Grid Canada

Certificate Policy
Certification Practice Statement

Version 1.1

February 2004

1 Introduction

This document is based on the structure suggested by the RFC 2527.

The terms used in this document are explained in the Glossary.

1.1 Overview

This document describes the set of rules and procedures followed by Grid Canada Certificate Authority (GC CA), the top level CA for all purposes of *Grid Canada* (http://www.gridcanada.ca/).

1.2 Identification

Document Title

GC CA Certificate Policy and Certification Practice Statement

Document Version

1.1

Document Date

February 18, 2004

OID: [NRC].[IIT].1.1

2.16.124.101.1.274.47.1.1

1.3 Community and Applicability

GC CA provides PKI services for the Canadian research community that are involved in Grid activities.

1.3.1 Certification Authorities

GC CA does not issue certificates to subordinate Certificate Authorities.

1.3.2 Registration Authorities

GC CA manages the functions of its Registration Authority. Additional RA's may be created as required. See the GC CA site for a current list (http://www.gridcanada.ca/ca/ra.html).

1.3.3 End Entities

The GC CA issues certificates for people, hosts, and host applications involved in the activities listed in section 1.3.

1.3.4 Applicability

Person certificates can be used to authenticate a person to research sites that have agreed to accept certificates from the GC CA, and may require the signing of Globus proxy certificates [PROXY]. While person certificates can be used for other purposes such as email signing, these are not supported.

Service certificates can be used to identify a named service on a specific host and for encryption of communication (SSL/TLS).

1.3.5 User Restriction

The ownership of a GC certificate does not imply automatic access to any kind of computing resources.

1.4 Contact Details

The GC CA is managed by the Grid Canada Security Group.

The contact persons for questions related to this document or the GC CA in general is:

Darcy Quesnel
Phone: +1 613 996-2144
Email : darcy.quesnel@canarie.ca

Ratilal Haria
Phone: +1 613 990 4433
Email : ratilal.haria@nrc.ca

1200 Montreal Road, M-50
Ottawa, Ontario
Canada K1A 0R6

Fax: +1 613 952 7151
Email : ca@gridcanada.ca
Web : http://www.gridcanada.ca/ca/

2 General Provisions

2.1 Obligations

2.1.1 CA and RA Obligations

The **GC CA** will:

- Accept certification requests from entitled entities;
- Notify the RA of certification request and accept authentication results from the RA;
- Issue certificates based on the requests from authenticated entities;
- Notify the subscriber of the issuing of the certificate;
- Publish the issued certificates (optionally, respective of privacy and other issues);
- Accept revocation requests according to the procedures outlined in this document;
- Authenticate entities requesting the revocation of a certificate, possibly by delegating this task to a GC RA;
- Issue a Certificate Revocation List (CRL);
- Publish the CRL issued; and
- Keep audit logs of the certificate issuance process.

A **GC RA** will:

- Accept authentication requests from the GC CA;
- Authenticate entity making the certification request according to procedures outlined in this document;
- Notify the GC CA when authentication is completed for a certification or revocation request;
- Accept revocation requests according to the procedures outlined in this document;
- Notify the GC CA of all revocation requests; and
- Will not approve a certificate with a lifetime greater than 12 months.

2.1.2 Subscriber Obligations

Subscribers must:

- Read and adhere to the procedures published in this document;

- Generate a key pair using a trustworthy method;
- Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
  - For Person Certificates:
    - Selecting a pass phrase of a minimum recommended 15 characters;
    - Protecting the pass phrase from others;
    - Always using the pass phrase to encrypt the stored private key; and
    - Never sharing the private key with other users;
  - For Service Certificates:
    - Storing them encrypted whenever possible; and
    - They may be kept unencrypted on the host that they represent;
- Provide correct personal information and optionally authorize the publication of the certificate;
- Notify the GC CA immediately in case of private key loss or compromise; and
- Use the certificates for the permitted uses only.

2.1.3 Relying Party Obligations

Relying parties must:

- Read the procedures published in this document;
- Use the certificates for the permitted uses only; and
- Do not assume any authorization attributes based solely on an entity's possession GC CA certificate.

Relying parties may:

- Verify that the certificate is not on the CRL before validating a certificate.

2.1.4 Repository Obligations

GC CA will provide access to GC CA information, as outlined in section 2.6.1, on its web site, http://www.gridcanada.ca/ca/.

2.2 Liability

The GC CA and its agents issue person certificates according to the practices described in this document to validate identity. No liability, implicit or explicit, is accepted.

GC CA and its agents make no guarantee about the security or suitability of a service that is identified by a GC certificate. The certification service is run with a reasonable level of security, but it is provided on a *best-effort* basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

GC CA denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

2.3 Financial Responsibility

GC CA assumes no financial responsibility with respect to use or management of any issued certificate.

2.4 Interpretation and Enforcement

This document must be treated according to Canadian laws. Legal disputes arising from the operation of the GC CA will be treated according to Canadian laws.

2.4.1 Governing Law

Interpretation of this CP and CPS is according to Canadian laws.

2.5 Fees

No fees are charged.

2.6 Publication and Repositories

2.6.1 Publication of CA information

GC CA will operate a secure online repository that contains:

- The GC CA's certificate;
- Certificates issued by the GC CA (optionally, respective of privacy and other issues);
- A Certificate Revocation List;
- A copy of this policy; and
- Other information deemed relevant to the GC CA.

2.6.2 Frequency of Publication

- Certificates will be published to the GC CA repository as soon after being issued (optionally, respective of privacy and other issues);
- CRLs will be published soon after a revocation is issued or refreshed once every month, 7 days before the month-long validity of the CRL expires;
- All GC CA documents will be published to the project website as they are updated; and
- Changes to this CP and CPS will be published as soon as they are approved and previous versions will remain available on-line.

2.6.3 Access Controls

The online repository is available on a substantially 24/7 basis, subject to reasonable scheduled maintenance.

GC CA does not impose any access control on its policy, its signing certificate and issued certificates, and its CRLs.

In the future, GC CA may impose access controls on issued certificates, their status information and CRLs at its discretion, subject to agreement between the CA, relying parties, and subscribers.

2.6.4 Repositories

The repository of certificates and CRLs are available at http://www.gridcanada.ca/ca/.

2.7 Compliance Audit

No external audit will be required, only self-assessment by the GC CA that its operation is according to this Policy.

2.8 Confidentiality

GC CA collects subscribers' full names and email addresses. Some of this information is used to construct unique, meaningful subject names in the issued certificates.

Information included in issued certificates and CRLs is generally not considered confidential. The GC CA does not collect any other kind of confidential information.

The GC CA does not have access to or generate the private keys of a digital signature key pair, such as those used in GC identity certificates. These key pairs are generated and managed by the client and are the sole responsibility of the subscriber.

2.9 Intellectual Property Rights

Parts of this document are inspired by [INFN], [CERN], [DOE], [FZKGRID], [GRIDEIRE], [CNRS], and [RFC2527].

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

The subject name is an X.500 name type, a *Distinguished Name*. It has one of the following forms:

- **Person**
  Must include the *full name* of the subject;
- **Service**
  Must include the *fully qualified domain name* of the host, and optionally the *named service*.

3.1.2 Name Meanings

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber.

3.1.3 Rules for Interpreting Various Name Forms

See sections 3.1.1 and 3.1.2.

3.1.4 Uniqueness of Names

The X.500 Distinguished Name (DN) must be unique for each subject name certified by the GC CA. The Common Name (CN) component of the DN will include the full name of the subscriber as described in 3.1.1.

For hosts and services the CN should contain the fully qualified domain name (FQDN) of the host.

The CN may contain an arbitrary alphanumeric qualifier that distinguishes it from certificates from the same subscriber.

Certificates must apply to unique individuals or resources. Users may not share certificates.

3.1.5 Name Claim Dispute Resolution Procedure

No stipulation.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.1.7 Method to Prove Possession of Private Key

No stipulation.

3.1.8 Authentication of Organization Identity

The GC CA verifies the identity of organizations by checking:

- That the organization is known to be part of a grid computing project or related experiments; and
- That the organization is operating in Canada, by checking contact information.

3.1.9 Authentication of Individual Identity

The Grid Canada RA verifies the identity of a person by checking:

- A certificate request (or renewal or revocation) must be sent to ca@gridcanada.ca with an email subject containing “Certificate Request” (or “Certificate Renewal” or “Certificate Revocation”) and originate from a valid email address from a known organization as specified in section 3.1.8; and
- A request will be accepted if the person is known to those listed in section 1.4; or
- A request is verified by an RA closely associated with the person’s organization; or
- A copy of an organization’s identity card for the requestor, manually-signed by a well-known contact person of that organization, is sent to those listed in section 1.4 along with contact information for confirmation.

3.2 Routine Rekey

Rekey (or renewal) before expiration can be accomplished by sending a rekey request based on a new public key. The GC CA will send renewal reminders at least a month before expiration.

Rekey after expiration follows the same authentication procedure as a new certificate.

3.3 Rekey After Revocation

Rekey after revocation follows the same authentication procedure as a new certificate.

3.4 Revocation Request

Certificate revocation requests must be sent by email to ca@gridcanada.ca**.** The GC CA checks the identity of the revoker as per 3.1.9.

4 Operational Requirements

4.1 Certificate Application

The minimum key length for all certificates is 1024 bits. The maximum validity period is one year. Each applicant must generate its own key pair using either Globus `grid-cert-request` or OpenSSL or similar software.

Certificate requests in PEM format are sent by email, as outlined in section 3.1.9.

4.2 Certificate Issuance

GC CA issues the certificate if, and only if, the authentication of the subject is successful according to section 3.1.9. The applicant will be notified about the issuance of the certificate by email or will be informed about the reason why the certificate could not be issued.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

- The subscriber's private key is lost or suspected to be compromised;
- The information in the subscriber's certificate is suspected to be inaccurate;
- The subject has failed to comply with the rules in this policy;
- The system to which the certificate has been issued has been retired;
- The subscriber no longer needs the certificate to access a relying parties' resources; and
- The subscriber violated his/her obligations.

4.4.2 Who Can Request Revocation

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting proof of knowledge of a circumstance of revocation.

4.4.3 Procedure for Revocation Request

A certificate revocation can be requested as outlined in section 3.1.9.

4.4.4 Revocation Request Grace Period

There is no revocation grace period.

4.4.5 Circumstances for Suspension

No stipulation.

4.4.6 Who Can Request Suspension

No stipulation.

4.4.7 Procedure for Suspension Request

No stipulation.

4.4.8 Limits on Suspension Period

No stipulation.

4.4.9 CRL Issuance Frequency

CRLs are issued after every certificate revocation or every month, 7 days before the month-long validity of the CRL has expired.

4.4.10 CRL Checking Requirements for Relying Parties

A relying party may verify a certificate against the most recent CRL issued, in order to validate the use of the certificate.

4.4.11 Online Revocation/Status Checking Availability

OCSP is not implemented.

4.4.12 Online Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisement Available

No stipulation.

4.5 Security Audit Procedures

Security auditing of the GC CA is not supported.

4.6 Records Archival

4.6.1 Types of Event Audited

The following events are recorded and archived:

- Certificate requests;
- Issued certificates;
- Issued CRLs; and
- All email correspondence with the GC CA.

4.6.2 Retention Period for Audit Logs

The minimum retention period is three years.

4.6.3 Protection of Archive

Records are backed up on removable media, which are stored in a room with restricted access.

4.6.4 Archive Backup Procedures

See section 4.6.3.

4.6.5 Time-Stamping Requirements

No stipulation.

4.6.6 Archive Collection System

See section 4.6.3.

4.6.7 Procedures to Obtain and Verify Archive Information

No stipulation.

4.7 Key Changeover

The CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA key should be generated one year before the old one becomes invalid. From that point on new certificates are signed by the new CA key.

The new CA public key is posted online at http://www.gridcanada.ca/ca/.

4.8 Compromise and Disaster Recovery

If the CA's private key is compromised - or suspected to be compromised - the CA will:

- Inform subscribers and other relying parties;

- Terminate the issuance and distribution of certificates and CRLs;
- Generate a new CA certificate (with a new key pair) and make it immediately available in the public repository at http://www.gridcanada.ca/ca/; and
- All subjects will have to recertify following the procedures in section 3.1.

4.9 CA Termination

Before the GC CA terminates its services, it will:

- Inform subscribers and subordinate RAs;
- Make widely available information of its termination; and
- Stop issuing certificates and CRLs.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

The GC CA operates in a controlled environment, where access is restricted to authorized people.

5.1.1 Site Location

The GC CA is located at the National Research Council of Canada (NRC) on the Montreal Road Campus (Ottawa, Ontario, Canada) at the Institute for Information Technology (Building M-50).

5.1.2 Physical Access

Physical access to the hardware is restricted to authorized personnel. All removable media is stored in secured area.

5.1.3 Power and Air Conditioning

The building has an air conditioning system and the CA machines are connected to a UPS system.

5.1.4 Water Exposure

The hardware is in a zone not subject to floods.

5.1.5 Fire Prevention and Protection

The building has a fire alarm system.

5.1.6 Media Storage

Backups are stored on removable storage media.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural Controls

No stipulation.

5.3 Personnel Security Controls

Access to servers and applications is limited to the GC CA Security Group who are staff or guest workers of NRC.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pairs for the GC CA are generated by the GC CA Security Group on a dedicated machine, not connected to any kind of network. The underlying software package used is OpenSSL.

Each end entity must generate its own key pair. The GC CA does not generate end entity private keys.

6.1.2 Private Key Delivery to Entity

The GC CA never has access to the end entity private key.

6.1.3 Public Key Delivery to Certificate Issuer

End entities' public keys must be delivered to the GC CA as per section 3.1.

6.1.4 CA Public Key Delivery to Users

The CA certificate is available from its public repository at http://www.gridcanada.ca/ca/.

6.1.5 Key Sizes

Keys of length less then 1024 bits will not be signed.

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

Key generation is performed by software (for example, OpenSSL).

6.1.9 Key Usage Purposes

GC certificates may be used only for authentication and signing proxy certificates [PROXY]. It is understood that they could be used in other capacities, but the GC CA does not recommend or warrant any other use of the certificates it signs.

The GC CA root private key will only be used to sign CRLs and end entity certificates.

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 GC CA root private key is kept encrypted in multiple locations.

6.3 Other Aspects of Key Pair Management

The current GC CA root certificate has a validity of five years, expires in ***2007-04-10***, and has a key length of 2048.

6.4 Activation Data

GC CA root private key is protected by a passphrase.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

GC CA servers include the following:

- Operating systems are maintained at a high level of security by applying all recommended and applicable security patches;
- Monitoring is done to detect unauthorized software changes; and
- Services are reduced to a minimum.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

No stipulation.

6.7 Network Security Controls

See section 6.5.1.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3.

7.1.2 Certificate extensions

Basic Constraints (CRITICAL)

Not a CA.

Key Usage (CRITICAL)

Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment

Subject Key Identifier

Authority Key Identifier
Subject Alternative Name
Subject's email address
Issuer Alternative Name

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Issuer
C=CA, O=Grid, CN=Grid Canada CA
Person
C=CA, O=Grid, OU=*domainName*, CN=*fullPersonName*[, Email=*emailAddress*]
Hosts
C=CA, O=Grid, [OU=*domainName*,] CN=host/*fullyQualifiedDomainName*
Service
C=CA, O=Grid, [OU=*domainName*,] CN=*serviceName/fullyQualifiedDomainName*

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints Extensions

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

No stipulation.

8 Specification Administration

8.1 Specification Change Procedures

Users may not be warned in advance of changes to GC CA's policy and CPS. Relevant changes will be made as widely available as possible.

8.2 Publication and Notification Procedures

The policy is available at http://www.gridcanada.ca/ca/.

8.3 CPS Approval Procedures

The GC CA Security Group is responsible for the CP and CPS. All changes must be approved by the Security Group.

Glossary

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

Certification Authority (CA)
: The entity / system that 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).

Certificates – or Public Key Certificates
: A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA that issued it

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 for the trading of goods within a given price range.

Certification Practice Statement (CPS)
: A statement of the practices, which a certification authority employs in issuing certificates.

Certificate Revocation Lists (CRL)
: A CRL is a time stamped list identifying revoked certificates that is signed by a CA and made freely available in a public repository.

End Entity
: A certificate subject that does not sign certificates (i.e., person, host, and service certificates).

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

Public Key Infrastructure (PKI)
: A term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. All of this implies a set of standards for applications that use encryption.

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

Policy Management Authority (PMA)
: For the GC CA this is a committee composed of the GC CA Security Group.

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

Private Key
: In a PKI, a cryptographic key created and kept private by a subscriber. It may be used to make digital signatures which may be verified by the corresponding public key; to decrypt the message encrypted by the corresponding public key; or, with other information, to compute a piece of common shared secret information.

Public Key
: In a PKI, a cryptographic key created and made public by a subscriber. It may be used to encrypt information that may be decrypted by the corresponding private key; or to verify the digital signature made by the corresponding private key.

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

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

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

Subscriber
: In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject.

Virtual Organization (VO)
: An organization that has been created to represent a particular research or development effort independent of the physical sites at which the scientist or engineers work.

Bibliography

[CERN]
: CERN CA Certificate Policy and Certification Practice Statement, Version 0.1. August 2001.

[CNRS]
: Certificate Policy and Certification Practice Statement CNRS/CNRS-Projets/Datagrid-fr, Version 0.3. August 2002.

[DOE]
: DOE Science Grid PKI Certificate Policy and Certification Practice Statement, Version 2.1. August 2002.

[FZKGRID]
: FZK-Grid-CA Certificate Policy and Certification Practice Statement, Version 0.2. June 2002.

[GRIDEIRE]
: Grid-Ireland Certification Authority Certificate Policy and Certification Practice Statement, Version 0.3. October 2001.

[INFN]
: INFN CA Certificate Policy and Certification Practice Statement, Version 1.0. December 2001.

[PROXY]
: S. Tuecke, et al., Internet X.509 Public Key Infrastructure Proxy Certificate Profile, Internet Draft. 2001.

[RFC2527]
: S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527. March 1999.