HellasGrid Certification Authority

Certificate Policy and Certification Practices Statement

15 July, 2006

Contents

1 INTRODUCTION **5**
- 1.1 Overview . . . 5
- 1.2 Document name and identification . . . 5
- 1.3 PKI participants . . . 6
  - 1.3.1 Certification Authorities . . . 6
  - 1.3.2 Registration Authorities . . . 6
  - 1.3.3 Subscribers . . . 6
  - 1.3.4 Relying parties . . . 6
  - 1.3.5 Other participants . . . 7
- 1.4 Certificate Usage . . . 7
  - 1.4.1 Appropriate certificate uses . . . 7
  - 1.4.2 Prohibited certificate uses . . . 7
- 1.5 Policy administration . . . 7
  - 1.5.1 Organization administering the document . . . 7
  - 1.5.2 Contact Person . . . 7
  - 1.5.3 Person determining CPS suitability for the policy . . . 8
  - 1.5.4 CPS approval procedures . . . 8
- 1.6 DEFINITIONS AND ACRONYMS . . . 9

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES **11**
- 2.1 Repositories . . . 11
- 2.2 Publication of certification information . . . 11
- 2.3 Time or frequency of publication . . . 12
- 2.4 Access control on repositories . . . 12

3 IDENTIFICATION AND AUTHENTICATION **13**
- 3.1 Naming . . . 13
  - 3.1.1 Types of names . . . 13
  - 3.1.2 Need for names to be meaningful . . . 13
  - 3.1.3 Anonymity or pseudonimity of subscribers . . . 13
  - 3.1.4 Rules for interpreting various name forms . . . 13
  - 3.1.5 Uniqueness of names . . . 13
  - 3.1.6 Recognition, authentication, and role of trademarks . . . 14
- 3.2 Initial identity validation . . . 14
  - 3.2.1 Method to prove possession of key . . . 14

3.2.2 Authentication of organization identity . . . 14
3.2.3 Authentication of individual identity . . . 14
3.2.4 Non-verified subscriber information . . . 15
3.2.5 Validation of Authority . . . 15
3.2.6 Criteria of interoperation . . . 15
3.3 Identification and authentication for re-key requests . . . 15
3.3.1 Identification and authentication for routine re-key . . . 15
3.3.2 Identification and authentication for re-key after revocation . . . 15
3.4 Identification and authentication for revocation request . . . 15

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 17
4.1 Certificate application . . . 17
4.1.1 Who can submit a certificate application . . . 17
4.1.2 Enrollment process and responsibilities . . . 17
4.2 Certificate application processing . . . 18
4.2.1 Performing identification and authentication functions . . . 18
4.2.2 Approval or rejection of certificate applications . . . 18
4.2.3 Time to process certificate applications . . . 19
4.3 Certificate issuance . . . 19
4.3.1 CA actions during certificate issuance . . . 19
4.3.2 Notification to subscriber by the CA of issuance of certificate . . . 19
4.4 Certificate acceptance . . . 19
4.4.1 Conduct constituting certificate acceptance . . . 19
4.4.2 Publication of the certificate by the CA . . . 20
4.4.3 Notification of certificate issuance by the CA to other entities . . . 20
4.5 Key pair and certificate usage . . . 20
4.5.1 Subscriber private key and certificate usage . . . 20
4.5.2 Relying party public key and certificate usage . . . 20
4.6 Certificate renewal . . . 20
4.6.1 Circumstance for certificate renewal . . . 20
4.6.2 Who may request renewal . . . 20
4.6.3 Processing certificate renewal requests . . . 21
4.6.4 Notification of new certificate issuance to subscriber . . . 21
4.6.5 Conduct constituting acceptance of a renewal certificate . . . 21
4.6.6 Publication of the renewal certificate by the CA . . . 21
4.6.7 Notification of certificate issuance by the CA to other entities . . . 21
4.7 Certificate re-key . . . 21
4.7.1 Circumstance for certificate re-key . . . 21
4.7.2 Who may request certification of a new public key . . . 21
4.7.3 Processing certificate re-keying requests . . . 21
4.7.4 Notification of new certificate issuance to subscriber . . . 22
4.7.5 Conduct constituting acceptance of a re-keyed certificate . . . 22
4.7.6 Publication of the re-keyed certificate by the CA . . . 22
4.7.7 Notification of certificate issuance by the CA to other entities . . . 22
4.8 Certificate modification . . . 22

4.8.1 Circumstance for certificate modification . . . 22
4.8.2 Who may request certificate modification . . . 22
4.8.3 Processing certificate modification requests . . . 22
4.8.4 Notification of new certificate issuance to subscriber . . . 22
4.8.5 Conduct constituting acceptance of modified certificate . . . 22
4.8.6 Publication of the modified certificate by the CA . . . 22
4.8.7 Notification of certificate issuance by the CA to other entities . . . 23
4.9 Certificate revocation and suspension . . . 23
4.9.1 Circumstances for revocation . . . 23
4.9.2 Who can request revocation . . . 23
4.9.3 Procedure for revocation request . . . 23
4.9.4 Revocation request grace period . . . 23
4.9.5 Time within which CA must process the revocation request . . . 23
4.9.6 Revocation checking requirement for relying parties . . . 24
4.9.7 CRL issuance frequency . . . 24
4.9.8 Maximum latency for CRLs . . . 24
4.9.9 On-line revocation/status checking availability . . . 24
4.9.10 On-line revocation checking requirements . . . 24
4.9.11 Other forms of revocation advertisements available . . . 24
4.9.12 Special requirements re key compromise . . . 24
4.9.13 Circumstances for suspension . . . 24
4.9.14 Who can request suspension . . . 24
4.9.15 Procedure for suspension request . . . 24
4.9.16 Limits on suspension period . . . 24
4.10 Certificate status services . . . 25
4.10.1 Operational characteristics . . . 25
4.10.2 Service availability . . . 25
4.10.3 Optional features . . . 25
4.11 End of subscription . . . 25
4.12 Key escrow and recovery . . . 25
4.12.1 Key escrow and recovery policy and practices . . . 25
4.12.2 Session key encapsulation and recovery policy and practices . . . 25

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 27
5.1 Physical controls . . . 27
5.1.1 Site location and construction . . . 27
5.1.2 Physical access . . . 27
5.1.3 Power and air conditioning . . . 27
5.1.4 Water exposures . . . 27
5.1.5 Fire prevention and protection . . . 27
5.1.6 Media storage . . . 28
5.1.7 Waste disposal . . . 28
5.1.8 Off-site backup . . . 28
5.2 Procedural controls . . . 28
5.2.1 Trusted roles . . . 28

5.2.2 Number of persons required per task . . . 28
5.2.3 Identification and authentication for each role . . . 28
5.2.4 Roles requiring separation of duties . . . 28
5.3 Personnel controls . . . 28
5.3.1 Qualifications, experience, and clearance requirements . . . 28
5.3.2 Background check procedures . . . 28
5.3.3 Training requirements . . . 29
5.3.4 Retraining frequency and requirements . . . 29
5.3.5 Job rotation frequency and sequence . . . 29
5.3.6 Sanctions for unauthorized actions . . . 29
5.3.7 Independent contractor requirements . . . 29
5.3.8 Documentation supplied to personnel . . . 29
5.4 Audit logging procedures . . . 29
5.4.1 Types of events recorded . . . 29
5.4.2 Frequency of processing log . . . 29
5.4.3 Retention period for audit log . . . 30
5.4.4 Protection of audit log . . . 30
5.4.5 Audit log backup procedures . . . 30
5.4.6 Audit collection system (internal vs. external) . . . 30
5.4.7 Notification to event-causing subject . . . 30
5.4.8 Vulnerability assessments . . . 30
5.5 Records archival . . . 30
5.5.1 Types of records archived . . . 30
5.5.2 Retention period for archive . . . 30
5.5.3 Protection of archive . . . 30
5.5.4 Archive backup procedures . . . 30
5.5.5 Requirements for time-stamping of records . . . 31
5.5.6 Archive collection system (internal or external) . . . 31
5.5.7 Procedures to obtain and verify archive information . . . 31
5.6 Key changeover . . . 31
5.7 Compromise and disaster recovery . . . 31
5.7.1 Incident and compromise handling procedures . . . 31
5.7.2 Computing resources, software, and/or data are corrupted . . . 31
5.7.3 Entity private key compromise procedures . . . 31
5.7.4 Business continuity capabilities after a disaster . . . 31
5.8 CA or RA termination . . . 32

6 TECHNICAL SECURITY CONTROLS 33
6.1 Key pair generation and installation . . . 33
6.1.1 Key pair generation . . . 33
6.1.2 Private key delivery to subscriber . . . 33
6.1.3 Public key delivery to certificate issuer . . . 33
6.1.4 CA public key delivery to relying parties . . . 33
6.1.5 Key sizes . . . 33
6.1.6 Public key parameters generation and quality checking . . . 33

6.1.7 Key usage purposes (as per X.509 v3 key usage field) 34
6.2 Private Key Protection and Cryptographic Module Engineering Controls . 34
6.2.1 Cryptographic module standards and controls 34
6.2.2 Private key (n out of m) multi-person control 34
6.2.3 Private key escrow 34
6.2.4 Private key backup 34
6.2.5 Private key archival 34
6.2.6 Private key transfer into or from a cryptographic module 34
6.2.7 Private key storage on cryptographic module 34
6.2.8 Method of activating private key 35
6.2.9 Method of deactivating private key 35
6.2.10 Method of destroying private key 35
6.2.11 Cryptographic Module Rating 35
6.3 Other aspects of key pair management 35
6.3.1 Public key archival 35
6.3.2 Certificate operational periods and key pair usage periods 35
6.4 Activation data 35
6.4.1 Activation data generation and installation 35
6.4.2 Activation data protection 35
6.4.3 Other aspects of activation data 36
6.5 Computer security controls 36
6.5.1 Specific computer security technical requirements 36
6.5.2 Computer security rating 36
6.6 Life cycle technical controls 36
6.6.1 System development controls 36
6.6.2 Security management controls 36
6.6.3 Life cycle security controls 36
6.7 Network security controls 36
6.8 Time-stamping 36

7 CERTIFICATE, CRL, AND OCSP PROFILES 37
7.1 Certificate profile 37
7.1.1 Version number(s) 37
7.1.2 Certificate extensions 37
7.1.3 Algorithm object identifiers 38
7.1.4 Name forms 38
7.1.5 Name constraints 38
7.1.6 Certificate policy object identifier 39
7.1.7 Usage of Policy Constraints extension 39
7.1.8 Policy qualifiers syntax and semantics 39
7.1.9 Processing semantics for the critical Certificate Policies extension . 39
7.2 CRL profile 39
7.2.1 Version number(s) 39
7.2.2 CRL and CRL entry extensions 39
7.3 OCSP profile 39

7.3.1 Version number(s) . . . 39
7.3.2 OCSP extensions . . . 39

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 41
8.1 Frequency or circumstances of assessment . . . 41
8.2 Identity/qualifications of assessor . . . 41
8.3 Assessor's relationship to assessed entity . . . 41
8.4 Topics covered by assessment . . . 41
8.5 Actions taken as a result of deficiency . . . 41
8.6 Communication of results . . . 41

9 OTHER BUSINESS AND LEGAL MATTERS 43
9.1 Fees . . . 43
9.1.1 Certificate issuance or renewal fees . . . 43
9.1.2 Certificate access fees . . . 43
9.1.3 Revocation or status information access fees . . . 43
9.1.4 Fees for other services . . . 43
9.1.5 Refund policy . . . 43
9.2 Financial responsibility . . . 43
9.2.1 Insurance coverage . . . 43
9.2.2 Other assets . . . 44
9.2.3 Insurance or warranty coverage for end-entities . . . 44
9.3 Confidentiality of business information . . . 44
9.3.1 Scope of confidential information . . . 44
9.3.2 Information not within the scope of confidential information . . . 44
9.3.3 Responsibility to protect confidential information . . . 44
9.4 Privacy of personal information . . . 44
9.4.1 Privacy plan . . . 44
9.4.2 Information treated as private . . . 44
9.4.3 Information not deemed private . . . 44
9.4.4 Responsibility to protect private information . . . 45
9.4.5 Notice and consent to use private information . . . 45
9.4.6 Disclosure pursuant to judicial or administrative process . . . 45
9.4.7 Other information disclosure circumstances . . . 45
9.5 Intellectual property rights . . . 45
9.6 Representations and warranties . . . 45
9.6.1 CA representations and warranties . . . 45
9.6.2 RA representations and warranties . . . 45
9.6.3 Subscriber representations and warranties . . . 45
9.6.4 Relying party representations and warranties . . . 45
9.6.5 Representations and warranties of other participants . . . 45
9.7 Disclaimers of warranties . . . 45
9.8 Limitations of liability . . . 46
9.9 Indemnities . . . 46
9.10 Term and termination . . . 46

9.10.1 Term 46
9.10.2 Termination 46
9.10.3 Effect of termination and survival 46
9.11 Individual notices and communications with participants 46
9.12 Amendments 46
9.12.1 Procedure for amendment 46
9.12.2 Notification mechanism and period 47
9.12.3 Circumstances under which OID must be changed 47
9.13 Dispute resolution provisions 47
9.14 Governing law 47
9.15 Compliance with applicable law 47
9.16 Miscellaneous provisions 47
9.16.1 Entire agreement 47
9.16.2 Assignment 47
9.16.3 Severability 47
9.16.4 Enforcement (attorneys' fees and waiver of rights) 47
9.16.5 Force Majeure 47
9.17 Other provisions 48

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 now 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 CA and specifies the minimum requirements and obligations for the signing and management of certificates.

1.2 Document name and identification

- Document title: HellasGrid CA Certification Policy and Certification Practice Statement
- Version: 2.0
- Document Date: 15 July, 2006
- O.I.D.: 1.3.6.1.4.1.23877.8.1.1.2.0

The following tabular describes the structure of the O.I.D.

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

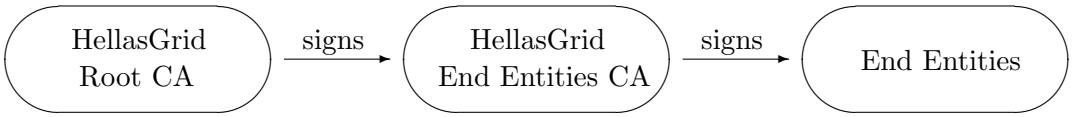
Table 1.1: O.I.D. description table

1.3 PKI participants

1.3.1 Certification Authorities

HellasGrid CA is a subordinate CA under the HellasGrid Root CA and signs only End Entity Certificates.

The following simple sketch clarifies the relationship among the HellasGrid Root CA and the HellasGrid CA. The HellasGrid Root CA signs the HellasGrid CA (subordinate) certificate, which in turn signs end entities' certificates.



1.3.2 Registration Authorities

The procedure of identification and authentication of the certificate applicants is performed by trusted parties (Registration Authorities), appointed by the HellasGrid CA. At any time the list of valid Registration Authorities is available in an on-line repository operated by the HellasGrid CA. See also section 2.2.

1.3.3 Subscribers

Subscribers eligible for certification by the HellasGrid CA are:

1. All Greek nationals or entities formally based and/or having offices in Greece, that are involved in research and/or education;

2. Digital processing entities, capable for performing cryptographic operations, located in Greece or owned by Greek organizations focused in research and/or education;

3. Services running on digital processing entities, located in Greece or owned by Greek organizations focused in research and/or education.

1.3.4 Relying parties

People and Organizations that are using the public keys found in certificates issued by the HellasGrid 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

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

1.4.1 Appropriate certificate uses

Certificates issued by the HellasGrid 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 CA CP/CPS is authored and administered by the GridAUTH Operations Center.

The HellasGrid 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-ca@grid.auth.gr
```

1.5.2 Contact Person

The contact person for questions about this document or any other HellasGrid 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

New versions of the Certification Practice Statement are reviewed internally in order to verify their suitabillity against the minimum requirements, which are defined by the IGTF. Internal approval is followed by the submission of the CPS to the EUGridPMA, in order to go through the EUGridPMA accredidattion procedure .

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 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.
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 lifetime.
Certification Practices 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 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 Identification and Authentication of certificate subscribers, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party (RP)	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Chapter 2

PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

The HellasGrid 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-ca@grid.auth.gr
```

2.2 Publication of certification information

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

1. the HellasGrid CA certificate;
2. valid issued certificates;
3. the latest CRL;
4. a copy of the current and all previous versions of this document;

5. a list with the current operational Registration Authorities;

6. other relevant information relating to certificates.

2.3 Time or frequency of publication

All information shall be published in the repository promptly after such information is available to the CA. Certificates issued by the HellasGrid CA that reference this Policy, will be published promptly upon acceptance of each 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 CA does not impose any access control 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 CA may impose a more restricted access control policy to the repository at its discretion.

The HellasGrid CA web site is maintained in 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:

1. in case of user certificate the subject name must include the person's name in the CN field;
2. in case of host certificate the subject name must include the DNS FQDN in the CN field;
3. in case of service certificate the subject name must include the service name and the DNS FQDN separated by a '/' in the CN field.

3.1.2 Need for names to be meaningful

The subject name must represent the subscriber in a way, that is easily understandable by humans. In addition, see subsection 3.1.1.

3.1.3 Anonymity or pseudonimity of subscribers

HellasGrid CA does not issue or sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

See subsection 3.1.1.

3.1.5 Uniqueness of names

The subject name listed in a certificate shall be unambiguous and uniquelly assigned to each End Entity for all certificates issued by the HellasGrid CA. If necessary, additional

numbers or letters may be appended to the real name ensuring the uniqueness of the name within the domain of certificates issued by the HellasGrid 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 CA proves possession of the private key, that is the companion to the HellasGrid CA certificate, by signing certificates and CRLs.

The HellasGrid CA verifies, that the subscriber possesses the private key relating to the certificate request by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to requester. A cryptographic challenge-response exchange may be used to prove possession of the private key at any point in time before certification of subscriber.

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

3.2.2 Authentication of organization identity

HellasGrid CA authenticates 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

Physical Person: The subject must contact personally the nearby RA in order to verify his identity and the validity of the request in a face to face meeting. The authentication of the subject is performed through the presentation of a valid photo ID document or passport as well as a valid official document stating that the subject is an acceptable end entity as defined in this document [see subsection 1.3.3].

Digital Processing Entity or Service: The entity must already have a valid DNS entry and be an acceptable end entity as defined in this document [see subsection 1.3.3]. The system administrator requesting the certificate must use his/her personal HellasGrid CA certificate to either authenticate to the HellasGrid CA web portal or digitally sign the request. The nearby RA must verify the relation between the host/service and the requestor.

3.2.4 Non-verified subscriber information

During the initial identity validation the requester's e-mail is not verified. This is done during the processing of the certificate application as described in subsection 4.2.2.

3.2.5 Validation of Authority

The requesteers must present valid documents stating their affiliation with the organizationi they belong to.

3.2.6 Criteria of interoperation

HellasGrid CA is an IGTF member and as such the basic criterium for interoperation within the federation is the accreditaton based on the adherence to the IGTF minimum requirements.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Expiration warnings will be issued to subscribers when re-key time arrives. Re-key before expiration can be accomplished by sending a re-key e-mail request signed with the current user certificate or by logging in the HellasGrid CA web portal using the current user certificate and asking for re-key. Re-key after expiration follows the same authentication procedure as new certificate. Once every three years the user has to be authenticated by the local RA.

3.3.2 Identification and authentication for re-key after revocation

See subsection 3.2.3.

3.4 Identification and authentication for revocation request

Certificate revocation requests should be submitted to Hellasgrid CA via e-mail [see subsection 1.5.1] or through the HellasGrid CA web portal. In case the revocation request is submitted via e-mail, it must be signed by a valid, non-expired, non-revoked HellasGrid CA personal certificate.

When e-mail is not an option, the request will be authenticated following the procedure described in subsection 3.2.3.

Chapter 4

CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

The subject must:

1. be an acceptable subscriber as defined in subsection 1.3.3;
2. read and adhere to the policies and procedures described in this document;
3. generate a key pair using a trustworthy method and the private must have at least 1024 bits;
4. use a strong pass phrase of at least 12 characters;
5. the request must obey the HellasGrid CA distinguished name scheme;
6. the distinguished name must unambiguous and unique;

4.1.2 Enrollment process and responsibilities

User Certificate: Users may apply for a digital certificate via

- email. The requesting subscriber sends an email requesting a digital certificate to his/her local RA. The RA sets up a face to face appointment with the requestor in order to authenticate him/her. After successful identification the RA contacts the CA and forwards the request, which is then processed and signed by the CA.
- the HellasGrid CA web portal. The user registers using the User Registration web based form. After successful validation of the user's email address (s)he may request for a digital certificate using the web browser cryptographic machine or a manual

CSR (Certificate Request) submission.The local RA must then authenticate the requesting subscriber via a face-to-face meeting and after successful authentication the signing procedure is performed by the CA.

If the subscriber wants to re key his/her certificate, then he/she must follow the procedures described in section 4.7.

Server or Service Certificate: The administrator of the subject must already have a valid HellasGrid CA certificate before requesting a server or service certificate. The submission of the certificate request can be done either via the HellasGrid CA web portal or via e-mail.

In the first case the subject will have first to import his/her HellasGrid CA certificate in the browser in order to be authenticated automatically by the HellasGrid CA web portal. Upon successful authentication the user will be able to submit the certificate request via a web based form.

In the second case the subject will have to send an e-mail signed via his/her HellasGrid CA certificate to Hellasgrid CA [see subsection 1.5.1]with the certificate requests attached and stating in the body of the e-mail that he is the person responsible for the server/service.

In both cases the certificate request will be forwarded to the appropriate RA, who will approve or disapprove the request according to subsections 4.2.1 and 4.2.2.

If the subscriber wants to re key his/her certificate, then he/she must follow the procedures described in section 4.7.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All the certificate applications will be authenticated and validated by the HellasGrid CA and RAs. In case of a new user certificate, the request will be validated by the web portal or by the RA in person if the request was submitted via email. In both cases the RA will have to authenticate the request. In all the other cases (re key of user certificate while current certificate is valid, request for host or service certificate) the authentication of the certificate application will take place by checking that the requester has a valid HellasGrid CA certificate. Upon successful authentication, the certificate application will be forwarded to the RA in order to validate the information included in the certificate request.

4.2.2 Approval or rejection of certificate applications

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

1. the certificate application must be authenticated first by the RA as described in subsection 4.2.1;

2. the subject must be an acceptable subscriber entity, as defined in subsection 1.3.3;

3. the request must obey the HellasGrid CA distinguished name scheme;
4. the distinguished name must unambiguous and unique;
5. the private key of the end entity must be at least 1024 bits long.

If the certificate request does not meet one or more of the above criteria, it will be rejected and signed notification e-mail will be sent by the RA to the subject with carbon copy to Hellasgrid CA.

4.2.3 Time to process certificate applications

Each certificate application will take no more that 3 working days to be processed from the time that the RA approves it.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Right after the subscriber's certificate is issued, an email is sent to the relevant RA manager informing him/her about the action.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Right after the subscriber's certificate is issued, an e-mail is sent to him/her with information on how to download his/her certificate from the HellasGrid CA web portal. There (s)he will be requested to login using his/her newly issued certificate to an SSL protected page in order to accept his/her personal certificate signed by the HellasGrid CA and that (s)he adheres to the CP/CPS under which it was signed.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber must login in the HellasGrid CA web portal using his/her X509 certificate, within 5 working days from the day that his/her certificate was issued, and accept a form stating that:

1. (s)he has read the CP/CPS under which his/her certificate was signed and accepts to adhere to it;
2. (s)he accepts his/her certificate signed by the HellasGrid CA;
3. (s)he assumes the responsibility to notify the HellasGrid CA immediately:
    - in case of possible private key compromise;
    - when the certificate is no longer required;
    - when the information in the certificate becomes invalid.

4.4.2 Publication of the certificate by the CA

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

4.4.3 Notification of certificate issuance by the CA to other entities

The RA that has handled communication with the subscriber will be notified of the certificate issuance.

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 CA can be used for:

1. email signing and decryption (S/MIME);
2. server authentication and encryption of communications;
3. authentication purposes in research and educational infrastructures.

4.5.2 Relying party public key and certificate usage

Relying parties can use the public keys and certificates of the subscribers for:

1. email signing and decryption (S/MIME);
2. server authentication and encryption of communications;
3. authentication purposes in research and educational infrastructures.

Relying parties must download the CRL at least once per day and implement its restrictions while validating certificates.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

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

4.6.2 Who may request renewal

HellasGrid CA does not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.3 Processing certificate renewal requests

HellasGrid CA does not renew subscribers 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 CA does not renew subscribers 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 does not renew subscribers 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 CA does not renew subscribers 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 CA does not renew subscribers 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

Subscribers must regenerate their key pair in the following circumstances:

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

4.7.2 Who may request certification of a new public key

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

4.7.3 Processing certificate re-keying requests

Expiration warnings will be issued to subscribers when re-key time arrives. Re-key before expiration can be accomplished by sending a re-key request signed with the current user certificate. Re-key after expiration follows the same authentication procedure as for a new certificate. At least once every 3 years the subscriber must go through the same authentication procedure as the one described for a new certificate.

In case the request for a new certificate is due to revocation or compromise of certificate the subscriber must follow the same procedure as the one described in for a new one.

4.7.4 Notification of new certificate issuance to subscriber

Same as in subsection 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Same as in subsection 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA

Same as in subsection 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

Same as in subsection 4.4.3.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

HellasGrid CA does not modify certificates. In case that modification is required the revocation and re-key procedures should be followed.

4.8.2 Who may request certificate modification

HellasGrid CA does not modify certificates. In case that modification is required the revocation and re-key procedures should be followed.

4.8.3 Processing certificate modification requests

HellasGrid CA does not modify certificates. In case that modification is required the revocation and re-key procedures should be followed.

4.8.4 Notification of new certificate issuance to subscriber

HellasGrid CA does not modify certificates. In case that modification is required the revocation and re-key procedures should be followed.

4.8.5 Conduct constituting acceptance of modified certificate

HellasGrid CA does not modify certificates. In case that modification is required the revocation and re-key procedures should be followed.

4.8.6 Publication of the modified certificate by the CA

HellasGrid CA does not modify certificates. In case that modification is required the revocation and re-key procedures should be followed.

4.8.7 Notification of certificate issuance by the CA to other entities

HellasGrid CA does not modify certificates. In case that modification is required the revocation and re-key procedures should be followed.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate will be revoked in the following circumstances:

1. the subject of the certificate has ceased being an eligible end entity for certification, as described in the policy under which the certificate was signed;
2. the subject does not require the certificate any more;
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.

4.9.2 Who can request revocation

The revocation of the certificate can be requested by:

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

4.9.3 Procedure for revocation request

The entity requesting the certificate is authenticated by signing the revocation request with a valid HellasGrid CA certificate. Otherwise authentication will be performed with the same procedure as described in subsection 3.2.3.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

HellasGrid CA processes 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 23 days;
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 subsection 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 CA.

4.9.10 On-line revocation checking requirements

Currently there are no on-line revocation/status services offered by the HellasGrid 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 CA does not suspend certificates.

4.9.14 Who can request suspension

HellasGrid CA does not suspend certificates

4.9.15 Procedure for suspension request

HellasGrid CA does not suspend certificates

4.9.16 Limits on suspension period

HellasGrid CA does not suspend certificates

4.10 Certificate status services

4.10.1 Operational characteristics

HellasGrid 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 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 CA is located at the Aristotle University of Thessaloniki Campus, in the GridAUTH Data Center, building 22d.

5.1.2 Physical access

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

5.1.3 Power and air conditioning

The HellasGrid 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 the appropriate levels by air conditioning system.

5.1.4 Water exposures

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

5.3.4 Retraining frequency and requirements

HellasGrid CA will perform operational audit of the CA/RA 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 month.

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 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 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 will be at least 1 year. For 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, RAs;
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

User Certificate: The user must first contact and inform an eligible RA. The RA must then ask for the certificate to be revoked. After the certificate is revoked, the user can follow the issuance procedure to issue a new certificate.

Server or Service Certificate: The administrator of the subject must ask for certificate to be revoked. After the certificate is revoked, the administrator can follow the issuance procedure to issue a new certificate.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

Upon termination the HellasGrid CA will:

1. Notify subscribers and RAs;
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 RAs and subscribers must be generated in such a way that private key is not known by any other than the owner of the key pair. Each subscriber must generate his/her own key pair.

HellasGrid CA does not generate private keys on behalf of subscribers.

6.1.2 Private key delivery to subscriber

The HellasGrid 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 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 CA or the TACAR web sites.

6.1.5 Key sizes

1. The minimum key length for person, service or server certificate is 1024 bit.
2. The minimum length for the HellasGrid 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)

User Certificate: This type of certificate key can be used for data encipherment (dataEncipherment), session establishment (keyEncipherment), message integrity (digitalSignature) and non-repudiation (nonRepudiation).

Service and server Certificate: This type of certificate key can be used for data encipherment (dataEncipherment), session establishment (keyEncipherment) and message integrity (digitalSignature).

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 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 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 End Entity certificates signed by the HellasGrid CA have a maximum lifetime of 1 year.

The lifetime of the HellasGrid CA root certificate must be no more than 10 years and no less than 5 years.

6.4 Activation data

6.4.1 Activation data generation and installation

HellasGrid CA does not generate activation data on behalf of subscribers. It's upon the subscriber to generate a secure pass phrase, at least 12 characters long, in order to be used as activation data for his/her private key.

The pass phrase used to activate the HellasGrid CA private key is generated on the computer used for the CA signing operations and must be at least 15 characters long. Every 180 days the pass phrase is regenerated by one of the HellasGrid CA Operators.

6.4.2 Activation data protection

- The subscriber is responsible to protect the activation data for his/her private key.
- The HellasGrid CA uses a pass phrase to activate it's private key, which is known only by the HellasGrid CA Manager and the HellasGrid 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 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/RA 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 CA signing machine is kept off-line;
2. CA/RA 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 signed by the HellasGrid CA that reference this policy will use the X.509 version 3 format and will include a reference to the specific version of this document that was in effect at the time of the signing.

7.1.2 Certificate extensions

- User certificates:
    1. Basic constraints (Critical): Not a CA.
    2. Key usage (Critical): Digital signature, non-repudiation, key encipherment, data encipherment.
    3. Subject key identifier
    4. Authority key identifier
    5. Subject alternative name
    6. Issuer alternative name
    7. CRL distribution points
    8. Certificate policies
- Host and Service certificates:
    1. Basic constraints (Critical): Not a CA.
    2. Key usage (Critical): Digital signature, key encipherment, data encipherment.
    3. Subject key identifier
    4. Authority key identifier
    5. Subject alternative name

6. Issuer alternative name
7. CRL distribution points
8. Certificate policies

- 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. Issuer alternative name
7. CRL distribution points
8. 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 CA 2006
```

Subject:

```
C=GR,
O=HellasGrid,
OU=UNIT,
CN=SUBJECT NAME
```

7.1.5 Name constraints

Subject attribute constraints:
countryName: Must be GR.
OrganizationName: Must be HellasGrid.
organizationalUnitName: Must be the DNS domain name of the Institution/Organization the subject belongs to.
commonName: First name and last name of the subject for user certificates, DNS FQDN for server or service certificates. In the latter case the DNS FQDN may be prefixed by the value 'host' or the name of the service separated with a '/' from the DNS FQDN.

7.1.6 Certificate policy object identifier

HellasGrid CA identifies this policy with the object identifier (OID) 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 the 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 HellasGrid CA does not operate a production level OCSP service.

7.3.2 OCSP extensions

Currently HellasGrid CA does not operate a production level OCSP service.

Chapter 8

COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The HellasGrid 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 are charged so there is no refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

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

9.2.2 Other assets

HellasGrid 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 CA does not collect any confidential or private information.

9.4.2 Information treated as private

HellasGrid CA does not collect any confidential or private information.

9.4.3 Information not deemed private

HellasGrid CA collects the following information which is not deemed as private:

1. subscriber's name;
2. subscriber's e-mail address;
3. subscriber's organization;
4. subscriber's office phone number;
5. subscriber's research domain;
6. subscriber's department;
7. subscriber's position;
8. subscriber's certificate.

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

HellasGrid CA does not collect any confidential or private information.

9.4.6 Disclosure pursuant to judicial or administrative process

HellasGrid CA does not collect any confidential or private information.

9.4.7 Other information disclosure circumstances

HellasGrid CA does not collect any confidential or private information.

9.5 Intellectual property rights

RFC 3647;
SEE-GRID CA CP/CPS;
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 CA guarantees to control the identity of the certification requests according to the procedures described in this document;
2. HellasGrid CA guarantees to control the identity of the revocation requests according to the procedures described in this document;
3. HellasGrid CA operates on best effort basis and does not give any guarantees about the service security or suitability;
4. HellasGrid CA shall not be held liable for any problems arising from its operation or improper use of the issued certificates;
5. HellasGrid 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 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.