

Grid-Ireland Certification Authority

Certificate Policy and Certification Practice Statement

Version 0.5 (DRAFT)
June, 2003

Introduction.....	5
1.1 Overview.....	5
1.1.1 General Definitions	5
1.2 Identification	5
1.3 Community and Applicability.....	5
1.3.1 Certification Authorities	5
1.3.2 Registration Authorities.....	5
1.3.3 End Entities.....	6
1.3.4 Applicability.....	6
1.4 Contact Details.....	6
2 General Provisions.....	7
2.1 Obligations	7
2.1.1 CA Obligations	7
2.1.2 RA Obligations	7
2.1.3 Subscriber Obligations	7
2.1.4 Relying Party Obligations	7
2.1.5 Repository Obligations	7
2.2 Liability.....	7
2.3 Financial Responsibility.....	8
2.4 Interpretation and Enforcement.....	8
2.4.1 Governing Law	8
2.4.2 Dispute Resolution Procedures.....	8
2.5 Fees	8
2.6 Publication and Repositories	8
2.6.1 Publication of CA information.....	8
2.6.2 Frequency of Publication	8
2.6.3 Access Controls	8
2.6.4 Repositories.....	8
2.7 Compliance Audit	8
2.8 Confidentiality	8
2.8.1 Confidential Information kept by the CA/RA.....	8
2.8.2 Types of Information not considered Confidential.....	8
2.8.3 Disclosure of Certificate Revocation/Suspension Information	9
2.8.4 Release of Information to Law Enforcement Officials.....	9
2.8.5 Information that can be revealed as Part of Civil Discovery	9
2.8.6 Conditions for Disclosure upon Owner’s Request	9
2.8.7 Other Circumstances for Disclosure of Confidential Information	9
2.9 Intellectual Property Rights	9
3 Identification and Authentication	10
3.1 Initial Registration.....	10
3.1.1 Types of names.....	10
3.1.2 Name Meanings	10
3.1.3 Uniqueness of names.....	10
3.1.4 Method to Prove Possession of Private Key.....	10
3.1.5 Authentication of Organization Identity.....	10
3.1.6 Authentication of Individual Identity.....	10
3.2 Routine Rekey	10
3.3 Rekey After Revocation	10
3.4 Revocation Request	10
4 Operational Requirements	11
4.1 Certificate Application.....	11
4.2 Certificate Issuance	11
4.3 Certificate Acceptance	11
4.4 Certificate Suspension and Revocation.....	11

4.4.1	Circumstances for Revocation	11
4.4.2	Who Can Request Revocation	11
4.4.3	Procedure for Revocation Request	11
4.4.4	Circumstances for Suspension	11
4.4.5	Who Can Request Suspension	11
4.4.6	Procedure for Suspension Request	11
4.4.7	Limits on Suspension Period	11
4.4.8	CRL Issuance Frequency	11
4.4.9	Online revocation/status checking availability	11
4.4.10	Online revocation checking requirements	11
4.4.11	Other forms of revocation advertisement available	12
4.5	Security Audit Procedures	12
4.5.1	Types of Event Audited	12
4.5.2	Retention period for Audit Logs	12
4.5.3	Protection of Audit Logs	12
4.6	Records Archival	12
4.6.1	Types of Event Recorded	12
4.6.2	Retention Period for Archives	12
4.6.3	Protection of Archives	12
4.7	Key Changeover	12
4.8	Compromise and Disaster Recovery	12
4.9	CA Termination	12
5	Physical, Procedural and Personnel Security Controls	13
5.1	Physical Security Controls	13
5.1.1	Site Location	13
5.1.2	Physical Access	13
5.1.3	Environmental Security	13
5.2	Procedural Controls	13
5.3	Personnel Security Controls	13
6	Technical Security Controls	14
6.1	Key Pair Generation and Installation	14
6.1.1	Key Pair Generation	14
6.1.2	Private Key Delivery to Entity	14
6.1.3	Public Key Delivery to Certificate Issuer	14
6.1.4	CA Public Key Delivery to Users	14
6.1.5	Key Sizes	14
6.1.6	Public Key Parameters Generation	14
6.1.7	Parameter Quality Checking	14
6.1.8	Hardware/Software Key Generation	14
6.1.9	Key Usage Purposes	14
6.2	Private Key Protection	14
6.2.1	Private Key (n out of m) Multi-person Control	14
6.2.2	Private Key Escrow	14
6.2.3	Private key Archival and Backup	14
6.3	Other Aspects of Key Pair Management	14
6.4	Activation Data	15
6.5	Computer Security Controls	15
6.5.1	Specific Computer Security Technical Requirements	15
6.5.2	Computer Security Rating	15
6.6	Life-Cycle Security Controls	15
6.7	Network Security Controls	15
6.8	Cryptographic Module Engineering Controls	15
7	Certificate and CRL Profiles	16
7.1	Certificate Profile	16
7.1.1	Version Number:	16
7.1.2	Certificate extensions	16
7.1.3	Algorithm object identifiers:	17

7.1.4	Name forms:.....	17
7.1.5	Name Constraints.....	17
7.1.6	Certificate Policy Object Identifier	17
7.1.7	Usage of Policy Constraints Extensions.....	17
7.1.8	Policy qualifier syntax and semantics	17
7.2	CRL Profile	17
7.2.1	Version	17
7.2.2	CRL and CRL Entry Extensions	17
8	Specification Administration	18
8.1	Specification Change Procedures	18
8.2	Publication and Notification Procedures	18
8.3	CPS Approval Procedures.....	18
9	Bibliography	19
10	List of changes.....	20

Introduction

1.1 Overview

This document is a draft, structured according to RFC 2527 [RFC2527].

This document describes the set of rules and operational practices used by the Grid-Ireland CA.

The Grid-Ireland CA is the top level Certification Authority for Grid-Ireland (<http://www.cs.tcd.ie/grid-ireland/>).

1.1.1 General Definitions

The document makes use of the following terms:

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).

Certificate Policy

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.

Issuing Certification Authority (Issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Policy Qualifier

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

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.

Set of provisions

A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS and employing the approach described in this framework.

1.2 Identification

Document title

Grid-Ireland CA Certificate Policy and Certification Practice Statement

Document version

0.5

Document date

June 2003.

Document validity

Valid until further notice.

ASN.1 OID

1.3.6.1.4.1.10977.10.1.1.0.5.

1.3 Community and Applicability

1.3.1 Certification Authorities

Grid-Ireland certificates are signed by the Grid-Ireland CA.

1.3.2 Registration Authorities

The Grid-Ireland CA manages the functions of its Registration Authority. Additional registration authorities may be created by the Grid-Ireland CA as required. The current list of Grid-Ireland Registration Authorities may be obtained from <http://www.cs.tcd.ie/grid-ireland/gi-ca/ra-list.txt>

1.3.3 End Entities

The Grid-Ireland CA issues certificates for:

- (a) Grid-Ireland employees;
- (b) Grid-Ireland partners;
- (c) Servers and services owned by Grid-Ireland or used for activities in which Grid-Ireland is involved.

1.3.4 Applicability

Certificates issued are of the following types:

- (a) **personal**: for e-mail signing and encryption (S/MIME), and user certification and encryption of communications (SSL/TSL);
- (b) **server**: for server certification and encryption of communications (SSL/TSL);
- (c) **services**: for service certification and encryption of communications (SSL/TSL).

The certificates issued by the Grid-Ireland CA may not be used for financial transactions or for any commercial usage.

1.4 Contact Details

The Grid-Ireland CA is managed by the Department of Computer Science, Trinity College Dublin (<http://www.cs.tcd.ie/>). The contact person for questions related to this document or the Grid-Ireland CA in general is:

Dr.B.A.Coghlan,

Grid-Ireland CA,

Dept.Computer Science,

Trinity College Dublin,

Ireland.

phone: (+353)-1-6081795

fax: (+353)-1-6772204

e-mail: grid-ireland-ca@cs.tcd.ie

2 General Provisions

2.1 Obligations

2.1.1 CA Obligations

The Grid-Ireland CA will:

- (a) Accept approved certificate requests from entitled entities;
- (b) Issue certificates based on approved certificate requests from authenticated entities;
- (c) Notify the subscriber of the issuing of the certificate;
- (d) Accept approved revocation requests from entitled entities;
- (e) Revoke certificates based on approved revocation requests from authenticated entities;
- (f) Issue a Certificate Revocation List (CRL) according to the procedures outlined in this document;
- (g) Publish the issued CRL;
- (h) Follow the policies and procedures described in this document.

2.1.2 RA Obligations

A Grid-Ireland RA will:

- (a) Authenticate entities according to the procedures outlined in this document;
- (b) Approve certificate requests according to the procedures outlined in this document;
- (c) Notify the Grid-Ireland CA of the approved certificate requests;
- (d) Approve revocation requests according to the procedures outlined in this document;
- (e) Notify the Grid-Ireland CA of the approved revocation requests;
- (f) Follow the policies and procedures described in this document.

2.1.3 Subscriber Obligations

Subscribers must:

- (a) Read and adhere to the procedures published in this document;
- (b) Generate a key pair using a trustworthy method;
- (c) Take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate, including:
 - (i) selecting a strong passphrase with a minimum of 15 characters
 - (ii) protecting the passphrase from others
- (d) Authorize the treatment and conservation of personal data;
- (e) Immediately notify the Grid-Ireland CA in case of private key loss or compromise;
- (f) Immediately notify the Grid-Ireland CA when the certificate is no longer needed;
- (g) Immediately notify the Grid-Ireland CA when the information in the certificate becomes wrong or inaccurate.

2.1.4 Relying Party Obligations

Relying parties must:

- (a) Read the procedures published in this document;
- (b) Verify the CRL before validating a certificate;
- (c) Use the certificates for the permitted uses only.

2.1.5 Repository Obligations

- (a) The Grid-Ireland CA will publish on its web server <http://www.cs.tcd.ie/grid-ireland/gi-ca/>
- (b) The Grid-Ireland CA will publish its public key on its web server;
- (c) The Grid-Ireland CA will publish its CRLs on its web server as soon as issued.

2.2 Liability

- (a) The Grid-Ireland CA only guarantees to control the identity of the subjects requesting a certificate according to the practices described in this document. No other liability, implicit or explicit, is accepted;
- (b) The Grid-Ireland CA will not give any guarantees about the security or suitability of the service;
- (c) The Grid-Ireland CA is run with a reasonable level of security, but it is provided on a best effort only basis;

- (d) The Grid-Ireland CA 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;
- (e) The Grid-Ireland CA denies any financial or any other kind of responsibilities for damages or impairments resulting from its operation.

2.3 Financial Responsibility

No financial responsibility is accepted.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Interpretation of this policy is according to the laws of the Republic of Ireland.

2.4.2 Dispute Resolution Procedures

Legal disputes arising from the operation of the Grid-Ireland CA will be resolved according to the laws of the Republic of Ireland.

2.5 Fees

No fees are charged.

2.6 Publication and Repositories

2.6.1 Publication of CA information

The Grid-Ireland CA operates an online repository that contains:

- (a) The Grid-Ireland CA certificate;
- (b) A Certificate Revocation List (CRL);
- (c) A copy of this document;
- (d) Other relevant information.

2.6.2 Frequency of Publication

CRLs will be published as soon as issued and at least every 30 days.

2.6.3 Access Controls

The online repository is available on a substantially 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance.

The Grid-Ireland CA does not impose any access control on its Policy, its CA Certificate and its issued CRLs. In the future, the Grid-Ireland CA may impose access controls at its discretion.

2.6.4 Repositories

The Grid-Ireland CA Web Server is at <http://www.cs.tcd.ie/grid-ireland/gi-ca/>

2.7 Compliance Audit

No stipulation.

2.8 Confidentiality

2.8.1 Confidential Information kept by the CA/RA

The only confidential information kept by the Grid-Ireland CA is a photocopy of the subscriber's ID card from their host institution.

2.8.2 Types of Information not considered Confidential

The Grid-Ireland CA collects:

- (a) The subscriber's e-mail address;
- (b) The subscriber's host department's DNS domain name;
- (c) The subscriber's certificate request file;
- (d) The subscriber's public key file.

Information included in issued certificates and CRLs is **not** considered confidential. Under no circumstances will the Grid-Ireland CA have access to the private keys of any subscriber to whom it issues a certificate.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

The CA will notify and inform the following entities:

- (a) The subject of the personal certificate;
- (b) The requester of the server or service certificate.

2.8.4 Release of Information to Law Enforcement Officials

The information collected by the Grid-Ireland CA will be made available to law enforcement officials upon request.

2.8.5 Information that can be revealed as Part of Civil Discovery

The information collected by the Grid-Ireland CA will be subject to Irish law.

2.8.6 Conditions for Disclosure upon Owner's Request

The information collected by the Grid-Ireland CA will be subject to Irish law.

2.8.7 Other Circumstances for Disclosure of Confidential Information

The information collected by the Grid-Ireland CA will be subject to Irish law.

2.9 Intellectual Property Rights

Parts of this document are inspired by [EuroPKI], [TrustID], [NCSA], [FBCA], [INFN].

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of names

The Distinguished Name must be as per Section 7: *Certificate and CRL Profiles*.

3.1.2 Name Meanings

The Distinguished Name must be as per Section 7: *Certificate and CRL Profiles*.

3.1.3 Uniqueness of names

The Distinguished Name must be as per Section 7: *Certificate and CRL Profiles*.

3.1.4 Method to Prove Possession of Private Key

No stipulation.

3.1.5 Authentication of Organization Identity

No stipulation.

3.1.6 Authentication of Individual Identity

A configuration file for OpenSSL/SSLeay is available from the Grid-Ireland CA web server. Non conforming requests are not accepted.

Procedures differ if the subject is a person, server or service:

Person requesting a certificate

- (a) The certificate must be requested from the Grid-Ireland RA in person;
- (b) The certificate request must be preceded by a secure online submission to the Grid-Ireland CA Public Server;
- (c) The certificate request must be accompanied by a photocopy of the subscriber's ID card from their host institution plus their e-mail address.

Server

Certificate requests must be made by a secure online submission to the Grid-Ireland CA Public Server, signed with a valid personal Grid-Ireland CA certificate.

Service

Certificate requests must be made by a secure online submission to the Grid-Ireland CA Public Server, signed with a valid personal Grid-Ireland CA certificate.

To approve a request, the Grid-Ireland RA must sign the request with their valid Grid-Ireland RA certificate.

The Grid-Ireland CA Public Server is at <http://www.cs.tcd.ie/grid-ireland/publicserver.htm>

3.2 Routine Rekey

It is expected that rekeying of certificates of persons before their expiration will be requested by submitting a rekey request to the Grid-Ireland CA Public Server, signed by the subscriber's current personal Grid-Ireland CA certificate. Otherwise the Grid-Ireland CA staff will adopt the same procedure used for the authentication of identity of a person.

Rekeying of expired certificates will follow the same rules as an initial registration.

3.3 Rekey After Revocation

Rekey after revocation will follow the same rules as an initial registration.

3.4 Revocation Request

Certificate revocation requests can be submitted to the Grid-Ireland CA Public Server, signed by a valid personal Grid-Ireland CA certificate. Otherwise the Grid-Ireland CA staff will adopt the same procedure used for the authentication of identity of a person.

4 Operational Requirements

4.1 Certificate Application

The subscriber must generate a key pair as per Section 6: *Technical Security Controls*.

The Distinguished Name must be as per Section 7: *Certificate and CRL Profiles*.

The subscriber must register with the Grid-Ireland CA as per Section 3: *Identification and Authentication*.

4.2 Certificate Issuance

The Grid-Ireland CA issues the certificate if, and only if, the authentication of the subject is successful. The subject will be notified by e-mail. If the subject is a person, the e-mail will be sent to the address accompanying the request. Otherwise the e-mail will be sent to the address specified in the request. In the case of rejection, the e-mail will state the reason.

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:

- (a) The private key is lost or suspected to be compromised;
- (b) The information in the certificate is suspected to be inaccurate;
- (c) The subscriber no longer needs the certificate to access Relying Parties' resources;
- (d) The subscriber has violated his/her obligations;
- (e) The subject's relationship with Grid-Ireland has ceased.

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 the private key compromise or of the variation of the subscriber's data.

4.4.3 Procedure for Revocation Request

As per Section 3: *Identification and Authentication*.

4.4.4 Circumstances for Suspension

No stipulation.

4.4.5 Who Can Request Suspension

No stipulation.

4.4.6 Procedure for Suspension Request

No stipulation.

4.4.7 Limits on Suspension Period

No stipulation.

4.4.8 CRL Issuance Frequency

CRLs are issued after every certificate revocation or at least 7 days before the current CRL expires.

4.4.9 Online revocation/status checking availability

No stipulation.

4.4.10 Online revocation checking requirements

No stipulation.

4.4.11 Other forms of revocation advertisement available

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of Event Audited

The following events are audited:

- (a) Certificate requests;
- (b) Revocation/rekey requests;
- (c) Issued certificates;
- (d) Issued CRLs;
- (e) Boot of CA signing machine;
- (f) Logins to the CA signing machine.

4.5.2 Retention period for Audit Logs

Minimum retention period is three years.

4.5.3 Protection of Audit Logs

Only authorized CA personnel and authorized external auditors are allowed to view and process audit logs. Audit logs are copied to an off-line medium stored in safe storage.

4.6 Records Archival

4.6.1 Types of Event Recorded

The following events are recorded and archived:

- (a) Certificate requests;
- (b) Revocation/rekey requests;
- (c) Issued certificates;
- (d) Issued CRLs;
- (e) Boot of CA signing machine;
- (f) Logins to the CA signing machine.
- (g) All e-mail messages sent to the Grid-Ireland CA;
- (h) All e-mail messages sent by the Grid-Ireland CA.

4.6.2 Retention Period for Archives

Minimum retention period is three years.

4.6.3 Protection of Archives

Only authorized CA personnel and authorized external auditors are allowed to view and process archives. Archives are copied to an off-line medium stored in safe storage.

4.7 Key Changeover

No stipulation.

4.8 Compromise and Disaster Recovery

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

- (a) Inform subscribers, RAs and cross-certifying CAs;
- (b) Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

4.9 CA Termination

Before the Grid-Ireland CA terminates its services, it will:

- (a) Inform subscribers, RAs and cross-certifying CAs;
- (b) Make the details of its termination widely available;
- (c) Stop issuing certificates and CRLs.

5 Physical, Procedural and Personnel Security Controls

5.1 Physical Security Controls

5.1.1 Site Location

The Grid-Ireland CA is located at the Department of Computer Science, Trinity College Dublin.

5.1.2 Physical Access

The Grid-Ireland CA operates in a secure machine room, where physical access is restricted to authorized people.

5.1.3 Environmental Security

The Grid-Ireland CA operates in an environmentally controlled machine room.

5.2 Procedural Controls

No stipulation.

5.3 Personnel Security Controls

Grid-Ireland CA personnel must be staff members of the Department of Computer Science, Trinity College Dublin.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each entity must generate its key pair. The Grid-Ireland CA does not generate private keys for its subjects.

6.1.2 Private Key Delivery to Entity

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

Entities' public keys must be delivered to the Grid-Ireland CA in a secure and trustworthy manner as per Section 3: *Identification and Authentication*.

6.1.4 CA Public Key Delivery to Users

The Grid-Ireland CA certificate can be downloaded from the Grid-Ireland CA Public Server.

6.1.5 Key Sizes

- (a) The minimum key length for a personal or server certificate is 1024 bits.
- (b) The minimum key length for the Grid-Ireland CA certificate is 2048 bits.

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

No stipulation.

6.1.9 Key Usage Purposes

Keys may be used for authentication, non-repudiation, data encipherment, message integrity and session key establishment.

The Grid-Ireland CA private key is the only key that can be used for signing Grid-Ireland certificates and CRLs.

The certificate key Usage field must be used in accordance with [RFC2459].

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 Grid-Ireland CA private key is kept, encrypted, in multiple copies and in different locations, on CD-ROMs. For emergencies, the passphrase is in a sealed envelope kept in a safe.

6.3 Other Aspects of Key Pair Management

The Grid-Ireland CA certificate has a validity of five years; other Grid-Ireland certificates have a maximum validity of 420days.

6.4 Activation Data

The Grid-Ireland CA private key is protected by a passphrase with a minimum of 15 characters.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Grid-Ireland CA servers include the following functionalities:

- (a) Operating systems are maintained at a high level of security by applying all recommended and applicable security patches;
- (b) Monitoring is done to detect unauthorized software changes;
- (c) Services are reduced to the bare minimum;
- (d) Machines are protected by a suitably configured firewall.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Certificates are issued on a machine that is not connected to any kind of network.

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

The Grid-Ireland CA certificate includes the following extensions:

- (a) Basic Constraints (Critical)
CA:TRUE
- (b) Key Usage (Critical)
Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
- (c) Subject Key Identifier
9A:E2:D7:80:68:DB:92:65:5E:5B:83:BD:37:4D:0E:A1:79:26:2C:57
- (d) Authority Key Identifier
keyid:9A:E2:D7:80:68:DB:92:65:5E:5B:83:BD:37:4D:0E:A1:79:26:2C:57
- (e) Subject Alternative Name
email:grid-ireland-ca@cs.tcd.ie
- (f) Issuer Alternative Name
email:grid-ireland-ca@cs.tcd.ie
- (g) Netscape Cert Type
SSL CA, S/MIME CA, Object Signing CA
- (h) Netscape Comment
Grid-Ireland CA Certificate

The Grid-Ireland user certificates include the following extensions:

- (a) Basic Constraints (Critical)
CA:FALSE
- (b) Key Usage (Critical)
Digital Signature, Non Repudiation, Key Encipherment
- (c) Subject Key Identifier
<subject's key identifier>
- (d) Authority Key Identifier
keyid:9A:E2:D7:80:68:DB:92:65:5E:5B:83:BD:37:4D:0E:A1:79:26:2C:57
- (e) Subject Alternative Name
email:<subject's e-mail address>
- (f) Issuer Alternative Name
email:grid-ireland-ca@cs.tcd.ie
- (g) Netscape Cert Type
SSL Client, S/MIME
- (h) Netscape Comment
Grid-Ireland User Certificate

The Grid-Ireland server and service certificates include the following extensions:

- (a) Basic Constraints (Critical)
CA:FALSE
- (b) Key Usage (Critical)
Digital Signature, Non Repudiation, Key Encipherment
- (c) Subject Key Identifier
<subject's key identifier>
- (d) Authority Key Identifier
keyid:9A:E2:D7:80:68:DB:92:65:5E:5B:83:BD:37:4D:0E:A1:79:26:2C:57
- (e) Subject Alternative Name
DNS:<subject's DNS fully qualified domain name (FQDN)>
- (f) Issuer Alternative Name
email:grid-ireland-ca@cs.tcd.ie
- (g) Netscape Cert Type
SSL Client, SSL Server

- (h) Netscape Comment
Grid-Ireland Server Certificate

7.1.3 Algorithm object identifiers:

No stipulation.

7.1.4 Name forms:

The subject name is of the X.500 name type. It has one of the following forms:

Grid-Ireland CA

“C=IE, O=Grid-Ireland, CN=Grid-Ireland Certification Authority“.

Person

“C=IE, O=Grid-Ireland, OU=*organizationalUnitName*, L=*locationName*, CN=*commonName*“, where the *organizationalUnitName* must uniquely identify the subject’s host department, the *locationName* must uniquely identify the RA that approved the certificate request, and the *commonName* must be the Forename and the Surname of the subject.

Server

“C=IE, O=Grid-Ireland, OU=*organizationalUnitName*, L=*locationName*, CN=*commonName*“, where the *organizationalUnitName* must uniquely identify the subject’s host department, the *locationName* must uniquely identify the RA that approved the certificate request, and the *commonName* must be the DNS FQDN of the server preceded by ‘host’.

Service

“C=IE, O=Grid-Ireland, OU=*organizationalUnitName*, L=*locationName*, CN=*commonName*“, where the *organizationalUnitName* must uniquely identify the subject’s host department, the *locationName* must uniquely identify the RA that approved the certificate request, and the *commonName* must be the DNS FQDN of the server preceded by ‘*serviceName*’ where *serviceName* must uniquely identify the service.

The Distinguished Name must be unique for each subject certified by the Grid-Ireland CA. If the name presented by the subscriber is not unique, additional numbers or letters are appended to the *commonName* to ensure uniqueness.

The canonical name in the certificate subject must be able to be obtained from the real subject name. Certificates must apply to unique individuals or resources. Subjects may not share certificates.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

The Object Identifier (OID) is specified in 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.

Version 1 is required for compatibility with Netscape Communicator.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8 Specification Administration

8.1 Specification Change Procedures

Users will not be warned in advance of changes to the Grid-Ireland CA's policy and CPS.

8.2 Publication and Notification Procedures

The policy is available at <http://www.cs.tcd.ie/grid-ireland/gi-ca/>.

8.3 CPS Approval Procedures

No stipulation.

9 Bibliography

- [EuroPKI] EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000.
- [FBCA] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA), Version 1.0, 18 December 1999.
- [NCSA] National Computational Science Alliance, Certificate Policy, Version 0.9.1, June 30, 1999.
- [OpenSSL] <http://www.openssl.org/>
- [RFC2459] R. Housley, W. Ford, W. Polk and D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999.
- [RFC2527] S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999.
- [TrustID] TrustID Certificate Policy <http://www.digsigtrust.com/certificates/policy/tsindex.html>
- [INFN] INFN CA Certificate Policy and Certification Practice Statement, Version 0.3 (Draft), March 2001.

10 List of changes

Version	Date	Changes
0.1	June 2001	Initial Draft
0.2	September 2001	Reduction in duplication of stipulations
0.3	October 2001	Added ASN.1 OID [1.2]
0.4	June 2002	Added service certificates [1.3.3, 1.3.4, 7.1.2, 7.1.4] Separated CA and RA obligations [2.1.1, 2.1.2] Removed certificate publication [2.1.1, 2.6.1, 2.6.2, 2.6.3, 2.6.4] Added CA Public Server: [3.1.6, 3.2, 3.4, 6.1.4] Changed min.passphrase length to 15 chars [2.1.3] Clarified CRL publication/issue frequency [2.6.2, 4.4.8] Clarified repository access controls [2.6.3] Designated user's ID card as confidential [2.8] Changed from email requests to online requests [3.1.6] Changed from email delivery to online download [3.1.6] Changed RA approval procedure [3.1.6] Changed CA public key delivery [6.1.4] Reduced lifetime of CA certificate to 5 years [6.3] Set lifetime for other certificates to 420 days [6.3] Added ra-list.txt [1.3.2] Added non-commercial restriction [1.3.4] Defined CA min.passphrase length [6.4] Updated certificate extensions [7.1.2] Changed DN forms [2.8.2, 7.1.4] Removed stipulation of policy qualifier [7.1.8]
0.5	June 2003	Changed the <i>organizationalUnitName</i> to uniquely identify the subject's host department [7.1.4]