HellasGrid
Certification Authority

Certificate Policy and Certification Practices Statement

Contents

Chapter 1

INTRODUCTION

1.1 Overview

This document describes the Certification Policy and the Certificate Practice statement of the HellasGrid Certification Authority, following the structure set out in RFC 3647.

HellasGrid CA is managed and operated by GRNET S.A. in cooperation with the Scientific Computing Center at A.U.Th.

1.2 Document name and identification

- Document title: HellasGrid CA Certification Policy and Certification Practice Statement
- Version: 3.0
- Document Date: 10 May, 2016
- O.I.D.: 1.3.6.1.4.1.16515.20.1.1.3.0

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

1.3.6.1.4.1	Prefix for IANA private enterprises
16515	GRNET S.A.
20	HellasGrid
1	HellasGrid CA
1	CP/CPS
3.0	Document Version

Table 1.1: O.I.D. description table

1.3 PKI participants

1.3.1 Certification Authorities

HellasGrid CA signs only End Entity 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. Communication between the RA and the CA may take place via signed e-mails or via the SSL protected CA web portal. At any time the list of valid Registration Authorities is available on the 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 used 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 CP/CPS was authored and is administered by GRNET S.A. in cooperation with the Scientific Computing Center at A.U.Th.

The HellasGrid CA address for operational issues is :

```
HellasGrid Certification Authority
GRNET S.A.
56, Mesogion Av.
11527 Athens,
GREECE
Phone: +302107474274
Fax: +302107474490
Email: ca@hellasgrid.gr
```

1.5.2 Contact Person

The contact persons for questions about this document or any other HellasGrid CA related issues are:

```
Kanellopoulos Christos
GRNET S.A.
56, Mesogion Av.
11527 Athens,
GREECE
Phone: +302107474274
Fax: +302107474490
E-mail 1: skanct@grnet.gr
E-mail 2: ca@hellasgrid.gr

Kostas Koumantaros
GRNET S.A.
56, Mesogion Av.
11527 Athens,
GREECE
Phone: +302107474274
Fax: +302107474490
E-mail 1: kkoum@grnet.gr
```

1.5.3 Person determining CPS suitability for the policy

The persons who determine the CPS suitability for this policy is:

```
Kanellopoulos Christos
GRNET S.A.
```

56, Mesogion Av.
11527 Athens,
GREECE
Phone: +302107474274
Fax: +302107474490
E-mail 1: skanct@grnet.gr
E-mail 2: ca@hellasgrid.gr

Kostas Koumantaros
GRNET S.A.
56, Mesogion Av.
11527 Athens,
GREECE
Phone: +302107474274
Fax: +302107474490
E-mail 1: kkoum@grnet.gr

Paschalis Korosoglou,
Scientific Computing Office, IT Center
Aristotle University of Thessaloniki,
University Campus,
54124 Thessaloniki,
GREECE
Phone: +302310998988
Fax: +302310999428
E-mail 1: pkoro@it.auth.gr

1.5.4 CPS approval procedures

New versions of the Certification Practice Statement are reviewed internally in order to verify their suitability against the IGTF minimum requirements for "classic X.509 CAs with secure infrastructures". After a successful internal review the CPS (with an updated version number and O.I.D.) is submitted to the EUGridPMA in order to go through the EUGridPMA accreditation 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 HellasGrid CA
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 that 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 to that certificate and/or to digital signatures verified using that certificate.
Robots	Robots, also known as automated clients, are entities that perform automated tasks without human intervention. Production ICT environments typically support repetitive, ongoing processes - either internal system processes or processes relating to the applications being run (e.g. by a site or by a portal system). These procedures and repetitive processes are typically automated, and generally run using an identity with the necessary privileges to perform their tasks.

Chapter 2

PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

All the on-line and off-line repositories of the HellasGrid CA are operated by GRNET S.A.

The HellasGrid CA contact details for issues regarding the repositories is :

```
HellasGrid Certification Authority
GRNET S.A.
56, Mesogion Av.
11527 Athens,
GREECE
Phone: +302107474274
Fax: +302107474490
Email: ca@hellasgrid.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 site accessible at http://ca.hellasgrid.gr and which contains:

1. the HellasGrid CA certificate;
2. link to a searchable database containing all valid issued certificates;
3. link to the latest CRL;
4. a copy of the current and all previous versions of this document;
5. link to a list with the current operational Registration Authorities;

6. other relevant information relating to certificates.

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

2.3 Time or frequency of publication

Information shall be published promptly to the repository after such information is available to the CA. Certificates issued by the HellasGrid CA, will be published promptly upon the successful acceptance by the subscriber of the terms and conditions that are written in this document. 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.

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 commonName component;

2. in case of host certificate the subject name must include the DNS FQDN in the commonName component; +

3. in case of service certificate the subject name must include the service name and the DNS FQDN separated by a '/' in the commonName component; +

4. in case of robot certificate the commonName component of the subject name must include the string 'Robot' followed by a humanly recognizable and meaningful description of the Robot along with an electronic mail address of the person or a persistent group of persons responsible for the robot operations separated from the 'Robot' string by a COLON ':'.

3.1.2 Need for names to be meaningful

The subject name must represent the subscriber in a way, that is understandable by humans.

In addition, see subsection 3.1.1.

3.1.3 Anonymity or pseudonimity of subscribers

HellasGrid CA neither issues nor signs 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 unique for all end entities to whom certificates have been issued by the HellasGrid CA. In the case of personal certificates, additional numbers or letters may be appended to the real name of the subscriber, when necessary, in order to ensure 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 the possession of the private key relating to certificates requests by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to the 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 will not generate the key pair on behalf of subscribers and will not accept or retain private keys generated by subscribers.

3.2.2 Authentication of organization identity

HellasGrid CA does not authenticate organization identity.

3.2.3 Authentication of individual identity

Physical Person: The subject must contact the RA in person, in order to verify his/her identity and the validity of the request. The authentication of the subject is performed through the presentation of a valid photo ID document (national ID, passport, driver license etc). The subject must also provide a copy of the receipt he or she received after the successful submission of his/her request and present a valid official document stating his/her relationship with the organization (or one of the organizations) the RA is serving. [see subsections 1.3.3 and 3.2.5]. In cases where the subject resides in a geographical location where access to an RA is not possible, identity vetting may be performed via video call. In this case, an authenticated photocopy of the required document (national ID, passport, driver license etc) must be delivered by mail or courier service to the RA prior to this online meeting.

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 authenticate to the HellasGrid CA web portal in order to submit the certificate request. The nearby RA must verify the relation between the host/service and the requestor.

Robot: The entity must be an acceptable end entity as defined in this document [see subsection 1.3.3]. At least one of the responsible persons for the operations of the Robot must use his/her personal certificate, issued by an IGTF accredited CA, to authenticate to the HellasGrid CA web portal in order to submit the certificate request.

3.2.4 Non-verified subscriber information

The telephone number of the user is not verified by HellasGrid CA.

3.2.5 Validation of Authority

The subscriber requesting services from the HellasGrid CA must present valid documents stating his/her affiliation with the organization.

3.2.6 Criteria of interoperation

HellasGrid CA is member of IGTF and as such the basic criterium for interoperation is the accreditation 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 logging into the HellasGrid CA web portal using his/her valid HellasGrid CA user certificate and requesting for re-key. Re-key after expiration follows the same authentication procedure as when requesting for a new certificate. At least once every five years the user has to be authenticated by an RA as when requesting a new certificate.

3.3.2 Identification and authentication for re-key after revocation

After the revocation of a certificate, the subscriber must generate a new key pair in order to request for a new certificate and follow the rules specified in section 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 for a user certificate, the e-mail must be signed by the private key corresponding to a valid HellasGrid CA certificate.

If the revocation request is for a host or service certificate, then the e-mail must be signed by the private key corresponding to the certificate of the person responsible of the host or service.

When signed e-mail or submission through the HellasGrid CA web portal is not an option, the request will be authenticated using the procedure described in section 3.2.3.

Chapter 4

CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

Any user who has completed the enrollment process described in section 4.1.2

4.1.2 Enrollment process and responsibilities

Users can enroll to the HellasGrid CA Identity Management System via the HellasGrid CA web portal. During the enrollment process the user is required to provide the following details: first name, last name, organization, e-mail address and telephone number. Upon successful verification of the user's e-mail address, the user is considered to have completed the enrollment process with the HellasGrid CA System. It is the responsibility of the user to keep this information up to date. All users who have successfully enrolled with the HellasGrid CA, are able to submit certificate request applications.

- User Certificate: The users can request to have their public keys signed via the HellasGrid CA website or via e-mail. Upon successful submission of the certificate request, the user receives an e-mail which acknowledges the receipt of the certificate request and which includes a randomly generated hash string which uniquely identifies the certificate request. The subscriber must be authenticated by the RA serving his/her organization following the procedure described in section 3.2.3. After successful authentication, the RA will approve the certificate request on the HellasGrid CA web portal.

- Server or Service Certificate: The requester must already be in the possession of a valid certificate, issued by an IGTF accredited CA, before requesting a server or service certificate. The submission of the certificate request will be performed via the HellasGrid CA web portal or via signed e-mail. The certificate request will be

forwarded to the RA serving the requester's organization in order to approve or disapprove the request.

- Robot Certificate: The requester must already be in the possession of a valid certificate, issued by an IGTF accredited CA, before requesting a Robot certificate. The submission of the certificate request will be performed via the HellasGrid CA web portal or via signed e-mail. The certificate request will be forwarded to the RA serving the requester's organization in order to approve or disapprove the request. In the certificate request the requester must include humanly-recognizable and meaningful description of the Robot along with an electronic mail address of a persistent group of people responsible for the Robot operations.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

For the first time and after that at least once every 5 years, a subscriber must be authenticated by the RA serving his/her organization following the procedure described in section 3.2.3. After successful authentication the RA will approve the certificate request at the HellasGrid CA web portal. If the subscriber requires to re-key his/her certificate, then he/she must follow the procedures described in section 4.7.

All certificate applications will be authenticated and validated by the HellasGrid CA and RAs. In the case of a new user certificate, the request will be authenticated by checking if the hash [see section 4.1.2] that the requester has supplied is correct. 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 End Entity, as defined in subsection 1.3.3;
3. the request must follow the HellasGrid CA distinguished name scheme;
4. the distinguished name must unambiguous and unique;
5. the private key 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 a signed notification e-mail will be sent by the HellasGrid CA to the requester.

4.2.3 Time to process certificate applications

Each certificate application will take no more that 2 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 a certificate is issued, emails are sent to the requester and to the relevant RA manager informing them about the action.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Right after a certificate is issued, an e-mail is sent to the requester with information on how to download his/her certificate from the HellasGrid CA web portal.

After the requester successfully downloads the issued certificate, (s)he is requested to login to an SSL protected page in order to accept the issued certificate and to accept the HellasGrid CA Policy as it is described in the version of the CP/CPS that is in effect at the time.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber must log in the HellasGrid CA web portal within 10 working days from the day that his/her certificate was issued and complete the certificate acceptance procedure in which (s)he will be stating that (s)he

1. (s)he has read CP/CPS that is in effect and accepts to adhere the policies and responsibilities that are described in it;

2. (s)he accepts his/her certificate signed by the HellasGrid CA;

4.4.2 Publication of the certificate by the CA

All the certificates issued by the HellasGrid CA will be published to an online searchable database 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 e-Infrastructures.

Subscribers' private keys must not be shared.

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 e-Infrastructures.

Relying parties are advised to download the CRL at least once per day and implement its restrictions when validating certificates.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

HellasGrid CA does not renew certificates. 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 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 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 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 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 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 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 a new key pair for each certificate they request to be signed by the HellasGrid CA.

4.7.2 Who may request certification of a new public key

Same as in subsection 4.1.1.

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 logging to the HellasGrid CA web portal with their personal certificates and submitting a new certificate request or by sending a digitally signed e-mail to the RA serving their organization. Re-key after expiration follows the same authentication procedure as for a new certificate as described in section 4.2.1

In case the request for a new certificate is due to revocation or expiration of the existing certificate or compromise of the private key the subscriber must follow the same procedure as 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 a 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 a 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 a 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 a 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 a 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 a 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 a 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 entity to whom the certificate has been issued to has ceased being an eligible end entity for certification, as described in this policy;
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 or the robot to which the certificate has been issued has been retired;
6. the subject has failed to comply with the rules of this policy.

An end entity (or in the case of host or service certificate, the person responsible for it) must request revocation of its certificate as soon as possible but within one working day after detection of key compromise or of invalid data contained in the certificate.

4.9.2 Who can request revocation

The revocation of the certificate can be requested by:

1. the certificate owner;
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 revocation of a certificate is authenticated by logging to the HellasGrid CA portal using a valid HellasGrid CA certificate or by verifying the digital signature in the e-mail request. Otherwise authentication will be performed with the same procedure as described in section 3.2.3.

4.9.4 Revocation request grace period

There is no grace period for revocation requests.

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 are advised to 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. The maximum CRL lifetime is 30 days;
4. 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. See also subsection 4.10.1.

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.

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

HellasGrid CA is hosted at the GRNET S.A. HellasGrid Node HG-03-AUTH (Afroditi) located at the Aristotle University of Thessaloniki. The CA signing machine is kept in a secure environment were access is controlled and limited to CA staff.

5.1.2 Physical access

The CA signing machine is located in a secure environment where access is controlled. Physical access to the CA system and the CA web server is restricted to authorized personnel. Such personnel may enter the room where the CA system and the CA web server reside only by using their magnetic cards and by entering their PIN number on an electronic key lock. Access logs are recorded on the electronic key log.

5.1.3 Power and air conditioning

The HellasGrid CA signing machine and the CA web portal are both protected by the Uninterruptible Power Supply and the Power Generator of the Data Center. The Data Center hosting the CA services is equipped with environmental controls that ensure the proper cooling and ventilation.

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

The Data Center where HellasGrid CA is hosted is located in a public building adhering to the Greek laws 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 may be kept in magnetic tape cartridges, floppies and CD-ROM.

5.1.7 Waste disposal

Waste carrying potential confidential information such as old CD-ROMs and USB sticks are physically destroyed before being trashed.

5.1.8 Off-site backup

There is one off-site backup of the private key of the CA at the GRNET S.A. headquarters. The backup is kept encrypted both in digital and printed on paper formats, in a tamper-evident envelope, in a fire-proof safe to which only GRNET authorized personnel has access.

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 GRNET S.A.

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
- 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, which is stored in safe storage.

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. Online 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 private signing key if the CA 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 along with the corresponding private key will be available in order to verify digital signatures and issue CRLs.

The private keys of the EE certificates have to be changed periodically. The overlap of the old and new key will be at most 1 month.

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 and IGTF;
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

If an entity private key is proved to be compromised, then the corresponding certificate will be revoked and the following entities will be notified:

1. The subscriber to whom the certificate has been issued to;
2. The RA who is serving the organization of the subject;
3. All relevant security contacts.

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, RAs and IGTF;
2. Terminate the issuance and distribution of certificates and CRLs;
3. Notify relevant security contacts;
4. Communicate 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.

6.1.2 Private key delivery to subscriber

The HellasGrid CA does not generate private keys on behalf of subscribers and 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

The HellasGrid 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 an End Entity certificate is 1024 bit. HellasGrid CA recommends the use of 2048 bits long private keys.

2. The minimum length for the HellasGrid CA private key is 4096 bits.

6.1.6 Public key parameters generation and quality checking

HellasGrid CA enforces checks to ensure quality of the submitted public keys. These checks are either done automatically on certificate request or manually by the CA/RA personnel on certificate request approval and signature procedure. These checks include (but not limited to) the following:

1. Usage of small exponent number (¡65537)
2. Usage of signature algorithm vulnerable to CVE-2008-5077
3. Usage of known week Debian OpenSSL keys

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

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 have access to the End Entity private keys and thus does not archive them.

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

See subsection 6.4.1

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 certificate must be no more than 20 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 of the pass phrase in written form 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 is 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 a dedicated machine.

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 central machines other than the signing machine are protected by a firewall.

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

- User and Robot certificates:
    1. Basic constraints (Critical): Not a CA.
    2. Key usage (Critical): Digital signature, key encipherment, data encipherment.
    3. Extended Key Usage (Not Critical): clientAuth
    4. Subject key identifier
    5. Authority key identifier
    6. Subject alternative name(s)
    7. Issuer alternative name
    8. CRL distribution points (pointing to one http URL)
    9. Certificate policies
- Host and Service certificates:
    1. Basic constraints (Critical): Not a CA.
    2. Key usage (Critical): Digital signature, key encipherment, data encipherment.
    3. Extended Key Usage (Not Critical): clientAuth, serverAuth
    4. Subject key identifier
    5. Authority key identifier

6. Subject alternative name(s)
7. Issuer alternative name
8. CRL distribution points (pointing to one http URL)
9. 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 (pointing to one http URL)
8. Certificate policies

7.1.3 Algorithm object identifiers

1. Hash Function: id-sha1 1.3.14.3.2.26, sha256 2.16.840.1.101.3.4.2.1, sha384 2.16.840.1.101.3.4.2.2, sha512 2.16.840.1.101.3.4.2.3

2. RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1

3. Signature Algorithm: sha1WithRSAEncryption 1.2.840.113549.1.1.5, sha256WithRSAEncryption 1.2.840.113549.1.1.11, sha384WithRSAEncryption 1.2.840.113549.1.1.12, sha512WithRSAEncryption 1.2.840.113549.1.1.13

7.1.4 Name forms

Issuer:

```
C=GR,
O=HellasGrid,
OU=Certification Authorities,
CN=HellasGrid CA 2016
```

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: See 3.1.1 and 3.1.5.

7.1.6 Certificate policy object identifier

HellasGrid CA identifies this policy with the object identifier (OID) specified in section 1.2. All the certificates issued under this policy will also include the O.I.D. of the "Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure" (1.2.840.113612.5.2.2.1).

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;

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;
INFN Certificate Policy and Certificate Practice Statement;
NIKHEF Certificate Policy and Certificate Practice Statement;
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

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

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

See subsection 1.5.4.

9.12.2 Notification mechanism and period

See subsection 1.5.4

9.12.3 Circumstances under which OID must be changed

See subsection 1.5.4

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 Greek Law.

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.