (in no particular order) from the AUSTRIANGRID, CERN, CNRS, the German Grid, UK e-Science, IRISGrid, GRID Canada, and may be indirectly from documents they draw from.

Anybody may freely copy from any version of the UNLP PKIGrid CA' s Certificate Policy and Certification Practices Statement provided they include an acknowledgment of the source.

The UNLP PKIGrid CA must grant to the TAGPMA and IGTF the right of unlimited re-distribution of its information.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The UNLP PKIGrid CA guarantees to issue certificates only to subscribers identified by requests received from RAs via secure routes. The UNLP PKIGrid CA will revoke a certificate only in response to an authenticated request from the subscriber, or the RA which approved the subscriber's request, or if it has itself reasonable proof that circumstances for revocation are fulfilled.

The UNLP PKIGrid CA does not warrant its procedures, nor takes responsibility for problems arising from its operation or the use made of the certificates it provides and gives no guarantees about the security or suitability of the service.

The CA only guarantees to verify subscriber's identities according to procedures described in this document.

The CA does not accept any liability for financial loss, or loss arising from incidental damage or impairment, resulting from its operation. No other liability, implicit or explicit, is accepted.

9.6.2 RA representations and warranties

All accredited RAs shall perform their task of identification of the requesting parties as described in 3.2.3 and 3.2.2 to the best of their ability. No other warranties are accepted.

An RA can conclude, at its strictly own risk, a more stringent agreement with its subscribers, but this shall never commit the UNLP PKIGrid CA nor any of its other accredited RAs.

It is the RA's responsibility to request revocation of a certificate if the RA is aware that circumstances for revocation are satisfied.

9.6.3 Subscriber representations and warranties

By requesting an UNLP PKIGrid CA certificate a subscriber commits itself to use and protect the certificate and the certified keys according to the stipulations of the CP/CPS document in effect at the date of issuance of the said certificate. (S)he may however apply more stringent observances.

Subscribers must:

- Read and adhere to the procedures published in this document
- Use the certificate for the permitted purposes only
- Authorize the processing and conservation of personal data (as required under the Data Protection Law)
- Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:
  - (Personal certificates) selecting a Strong Passphrase;
  - (Personal certificates) protecting the passphrase from others;
- Notifying immediately the UNLP Grid CA and any relying parties if the private key is lost or compromised;
- Requesting revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate.

In case of a breach of stipulations of the CP/CPS document that the subscriber has agreed to by requesting the UNLP PKIGrid CA certificate the certificate shall be revoked immediately. No further warranties are required from the subscriber.

9.6.4 Relying party representations and warranties

A relying party should accept the subscriber's certificate for authentication purposes if:

- The relying party is familiar with the CA's CP and the CPS that generated the certificate before drawing any conclusion on trust of the subscriber's certificate; and
- The reliance is reasonable and in good faith in light of all circumstances known to the relying party at the time of reliance; and
- The certificate is used for permitted purposes only; and
- The relying party checked the status of the certificate to their own satisfaction prior to reliance.

The CRL must be validated by the relying party and the subscriber's certificate must be check against the CRL.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

The UNLP PKIGrid CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness

Also the UNLP PKIGrid CA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who got in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.

Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

9.8 Limitations of liability

Except if explicitly dictated otherwise by the Argentine law the UNLP PKIGrid CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party.

It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP/CPS.

9.9 Indemnities

The UNLP PKIGrid CA declines any payment of indemnities for damages arising from the use or rejection of certificates it issues.

End entities shall indemnify and hold harmless the UNLP PKIGrid CA and all appropriate RAs operating under this CP/CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CP/CPS document.

9.10 Term and termination

9.10.1 Term

This document becomes effective after its publication on the Web site of the UNLP PKIGrid CA starting at the date announced there.

No term is set for its expiration.

9.10.2 Termination

This CP/CPS remains effective until it is superseded by a newer version.

9.10.3 Effect of termination and survival

Its text shall remain available for 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

All e-mail communications between the CA and its accredited RAs MUST be signed with a certified key.

All e-mail communications between the CA or an RA and a subscriber MUST be signed with a certified key in order to have the value of a proof.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are not considered amendments.

9.12.2 Notification mechanism and period

The amended CP/CPS document shall be published on the UNLP PKIGrid CA Web pages at least 2 weeks before it becomes effective.

The UNLP PKIGrid CA will inform its subscribers and all relying parties it knows of by means of an e-mail.

9.12.3 Circumstances under which OID must be changed

Each new version of the CP/CPS MUST change the OID. The decision of change the version is made by the manager of the UNLP PKIGrid CA and submitted to the TAGPMA for approval.

9.13 Dispute resolution provisions

Disputes arising out of the CP/CPS shall be resolved by the Manager of the UNLP PKIGrid CA.

9.14 Governing law

The UNLP PKIGrid CA and its operation are subject to the Argentine law. All legal disputes arising from the content of this CP/CPS document, the operation of the UNLP PKIGrid CA and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by UNLP PKIGrid CA shall be treated according to Argentine law.

9.15 Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of a UNLP PKIGrid CA certificate must comply with the Argentinian law.

Activities initiated from or destined for another country than Argentina must also comply with that country's law

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS document supersedes any prior agreements, written or oral, between the parties covered by this present document.

9.16.2 Assignment

No provisions.

9.16.3 Severability

Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

Events, compromising the UNLP PKIGrid CA services, that are outside the reasonable control of the UNLP will be dealt with immediately by the TAGPMA and IGTF.

9.17 Other provisions

No stipulation.

10 References

- Certification Authority AustrianGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.0.0, March 2005 https://ca.austriangridca.at/CP_CPS/AustrianGridCA_CP_CPS_1_0_0.pdf.
- SWITCH (the Swiss Education & Research Network) Certificate Policy and Certification Practice Statement (CP/CPS) ver:1.1.6 http://www.switch.ch/pki/SWITCH_CP-CPS.pdf
- DOEGrids Certificate Policy And Certification Practice Statement. Version 2.6. http://www.doegrids.org/Docs/CP-CPS.pdf
- Esnet Root CA Certificate Policy And Certification Practice Statement, Version 1.3, September 2003 http://www.ar.net/CA/d1b603c3/Certificate%20Policy.pdf
- Eugridpma. European Policy Management Authority for Grid Authentication http://www.eugridpma.org/
- Grid Canada Certification Authority Certificate Policy and Certification Practices Statement. http://www.gridcanada.ca/ca/gc-ca-cp-cps-1.1.htm
- IGTF. International Grid Trust Federation. http://www.gridpma.org/
- R. Housley, W. Ford, W. Polk and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and CRL Profile" , RFC 2459,January 1999 http://www.ietf.org/rfc/rfc2459.txt
- R. Housley, W. Polk, W. Ford and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" , RFC 3280, April 2002 http://www.ietf.org/rfc/rfc3280.txt
- RedIris Certification Authority Certificate Policy and Certification Practices Statement http://www.irisgrid.es/pki/policy/1.3.6.1.4.1.7547.2.2.4.1.0.0/
- S. Chokani and W. Ford, " Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework" , RFC 2527, March 1999 http://www.ietf.org/rfc/rfc2527.txt
- S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, " Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" , RFC 3647, November 2003 [replaces RFC 2527] http://www.ietf.org/rfc/rfc3647.txt
- TAGPMA. The Americas Grid Policy Management Authority. http://www.tagpma.org/
- The Americas Grid. Policy Management Authority Charter. September 20, 2005

- UK eScience Certification Authority Certificate Policy and Certification Practices Statement, Version 1.1, March 2005 http://www.grid-support.ac.uk/files/cps/cps-1.1.pdf