HellasGrid Task Force

HellasGrid CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Table of Contents

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 decided to implement a Certification Authority (HellasGrid CA), 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 of the Greek National Research & Education Network – GRNET. GRNET is owned and supervised by the General Secretariat of Research and Technology, Greek Ministry of Development.

The Hellasgrid CA is operated by the Computer Center of the Department of Physics at the Aristotle University of Thessaloniki under the supervision of Hellas Grid coordinator.

This draft document, following the structure set out in RFC 2527, defines the Certification Policy and the Certification Practice Statement of the HellasGrid CA and specifies the minimum requirements and obligations for the issuance and management of certificates that may be used in verifying digital signatures on the categories of electronic communications as specified in this document.

1.2 POLICY IDENTIFICATION

- Document title: **"HellasGrid CA Certification Policy and Certificate Practice Statement"**
- Version: **1.4**
- Document Date: **March 2004**
- O.I.D. **1.3.6.1.4.1.13089.2.1.10.1.4**

1.3 COMMUNITY AND APPLICABILLITY

1.3.1 Certification Authorities

HellasGrid certificates are signed by the HellasGrid CA, which is defined as a medium security CA.

1.3.2 Registration Authorities

HellasGrid CA manages the functions of its Registration Authority. Additional Registration Authorities may be created by HellasGrid CA as required.

1.3.3 End Entities

The HellasGrid CA will issue certificates to natural persons and computer entities. Entities eligible for certification from the HellasGrid CA are :

1. All those entities formally based and/or having offices in Greece, that are involved in research or deployment of multi-domain distributed computing infrastructure, intended for cross-organizational sharing of resources. The focus of these organizations should also be in research and/or education.

1.3.4 Applicability

There will be three categories of certificates:

1. server certificates: authentication, non-repudiation, data encryption and communication encryption;

2. user certificates: authentication, non-repudiation, data encryption and communication encryption;
3. service certificates: authentication, non-repudiation, data encryption and communication encryption.

1.3.5 User Restrictions

Certificates issued by the HellasGrid CA are only valid in the context of Grid research activities, any other usage such as financial transactions is strictly forbidden.

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

1.4 CONTACT DETAILS

The HellasGrid CA was created by the Department of Physics Computer Center, Aristotle University of Thessaloniki,. Since December 2003 HellasGrid CA operates in the context of the Network and Telecommunications Committee of the Aristotles University of Thessaloniki.

The HellasGrid CA address for operational issues is :

HellasGrid Certification Authority
Department of Physics
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE

Phone: (+ 30)2310998223
Fax: (+ 30)2310999428
Email: hellasgrid-ca@physics.auth.gr

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

Kanellopoulos Christos
Department of Physics
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE

Phone: (+ 30)2310998223
Fax: (+ 30)2310999428
E-mail: C.Kanellopoulos@physics.auth.gr

2 General Provisions

2.1 OBLIGATIONS

2.1.1 HellasGrid CA Obligations

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

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

2.1.2 HellasGrid RA Obligations

1. the application/enrollment procedure ;
2. the identification procedure ;
3. the authentication procedure ;

2.1.3 Subscriber Obligations

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

1. read and accept the policies and procedures published in this document;
2. generate a key pair using a trustworthy system, and take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key;
3. use a strong pass phrase with a minimum length of 15 characters to protect the private key of personal certificates;
4. acknowledge that by accepting the certificate he/she warrants all information and representations in the certificate to be true;
5. use the certificate exclusively for authorized and legal purposes, consistent with this Policy;
6. notify the HellasGrid CA when the certificate is no longer required;
7. notify the HellasGrid CA when the information in the certificate becomes wrong or inaccurate;
8. instruct the HellasGrid CA to revoke the certificate promptly upon an actual or suspected loss, disclosure, or other compromise of the subscribers private key.

2.1.4 Repository Obligations

The HellasGrid CA is responsible for providing a public repository, accessible through the World Wide Web at http://pki.physics.auth.gr/hellasgrid-ca.

1. HellasGrid CA will publish its public key on the above website;
2. HellasGrid CA will publish on the above website the CRLs as soon as they are issued.

2.1.5 Relying Party Obligations

A Qualified Relying Party is required to :

1. read and accept the policies and procedures published in this document;
2. use the certificates only for the authorized uses as they have been set out in this document;
3. check periodically the Certificate Revocation List (CRL) published on the website of the HellasGrid CA [section 4.4.6].

2.2 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 is run on a 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 inproper use of the issued certificates ;
5. HellasGrid CA denies any kind of responsibilities for damages or impairments resulting from its operation.

2.3 FINANCIAL RESPONSIBILITY

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

2.4 INTERPRETATION

2.4.1 Governing Law

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

2.4.2 Dispute Resolution Procedures

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

2.5 FEES

No fees shall be charged.

2.6 PUBLICATION AND REPOSITORIES

2.6.1 Publication of CA Information

The HellasGrid CA is obligated to maintain a secure on-line repository that is available to Qualified Relying Parties through a web interface at http://pki.physics.auth.gr/hellasgrid-ca and which contains:

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

2.6.2 Frequency of Publication

All information to be published in the repository shall be published 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 such certificate by the subscriber. Information relating to the revocation of a certificate will be published as described in section 4.4.5.

2.6.3 Access Controls

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

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 most of the time.

2.7 COMPLIANCE AUDIT

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.

2.8 CONFIDENTIALITY POLICY

2.8.1 Confidential Information Kept by the HellasGrid CA and RA

The HellasGrid CA does not keep any confidential information.

2.8.2 Types of Information not considered Confidential

The CA collects the following non-confidential information:

1. Subscriber's full name;
2. Subscriber's E-mail address;
3. Subscriber's organization;
4. Subscriber's public key.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

The CA will notify and inform the following entities:

1. the subject of the personal certificate;
2. the requester of the server certificate;
3. the HellasGrid security officer in case of security compromise.

2.8.4 Release of Information to Law Enforcement Officials

The information collected by the HellasGrid CA is considered non confidential and therefore will be available to law enforcement officials upon request.

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

The information collected by the HellasGrid CA is considered non confidential and therefore will be available to law enforcement officials upon request. Any confidential information collected by the HellasGrid CA will be subject to Greek law.

2.8.6 Conditions of Disclosure upon owner's request

The information collected by the HellasGrid CA is considered non confidential and therefore will be available to law enforcement officials upon request. Any confidential information collected by the HellasGrid CA will be subject to Greek law.

2.8.7 Other Circumstances for Disclosure of Confidential Information

The information collected by the HellasGrid CA is considered non confidential and therefore will be available to law enforcement officials upon request. Any confidential information collected by the HellasGrid CA will be subject to Greek law.

2.9 INTELLECTUAL PROPERTY RIGHTS

1. RFC 2527;
2. EuroPKI Certificate Policy;
3. TrustID Certificate Policy;
4. NCSA Certificate Policy;
5. FBCA Certificate Policy;
6. INFN Certificate Policy and Certificate Practice Statement;
7. NIKHEF Certificate Policy and Certificate Practice Statement;
8. LIP Certificate Policy and Certificate Practice Statement.

3 Identification and Authentication

3.1 INITIAL REGISTRATION

3.1.1 Types of names

The subject names for the certificate applicants shall follow the X.509 standard:

1. In case of personal certificate the subject name must include the persons name.
2. In case of server certificate the subject name must include the DNS FQDN.

3.1.2 Name Meanings

1. The format of a HellasGrid distinguished name is: "C=GR, O=HellasGrid, OU=*unit,* CN=*subject-name".*
2. The common name in the certificate subject must be obtainable from the real name of the subject or from the FQDN of the server.
3. The organizationalUnitName OU must be the DNS domain name for the subject's organizational unit within the subject's host institution.

3.1.3 Name Uniqueness

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

3.1.4 Verification of Key Pair

Not yet defined.

3.1.5 Authentication of Organization

Not yet defined.

3.1.6 Authentication of Individual

3.1.6.1 Person requesting a certificate

1. The subject must contact personally the CA/RA staff in order to verify his identity and the validity of the request;
2. The subject authentication is performed through the presentation of a valid official document stating that the subject is an acceptable end entity as defined in this document [1.3.3].

3.1.6.2 Server or service certificate

1. Requests must be signed by the personal HellasGrid CA certificate of the corresponding system administrator.

3.1.6.3 Person not requesting a certificate (revocation)

1. Individual identity may be authenticated by personal acquaintance with HellasGrid CA/RA staff;
2. By physical presence and proof of identity through a passport or identity card;
3. By consulting a public directory and verifying whether that person made a request.

3.2 ROUTINE REKEY

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 new certificate.

3.3 REKEY AFTER REVOCATION

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

3.4 REVOCATION REQUESTS

Certificate revocation requests should be submitted by:

1. Email sent to hellasgrid-ca@physics.auth.gr signed with a valid HellasGrid CA certificate.
2. When e-mail is not an option, the request will be authenticated using the procedure described in section 3.1.6.3.

4 Operational Requirements

4.1 CERTIFICATE APPLICATIONS

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

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

Certification requests should be submitted via e-mail to hellasgrid-ca@physics.auth.gr.

4.2 CERTIFICATE ISSSUANCE

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

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

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

4.3 CERTIFICATE ACCEPTANCE

Following issuance of a certificate, the HellasGrid CA shall require the subscriber to expressly indicate acceptance or rejection of the certificate to the HellasGrid CA by sending a signed email to hellasgrid-ca@physics.auth.gr.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances of 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 Section 1.3.3.
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.

4.4.2 Who can request revocation

The revocation of the certificate can be requested by:

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

4.4.3 Procedure of Revocation Request

The entity requesting the certificate is authenticated by:

1. signing the revocation request with a valid HellasGrid CA certificate.

Otherwise authentication will be performed with the same procedure as described in section 3.6.1.3.

4.4.3.1 Repository/CRL Update

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

4.4.4 Certificate Suspension

The procedures and requirements stated for certificate revocation must also be followed for certificate suspension where implemented.

4.4.5 CRL Issuance Frequency

1. CRLs will be published as soon as issued and at least once each 30 days;
2. The minimum CRL lifetime is 7 days;
3. CRLs are issued at least 7 days before expiration.

4.4.6 CRL Checking Requirements for Relying Parties

Download the CRL at least once a day and implement it's restrictions while validating certificates.

4.4.7 On line Revocation/Status Checking Availability

Currently no On line Revocation/Status Checking service is offered by the HellasGrid CA.

4.4.8 Variations of the above in case of private key compromise

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

4.5 SECURITY AUDIT PROCEDURES

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

4.5.1 Types of Events Audited

- System boots and shutdowns
- Interactive system logins
- periodic message digests of all system files
- requests for certificates
- identity verification procedures
- certificate issuing
- requests for revocation
- CRL issuing

4.5.2 Processing Frequency of Audit Logs

Audit logs will be processed at least once per month.

4.5.3 Retention Period of Audit Logs

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

4.5.4 Protection of Logs

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

4.5.5 Backup Procedures

Audit logs are copied to an off line medium, which is stored in safe storage.

4.5.6 Accumulation system

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

4.6 RECORDS ARCHIVAL

4.6.1 Types of Records Archived

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

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

4.6.2 Processing Frequency of Audit Logs

Not defined yet.

4.6.3 Retention Period for audit logs

Logs will be kept for a minimum of three years.

4.6.4 Protection of Audit Logs

4.6.4.1 Access

Audit logs may be consulted by:

1. CA personnel;
2. authorized external auditors.

4.6.4.2 Protection against modification and deletion

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

4.6.5 Backup Procedures

Audit events are copied to an off-line medium.

4.6.6 Archive Collection System

The archive collection system is internal to the HellasGrid CA.

4.7 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 older, but still valid certificate, will be available to verify old signatures until all the certificates signed using the associated private key have also expired.

4.8 COMPROMISE AND DISASTER RECOVERY

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

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

4.9 CA TERMINATION

Upon termination the HellasGrid CA will:

1. Notify subscribers, RAs and cross-certifying CAs;
2. Terminate the issuance and distribution of certificates and CRLs;
3. Notify relevant security contacts;
4. Notify widely as possible the end of the service.

5 Physical, Procedural and Personnel Security Controls

5.1 PHYSICAL SECURITY – ACCESS CONTROLS

5.1.1 Site Location

The HellasGrid CA is located at the Aristotle University of Thessaloniki, in the Department of Physics.

5.1.2 Physical Access

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

5.1.3 Power and Air Conditioning

The HellasGrid CA signing machine and the RA web server are both protected by uninterruptable power supplies. Environment temperature in rooms containing CA related equipment is maintained by an appropriate level air conditioning system.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

1. The HellasGrid CA 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's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this Policy, be considered as serving in a trusted role. Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, and executives who are designated to oversee the CA's operations.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Background Checks and Clearance Procedures for CA Personnel

HellasGrid CA personnel is selected in mutual agreement by the HellasGrid Coordinator (GRNET) and the respective HellasGrid CA operating organization (Department of Physics, A.U.Th)

5.3.2 Background Checks and Security Procedures for other personnel

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

5.3.3 Training Requirements and Procedures

Internal training is given to HellasGrid CA operators.

5.3.4 Training Period and Retraining Procedures

Not defined yet.

6 Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key pair generation

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

6.1.2 Private Key delivery to Entity

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

6.1.3 Subscriber Public Key Delivery to HellasGrid CA

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

6.1.4 Public Key delivery to Entity

Public keys are delivered by signed E-mail, floppy disk, CD-ROM or transferred by floppy and copied to the user directory by HellasGrid CA personnel.

6.1.5 CA Public Key delivery to users

CA certificate can be downloaded from the HellasGrid CA web site.

6.1.6 Key Sizes

1. The minimum key length for person, service or server certificate is 1024 bit.
2. The HellasGrid CA key length is 2048 bits.

6.1.7 Public Key Parameters Generation

Not defined yet.

6.1.8 Parameter quality testing

Not defined yet.

6.1.9 Hardware/software key generation

Not defined yet.

6.1.10 Key Usage Purposes

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

6.2 PRIVATE KEY PROTECTION

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

Not defined yet.

6.2.2 Private Key Escrow

Not defined yet.

6.2.3 Private Key Archival and Backup

The HellasGrid CA private key is kept encrypted in multiple copies in floppy disks and CD-ROMs in safe places. The pass phrase is in a sealed envelope kept in a safe.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

The HellasGrid CA private key has currently a validity of five years.

6.4 ACTIVATION DATA

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

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Security Technical Requirements

1. the operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;
2. monitoring is performed to detect unauthorized software changes;
3. CA systems configuration is reduced to the bare minimum;
4. the signing machine is kept powered off between uses.

6.5.2 Computer Security Rating

Not defined yet.

6.6 LIFE CYCLE SECURITY CONTROLS

Not defined yet.

6.7 NETWORK SECURITY CONTROLS

1. The CA signing machine is kept off-line;
2. CA/RA machines other than the signing machine are protected by a firewall.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Not defined yet.

7 Certificate and CRL profile

7.1 CERTIFICATE PROFILE

7.1.1 Version

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

7.1.2 Certificate Extensions (End Entity)

- Basic constraints (Critical):
  Not a CA.
- Key usage (Critical):
  Digital signature, non-repudiation, key encipherment, data encipherment.
- Subject key identifier
- Authority key identifier
- Subject alternative name
- Issuer alternative name
- CRL distribution points
- Certificate policies
- Netscape cert type

7.1.3 Algorithm Object Identifiers

Not defined yet.

7.1.4 Name Forms

Issuer:

C=GR,
O=HellasGrid,
CN=HellasGrid CA

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 for the subject's organizational unit within the subject's host institution.

commonName:
First name and last name or DNS FQDN of the subject. In case of host or service certificates the DNS FQDN may be prefixed with the service name.

7.1.6 Certificate Policy Identifier

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

7.1.7 Policy Qualifier Syntax and Semantics

Not defined yet.

7.2 CRL PROFILE

7.2.1 Version

All CRLs will issued in both X.509 version 1 and X.509 version 2 format.

8 Policy Administration

8.1 SPECIFICATION CHANGE AND PROCEDURES

Relevant changes will be made as widely available as possible.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

The HellasGrid CA policy is available at http://pki.physics.auth.gr/hellasgrid-ca/CPS

8.3 CPS APPROVAL PROCEDURES

Not defined yet.