UNIVERSITY OF CYPRUS
DEPARTMENT OF COMPUTER SCIENCE
HIGH-PERFORMANCE COMPUTER SYSTEMS LAB

CyGrid CA

CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

Version 1.0.8
Jun. 2013

TABLE OF CONTENTS

1 Introduction

1.1 OVERVIEW

This document is structured according to RFC2527. Not all sections of RFC2527 are used. Sections that are not included have a default value of “No stipulation”.

The document defines the Certification Policy and the Certification Practice Statement of the CyGridCA (Cyprus Grid Certification Authority) and specifies the minimum requirements and obligations for the issuance and management of certificates that may be used in verifying digital signatures on the categories of electronic communications as specified in this document.

1.2 POLICY IDENTIFICATION

- Document title: **“CyGrid CA Certification Policy and Certificate Practice Statement”**
- Version: **1.0.8**
- Document Date: Jun**. 2013**
- O.I.D.: 1.3.6.1.4.1.14819.2.2.1.7
- Expiration: This document is valid until further notice.

1.3 COMMUNITY AND APPLICABILITY

1.3.1 Certification Authorities

CyGrid CA self-certifies its own certificate. It does not issue certificates to subordinate Certification Authorities.

1.3.2 Registration Authorities

The CyGrid CA manages the functions of its Registration Authority. Additional registration authorities may be created by the CyGrid CA as required.

1.3.3 End Entities

The CyGrid CA will issue certificates to natural persons and computer entities. Entities eligible for certification from the CyGrid CA are: All those entities formally based and/or having offices in Cyprus, that are involved in research or deployment of multi-domain distributed computing infrastructure, intended for cross-organizational sharing of resources. The focus of these organizations should also be in research and/or education.

1.3.4 Applicability

There will be three categories of certificates:

1.Server certificates: authentication, non-repudiation and communication encryption.

2.User certificates: authentication, non-repudiation, data encryption and communication encryption.

3.Services certificates: authentication, non-repudiation, data encryption and communication encryption.

1.3.5 User Restrictions

Certificates issued by the CyGrid CA are only valid in the context of the EGEE, CyGrid and CrossGrid research activities. Any other usage such as financial transactions is strictly forbidden.

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

1.4 CONTACT DETAILS

The CyGrid CA is created and managed by the High-Performance Computing Laboratory, Department of Computer Science, University of Cyprus.

The CyGrid CA address for operational issues is:

CyGrid Certification Authority
High-Performance Computer systems Lab
Department of Computer Science
University of Cyprus
P. O. Box 20537
CY-1678 Nicosia
Cyprus

Phone: (+ 357) 22.89.26.63
Fax: (+ 357) 22.89.27.01
Email: cygrid-ca@ucy.ac.cy

The contact person for questions related with this document or any other CyGrid CA related issues is:

Andoena Balla
High Performance Computer Systems Lab
Department of Computer Science
University of Cyprus
P. O. Box 20537
CY-1678 Nicosia
Cyprus

Phone: (+ 357) 22.89.26.63
Fax: (+ 357) 22.89.27.01
E-mail: andoena@cs.ucy.ac.cy

1.5 DEFINITIONS AND ACRONYMS

AUTHENTICATION	The process of establishing that individuals or organizations are who they claim to be. This process corresponds to the second process involved in identification.
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.
Certificate Revocation List (CRL)	A time stamped list identifying revoked certificates which is signed

	by a CA and made freely available in a public repository.
Certification Authority (CA)	An authority trusted by one or more subscribers to create and assign public key certificates and to be responsible for them during their whole life time.
Certification Practice Statement (CPS)	A statement of the practices, which a certification authority employs in issuing certificates.
End Entity (EE)	Subscribers (users, hosts and services) of the CyGRID CA
Registration Authority (RA)	An individual or group of people appointed by an organization that is responsible for Identification and Authentication of certificate subscribers, but that does not sign or issue certificates.
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.
CyGridCA	Cyprus Grid Certification Authority

2 General Provisions

2.1 OBLIGATIONS

2.1.1 CyGrid CA Obligations

The CyGrid CA is responsible for the following aspects of issuance and management of certificates:

1. The acceptance of certification requests from entitled entities;
2. the actual certificate signing procedure;
3. the publication of the certificate;
4. the certificate revocation procedures;
5. the publication of the CRLs;
6. the certificate renewal procedures;
7. ensuring that all aspects of the CA Services, CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representation and warranties of this Policy.

2.1.2 CyGrid RA Obligations

The CyGrid RA is responsible for the following:

1. authenticate entities according to the procedures described in this document;
2. send validated certificate requests to CyGrid CA by secure communications;
3. create and send validated revocation requests to the CyGrid CA by secure communications;
4. follow the policies and procedures described in this document.

2.1.3 Subscriber Obligations

In all cases, the CyGrid CA shall require the subscriber to:

1. Read and accept the policies and procedures published in this document;
2. generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key;
3. use a strong passphrase with a minimum length of 15 characters to protect the private key of personal certificates;

4. acknowledge that by accepting the certificate he/she warrants all information and representations in the certificate to be true;

5. use the certificate exclusively for authorized and legal purposes, consistent with this Policy;

6. notify the CyGrid CA when the certificate is no longer required;

7. notify the CyGrid CA when the information in the certificate becomes wrong or inaccurate;

8. instruct the CyGrid CA to revoke the certificate promptly upon an actual or suspected loss, disclosure, or other compromise of the subscribers private key;

9. user certificates must not be shared.

2.1.4 Repository Obligations

The CyGrid CA is responsible for providing a public repository, accessible through the World Wide Web at http://cygrid.org.cy/.

1. CyGrid CA will publish its public key on the above website;

2. CyGrid CA will publish on the above website the CRLs as soon as they are issued.

2.1.5 Relying Party Obligations

A Qualified Relying Party is required to:

1. Read and accept the policies and procedures published in this document.

2. Use the certificates only for the authorized uses as they have been set out in this document.

3. Check periodically the Certificate Revocation List (CRL) published on the website of the CyGrid CA [section 4.4.6].

2.2 LIABILITY

1 CyGrid CA guarantees to control the identity of the certification requests according to the procedures described in this document.

2 CyGrid CA guarantees to control the identity of the revocation requests according to the procedures described in this document.

3 CyGrid CA is run on a best effort basis and does not give any guarantees about the service security or suitability.

4 CyGrid CA shall not be held liable for any problems arising from its operation or improper use of the issued certificates.

5 CyGrid CA denies any kind of responsibilities for damages or impairments resulting from its operation.

2.3 FINANCIAL RESPONSIBILITY

CyGrid CA denies any financial responsibilities for damages or impairments resulting from its operation.

2.4 INTERPRETATION

2.4.1 Governing Law

The enforceability, construction, interpretation, and validity of this policy shall be governed by the Laws of the Republic of Cyprus.

2.4.2 Dispute Resolution Procedures

Legal disputes arising from the operation of the CyGrid CA will be resolved according to the Cyprus Law.

2.5 FEES

No fees shall be charged.

2.6 PUBLICATION AND REPOSITORIES

2.6.1 Publication of CA Information

The CyGrid CA is obligated to maintain a secure on-line repository that is available to Qualified Relying Parties through a web interface at http://cygrid.org.cy and which contains:

1. The CyGrid CA certificate for its signing key;
2. the latest CRL;
3. a copy of this document which specifies the CP and CPS;
4. other relevant information relating to certificates that refer to this Policy.

2.7 Frequency of Publication

All information to be published in the repository shall be published promptly after such information is available to the CA. Information relating to the revocation of a certificate will be published as described in section 4.4.5.

2.8 Access Controls

CyGrid CA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL, LDAP repository with public keys and a copy of this document containing the CP and CPS.
CyGrid CA may impose a more restricted access control policy to the repository at its discretion.
The CyGrid CA web site is maintained in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available most of the time.

2.9 COMPLIANCE AUDIT

The CyGrid CA may be audited by other trusted CAs to verify its compliance with the rules and procedures specified in this document. Any costs associated with such an audit must be covered by the requesting party.

2.10 CONFIDENTIALITY POLICY

CyGrid CA collects personal information about the subscribers (e.g. full name, organization, email address). These data will be protected according to the law of Republic of Cyprus.

2.10.1 Confidential Information Kept by the CyGrid CA and RA

All information about subscriber that is not present in the certificate and CRL is considered confidential and will not be released outside.

2.10.2 Types of Information not considered Confidential.

Information included in issued certificates and CRLs is not considered confidential.

2.10.3 Disclosure of Certificate Revocation/Suspension Information

The CyGrid CA will notify and inform the following entities:

1. The subject of the personal certificate;
2. the requester of the server certificate.

2.10.4 Release of Information to Law Enforcement Officials

Any confidential information collected by the CyGrid CA will be subject to the law of Republic of Cyprus.

2.10.5 Information that can be revealed as a Part of Civil Discovery

Any confidential information collected by the CyGrid CA will be subject to the law of Republic of Cyprus.

2.10.6 Conditions of Disclosure upon owner's request

Any confidential information collected by the CyGrid CA will be subject to the law of Republic of Cyprus.

2.10.7 Other Circumstances for Disclosure of Confidential Information

Any confidential information collected by the CyGrid CA will be subject to the law of Republic of Cyprus.

3 Identification and Authentication

3.1 INITIAL REGISTRATION

3.1.1 Types of names

The subject names for the certificate applicants shall follow the X.500 standard:

1. In case of personal certificate the subject name must include the person’s name.
2. In case of server certificate the subject name must include the DNS Fully Qualified Domain Name (FQDN) name. It may be prefixed with “host/”.
3. In case of service certificate the subject name must include the DNS FQDN name, prefix with the service name.

See also section 7.1.4 for more details.

3.1.2 Name Meanings

1. The format of a CyGrid distinguished name is:
   “C=CY, O=CyGrid, O=organisation, CN=subject-name”.
2. The common name in the certificate subject must be obtainable from the real name of the subject or from the FQDN of the server.
3. The distinguished name must be one of the organizations involved in CyGrid activities.
4. Currently a list of values available for distinguished name O (organisation) can be found at URL http://grid.ucy.ac.cy/CyGridCA/ra.html

3.1.3 Name Uniqueness

The subject name listed in a certificate shall be unambiguous and unique for all certificates issued by the CyGrid CA. If necessary, additional numbers or letters may be appended to the real name to ensure the name’s uniqueness within the domain of certificates issued by the CyGrid CA.

3.1.4 Method to Prove Possession of Private Key

Obtaining a personal or individual certificate is initiated by a key generation tag or control which the individual’s web browser reads on the CA’s user registration web page. Key generation and certificate signing request generation and submission are tied together in a single session, and there is a reasonable presumption of possession of private key in requests originating in web browser functions. Keys generated by other means (such as openssl), whether for persons or services, have separate key generation, csr generation, and submission stages. No proof of possession of private key test is made in these cases. Renewal and revocation functions employ a proof of possession of private key test.

3.1.5 Authentication of Organization

CyGrid CA verifies the Authentication of Organization by checking if:

- the organization is known to be part of a grid-computing project or related partner; approved by the CyGrid manager, or
- the organization is registered and operating in Cyprus. Registration in Cyprus will be validated through proper public authorities.

3.1.6 Authentication of Individual

3.1.6.1 Person requesting a certificate

1. The certificate request must be delivered to RA in person by the person requesting the certificate.
2. The subject authentication is performed through the presentation of a valid official identification

document, which can either be a passport or an identity card. The email address must have a domain that belongs to an organization as defined in 3.1.5 and is further validated by a random number given (in person) to the person requesting the certificate. We denote this random number as URND. In addition, the RA manager generates another random number (denoted as RARND) and pairs it with URND. The RA manager informs the subject that he/she will receive an email by the RA within one (1) week, asking a reply that includes the URND in the reply body. The RA manager directs the subject to reply without changing the email subject and body and must only provide the URND. Furthermore, the initial email from the RA manager is: (i) digitally signed with the RA manager's certificate to enable identity verification and (ii) also includes the RARND. The subject is obliged to reply back to the RA manager within one(1) week. If the subject does not reply with a matching URND-RARND pair and within the specified time frame, then the certificate is not issued.

3.1.6.2 Server or service certificate

1. Requests must be signed with the personal CyGrid CA certificate of the corresponding system administrator.

3.1.6.3 Person not requesting a certificate

1. Individual identity may be authenticated by personal acquaintance with CyGrid CA/RA staff;

2. By physical presence and proof of identity through a passport or identity card.

3.2 ROUTINE REKEY

Expiration warnings will be issued to subscribers when rekey time arrives. Rekey before expiration can be accomplished by sending a rekey request signed with the current user certificate. Rekey after expiration follows the same authentication procedure as new certificate. User must generate a new key pair.
Re-verification and authentication of identity processes is required for entities on or prior to 5 years from the original/initial identity authentication.

3.3 REKEY AFTER REVOCATION

Revoked or expired certificates shall not be renewed. Applicants without a valid certificate from the CyGrid CA shall be re-authenticated by the RA on certificate application, just as with a first time application.

3.4 REVOCATION REQUESTS

Certificate revocation requests should be submitted by:

1. Email sent to cygrid-ca@ucy.ac.cy signed by the corresponding CyGrid CA certificate. When e-mail is not an option, the request will be authenticated using the procedure described in section 3.1.6.3.

2. Someone presents irrefutable proof that the private key is compromised.

4 Operational Requirements

4.1 CERTIFICATE APPLICATIONS

The necessary provisions that must be followed in any certificate application request to the CyGrid CA are:

1. The subject must be an acceptable end user entity, as defined by this Policy;
2. the request must obey the CyGrid CA distinguished name scheme;
3. the distinguished name must unambiguous and unique;
4. the key must have at least 1024 bits.

4.2 CERTIFICATE ISSUANCE

The following requirements must be met for a certificate to be issued:

1. The subject identity verification must be successful;
2. the maximum validity period for a certificate must be 1 year.

The subject will be notified by E-mail about the certificate issuance or rejection. In the case of rejection, the E-mail will state the reason.

4.3 CERTIFICATE ACCEPTANCE

An issued certificate is delivered to an end user in person or via email. Upon receipt of the certificate, the end user must verify that the certificate corresponds to his/her private that had been used to issue the certificate request. If there are any objections, then the Cygrid CA must immediately be notified. If no objections have been received within a week (starting from the day that the certificate was delivered), then the certificate is regarded that it has been accepted by the user.

4.4 CERTIFICATE REVOCATION

4.4.1 Circumstances of Revocation

A certificate will be revoked in the following circumstances:

1. The subject of the certificate has ceased his relation with the EGEE, CyGrid or Crossgrid projects;
2. the subject does not require the certificate anymore;
3. the private key has been lost or compromised;
4. the information in the certificate is wrong or inaccurate;
5. the system to which the certificate has been issued has been retired;
6. the subject has failed to comply with the rules of this policy.

4.5 Who can request revocation

The revocation of the certificate can be requested by:

1. The certificate subscriber;
2. any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data.

4.6 Procedure of Revocation Request

The entity requesting the certificate revocation is authenticated by signing the revocation request with a valid CyGrid CA certificate.
Otherwise authentication will be performed with the same procedure as described in section 3.1.6.3.

4.6.1.1 Repository/CRL Update

Promptly following revocation, the CRL or certificate status database in the repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the CyGrid CA shall be archived.

4.6.2 CRL Issuance Frequency

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

2. the minimum CRL lifetime is 7 days;

3. CRLs are issued at least 7 days before expiration.

4. A CRL is issued immediately after a revocation

4.6.3 CRL Checking Requirements for Relying Parties

Download the CRL at least once a day and implement its restrictions while validating certificates.

4.6.4 On line Revocation/Status Checking Availability

Currently no Online Revocation/Status Checking service is offered by the CyGrid CA.

4.6.5 Variations of the above in case of private key compromise

If a major security problem may be generated from a compromised certificate the CyGrid CA may choose to warn the known relying parties using any means seem fit.

4.7 SECURITY AUDIT PROCEDURES

All significant security events on the CA system should be automatically recorded in audit trail file. Such files shall be retained at least six months on site, and thereafter shall be securely archived as per Section 4.6.

4.7.1 Types of Events Audited

- System boots and shutdowns
- Interactive system logins
- Periodic message digests of all system files
- Requests for certificates
- Identity verification procedures
- Certificate issuing
- Requests for revocation
- CRL issuing

4.7.2 Processing Frequency of Audit Logs

Audit logs will be processed at least once per month.

4.7.3 Retention Period of Audit Logs

Audit logs will be retained for a minimum of 3 years.

4.7.4 Protection of Logs

Only authorized CA personnel is allowed to view and process audit logs. Audit logs are copied to an offline medium.

4.7.5 Backup Procedures

Audit logs are copied to an offline medium, which is stored in a safe location.

4.7.6 Accumulation system

The audit log accumulation system is internal to the CyGrid CA.

4.8 RECORDS ARCHIVAL

4.8.1 Types of Records Archived

The following data and files will be archived by the CyGrid CA:

1. All certificate application data, including certification, revocation and suspension requests;
2. all certificates and all CRLs or certificate status records generated;
3. all the email messages sent and received by the CyGrid CA and RA.

4.8.2 Processing Frequency of Audit Logs

Not defined yet.

4.8.3 Retention Period for audit logs

Logs will be kept for a minimum of three years.

4.8.4 Protection of Audit Logs

4.8.4.1 Access

Audit logs may be consulted by:

1. CA personnel;
2. authorised external auditors.

4.8.4.2 Protection against modification and deletion

Audit logs are copied to an off-line medium, which is stored in safe storage. Online logs are protected by ACLs in the file system used by operating system.

4.8.5 Backup Procedures

Audit events are copied to an off-line medium.

4.8.6 Archive Collection System

The archive collection system is internal to the CyGrid CA.

4.9 KEY CHANGEOVER

In the future an on line system for key changeover may be provided.

4.10 COMPROMISE AND DISASTER RECOVERY

If the CA private key is compromised or destroyed the CA will:

1. Notify subscribers, RAs and cross-certifying CAs;
2. terminate the issuance and distribution of certificates and CRLs;
3. notify relevant security contacts.

4.11 CA TERMINATION

Upon termination the CyGrid CA will:

1. Notify subscribers, RAs and cross-certifying CAs;
2. terminate the issuance and distribution of certificates and CRLs;

3. notify relevant security contacts;
4. notify widely as possible the end of the service;
5. all private keys of the terminating CA will be destroyed.

5 Physical, Procedural and Personnel Security Controls

5.1 PHYSICAL SECURITY – ACCESS CONTROLS

5.1.1 Site Location

The CyGrid CA is located at the High-Performance Computing Laboratory, Department of Computer Science, University of Cyprus.

5.1.2 Physical Access

Physical access to the CyGrid CA is restricted to authorized personnel.

5.1.3 Power and Air Conditioning

The CRL web server is protected by uninterruptible power supply. Environment temperature in rooms containing CA related equipment is maintained by an appropriate level air conditioning system.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

CyGrid CA facilities obey to the law of Republic of Cyprus regarding fire prevention and protection in public buildings, and the regulation of the University of Cyprus .

5.1.6 Media Storage

1. The CyGrid CA key is kept in several removable storage media, which locked in a single access-controlled room.

2. Backup copies of CA related information are kept in magnetic tape cartridges, floppies and CD-ROM. There are backups of the passphrase, which know only by CyGrid CA.

5.1.7 Waste Disposal

Wastes carrying potential confidential information such as old floppy disks are physically destroyed before being trashed.

5.1.8 Off site Backup

No off-site backups are currently performed.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

All employees, contractors, and consultants of the CyGrid CA (collectively “personnel”) that have access to or control over cryptographic operations that may materially affect the CA’s issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA’s repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA’s operations.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Background Checks and Clearance Procedures for CA Personnel

CyGrid CA personnel are recruited from the Department of Computer Science, University of Cyprus.

5.3.2 Background Checks and Security Procedures for other personnel

No other personnel is authorized to access the CyGrid CA facilities without the physical presence of CyGrid CA personnel.

5.3.3 Training Requirements and Procedures

Internal training is given to CyGrid CA operators.

5.3.4 Training Period and Retraining Procedures

Not defined yet.

6 Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key pair generation

Key pairs for CAs, RAs and subscribers must be generated in such a way that private key is not known by other than the authorized user of the key pair. Each subscriber must generate his/her own key pair. The CyGrid CA does not generate private keys for subjects.

6.1.2 Private Key delivery to Entity

The CyGrid CA does not generate private keys hence does not deliver private keys.

6.1.3 Subscriber Public Key Delivery to CyGrid RA

The subscriber's key must be transferred to the CyGrid RA in a way that ensures that it has not been altered.

6.1.4 Public Key delivery to Entity

Public keys are delivered by signed E-mail, floppy disk or CD-ROM.

6.1.5 CA Public Key delivery to users

CA certificate can be downloaded from the CyGrid CA web site at http://cygrid.org.cy/CyGridCA/afe55e66.0

6.1.6 Key Sizes

1. The minimum key length for a personnel or server certificate is 1024 bit.
2. The CyGrid CA key length is 2048 bits.

6.1.7 Public Key Parameters Generation

Not defined yet.

6.1.8 Parameter quality testing

Not defined yet.

6.1.9 Hardware/software key generation

Not defined yet.

6.1.10 Key Usage Purposes

Keys may be used for authentication, non-repudiation, data ciphering, message integrity and session establishment. Certificates and CRLs are signed by the CA private key.

6.2 PRIVATE KEY PROTECTION

6.2.1 Private key (N-M) Multi-Person Control

Not defined yet.

6.2.2 Private Key Escrow

CA does not have access to private keys

6.2.7 Private Key Archival and Backup

The CyGrid CA private key is kept encrypted in multiple copies in floppy disks and CD-ROMs in safe places. The pass phrase is in a sealed envelope kept in a safe. The passphrase is not stored in any electronic form.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

The CyGrid CA private key has currently a validity of eight years.

6.4 ACTIVATION DATA

The CyGrid CA private key is protected by a pass phrase with a minimum length of 15 characters.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Security Technical Requirements

1. The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches.

2. Monitoring is performed to detect unauthorized software changes.

3. CA systems configuration is reduced to the bare minimum.

4. The signing machine is kept powered off between uses.

6.5.2 Computer Security Rating

Not defined yet.

6.6 LIFE CYCLE SECURITY CONTROLS

Not defined yet.

6.7 NETWORK SECURITY CONTROLS

1. The CA signing machine is kept off-line.

2. CA/RA machines other than the signing machine are protected by a firewall.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

No hardware cryptographic module has been installed but the CA machine is never online.

7 Certificate and CRL profile

7.1 CERTIFICATE PROFILE

7.1.1 Version

All certificates that reference this Policy will be issued in the X.509 version 3 format and will include a reference to the O.I.D. of this Policy within the appropriate field.

7.1.2 Certificate Extensions

- Basic constraints (Critical):
  Not a CA.
- Key usage (Critical):
  Digital signature, key ciphering, data ciphering.
- Subject key identifier
- Authority key identifier
- Subject alternative name: subject's e-mail address
- Issuer alternative name: issuer's e-mail address
- CRL distribution points
- Certificate policies

7.1.3 Algorithm Object Identifiers

RSA with SHA1

7.1.4 Name Forms

Issuer:
C=CY,
O=CyGrid,
CN=CyGridCA
Subject:
C=CY,
O=CyGrid,
O=Organisation,
CN=*SUBJECT-NAME*

7.1.5 Name Constraints

Different certificates can not have the same CN. If a user has the same common name (i.e. full name) with a user already having a certificate, then an additional characteristic, like a middle name, is added to the newly created certificate.

7.2 Certificate Policy Identifier

CyGrid CA identifies this policy with the object identifier (O.I.D.):
As specified in Section 1.2

7.2.1 Policy Qualifier Syntax and Semantics

Not defined yet.

7.3 CRL PROFILE

7.3.1 Version

All CRLs will be issued in X.509 version 2.

8 Policy Administration

8.1 SPECIFICATION CHANGE AND PROCEDURES

Relevant changes will be made as widely available as possible.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

The CyGrid CA policy is available at http://cygrid.org.cy/CyGridCA/CyGrid-CPS.pdf

8.3 CPS APPROVAL PROCEDURES

Whenever there is a change in the CPS that significantly impacts its users, all changes must be announced to the EugridPMA, but signing the certificates continue unless there is specific request from PMA to stop.