RDIG Certification Authority Certificate Policy and Certification Practice Statement

Version:	1.0
Date:	June 14, 2005
OID:	1.3.6.1.4.1.22139.1.1.0

Contents

1 Introduction

1.1 Overview

This Certification Policy and Practice Statement (CP/CPS) is structured according to RFC2527. It describes the set of rules used by RDIG Certification Authority (RDIG-CA), operated by the Grid team of the Russian Research Centre “Kurchatov Institute” (RRC KI). RDIG stands for Russian Data Intensive Grid.

This document is currently a draft. This document can be referred as *RDIG Certification Authority Certificate Policy and Certification Practice Statement version 1.0* or *OID 1.3.6.1.4.1.22139.1.1.0*.

1.2 Identification

Document name:	RDIG Certification Authority Certificate Policy and Certification Practice Statement.
Version:	1.0 (working draft).
Date:	August 6, 2005.
OID:	1.3.6.1.4.1.22139.1.1.0.

1.3 Community and Applicability

1.3.1 Certification authorities

RDIG Certification Authority is the root certification authority for RDIG project.

1.3.2 Registration Authorities

The current list of registration authorities for RDIG-CA may be obtained from the following URL:
http://ca.grid.kiae.ru/RDIG/ra-list.html.

1.3.3 End entities

RDIG-CA may issue certificates for people, hosts and host applications (services) involved in the Russian Data Intensive Grid project.

1.3.4 Applicability

- 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 server authentication and communication encryption.

- The host application certificates may be used for server applications authentication and communication encryption.

The certificates issued by RDIG-CA may not be used in financial transactions of any sort.

1.4 Contact Details

1.4.1 Contact Person

The RDIG-CA is operated by:

Eygene Ryabinkin, RRC KI,
Russia, 123098, Moscow, Kurchatov square, 1.
phone: +7 095 1969519.
e-mail: rea@mbslab.kiae.ru.
Generic contact for the RDIG-CA:

e-mail: rdig-ca@grid.kiae.ru.

1.4.2 CP/CPS Contact Person

The contact person for this CP/CPS is:

Eygene Ryabinkin, RRC KI,
Russia, 123098, Moscow, Kurchatov square, 1.
phone: +7 095 1969519.
e-mail: rea@mbslab.kiae.ru.

1.4.3 Online repositories

General URL:
http://ca.grid.kiae.ru/RDIG/.
Policy documents:
http://ca.grid.kiae.ru/RDIG/policy/.
Certificate repository:
http://ca.grid.kiae.ru/RDIG/certs/.
Certificate revocation list:
http://ca.grid.kiae.ru/RDIG/cacrl.pem.
CA root certificate:
http://ca.grid.kiae.ru/RDIG/cacrt.pem.

2 General Provisions

2.1 Obligations

2.1.1 RDIG-CA obligations

The RDIG-CA:

- accepts all requests validated by the registration authorities,
- creates and delivers certificates to registration authorities,
- publishes the issued certificates to publicly-accessible on-line stores,
- accepts all revocations from the registration authorities,
- issues and publishes a CRL,
- revoke any issued certificate if RDIG-CA possesses the proofs of certificate compromise or certificate usage that violates the RDIG-CA CP/CPS.

2.1.2 RDIG-CA Registration Authorities obligations

The RDIG-CA Registration Authorities:

- authenticates the person requesting a person certificate,
- (for user certificate) determines if the person has the right to have a RDIG-CA certificate,
- sends validated person certificate requests to the RDIG-CA,
- (for a host or host application certificate) determines if the host has the right to have a RDIG-CA certificate,
- sends validated host and host application certificate requests to the RDIG-CA,
- delivers certificates to the subscribers if it was not done by the RDIG-CA itself,
- creates and sends revocation requests to the CA,
- communicates with RDIG-CA using signed electronic mail or via voice conversations with known persons.

It is up to the Registration Authority to decide wheither user or host has the rights to have a RDIG-CA certificate. In the process of making such a decision, Registration Authority can contact the superior person of a requester to verify the requester's participation in the RDIG projects.

2.1.3 Subscriber obligations

Subscribers:

- must be involved in the RDIG project,
- must provide accurate information in their certificate requests,
- must protect their private key with the strong password, that is at least fifteen characters in length,
- must not keep their private key in unencrypted form and must not keep private key password along with the key itself,
- must immediately notify the RDIG-CA Registration Authority in the case of actual or suspected key loss, disclosure or other compromise.
- must be familiar with the RDIG-CA CP/CPS document and follow the rules of the certificate usage specified in the CP/CPS document.
- should ask for certificate revocation if the certificate is no longer needed or the certificated entity leaves the RDIG project.
- should ask for certificate revocation if the data provided in the certificate is no longer valid.

2.1.4 Relaying party obligations

Relying party:

- must be familiar with this CP/CPS before making any decisions on a thrustworthness of a certificate issued by RDIG-CA,
- must use the certificate only for purposes that are permitted by this CP/CPS,
- must check the authencity of RDIG-CA root certificate before using it,
- must verify the current CRL before validating a certificate,
- should update local CRL copy at least once per day.

2.1.5 Repository obligations

RDIG-CA will upload all issued certificates to the publicly-accessible on-line repository. RDIG-CA will maintain Certificate Revocation List (CRL). RDIG-CA may publish information about pending certificate requests.

2.2 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.

2.3 Financial responsibility

No financial responsibility is accepted.

2.4 Interpretation and Enforcement

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 with the Russian Federation law.

2.5 Fees

No fees are charged.

2.6 Publication and Repository

2.6.1 Publication of RDIG-CA information

RDIG-CA operates a public web site http://ca.grid.kiae.ru/RDIG/ that contains:

- the certificate for CA signing key,
- current Certificate Revocation List (CRL) signed by RDIG-CA,
- all certificates issued by RDIG-CA,
- past and current versions of RDIG-CA CP/CPS document,
- various information about RDIG-CA and certificates, that can be helpful to users of RDIG-CA.

2.6.2 Frequency of publication

The user, host and host application certificates are published as soon as they are generated. The new Certificate Revocation List (CRL) is issued after each revocation and at least 7 days before expiration of previous CRL. The CRL has 30 days validity time.

2.6.3 Access controls

No access controls to these publications are performed.

2.7 Compliance audit

RDIG-CA can be audited by the accredited EUGridPMA CA managers to confirm its compliance to the EUGridPMA Minimum Requirements.

2.8 Confidentiality

RDIG-CA collects subscriber's full name, organization and unit names and electronic mailing address. Subscriber's organization, unit name and full name is included in the user certificate. All collected information is not confidential. RDIG-CA will not publish subscriber's electronic mailing address in the list of issued certificates on the RDIG-CA web site.

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.

2.9 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; 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.

3 Identification and authentication

3.1 Initial Registration

3.1.1 Types of names

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

- distinguished names for a person 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 person 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 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. In cases when user's first name and last name coincide with existing certificate ones, middle name or initial may be inserted into the CN field of the distinguished name.

3.1.2 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 will neither generate nor store any private keys for subscribers.

3.1.3 Authentication of organization identity

RDIG-CA Registration Authority verifies the organization identity by checking:

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

3.1.4 Authentication of individual identity

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

3.2 Routine Rekey

Routine re-keying is allowed to current subscribers of RDIG-CA and must take place before expiration of subscriber's current certificate. The re-key request must be consisted of certificate request with the new key pair and is to be signed with the private key of subscriber's current certificate. Resigning of existing public key is not allowed.

3.3 Rekey after Revocation

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 3.1.

3.4 Revocation request

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 which verifies user's identity using procedures simular to those described in section 3.1.2.

4 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 1024 bits. The maximum validity time for each certificate is one year.

Generated certificate request must be sent by electronic mail to the corresponding RDIG-CA Registration Authority. Mail message must be sent from electronic mail address that does exists and can be mailed to.

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.

4.2 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 3.1. 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.

4.3 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 3.1.1.
- 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://ca.grid.kiae.ru/RDIG/cacrl.pem.
- 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.

4.4 Certificate Suspension and Revocation

4.4.1 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 participated in the RDIG project, or
- RDIG-CA have the proofs that certificate usage violates RDIG-CA CP/CPS rules.

4.4.2 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.

4.4.3 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. The rules for passing revocation request to the RDIG-CA Registration Authority are described in section 3.4.

4.4.4 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 revocation request. The rules for passing cancellation request to the RDIG-CA Registration Authority are just the same as in section 3.4.

4.4.5 Circumstances for suspension

Certificate suspension is not currently supported.

4.4.6 Who can request suspension

Certificate suspension is not currently supported.

4.4.7 Procedure for suspension request

Certificate suspension is not currently supported.

4.4.8 Limits on suspension period

Certificate suspension is not currently supported.

4.4.9 CRL issuance frequency

The Certificate Revocation List (CRL) is issued after each revocation and at least every 7 days. The lifetime of CRL is 30 days. CRL will be made available for downloading as soon as it was published.

4.4.10 CRL checking requirements

- The CRL must have a valid RDIG-CA signature and must not be expired.
- To guarantee the maximum level of security one should download the new CRL just before validating the certificate.

4.4.11 Online revocation/status checking availability

All valid certificates issued by RDIG-CA are available online the following URL:
http://ca.grid.kiae.ru/RDIG/certs/.

4.4.12 Online revocation checking requirements for relying parties

Not applicable.

4.4.13 Other forms of revocation advertisements

The certificate holder is notified if some other person asks for his/her certificate revocation.

4.4.14 Other forms of revocation advertisements checking requirements for relying parties

Not applicable.

4.4.15 Private key compromise

When the certificate revocation is a result of a private key compromise all RDIG-CA Registration Authorities and the holder of the private key are notified by email about this case immediately after new CRL issuance.

4.5 Security Audit Procedures

4.5.1 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.

4.5.2 Processing Frequency of Audit Logs

Not defined.

4.5.3 Retention period for Audit Logs

Audit logs will be kept for at least 3 years.

4.5.4 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.

4.5.5 Audit log backup procedures

Audit logs are copied to an offline medium.

4.5.6 Audit collection system

The audit logs archive is internal to the RDIG-CA.

4.5.7 Vulnerability assessments

No stipulation.

4.5.8 Operational audits

Operational audit is performed twice per year and includes auditing of all RDIG-CA staff including Registration Authorities.

4.6 Records Archive

4.6.1 Types of event recorded

The following types of events are recorded:

- certificate requests (by persons),
- certificate acceptations (by Registration Authority),
- revocation requests (by Registration Authority),
- certificate issuance,
- CRL issuance,
- email messages sent and received by RDIG-CA.

4.6.2 Retention period for the archive

Records will be kept for at least 3 years.

4.6.3 Protection of the archive

Records may be consulted only by:

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

All records are copied to an offline medium. Online records are protected using the file system security.

4.6.4 Archive backup procedures

No stipulation.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system

The records archive is internal to the RDIG-CA.

4.6.7 Procedures for obtaining and verifying archive information

No stipulation.

4.7 Key Changeover

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

4.8 Compromise and Disaster Recovery

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

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

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

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

4.9 Certification Authority termination

Upon termination RDIG-CA will:

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

5 Physical, procedural and personnel security controls

5.1 Physical controls

5.1.1 Site location

The RDIG-CA is located at the Russian Research Centre “Kurchatov Institute” in Moscow, Russia and is hosted on a professional collocation 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 in several removable storage media. Backup copies of RDIG-CA related information are kept on CD-ROM and flash disks.

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 personnel of corresponding institutions.

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 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.

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/certs/.

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 1024 bits. The RDIG-CA key length is 4096 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.

6.1.9 Key usage purposes

Keys must be used according to the value of X.509v3 keyUsage field.

6.2 Private key protection

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

No stipulation.

6.2.2 Private key escrow

No stipulation.

6.2.3 Private key archival and backup

The RDIG-CA private key is kept encrypted in multiple copies on CD-ROM and flash disks in safe places. One copy of encrypted key and its passphrase is sealed in the envelope and kept in a safe.

6.3 Other aspects of key pair management

The RDIG-CA private key validity period is 10 years.

6.4 Activation data

Each copy of the RDIG-CA private key is protected by its own passphrase which is at least 15 characters long.

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 Cryptographic module engineering controls

No stipulation.

7 Certificate and CRL 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,issuer:always
- **basicConstraints** (CRITICAL): CA:false
- **keyUsage** (CRITICAL): digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement
- **certificatePolicies**: OID 1.3.6.1.4.1.22139.1.1.0
- **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, objsign
- **nsCertType**: (for host certificates) server, objsign

7.1.3 Algorithm Object Identifiers

No stipulation

7.1.4 Name forms

Issuer: C=RU,O=RDIG,CN=Russian Data-Intensive Grid CA.
For Subject field name forms check section 3.1.1.

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 3.1.1.
- **commonName**: determined according to section 3.1.1.

7.1.6 Certificate Policy Object Identifier

This policy is identified by OID 1.3.6.1.4.1.22139.1.1.0.

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 v1.

7.2.2 CRL and CRL Entry extensions

None.

8 Specification administration

8.1 Specification change procedures

Minor changes to this document can be made without announcements to subscribers and relying parties. Substantial changes in policy will be notified to all subscribers, relying parties and cross-certifying Certification Authorities. It will be also announced on the EUgridPMA mailing list.

8.2 Publication and notification policies

The last version of this document is available at the following URL:
http://ca.grid.kiae.ru/RDIG/policy/.

8.3 CPS approval procedures

No stipulation.

9 Versions

9.1 Change log

- version 1.0, 14 Jun 2005. Changed root certificate lifetime to 10 years. Changed namespace to conform to the PKIX recommendations: transformed extra `O` components to `OU` components.
- version 0.5 drafted 26 May 2005.
- version 0.4 drafted 18 May 2005.
- version 0.3 drafted 04 May 2005.
- version 0.2 drafted 04 May 2005.
- version 0.1 drafted August 2005.
- version 0.0 drafted December 2004.