



**Certification Authority
pkIRISGrid CA**

**Certificate Policy and
Certification Practice Statement
Changelog**

Version 1.4.3

September 10, 2013

List of Changes

1.4.3 – September 10, 2013

Several Sections

- Fixed orthographic erratas
- Changed “online repository” and “online server” for “web repository”
- Changed “offline host” for “CA machine”

Section 4.1.2

- Added details about the generation and storage of the private key for robot certificates.

Section 5.4.5

- Shortened/corrected paragraph.

Section 6.1.1

- Added details about the generation of the key pairs for robot certificates.

Section 6.1.2

- Added details about the generation of the key pairs for robot certificates.

1.4.2 – May 22, 2013

Section 1.1.1

- Added “is the only CA working for the spanish e-science”

Section 1.3.3

- Added the requirements for subscribers.

Section 3.3.1

- Added “and the subject must meet the requirements detailed in section 1.3.3”

Section 5.4.1

- Added details about pkIRISGrid RAs Operational Audits

Section 5.6

- Changed to include details about the CA cryptographic data. Now, we explain the process of re-keying the CA signing key.
- Moved “The CA certificate has a validity period of 10 years.” from section 6.3.2 to section 5.6

Section 6.2.8

- Added “In case of user, server or robot certificates, see 4.1.2”

Section 7.1.2

- Changed the CRL format from PEM to DER. Changed the cRLDistributionPoints to .crl

1.4.1 - February 04, 2013

Section 3.1.1

- Added the option to include a dash in the CN component of a natural person certificate.
- Changed the default example for a natural person to better understand the rules.

Section 3.1.4

- Added the option to include a dash in the CN component of a natural person certificate.
- Changed the default example for a natural person to better understand the rules.
- Fixed errata: “natural personal” -> “natural person”

Section 9.12.2

- Added “Users will not be warned in advance of changes made to the pkIRISGrid CA CP/CPS”.

1.4.0 - November 22, 2012

Section 1.3.3

- Added a new certificate profile: robot.

Section 1.4.1

- Added the word “robots” to accept authentication of robots.

Section 3.1.1

- Added a better example about the CN of personal certificates.
- Added complete information about the CN of robot certificates.

Section 3.1.4

- Added detailed information about the form of the CN's in robot certificates.

Section 4.1.1

- Added “robots, which are responsibility of a natural person or organization,”

Section 7.1.2

- Added robot profile to the certificate extensions table.

Section 7.1.4

- Added the name form of the robot certificates:
“Robot - <robot purpose> managed by <owner>”

- Added the line:

Note: [] denotes an optional component and is not written in the CN.
 < > denotes a nickname or description of the text and it is not written
 either.” for better explaining of the notation.

Section 7.1.6

- Added new two OID's which are being used for robot certificates
 - The OID referring to an non human client or robot entity is 1.2.840.113612.5.2.3.3.1
 - The OID of PKP regarding key material held in files is 1.2.840.113612.5.2.3.1.2.1

1.3.0 - October 30, 2012

Section 1.2

- Added CP/CPS download URL <http://pki.irisgrid.es/ca/policy/>

Section 1.3.1

- Added additional details about the running of pkIRISGrid CA.

Section 3.2.1

- Added method to prove possession of private key.

Section 3.2.3

- Changed to accept personal identity documentation in the European Union.

Section 3.3.1

- Modified to explain in detail the identification and authentication for routine re-key.

Section 3.3.2

- Changed text to “Re-key after revocation follows the same rules as an initial registration.”

Section 4.7.1

- Now describes the 3 common cases for re-keying certificates.

Section 4.9.5

- Now “The pkIRISGrid CA must process revocation requests within one working day.”

Section 5.1.1

- Modified section in order to give additional data and reorganize the current information between these two related sections about physical protection.

Section 5.1.2

- Modified section in order to give additional data and reorganize the current information between these two related sections about physical protection.

Section 5.1.4

- Added “No water-cooled systems are used and there are no water pipes or water sources near the CA.”

Section 5.5.1

- Added details about the logs: “All logs of issued certificates are stored in LDAP DB and logs lines are signed.”

Section 7.1.2:

- Overhaul of this section. Extensions featured in table format.
- Removed Netscape Cert Type and Comment from natural person and server certificates. Netscape extensions are deprecated.
- Added Subject Alternative Name and Issuer Alternative Name for natural person and server certificates. We had them in the CA but not written in the CP.
- Removed timeStamping from user and server certificates. Not needed.
- Removed codeSigning from user and server certificates. Not needed.
- Removed nonRepudiation from user and server certificate following “Grid Certificate Profile” (GWD-R. 125Bis version 5 from June 2012)
- Removed emailProtection from server certificates (not needed) and marked as Optional in user certificates.

1.2.0 - May 02, 2012

Section 4.6

- Correction of the renewal section

Section 4.7.1

- Added information about circumstances for certificate re-key

Section 4.9.1

- Subscribers must request revocation in some cases

1.1.5 - January 20, 2012

Section 6.7

- Removed “It has not any network adapter”

Section 7.1

- CRL is no longer registered by LDAP

1.1.4 - January 13, 2010

• Section 7.1.6

- Added “Classic X.509 Certification Authorities with Secured Infrastructure” OID 1.2.840.113612.5.2.2.1
- Added reference to GFD-C.125 Grid Certificate Profile

1.1.3 - January 28, 2008

Section 1.1

- pkIRISGrid URL changed to <http://pki.irisgrid.es/> from <http://www.irisgrid.es/pki/>

Section 1.3.2

- pkIRISGrid URL changed to <http://pki.irisgrid.es/> from <http://www.irisgrid.es/pki/>

Section 1.5.2

- Added fax number

Section 2.1

- pkIRISGrid URL changed to <http://pki.irisgrid.es/> from <http://www.irisgrid.es/pki/>

1.1.2 - May 11, 2007

Document

- Font family changed to Arial from Luxi-sans

Section 7.7.3

- Fixed typing errors

Section 6.1.4

- Fixed typing errors

Section 11

- Changed List of Changes section

1.1.1 - February 04, 2006

Document

- First official release after EUGridPMA accreditation

Before EUGridPMA accreditation

Document

- January 14, 2006. Official release presented to EUGridPMA
- November 11, 2005. First official release before EUGridPMA accreditation
- September 21, 2005. Beta release
- July 15, 2005. Initial alpha release CP/CPS