RDIG Certification Authority Certificate Policy and Certification Practice Statement, v. 1.2.2

August 19, 2021

Contents

Chapter 1

Introduction

1.1 Overview

This Certification Policy and Practice Statement (CP/CPS) is structured according to RFC 3647. It describes the set of rules used by RDIG Certification Authority (RDIG CA), operated by the Grid team of the National Research Centre “Kurchatov Institute” (NRC KI). RDIG stands for Russian Data-Intensive Grid.

This document can be referred as RDIG Certification Authority Certificate Policy and Certification Practice Statement version 1.2.2 or OID 1.3.6.1.4.1.22139.1.1.2.2.

1.2 Document Name and Identification

- Document name: RDIG Certification Authority Certificate Policy and Certification Practice Statement
- Version: 1.2.2
- Date:04.06.2021
- OID: 1.3.6.1.4.1.22139.1.1.2.2

1.3 PKI Participants

RDIG CA is one-level certification authority that issues X.509-certificates directly to its clients serving the respective (client) organizations.

RDIG CA Registration Authorities are nominated by the organizations from their staff members. One may consult the list of Registration Authorities if he/she seeks for more specific information.

RDIG CA subscribers are entities who are employed by or associated with the client organizations.

The set of RDIG CA relying parties is not strictly controlled: any relying party who finds RDIG CA and its practices suitable may elect themselves to put trust on the material issued by our CA and its processes, staff and infrastructure.

1.4 Certificate Usage

- The person certificates may be used for user authentication and data integrity checking in various applications: Globus, LCG, gLite and similar GRID middleware, electronic mail, Web server access, etc.
- The host certificates may be used for client/server authentication and communication encryption.
- The host application certificates may be used for client/server applications authentication and communication encryption.

All issued certificates must not be used for purposes that violate the applicable laws.

Issued certificates may not be used for financial transactions and for qualified digital signatures as described in Russian federal laws «On the electronic digital signatures» and related documents.

1.5 Policy Administration

1.5.1 Contact Person

The RDIG CA is operated by: Eygene Ryabinkin, NRC KI, Russia, 123128, Moscow, Kurchatov square, 1. Phone: +7 499 196-77-77, e-mail: rea@grid.kiae.ru.

1.5.2 Generic contact for the RDIG CA

E-mail: rdig-ca-support@grid.kiae.ru.

1.5.3 CP/CPS Contact Person

The contact person for this CP/CPS is: Eygene Ryabinkin, NRC KI, Russia, 123128, Moscow, Kurchatov square, 1. Phone: +7 499 196-77-77, e-mail: rea@grid.kiae.ru.

1.6 Definitions and Acronyms

- RDIG: Russian Data-Intensive Grid
- RA: Registration Authority
- CA: Certification Authority

- NRC KI: National Research Centre “Kurchatov Institute”
- CSR: certificate signing request

Chapter 2

Publication and Repository

The RDIG CA operates its own repository of all associated material: issued certificates, list of RAs, CRL, CP/CPS, guidelines, how-to documents and contact information. It is available online.

All described information is freely accessible to anyone.

All certificates are published upon their issuance and are kept available at least till they get superseded, revoked or expired,

New CRL is published upon its issuance. Issuances are done after each revocation and at least 7 days before expiration of previous CRL. The CRL validity time is 30 days.

New organizations are added to the subscribers list after their approval by RDIG management and short internal audit by the CA staff.

Contact information for new RA is published after reception of their initial contact details.

Other material is kept online since the beginning of CA operations and is refreshed on the "as needed" basis.

Chapter 3

Identification and Authentication

3.1 Naming

RDIG CA uses the following types of names for different types of certificates:

- distinguished names for a personal certificate: /C=RU/O=RDIG/OU=users/OU=Organisation/CN=Name
- distinguished name for a host certificate: /C=RU/O=RDIG/OU=hosts/OU=Organisation/CN=FQDN
- distinguished name for a host application certificate: /C=RU/O=RDIG/OU=services/OU=Organisation/CN=service name/FQDN

CN component of distinguished name for a personal certificate must contain the person's first and last names.

An optional OU attribute can be inserted between OU=Organisation component and the CN component in the cases when sole organisation name is not enough to clearly identify the administrative domain for the certificate holder. One example of such a situation is the organisation with rich administrative infrastructure and the loose administrative coupling between its units.

All distinguished names are unique: no different entities that are identified by RDIG CA certificates will posses the same DNs. In cases when user's first and last names coincide with existing (certified) ones, middle name or initial may be inserted into the CN field of the distinguished name. Other disambiguation types that add extra information to the first/last names pair can also be used.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

Each request must be signed with the private key corresponding to the public key provided in certificate request.

RDIG CA users fill the paper form, where the part of the request public key (10 initial and 10 ending digits) are specified: request generation procedure requires this. This form is presented to the RDIG CA Registration Authority, who checks the parts of the public key against the incoming electronic certificate request. Since the latter is digitally signed with the corresponding private key, this procedure both enables Registration Authority to prove user's possession of the private key (via the digital signature check) and the lack of electronic request modification (via the public key validation).

RDIG CA will neither generate nor store any private keys for subscribers.

3.2.2 Authentication of organization identity

RDIG CA Registration Authority verifies the organization identity by checking:

- that the organisation is known to participate in RDIG consortium,
- and the organisation is located in Russia or ex-USSR, by checking organisational contact information.

3.2.3 Authentication of individual identity

The RDIG CA Registration Authority verifies person's identity and its affiliation with the claimed organisation entity by face-to-face meeting with the person, who requests the certificate.

Person's identity is validated via the national ID or institutional ID (if the latter is created using person's personal data and is subjected to the data verification during creation/renewal; the details of the institutional ID issuance process are specific to each organization and Registration Authorities are obliged to make themselves to be familiar with the technical details for every type of IDs they intend to use during the validation).

Paper form for each request contains first and last names for the requestor (certificate user, host/service administrator); they are also a subject to this check. Additionally, for user certificates the Common Name component of the requested DN are requred to contain first and last names of the certificate owner (consult Section 3.1 for the relevant details on DN components).

3.2.4 Authentication of Registration Authority

Registration Authority, being the natural person, must be authenticated via the outlined mechanisms for the ordinary users, but in addition he/she must present the official paper request stamped and signed by responsible person within the organization he requests RA rights for.

3.3 Identification and Authentication for Re-key Requests

Registration Authorities can authenticate themselves in the re-keying process by signing their new CSR with the existing non-expired key of their current certificate.

If RA personal certificate is expired at the re-key time, he/she uses the ordinary route for authentication (the same as for the initial request authentication, see Section 3.2).

All other users follow the procedure of initial requets authentication for each re-key request.

Re-signing of an existing public key will not be done in any curcumstances.

RDIG CA will not recertify a revoked key. User of a revoked certificate must obtain a new one following the procedure of initial registration, described in Section 3.2.

3.4 Identification and Authentication for Revocation Requests

Revocation request must be authenticated, unless RDIG CA can independently verify that a key compromise has happened. The preferred method for authentification is electronic mail message, digitally signed with a non-expired and previously non-revoked certificate issued by RDIG CA.

If this is not possible, subscriber must contact the RDIG CA Registration Authority that verifies user's identity using procedures similar to those described in Section 3.2.1.

Chapter 4

Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

Applicants must generate their own key pair themselves; RDIG CA will never generate a key pair for an applicant. RDIG CA will not accept private key escrow responsibilities and will reject any certificate request containing the private key.

The minimum key length for all applications is 2048 bits. The maximum validity time for each certificate is one year and 31 days.

Generated certificate request must be sent via electronic mail or CA Web interface form to the designated RDIG CA certificate processing endpoint. This is attempted to be done automatically by request generation software; in the case of failure user is provided with detailed instructions on the manual application process.

4.2 Certificate Application Processing

RDIG CA will reject all non-legitimate certification requests; in the case of rejection applicant will be notified by electronic mail, except for obvious nonsense requests that will be rejected silently.

Legitimate requests will be made available to the respective registration authorities. Applicants will be supplied with the unique request identification number they can use to refer to their request at all times.

4.3 Certificate Issuance

Upon a receipt of a certificate request that is qualified to be valid according to this CP/CPS, RDIG CA Registration Authority will verify the request and authenticate applicant as described in Section 3.2. After successful verification and authentication, RDIG CA Registration Authority digitally signs new request and transfers it to RDIG CA, where certificate will be issued.

The applicant will be notified of issuance by electronic mail or using another means of communication, if requested by a subscriber. If communication fails permanently, the certificate will be revoked without further notice.

A certification request is normally handled in the period of one week, however, during vacation or national holidays periods the response time can increase to three weeks.

4.4 Certificate Acceptance

Valid certificate issued by the RDIG CA must pass the following requirements:

- Certificate must not be expired;
- Distinguished name must be in the RDIG CA name space, i.e. it must match one of the name templates described in Section 3.1;
- Certificate must have a valid RDIG CA signature which can be validated with RDIG CA certificate, that is available on the URL http://ca.grid.kiae.ru/RDIG/cacrt.pem
- Certificate must not be listed in the Certificate Revocaton List (CRL) issued by RDIG CA, that is available on the URL http://ice.grid.kiae.ru/ca/RDIG/cacrl.der
- The CRL must have a valid RDIG CA signature and must not be expired;
- To guarantee the maximum level of security one should check for new CRL just before validating the certificate.

No special steps must be taken by the applicant to constitute certificate acceptance. RDIG CA will publish the issued certificate at its Web site.

4.5 Key Pair and Certificate Usage

Subscribers and relying parties must use/validate certificate usage basing on the set of the key usage fields present in the respective certificate.

4.6 Certificate Renewal

No renewals are allowed.

4.7 Certificate Re-key

Certificate re-key can take place at any time and may be the result of nearing or actual certificate expiration, certificate revocation due to any curcumstances or loss of access to the corresponding private key.

Re-key process technically coincides with the oridinary certificate application process; its authentication is described in Section 3.3.

4.8 Certificate Modification

No certificate modifications are done.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

A certificate will be revoked when

- the information it contains is no longer correct or proved to be incorrect, or
- the private key is lost or suspected to be compromised, or
- the certification entity is no longer participates in the RDIG consortium projects, or
- RDIG CA have the proofs that certificate usage violates RDIG CA CP/CPS rules.

4.9.2 Who can request revocation

The certificate holder or any other entity presenting proof of knowledge of the private key compromise or subscriber's data variation can request a certificate revocation.

4.9.3 Procedure for the revocation request

RDIG CA will handle any revocation request, authenticated or unauthenticated. If RDIG CA can independently verify that a certificate has been compromised or misused, RDIG CA will revoke the certificate. In all other cases, the revocation request will be authenticated as described in Section 3.4.

Revocation request must be passed to the RDIG CA Registration Authority who signed the certificate request for the certificate to be revoked or his peer RA from the same administrative domain. The rules for passing revocation request to the RDIG CA Registration Authority are described in Section 3.4.

4.9.4 Revocation request grace period

Revocation request can be canceled within 24 hours after it was received at the RDIG CA. But in the case of proved compromise the certificate will be revoked immediately.

For cancellation of the revocation request the certificate holder must contact the same RA, as for the revocation request in question. The rules for passing cancellation request to the RDIG CA Registration Authority are just the same as in Section 3.4.

4.9.5 CRL issuance frequency

New CRL is published upon its issuance. Issuances are done after each revocation and at least 7 days before expiration of previous CRL. The CRL validity time is 30 days.

4.10 Certificate Status Services

RDIG CA maintains its CRL and publishes its up-to-date version at http://ice.grid.kiae.ru/-ca/RDIG/cacrl.der. RDIG CA technical staff makes all efforts to make the above endpoint to be available on the 24x7 basis.

4.11 End of Subscription

When RDIG CA subscriber decides to finish its usage of CA services (including all issued certificates) it notifies Registration Authority or CA personnel of this decision. Subscriber authentication steps are described in Section 3.4.

All active certificates associated with this subscriber are revoked upon verification of termination request.

4.12 Key Escrow and Recovery

No such services are provided by RDIG CA.

Chapter 5

Facilities, Management, and Operational Controls

5.1 Physical Security Controls

5.1.1 Site location

The RDIG CA is located at the National Research Centre “Kurchatov Institute” in Moscow, Russia and is hosted on a professional military-grade co-location area.

5.1.2 Physical access

Physical access to the RDIG CA hosts is restricted to authorized personnel.

5.1.3 Power and air conditioning

The RDIG CA signing machine and the RDIG CA Web server are both protected with uninterruptable power supplies. Environmental temperature in room containing RDIG CA related equipment is maintained at appropriate level by an air conditioning system.

5.1.4 Water exposures

Due to the location of RDIG CA facilities floods are not expected.

5.1.5 Fire prevention and protection

Buildings containing RDIG CA facilities obey to the Russian laws regarding fire prevention and protection of buildings.

5.1.6 Media storage

The RDIG CA key is kept on several removable storage media. Backup copies of CAname; related information are kept on CD-ROM and flash disks.

Both key material and backup copies are kept in the locked safe in the rooms accessible only by an authorized personnel.

5.1.7 Waste disposal

Waste carrying potential confidential information such as old storage media are physically destroyed before being trashed.

5.1.8 Off-site backup

No off-site backups are currently performed.

5.2 Procedural Controls

No stipulation.

5.3 Personnel Security Controls

5.3.1 Background checks and clearance procedures for RDIG CA personnel

RDIG CA personnel is recruited from the "Kurchatov Institute" Grid team. Registration Authorities personnel is recruited from the staff of the corresponding institutions/organizations.

5.3.2 Background checks and clearance procedures for other personnel

No other personnel is authorized to access RDIG CA facilities without the physical presence of and guidance by RDIG CA personnel.

5.3.3 Training requirements and procedures

Internal training is given to the RDIG CA operators and Registration Authorities operators.

5.3.4 Training period and retraining procedures

Repeated training is given on every change of this document or used software.

5.3.5 Frequency and sequence of job rotation

Job rotation is not performed.

5.3.6 Sanctions against personnel

No stipulation.

5.3.7 Controls on contracting personnel

No stipulation.

5.3.8 Documentation supplied to personnel

All personnel is supplied with copies of this document and RDIG CA Operation Manual.

5.4 Audit Logging Procedures

5.4.1 Types of event recorded

The following events are recorded:

- certificate requests (by persons),
- certificate acceptations (by Registration Authority),
- revocation requests (by Registration Authority),
- certificate issuance,
- certificate rekey and renewal requests.

5.4.2 Processing Frequency of Audit Logs

Not defined.

5.4.3 Retention period for Audit Logs

Audit logs will be kept for at least 3 years.

5.4.4 Protection of audit log

Audit logs may be consulted only by:

- RDIG CA personnel,
- authorized external auditors, including accredited EUGridPMA CA managers.

Audit logs are copied to an offline medium. Online audit logs are protected using the file system security.

5.5 Records Archival

5.5.1 Audit log backup procedures

Digital audit logs are copied to an offline medium.

Paper-based audit logs are kept in the secured archival area of RDIG CA facilities.

5.5.2 Audit collection system

The audit logs archive is internal to the RDIG CA.

5.6 Key Changeover

Public keys are distributed by electronic mail or using online system at the following URL: http://ca.grid.kiae.ru/RDIG/certificates/.

5.7 Compromise and Disaster Recovery

In case the RDIG CA private key is compromised the RDIG CA will:

- Notify all subscribers and cross-certifying Certification Authorities.
- Notify Registration Authorities.
- Terminate the issuance and distribution of the certificates and CRLs.
- Notify relevant security contacts.
- Notify as widely as possible about service termination.

In case the RDIG CA Registration Authority private key is compromised the RDIG CA will:

- Notify all subscribers and cross-certifying Certification Authorities.
- Notify Registration Authorities.
- Terminate the operation of the compromised Registration Authority.
- Revoke all certificates validated by the compromised Registration Authority.
- Notify as widely as possible about Registration Authority compromise.

5.8 CA or RA Termination

5.8.1 Certification Authority termination

Upon termination RDIG CA will:

- Notify all subscribers and cross-certifying Certification Authorities.

- Notify Registration Authorities.
- Terminate the issuance of certificates and CRLs.
- Notify relevant security contacts.
- Notify as widely as possible about service termination.

5.8.2 Registration Authority termination

Upon termination of RDIG CA Registration Authority the RDIG CA will:

- Notify other Registration Authorities in the same administrative domain.
- Remove Registration Authority from the list of active RAs.

Chapter 6

Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each subscriber must generate its own key pair. RDIG CA does not generate private keys for subscribers.

6.1.2 Private Key Delivery to Entity

Private key deliverance is not supported.

6.1.3 Public Key Delivery to Users

Public keys are delivered by electronic mail. They are also accessible from public Web page at http://ca.grid.kiae.ru/RDIG/certificates/.

6.1.4 RDIG CA Public Key Delivery to Users

RDIG CA public key is accessible from public Web page at http://ca.grid.kiae.ru/RDIG/cacrt.pem.

6.1.5 Key Sizes

The minimum key length for user, host or host application certificate is 2048 bits. The RDIG CA key length is 2048 bits.

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Key Generation Method

Keys are generated using software algorithms.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Private Key Protection

Each copy of the RDIG CA private key is protected by its own passphrase which is at least 22 characters long.

Private keys which correspond to the user certificates (be it an ordinary user or Registration Authority) must be protected by password with length of 15 or more characters.

All private keys must be protected with filesystem security controls which are configured on the "least sufficient privilege set".

No private keys are to be made accessible to

- (for user certificates) entities other than certificate owner;
- (for other certificate types) entities other than host/service administrators.

6.2.2 Cryptographic Module Engineering Controls

No stipulation.

6.3 Other Aspects of Key Pair Management

Maximal lifetime for each certificate is one year and 31 days.

6.4 Activation Data

See Section 6.2.1.

6.5 Computer Security Controls

6.5.1 Specific security technical requirements

The RDIG CA operating systems are maintained at a high level of security by applying all relevant patches. Monitoring is performed to detect unauthorized software changes.

6.5.2 Computer security rating

Not tested.

6.6 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The RDIG CA public-interface machine is protected by a firewall. The server access is restricted to a few stations.

6.8 Time-Stamping

No stipulation.

Chapter 7

Certificate, CRL, and OCSP Profile

7.1 Certificate Profile

7.1.1 Version number

X.509 v3.

7.1.2 Certificate extensions

The following extensions may be included in the certificate issued by RDIG CA:

- subjectKeyIdentifier: hash
- authorityKeyIdentifier: keyid:always
- basicConstraints (CRITICAL): CA:false
- keyUsage (CRITICAL): digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement
- certificatePolicies: OID 1.3.6.1.4.1.22139.1.1.2.2, Classic IGTF profile OID 1.2.840.113612.5.2.2.1
- issuerAlternativeName: e-mail address of RDIG CA
- subjectAlternativeName: subscriber's e-mail address for user certificate or FQDN for host/service certificate
- cRLDistributionPoints: URI
- nsCaPolicy: URL
- nsComments: an issuer description

- nsCertType: (for user certificates) client, email (S/MIME), objsign
- nsCertType: (for host/service certificates) client, server, objsign

7.1.3 Algorithm Object Identifiers

Certificates and certificate revocation lists must use at least SHA-256 signature digest and may use SHA-384 and SHA-512 digests.

7.1.4 Name forms

Issuer: C=RU,O=RDIG,CN=Russian Data-Intensive Grid CA. For Subject field name forms check Section 3.1.

7.1.5 Name constraints

Subject attribute constraints:

- countryName: must be “RU”
- organizationName: must be “RDIG”
- organisationalUnit: first component must be either “users”, “hosts” or “services” as determined by the certificate type, see Section 3.1.
- commonName: determined according to Section 3.1.

7.1.6 Certificate Policy Object Identifier

This policy is identified by OID 1.3.6.1.4.1.22139.1.1.2.2.

7.1.7 Usage policy Object Identifier

No stipulation.

7.1.8 Policy qualifier syntax and semantics

No stipulation.

7.2 CRL Profile

7.2.1 Version

X.509 v2.

7.2.2 CRL and CRL Entry extensions

None.

7.3 OCSP Profile

No stipulation.

Chapter 8

Compliance audit

RDIG CA can be audited by the accredited EUGridPMA CA managers to confirm its compliance to the EUGridPMA and/or IGTF Minimum Requirements.

Frequency of EUGridPMA is determined by EUGridPMA/IGTF rules and best practices.

Chapter 9

Other Business and Legal Matters

9.1 Fees

RDIG CA does not require its subscribers to pay any fees for any provided services.

9.2 Financial Responsibility

RDIG CA accepts no financial responsibilities of any kind.

9.3 Confidentiality of Business Information

9.4 Privacy of Personal Information

RDIG CA collects subscriber's full name, organization and unit names and electronic mailing address. Subscriber's organization, unit name, e-mail address and full name is included in the user certificate. All collected information is not confidential.

RDIG CA by no means wants to access user's, host's or host application's private key. Private key is generated only by users or host/service administrators and must not be disclosed to anyone else. RDIG CA by no means asks users to pass their private keys along with the certificate requests.

Publicly-accessible sensitive data, such as user e-mail, will be mangled to avoid simple data gathering attempts by general-purpose automated grabbers. No attempts to withstand the grabbing by the specialized (for RDIG CA or some subset of world CAs) software are generally made, but CA security team acts on the best-effort basis to protect the published data from automated grabbing.

RDIG CA acts in the "only needed knowledge" paradigm and publishes the smallest possible subset of personal information that is needed for its operations. Users are made aware of the types of data and no publications are made without their prior agreement. RDIG CA doesn't disclose other types of user information to the third parties of any kind.

9.5 Intellectual Property Rights

RDIG CA does not claim any intellectual property rights on issued certificates and Certificate Revocation Lists.

Parts of this document are inspired by the following sources: RFC 2527; RFC 3647; EuroPKI Certificate Policy; TrustID Certificate Policy; NCSA Certificate Policy; INFN Certificate Policy and Certificate Practice Statement; NIKHEF Certificate Policy and Certificate Practice Statement; Russian DataGrid Certificate Policy and Certificate Practice Statement.

9.6 Representations and Warranties

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

The certification service is run with a reasonable level of security but is provided on a best effort basis. RDIG CA takes no responsibility for problems arising from its operation or from the use of certificates it provides. RDIG CA denies any financial or other kind of responsibility for damages or inpayments resulting from its operation.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

CP/CPS is valid until the next version is rolled out and made publicly available.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

All changes in CP/CPS will result in policy OID bump and new version of this document.

9.13 Dispute Resolution Procedures

This document must be treated according to the current law of Russian Federation. Legal disputes arising from the operation of the RDIG CA will be resolved according to the Russian Federation law.

9.14 Governing Law

See Section 9.13.

9.15 Compliance with Applicable Law

See Section 9.13.

9.16 Miscellaneous Provisions

No stipulation.

9.17 Other Provisions

No stipulation.

Chapter 10

Document versions

10.1 Version 1.2.2

- Created: July 4th 2021
- Reviewed by EUGridPMA: August 19th 2021

Changes since 1.2.1:

- Adopted content to the recommendations of RFC 3647
- Changed certificate digest type to SHA-256 and higher
- Dropped «issuer» information from the Authority key identifier extension: this enables re-issuing the root certificate
- Clarified the practical scheme of user identity and request integrity verifications by a Registration Authority with the help of the paper forms
- Changed the link to the RDIG CA CRL to point to the DER-encoded variant

10.2 Version 1.2.1

- Created: April 16th 2010

Changes since 1.2:

- Added “SSL Client” to the Netscape Certificate Type to synchronize it with digitalSignature bit in the keyUsage

10.3 Version 1.2

- Created: February 12th 2008

Changes since 1.1:

- Changed end-entity certificate lifetime from one year to one year and 31 days
- Corrected contact phones: area code had changed.
- Replaced old CRL location with the new one: new CRL download point provides much higher throughput and reliability. Old location stopped and the new one started to be announced via EUGridPMA/IGTF since IGTF distribution 1.5, dated 19 June 2006

10.4 Version 1.1

- Created: August 24th 2005

Changes since 1.0:

- Changed root certificate key length to 2048 bits to avoid problems with current gLite software
- Clarified user obligations for host and service certificates
- Changed "RDIG project" to "RDIG consortium"

10.5 Version 1.0

- Created: June 14th 2005

Changes since earlier drafts:

- Changed root certificate lifetime to 10 years
- Changed namespace to conform to the PKIX recommendations: transformed extra O components to OU components