HellasGrid Root Certification Authority

Certificate Policy and Certification Practices Statement

15 July, 2006

Contents

Chapter 1

INTRODUCTION

1.1 Overview

During the first quarter of 2002, the Computer Center of the Department of Physics at the Aristotle University of Thessaloniki implemented the HellasGrid Certification Authority, in order to facilitate the needs of Grid Computing in Greece.

In January 2003, the National Grid Initiative, named 'Hellas Grid Task Force', was established by the Secretariat for the Information Society, Ministry of Economy & Finance under the coordination Greek National Research & Education Network GRNET. GRNET is owned and supervised by Secretariat of Research and Technology, Greek Ministry of Development.

The HellasGrid CA is operated by the GridAUTH Operations Center at the Aristotle University of Thessaloniki in the context of the HellasGrid National Grid Infrastructure.

This document, following the structure set out in RFC 3647, defines the Certification Policy and the Certification Practice Statement of the HellasGrid Root CA and specifies the minimum requirements and obligations for the signing and management of certificates.

1.2 Document name and identification

- Document title: HellasGrid Root CA Certification Policy and Certification Practice Statement
- Version: 1.0
- Document Date: 15 July, 2006
- O.I.D.: 1.3.6.1.4.1.23877.8.0.1.1.0

Table 1.1 describes the structure of the O.I.D.

1.3 PKI participants

1.3.1 Certification Authorities

HellasGrid Root CA, which is defined as a medium security CA, only signs CA certificates.

1.3.6.1.4.1	Prefix for IANA private enterprises
23877	GridAUTH Operation Center
8	PKI
0	HellasGrid Root CA
1	CP/CPS
1.0	Document Version

Table 1.1: O.I.D. description table

1.3.2 Registration Authorities

HellasGrid Root CA performs the task of the RA.

1.3.3 Subscribers

Subscribers eligible for certification by the HellasGrid Root CA are only Certification Authorities serving the Greek research and educational community.

1.3.4 Relying parties

People and Organizations that are using the public keys, in certificates issued by the HellasGrid Root CA for the purposes of signature verification and/or encryption, will be considered as relying parties.

1.3.5 Other participants

No stipulation.

1.4 Certificate Usage

No stipulation.

1.4.1 Appropriate certificate uses

Certificates issued by the HellasGrid Root CA are only valid in the context of research and educational activities.

1.4.2 Prohibited certificate uses

Any other kind of usage such as financial transactions is strictly forbidden.

1.5 Policy administration

1.5.1 Organization administering the document

The HellasGrid Root CA CP/CPS was authored and is administered by the GridAUTH Operations Center.

The HellasGrid Root CA address for operational issues is :

```
HellasGrid Certification Authority
Building 22d, 4th Floor, Office 4'6B
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE
Phone: (+ 30)2310998223
Fax: (+ 30)2310994309
Email: hellasgrid-root-ca@grid.auth.gr
```

1.5.2 Contact Person

The contact person for questions about this document or any other HellasGrid Root CA related issues is:

```
Kanellopoulos Christos
Building 22d, 4th Floor, Office 4'6B
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE
Phone: (+ 30)2310998223
Fax: (+ 30)2310994309
E-mail 1: c.kanellopoulos@grid.auth.gr
E-mail 2: contact@grid.auth.gr
```

1.5.3 Person determining CPS suitability for the policy

The person who determines the CPS suitability for this policy is:

```
Kanellopoulos Christos
Building 22d, 4th Floor, Office 4'6B
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE
Phone: (+ 30)2310998223
Fax: (+ 30)2310994309
E-mail: c.kanellopoulos@grid.auth.gr
```

1.5.4 CPS approval procedures

No stipulation.

1.6 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 certicate to a particular community and/or class of application with common security requirements. For example, a particular certicate policy might indicate applicability of a type of certicate to the authentication of electronic data interchange transactions.
Certificate Revocation List (CRL)	A time stamped list identifying revoked certicates 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 certicates and to be responsible for them during their whole lifetime.
Certification Practices Statement (CPS)	A statement of the practices, which a certication authority employs in issuing certicates.
End Entity (EE)	Subscribers (users, hosts and services) of the Hellas-Grid CA
GridAUTH	The GridAUTH Operations Center, which operates in the context of the Network and Telecommunications Committee of the Aristotle University of Thessaloniki
Identification	The process of establishing the identity of an individual or organization. It involves two subprocesses in the context of PKI. (1) Establishing that a given name corresponds to a real-world identity and (2) establishing an individual or organization under that name is in fact the named individual or organization.
Registration Authority (RA)	An individual or group of people appointed by an organization that is responsible for Identication and Authentication of certicate subscribers, but that does not sign or issue certicates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party (RP)	A recipient of a certicate who acts in reliance on that certicate and/or digital signatures veried using that certicate.

Chapter 2

PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

All the on-line and off-line repositories of the HellasGrid Root CA are operated by the GridAUTH Operations Center.

The HellasGrid Root CA communication information for issues regarding the repositories is :

```
HellasGrid Certification Authority
Building 22d, 4th Floor, Office 4'6B
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE
Phone: (+ 30)2310998223
Fax: (+ 30)2310994309
Email: hellasgrid-root-ca@grid.auth.gr
```

2.2 Publication of certification information

The HellasGrid Root CA maintains a secure on-line repository that is available to all Relying Parties through a web interface at http://www.grid.auth.gr/pki/hellasgrid-root-ca and which contains:

1. the HellasGrid Root CA certificate;
2. valid issued certificates;
3. the latest CRL;

4. a copy of the current and all previous versions of this document;

5. other relevant information relating to certificates.

2.3 Time or frequency of publication

All information due to be published in the repository shall be published promptly after such information is available to the CA. Certificates issued by the HellasGrid Root CA that reference this Policy, will be published promptly upon acceptance of such certificate by the subscriber. Information relating to the revocation of a certificate will be published as described in subsection 4.9.7.

2.4 Access control on repositories

HellasGrid Root CA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS.

HellasGrid Root CA may impose a more restricted access control policy to the repository at its discretion.

The HellasGrid Root CA web site is maintained on a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available 24×7.

Chapter 3

IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

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

3.1.2 Need for names to be meaningful

The subject names for the certificate applicants shall follow the X.500 standard. The CN field must describe the sub-ordinate CA.

3.1.3 Anonymity or pseudonimity of subscribers

HellasGrid CA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

Allowed characters are: `a-z A-Z 0-9 . , ( ) = :` space

Characters can be encoded in one of the following forms:

```
PrintableString;
T61String;
IA5String
```

See also section 3.1.1.

3.1.5 Uniqueness of names

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

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of key

The HellasGrid Root CA proves possession of the private key, that is the companion to the HellasGrid Root CA certificate, by issuing certificates and signing CRLs.

The HellasGrid Root CA verifies the possession of the private key associated to a certificate request by asking for a cryptographic challenge-response exchange at any point in time either before or after certification of the subscriber.

The HellasGrid Root CA will not generate the key pair for subscribers and will not accept or retain private keys generated by subscribers.

3.2.2 Authentication of organization identity

HellasGrid Root CA authenticates an organization by:

- checking that the organization is focused on education or research and in addition legal with respect to the Greek Law;
- contacting the person who represents the organization.

3.2.3 Authentication of individual identity

The manager of the requesting Certification Authority must contact in person the HellasGrid Root CA. The authentications of the manager's identity is performed through the presentation of a valid photo ID document along with a valid official document stating that the manager represents an acceptable Certification Authority.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria of interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

A revoked key will not be re-certified.

3.4 Identification and authentication for revocation request

No stipulation.

Chapter 4

CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Certification Authorities operating in the context of research or educational activities in Greece.

4.1.2 Enrollment process and responsibilities

The requesting Certification Authority shall present a CP/CPS describing its certificate policies and certification practices. The requesting Certification Authority must sign a clearly defined namespace that will not class with a namespace that is being used by another Certification Authority.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

HellasGrid Root CA does not issue end entity certificates.

4.2.2 Approval or rejection of certificate applications

HellasGrid Root CA does not issue end entity certificates.

4.2.3 Time to process certificate applications

HellasGrid Root CA does not issue end entity certificates.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

No stipulation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

All the certificates issued by the HellasGrid Root CA will be published in the on-line repository operated by the HellasGrid Root CA.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscribers' private keys along with the certificates issued by the HellasGrid Root CA can be used for:

1. CRL signature;
2. Key Certificate signature

4.5.2 Relying party public key and certificate usage

Relying parties can use the HellasGrid Root CA public key and certificate to verify and validate sub-ordinate certificates.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

HellasGrid Root CA will not renew a subscribers certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.2 Who may request renewal

HellasGrid Root CA will not renew a CAs certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.3 Processing certificate renewal requests

HellasGrid Root CA will not renew a CAs certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.4 Notification of new certificate issuance to subscriber

HellasGrid Root CA will not renew a CAs certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.5 Conduct constituting acceptance of a renewal certificate

HellasGrid CA will not renew a CAs certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.6 Publication of the renewal certificate by the CA

HellasGrid Root CA will not renew a CAs certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.7 Notification of certificate issuance by the CA to other entities

HellasGrid Root CA will not renew a CAs certificate. Subscribers must follow the re-key procedure as defined in section 4.7.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

A sub-ordinate CA must re-key in the following circumstances:

1. expiration of their certificate signed by the HellasGrid Root CA;
2. compromise of their private key;
3. revocation of their certificate by the HellasGrid Root CA.

4.7.2 Who may request certification of a new public key

Same as in section 4.1.1 under the circumstances given in 4.7.1.

4.7.3 Processing certificate re-keying requests

HellasGrid Root CA does not sign certificates for end entities.

4.7.4 Notification of new certificate issuance to subscriber

Same as in section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Same as in section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Same as in section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

Same as in section 4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate will be revoked under the following circumstances:

1. the private key has been lost or compromised;
2. the information in the certificate is wrong or inaccurate;

4.9.2 Who can request revocation

The revocation of the certificate can be requested by anyone presenting proof of knowledge of the private key compromise.

4.9.3 Procedure for revocation request

No stipulation.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

HellasGrid Root CA will process all revocation requests within 1 working day.

4.9.6 Revocation checking requirement for relying parties

Relying parties must download the CRL from the on-line repository [section 2.2] at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL issuance frequency

1. CRLs will be published in the on-line repository as soon as issued and at least once every 6 months;
2. The minimum CRL lifetime is 7 days;
3. CRLs are issued at least 7 days before expiration.

4.9.8 Maximum latency for CRLs

See section 4.9.7.

4.9.9 On-line revocation/status checking availability

Currently there are no on-line revocation/status services offered by the HellasGrid Root CA.

4.9.10 On-line revocation checking requirements

Currently there are no on-line revocation/status services offered by the HellasGrid Root CA.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

HellasGrid Root CA does not suspend certificates.

4.9.14 Who can request suspension

HellasGrid Root CA does not suspend certificates

4.9.15 Procedure for suspension request

HellasGrid Root CA does not suspend certificates

4.9.16 Limits on suspension period

HellasGrid Root CA does not suspend certificates

4.10 Certificate status services

4.10.1 Operational characteristics

HellasGrid Root CA operates an on-line repository that contains all the CRLs that have been issued. Promptly following revocation, the CRL or certificate status database in the repository shall be updated, as applicable.

4.10.2 Service availability

The HellasGrid Root CA on-line repository is maintained on best effort basis with intended availability of 24×7.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

Chapter 5

FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The HellasGrid Root CA is located at the Aristotle University of Thessaloniki Campus, in the Department of Physics at building 22d.

5.1.2 Physical access

Physical access to the HellasGrid Root CA is restricted to authorized personnel only.

5.1.3 Power and air conditioning

The HellasGrid Root CA signing machine and the CA web server are both protected by uninterruptable power supplies. Environment temperature in rooms containing CA related equipment is maintained at appropriate levels by air conditioning systems.

5.1.4 Water exposures

HellasGrid Root CA facilities adhere to the Greek law regarding flood prevention and protection in public buildings.

5.1.5 Fire prevention and protection

HellasGrid CA facilities adhere to the Greek law regarding fire prevention and protection in public buildings.

5.1.6 Media storage

1. The HellasGrid Root CA private key is kept in several removable storage media;
2. Backup copies of CA related information are kept in magnetic tape cartridges, floppies and CD-ROM.

5.1.7 Waste disposal

Waste 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 HellasGrid Root CA (collectively personnel) that have access to or control over cryptographic operations that may materially affect the CAs issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CAs 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 CAs operations.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

HellasGrid Root CA personnel is selected by the GridAUTH Operations Center.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to HellasGrid Root CA operators.

5.3.4 Retraining frequency and requirements

HellasGrid Root CA will perform operational audit of the CA staff at least once per year. If the results of the operational audit are not satisfactory, retraining will be considered.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

Documentation regarding all the operational procedures of the CA is supplied to personnel during the initial training period.

5.4 Audit logging procedures

5.4.1 Types of events recorded

- 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

5.4.2 Frequency of processing log

Audit logs will be processed at least once per 6 months.

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

5.4.5 Audit log backup procedures

Audit logs are copied to an off line medium, located within the GridAUTH operational center premises.

5.4.6 Audit collection system (internal vs. external)

The audit log accumulation system is internal to the HellasGrid Root CA.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

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

1. all certificate application data, including certification and revocation;
2. all certificates and all CRLs or certificate status records generated;
3. the login/logout/reboot of the issuing machine.

5.5.2 Retention period for archive

Logs will be kept for a minimum of three years.

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

Audit events are copied to an off-line medium.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

Audit events are copied to an off-line medium.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

The CA's private signing key is changed periodically; from that time on only the new key will be used for certificate signing purposes. The overlap of the old and new key must be sufficient to cover the validity period of all the certificates signed by the HellasGrid Root CA. During this overlapping period, the older but still valid certificate will be available to verify old signatures and the private key to sign CRLs.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

1. Notify subscribers and subordinate CAs;
2. Terminate the issuance and distribution of certificates and CRLs;
3. Notify relevant security contacts.

5.7.2 Computing resources, software, and/or data are corrupted

Both private and public CA data is backed up every time they are changed.

5.7.3 Entity private key compromise procedures

No stipulation.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

Upon termination the HellasGrid Root CA will:

1. Notify sub-ordinate CAs;
2. Terminate the issuance and distribution of certificates and CRLs;
3. Notify relevant security contacts;
4. Notify as widely as possible the end of the service.

Chapter 6

TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs for CAs must be generated in such a way that private key is not known by any other than the owner of the key pair.

HellasGrid Root CA does not generate private keys on behalf of sub-ordinate CAs.

6.1.2 Private key delivery to subscriber

The HellasGrid Root CA does not generate private keys hence does not deliver private keys.

6.1.3 Public key delivery to certificate issuer

The subscriber's public key must be transferred to the HellasGrid Root CA in a way that ensures that it has not been altered.

6.1.4 CA public key delivery to relying parties

CA certificate can be downloaded from the HellasGrid Root CA web portal.

6.1.5 Key sizes

1. The minimum key length for the private keys of subordinate CAs is 2048 bit.
2. The minimum length for the HellasGrid Root CA private key is 2048 bits.

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

CA Certificate: The CA key can be used for CRL signing (cRLSign) and for certificate signing (keyCertSign)

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

The HellasGrid Root CA private key is kept in encrypted form in media storage as described in section 5.1.6. All media is located in safe places where access is restricted to authorized personnel only.

6.2.5 Private key archival

HellasGrid Root CA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private key storage on cryptographic module

No stipulation.

6.2.8 Method of activating private key

No stipulation.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

All certificates issued to sub-ordinate CAs by the HellasGrid Root CA must have a maximum lifetime of no more than 10 years.

The lifetime of the HellasGrid Root CA root certificate must be no more than 20 years and no less than 10 years.

6.4 Activation data

6.4.1 Activation data generation and installation

The pass phrase used to activate the HellasGrid Root CA private key is generated on the computer used for the Root CA signing operations and must be at least 15 characters long. Every 6 months the pass phrase is regenerated by one of the HellasGrid Root CA Operators.

6.4.2 Activation data protection

The HellasGrid Root CA uses a pass phrase to activate its private key, which is known only by the HellasGrid Root CA Manager and the HellasGrid Root CA Operators. A copy in written form of the pass phrase is sealed in an envelope and kept in a safe. Access to the safe is restricted only to the HellasGrid Root CA Manager and Operators. Old activation data are destroyed according to current best practices.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

1. The Root CA signing machine is kept off-line;
2. Root CA machines other than the signing machine are protected by a firewall;
3. Passive monitoring is performed in order to detect malicious network activity.

6.8 Time-stamping

No stipulation.

Chapter 7

CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

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

CA certificates:

1. Basic constraints (Critical): CA.
2. Key usage (Critical): CRL signature, key certificate signature.
3. Subject key identifier
4. Authority key identifier
5. Subject alternative name
6. Issuer alternative name
7. CRL distribution points
8. Certificate policies

Root CA certificate:

1. Basic constraints (Critical): CA.
2. Key usage (Critical): CRL signature, key certificate signature.
3. Subject key identifier

4. Authority key identifier
5. Subject alternative name
6. CRL distribution points
7. Certificate policies

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

Issuer:

```
C=GR,
O=HellasGrid,
OU=Certification Authorities,
CN=HellasGrid Root CA 2006
```

Subject:

```
C=GR
O=HellasGrid,
OU=Certification Authorities,
CN=SUBJECT NAME
```

7.1.5 Name constraints

Subject attribute constraints:
countryName: Must be GR.
OrganizationName: Must be HellasGrid.
organizationalUnitName: Must be Certification Authorities
commonName: Must describe the subject

7.1.6 Certificate policy object identifier

HellasGrid Root CA identifies this policy with the object identifier (O.I.D.) specified in section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

CRLs have only the Authority key identifier extension.

7.3 OCSP profile

7.3.1 Version number(s)

Currently there is no production level OCSP service in HellasGrid Root CA.

7.3.2 OCSP extensions

Currently there is no production level OCSP service in HellasGrid Root CA.

Chapter 8

COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The HellasGrid Root 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.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

No stipulation.

Chapter 9

OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees shall be charged.

9.1.2 Certificate access fees

No fees shall be charged.

9.1.3 Revocation or status information access fees

No fees shall be charged.

9.1.4 Fees for other services

No fees shall be charged.

9.1.5 Refund policy

No fees shall be charged so there is no refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets

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

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

HellasGrid Root CA does not collect any confidential or private information.

9.4.2 Information treated as private

HellasGrid Root CA does not collect any confidential or private information.

9.4.3 Information not deemed private

HellasGrid Root CA does not collect any confidential or private information.

9.4.4 Responsibility to protect private information

HellasGrid Root CA has not responsibility to protect private information as all the information it collects is public.

9.4.5 Notice and consent to use private information

HellasGrid Root CA does not collect any confidential or private information.

9.4.6 Disclosure pursuant to judicial or administrative process

HellasGrid Root CA does not collect any confidential or private information.

9.4.7 Other information disclosure circumstances

HellasGrid Root CA does not collect any confidential or private information.

9.5 Intellectual property rights

```
RFC 3647;
HellasGrid CA Certificate Policy v1.4;
SEE-GRID CA Certificate Policy;
UK e-Science CA CP/CPS.
```

9.6 Representations and warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

1. HellasGrid Root CA guarantees to control the identity of the certification requests according to the procedures described in this document;
2. HellasGrid Root CA guarantees to control the identity of the revocation requests according to the procedures described in this document;
3. HellasGrid Root CA is run on a best effort basis and does not give any guarantees about the service security or suitability;

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

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

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

Legal disputes arising from the operation of the HellasGrid Root CA will be resolved according to the Greek Law.

9.14 Governing law

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

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.