Certification Authority
pkIRISGrid CA

Certificate Policy and
Certification Practice Statement

Version 1.3.0

Document OID: 1.3.6.1.4.1.7547.2.2.4.1.3.0

October 30, 2012

Contents

1 Introduction

This document is structured according to RFC 3647. Not all sections of RFC 3647 are used. Sections that are not included have a default value of “No stipulation”. This document describes the set of rules and procedures established by RedIRIS for the operations of the pkIRISGrid CA service. RedIRIS has premises in two Spanish cities: Madrid and Seville. The data center housing the pkIRISGrid CA server is located in Seville.

This document will include both the Certificate Policy and the Certification Practice Statement for the pkIRISGrid 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

IRISGrid is the infrastructure to support e-science activities provided by the Spanish NREN RedIRIS.

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

http://pki.irisgrid.es/

1.2 Document name and identification

Title:	pkIRISGrid CA Certificate Policy (CP) and Certification Practice Statement (CPS)
Version:	1.3.0, October 30, 2012
Expiration:	This document is valid until further notice.
OID assigned:	1.3.6.1.4.1.**7547.2.2.4**.*1.3.0*
OID structure:	
1.3.6.1.4.1	IANA iso(1). org(3). dod(6). internet(1). private(4). enterprise(1)
7547	RedIRIS
2	Objects related to PKI-X.509
2	Objects related to digital identities
4	pkIRISGrid CA Certification Policy and CPS
1.3.0	Version of this CP/CPS

The currently valid version of the text is available from http://pki.irisgrid.es/ca/policy/

1.3 PKI participants

1.3.1 Certification authorities

The pkIRISGrid CA does not certificate to subordinate Certification Authorities.

Certificates of the pkIRISGrid CA are issued by people of the CA Operations Staff: no automated issuing is allowed. The CA operating personnel is designated by the pkIRISGrid CA Manager, and the manager and operators are responsible for the operational service of the pkIRISGrid CA. Information about the CA Manager can be found in section 1.5.2.

1.3.2 Registration authorities

The pkIRISGrid CA does not perform the role of RA.

Each participant in IRISGrid may appoint an individual who will act as RA for its own members and servers. It's also possible that one RA can manage members and servers for others participants in IRISGrid if there not exists any RA for these users.

The list of RAs for the IRISGrid is available from the pkIRISGrid website

http://pki.irisgrid.es/

1.3.3 Subscribers

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

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 pkIRISGrid CA.

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

They may only be used or accepted for actions authorized by the certificate keys.

1.4.2 Prohibited certificate uses

The certificates issued by pkIRISGrid CA must not be used for financial transactions.

They must not be used for purposes that violate Spanish law 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

RedIRIS is responsible for registration, maintenance, and interpretation of this CP/CPS. It is reachable at:

RedIRIS
Edificio Bronce
Plaza de Manuel Gómez Moreno s/n – 2ª planta
28020. Madrid
Spain

Home page: http://www.rediris.es

1.5.2 Contact person

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

Javi Masa (manager of the pkIRISGrid CA)
RedIRIS
Edificio CICA.
Avenida Reina Mercedes s/n.
41012. Seville
Spain

Phone: +34 95 505 66 23
Fax: +34 95 505 66 27
e-mail: pkirisgrid-ca@rediris.es

1.5.3 Person determining CPS suitability for the policy

The manager of the pkIRISGrid 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 EUGridPMA 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.

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).

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 message’s sender.

Certification Authority (CA)

> An authority trusted by one or more subscribers to create and assign public key certificates and to be responsible for them during their whole lifetime. That entity / system issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA)

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.

Community RM

> One or more RMs that serve multiple, low request rate, sites / Virtual Organizations.

Host Certificate

> A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine. Host Certificates are used internally by the PKI service and are not issued to other sites/VOs

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.

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.

Point of Contact

The member of a site/VO RA that has been chosen to handle all communications about policy matters with the pkIRISGrid manager.

Private RM

RMs that serve high certificate request rate sites / Virtual Organizations, and that are operated by the site/VO.

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).

Registration Agent (RAg) or “Agent”

RAg is the entity that interacts with the RM in order to cause the CA to issue certificates.

Registration Manager (RM)

The RM is a front-end Web server for the CA that provides a Web user interface for CA subscribers and agents. The RM forwards certificate signing requests to the actual CA to issue X.509 certificates.

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 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. (i.e. PPDG, FNC, EDG, etc).

2 Publication and repository responsibilities

2.1 Repositories

The online repository of information from the pkIRISGrid CA is accessible ate the URI http://pki.irisgrid.es/

2.2 Publication of CA information

The pkIRISGrid CA will operate a secure online repository that contains:

- The pkIRISGrid CA's certificate, and all previous ones necessary to check still valid certificates,
- The certificates issued by the PKI,
- A Certificate Revocation List,
- A copy of the most recent version of this policy and all previous versions,
- Other information deemed relevant to the pkIRISGrid CA service.

2.3 Time of frequency of publication

All information published shall be up-to-date.

Certificates will be published to the pkIRISGrid CA repository as soon as issued.

The certificate revocation list (CRL) shall have a lifetime of at most 30 days. The pkIRISGrid 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 Monday-Friday it may run unattended "at risk".

The pkIRISGrid 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 `CN=javi.masa`
- For Server the server fully qualified domain name (FQDN). The name must be in lower case. IP address are nor accepted
- For Services the name of the service, the character '/' and the FQDN of the server. The name must be in lower case. IP address are nor accepted

Common Names (CNs) must be encoded as PrintableStrings. The maximal length of the CN is 128 characters for all types of certificates. The character set allowed for Common Names in personal certificates is

'0' - '9', 'a' - 'z', '.', '-'

that is, decimal digits, lower case US ASCII letters full stop and hyphen. If Common Name includes letters which are not present among letters present in the above list, then those letters MUST be substituted with the appropriated letters according to the rules given in the document named "*Guía Básica sobre la Gestión del Servicio de Directorio*"

`http://www.rediris.es/ldap/doc/gb/gb-ldap-01.txt`

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. Subscribers can neither be anonymous nor pseudonymous.

3.1.3 Anonymity or pseudonymity of subscribers

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 (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=javi.masa`

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

  ```
  CN=serv1.rediris.es
  ```

- 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/serv1.rediris.es
  ```

3.1.5 Uniqueness of names

The Distinguished Name must be unique for each subject name certified by the pkIRISGrid CA service. The pkIRISGrid 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.

Subscribers must not share certificates.

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

A request of a certificate is initiated by a key generation tag or control which the user's web browser reads on the CA's user registration web page. Key and certificate signing request generation and submission are tied together in a single SSL session, and there is a reasonable presumption of possession of private key in requests originating in web browser functions.

A downloadable PDF file containing a hash verification code is generated based upon the CSR and other subject's data. This hash code is also generated by the RA and verified afterwards.

Re-keying employs a proof of possession of private key.

3.2.2 Authentication of organization identity

The RA 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 pkIRISGrid 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 appropriate RA and the pkIRISGrid CA. The RA has to ascertain that the organization or organizational unit exists and is entitled to request an IRISGrid 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.

Accepted documents:

- Spanish citizens: NID, passport or driving license.
- Europe Union citizen: Passport or NID with portrait photography.

- Foreign citizens: Passport or definitive NIE card (Foreigners Identification Number in spanish).

The use of electronic NID will not avoid a face to face meeting with the RA Operator.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

Any organization or unit willing to apply for pkIRISGrid certificates shall appoint one or more representatives who are entitled to request server or service/application certificates and answer all questions related to natural-person certificate requests.

These representatives shall be the first in their organization/unit to request individual certificates according to the provisions outlined in 3.2.3. The signatures of these individuals with the private key associated with the certified public key shall be sufficient for all future information exchanges with or requests from that organization/unit.

When the organization/unit rescinds the individual's authorization it has to inform the RA and the pkIRISGrid CA in the same way as it has made the authorization known.

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

Before the certificate expires, and providing that the last identification in accordance to Section 3.2.3 is not older than 5 years, re-key can be done using a secure web interface which checks the validity of the subject's certificate . Expiration warnings will be sent to subscribers 30 days and 7 days before it is re-key time.

In all the other cases re-keying follows the same rules as an initial registration.

3.3.2 Identification and authentication for re-key after revocation

Re-key after revocation follows the same rules as an initial registration.

3.4 Identification and authentication for revocation request

Unless the revocation request originates from the pkIRISGrid CA 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. Before revoking a certificate the pkIRISGrid CA has to authenticate the source of the request as it did for the request for certification.

In case of emergency the revocation can be initiated via oral communication with the appropriate RA or the pkIRISGrid CA. The RA or the pkIRISGrid CA have to use their best effort to authenticate the request.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The pkIRISGrid CA issues certificates to members of IRISGrid for:

- natural persons for which they take full responsibility,
- hosts administered by the requesting organization, and
- services provided on a host that is administered by an eligible organization.

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 pkIRISGrid web site. 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:
  - Selecting a strong passphrase;
  - Protecting the passphrase from others;
  - Notifying immediately the IRISGrid 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 pkIRISGrid administration module to shows all validate pending CSRs. In the case of a server/service request it must also check that the user is a representative (see 3.2.5) of the organization or unit responsible for the host.

4.2.2 Approval or rejection of certificate applications

Upon successful authentication an electronic copy of the requesting party's identification document and the certification request shall be sent signed by the RA to the pkIRISGrid CA. Alternatively, a secure transmission to the pkIRISGrid CA may be used, if it is at least as secure as a signed e-mail.

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.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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

4.3.2 Notification to subscriber by the CA of issuance of certificate

The pkIRISGrid 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 will be valid for one year 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 pkIRISGrid CA of the rejection of a certificate, explaining the pkIRISGrid CA an the RA the reasons for the rejection. Certificates whose rejection have not been received by the pkIRISGrid CA within a week shall be considered accepted.

4.4.2 Publication of the certificate by the CA

The pkIRISGrid 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 pkIRISGrid 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.

4.5.2 Relying party public key and certificate usage

A relying party must, upon being presented with a certificate issued by the pkIRISGrid CA check

- its validity by

- checking that it trusts the CA that issued the certificate,
- checking that the certificate hasn't expired
- consulting the pkIRISGrid CA CRL in effect at the time of use of the certificate or querying the certificate's validity using the OCSP facility, after its planned installation.

- the appropriate usage as outlined in the CP pointed to by the certificate and in the usage keys included in the certificate.

4.6 Certificate renewal

The pkIRISGrid CA SHALL NOT support certificate renewal. See 4.7 for more information.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

A certificate re-key will take place in these scenarios:

- The certificate is about to expire. See section 3.3.1 for more information.
- The certificate is expired: follows the same rules as an initial registration.
- The certificate is revoked: follows the same rules as an initial registration.

A subscriber MAY request for a certificate re-key at his/her own discretion.

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

4.7.4 Notification of new certificate issuance to subscriber

The pkIRISGrid CA shall notify the subscriber of the issuance as describes 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 pkIRISGrid 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 pkIRISGrid CA have been compromised or lost.

Subscribers must request revocation of its certificate as soon as possible, but within one working day after detection of:

- He/she lost or compromised the private key pertaining to the certificate.
- The data in the certificate are no longer valid.

4.9.2 Who can request revocation

A certificate revocation can be requested by

- the owner of the certified key
- the pkIRISGrid 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 private key;
- 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 pkIRISGrid 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 emergency, 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 pkIRISGrid 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. The pkIRISGrid CA shall process the authenticated request with priority and publish the revocation as fast as possible.

4.9.5 Time within which CA must process the revocation request

The pkIRISGrid CA must process revocation requests within one working day.

4.9.6 Revocation checking requirement for relying parties

Before using a certificate the relying party must validate it against the CRL (or, later, using the planned OCSP facility) most recently published in the pkIRISGrid CA repository.

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 pkIRISGrid web site. The pkIRISGrid CA shall publish the CRL in effect in its repository (see 2.1). No other on-line checking is available now, but it is planned to setup an OCSP facility.

4.9.10 On-line revocation checking requirements

Relying parties must check the CRL before they use and trust a certificate. No access control shall limit the possibility to check the CRL.

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

- the root CA certificate
- all valid certificates, and
- the most up-to-date CRL

4.10.2 Service availability

The pkIRISGrid CA shall run this service available continuously, except for unavoidable activities. Due to the nature of the Internet this service can not be guaranteed to be always accessible.

4.10.3 Optional features

It is planned that the pkIRISGrid CA will offer an OSCP service at a later date

4.11 End of subscription

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

5.1.1 Site location and construction

The pkIRISGrid CA is located at the following address:

RedIRIS
Edificio CICA.
Avenida Reina Mercedes s/n.
41012. Seville
Spain

The pkIRISGrid CA is located at RedIRIS premises in Seville, inside CICA building. Access to this building is monitored via closed- circuit TV and by construction suitably protected against burglary and break-ins. A security guard asks to visitors for their accreditation and there is a metal detector at entrance.

5.1.2 Physical access

The pkIRISGrid CA is offline at all times and in a safe when not in use.

RedIRIS maintains a limited (eyed) access procedure to the system. All accesses to the server are limited to the pkIRISGrid CA staff and system support staff of RedIRIS.

The CA operates in a controlled environment (locked room inside CICA building) where access is restricted to authorized RedIRIS staff and logged. The machine hosting the CA and a paper audit trail archive are kept locked in a PIN protected electronic safe while the private key is locked in a different safe. Only CA operators and managers have access to these safes.

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

5.1.4 Water exposures

The machine hosting the CA is stored at a height of 120 cm in the first floor of a building (approx, 350 cm from ground level). No water-cooled systems are used and there are no water pipes near the CA.

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

No stipulation

5.2 Procedural controls

5.2.1 Trusted roles

No stipulations.

5.2.2 Number of persons required per task

One.

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 pkIRISGrid CA require separation of duties.

Information about a subscriber stored at the site of the pkIRISGrid 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 pkIRISGrid 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 pkIRISGrid service is limited to RedIRIS 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 RedIRIS 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 pkIRISGrid 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 "IRISGrid CA Operator's Procedure".
- It is the responsibility of the CA Manager to provide the RA Manager with a copy of the "pkIRISGrid Manager's Procedure".
- It is the responsibility of the RA Manager to provide the RA Operator with a copy of the "pkIRISGrid Operator's Procedure".

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events shall be recorded:

- pkIRISGrid CA host
  - login / logout / reboot
  - creation and signing of certificates
  - revocation of certificates
  - CRL issues
- pkIRISGrid web/LDAP online server
  - receipt of certificate request
  - 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

All logs of issued certificates are stored in LDAP DB and logs lines are signed .

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 pkIRISGrid CA operators and managers. The protection shall be state-of-the-art best effort.

5.4.5 Audit log backup procedures

The audit logs shall be backed-up on a removable medium every night except on weekends and holidays when no activity happens on the offline host and only read access to the online repositories happens on the online server.

5.4.6 Audit collection system (internal vs. external)

internal

5.4.7 Notification to event-causing subject

Not defined

5.4.8 Vulnerability assessments

Not defined

5.5 Records archival

5.5.1 Types of records archived

See 5.4.1

5.5.2 Retention period for archive

The minimum retention period is 3 years.

5.5.3 Protection of archive

The archive shall be accessible to the pkIRISGrid 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 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

Not defined.

5.6 Key changeover

As the key generation is done by each entity (using a web browser) for their own use, no provision is made for a key changeover.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

- If the keys of an end entity are lost or compromised due to corruption of their computing basis, the appropriate RA has to be informed immediately in order to start the certificate revocation process.
- 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:
  - Inform the Registration Authorities, subscribers, relying parties, and cross-certifying CAs of which the CA is aware
  - Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key

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 pkIRISGrid 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 or an RA 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.

In case the private key of the pkIRISGrid CA is compromised (or suspected to be) the CA shall:

- 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 pkIRISGrid CA repository.

5.7.4 Business continuity capabilities after a disaster

The pkIRISGrid 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 pkIRISGrid 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 an publish CRL
- Destroy its private keys and all copies

An advance notice of no less than 60 days will be given in the case of normal (scheduled) termination. 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 pkIRISGrid CA is generated by authorized CA staff on a computer which is not connected to the network. The keys are generated by 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 pkIRISGrid 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 HTTP protocol via the pkIRISGrid'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 pkIRISGrid online web server. It can be downloaded from the repository (see 2.1).

6.1.5 Key sizes

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

6.1.6 Public key parameters generation and quality checking

Not defined.

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 and signing

- With an RA certificate for
  - some activities needed for the work of an RA agent
- 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 pkIRISGrid web site for key and CSR generation.

The pkIRISGrid CA private key is generated using OpenSSL.

Each CA operator shall have his/her own personal copy of the CA private key encrypted with a passphrase of at least 15 characters and only known to him/her. These encrypted private keys shall be stored on the offline computer of the pkIRISGrid CA.

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 envelop 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.

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 pkIRISGrid CA is defined by this CP/CPS document.

subscribers' certificates have a validity period of one year or less if the affiliation of the requesting party to the group participating in IRISGrid is less than one year.

The CA certificate has a validity period of 10 years.

6.4 Activation data

6.4.1 Activation data generation and installation

Each private key are protected by a strong passphrase which consist of at least 15 characters.

6.4.2 Activation data protection

All pkIRISGrid 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

Not defined.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The server hosting the CA product is run on a Guadalinex (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 RedIRIS staff.

6.5.2 Computer security rating

Not defined.

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 Certificate Authority will never be connected to a computer network under any circumstances. Certificates are generated 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 pkIRISGrid CA is based on the network time provided by the time server of RedIRIS, synchronized with the official providers of time signals in Spain.

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 manually by the operator whenever the host starts.

7 Certificate, CRL and OSCP profiles

7.1 Certificate profile

All certificates issued by the pkIRISGrid 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 IRISGrid CA.

7.1.2 Certificate extensions

The following certificate extensions are used for the issuance of certificates.

'O' stands for 'Optional'.

Certificate Extension	CA	User	Server
basicConstraints			
• *critical*	M	M	M
• *CA: TRUE*	M		
keyUsage			
• *critical*	M	M	M
• *digitalSignature*	M[1]	M	M
• *keyEncipherment*		M	M
• *dataEncipherment*		M	M
• *nonRepudiation*	M[1]		
• *keyCertSign*	M		
• *cRLSign*	M		
extendedKeyUsage			
• *clientAuth*		M	M
• *emailProtection*		O	
• *serverAuth*			M
nsCertType[1]			
• *SSL Certificate Authority*	M		
• *Email Certificate Authority*	M		
• *Object Signing*	M		
nsComment[1]			
• *STRING*	M		
cRLDistributionPoints			
• *URI: http://pki.irisgrid.es/ca/crl/cacrl.pem*	M	M	M
authorityKeyIdentifier			
• *KeyID*	M	M	M
subjectKeyIdentifier			
• *KeyID (hash)*	M	M	M
certificatePolicies			
• *(CP/CPS)*	M	M	M
• *(Classic CA) 1.2.840.113612.5.2.2.1*		M	M
subjectAlternativeName			
• *URI*		M	M
• *EMAIL*		O	
• *DNS*			M
issuerAlternativeName			
• *URI: http://pki.irisgrid.es/*		M	M

[1] Will be removed in the next CA certificate, which will be re-keyed in 2015.

7.1.3 Algorithm object identifiers

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

- hash function: id-sha1 1.3.14.3.2.26
- encryption: rsaEncryption 1.2.840.113549.1.1.1
- signature: sha1WithRSAEncryption 1.2.840.113549.1.1.5

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 pkIRISGrid CA. The DN shall be structured as defined in ITU-T Standards Recommendation X.501.

RedIRIS prefers that organizations use domain component naming.

Issuer:

DC=es, DC=irisgrid, CN=IRISGridCA

Subject:

DC=es, DC=irisgrid, O=string, CN=name.surname

DC=es, DC=irisgrid, O=string, CN=FQDN

The subject field contains the Distinguished Name of the entity with the following attributes:

Top-level domain (Spain)	es
IRISGrid domain	irisgrid
[Organization string]	[string]
CommonName	name [“.” surname]
	[service ”/”] FQDN

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 is: 1.3.6.1.4.1.7547.2.2.4.1.3.0

The OID referring to the IGTF Authentication Profile for “Classic X.509 Certification Authorities with Secured Infrastructure”, is 1.2.840.113612.5.2.2.1

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 pkIRISGrid CA creates and publish X.509 v2 CRLs.

7.2.2 CRL and CRL entry extensions

The pkIRISGrid 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

The CRL entry extensions that will be included are:

- CRL Reason Code
- Invalidity Date

7.3 OCSP profile

Not yet used.

7.3.1 Version number(s)

Not yet defined.

7.3.2 OCSP extensions

Not yet defined.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

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

8.2 Identity/qualifications of assessor

Not defined

8.3 Assessor's relationship to assessed entity

The assessments are made by personnel of the pkIRISGrid CA or members of the IRISGrid community.

An external audit can be performed by any Spanish 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 pkIRISGrid 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 pkIRISGrid 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 RedIRIS 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. The CA reserves the right to charge a fee for the release of personal information, as described in section 9.4.7.

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

The pkIRISGrid 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 pkIRISGrid CA have access to the private keys of any subscriber to whom it issues a certificate.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

The subscriber's e-mail address will be kept confidential unless the subscriber decides to make it public. The information provided by the subscriber to verify his/her identity will be kept confidential

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 pkIRISGrid CA and all its accredited RAs.

9.4.5 Notice and consent to use private information

In case the pkIRISGrid 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 regular warrant.

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. The CA reserves the right to charge a reasonable fee for the service in this case.

9.5 Intellectual property rights

The pkIRISGrid 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 AUSTRALIAGRID, CERN, CNRS, the German Grid, UK e-Science, and may be indirectly from documents they draw from.

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

This document typeset with OpenOffice.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The pkIRISGrid CA guarantees to issue certificates only to subscribers identified by requests received from RAs via secure routes. The pkIRISGrid 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 pkIRISGrid 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 knowledge. 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 pkIRISGrid 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 pkIRISGrid 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:
  - Selecting a Strong Passphrase;
  - Protecting the passphrase from others;

- Notifying immediately the IRISGrid 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 pkIRISGrid 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.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

The pkIRISGrid 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 pkIRISGrid 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 Spanish law the pkIRISGrid 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 pkIRISGrid 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 pkIRISGrid 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 pkIRISGrid 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. All requests for any action must be signed.

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 pkIRISGrid CA Web pages at least 2 weeks before it becomes effective.

The pkIRISGrid 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

Substantial changes shall cause the OID to be changed. The decision is made by the manager of the pkIRISGrid CA and submitted to the EUGridPMA for approval.

9.13 Dispute resolution provisions

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

9.14 Governing law

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

9.15 Compliance with applicable law

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

Activities initiated from or destined for another country than Spain 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 that are outside the control of the IRISGrid CA will be dealt with immediately by the EUGridPMA.

9.17 Other provisions

No stipulation.

10 References

- GFD-C.125 Grid Certificate Profile, CAOPS-WG, Open Grid Forum, 2008
  http://www.ogf.org/documents/GFD.125.pdf
- 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
- 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
- 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
- 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
- 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
- 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
- Esnet Root CA Certificate Policy And Certification Practice Statement, Version 1.3, September 2003
  http://www.es.net/CA/d1b603c3/Certificate%20Policy.pdf