SEE-GRID CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Table of Contents

1 INTRODUCTION

1.1 Overview

On July 2004, the GridAUTH Operations Center of the Aristotle University of Thessaloniki, implemented the SEE-GRID Certification Authority, in order to facilitate the needs for Grid computing in the wider area of the Balkans.

The scope of the SEE-GRID CA is to provide PKI services to the SEE countries – members of the SEE-GRID project – that did not have yet the opportunity to establish their own national grid PKI infrastructure.

The SEE-GRID CA is operated by the GridAUTH Operations Center at the Aristotle University of Thessaloniki under the supervision of GRNET as the SEE-GRID Coordinator. GRNET is supervised by the General Secretariat of Research and Technology, Greek Ministry of Development.

This draft document, following the structure set out in RFC 3647, defines the Certification Policy and the Certification Practice Statement of the SEE-GRID CA and specifies the minimum requirements and obligations for the issuance and management of certificates.

1.2 Document name and identification

- Document title: **"SEE-GRID CA Certification Policy and Certificate Practice Statement"**
- Version: **1.1**
- Document Date: **26 September 2004**
- O.I.D. **1.3.6.1.4.1.13089.2.1.11.1.1**

1.3 PKI participants

1.3.1 Certification Authorities

SEE-GRID certificates are signed by the SEE-GRID CA, which is defined as a medium security CA. SEE-GRID CA does not issue certificates to subordinate certification authorities.

1.3.2 Registration Authorities

The procedures of identification and authentication of the certificate applicants are performed by trusted individuals (Registration Authorities), appointed by the SEE-GRID Project Steering Committee (PSC). At any time the current list of valid Registration Authorities will be available in an on-line repository operated by the SEE-GRID CA.

1.3.3 Subscribers

Subscribers eligible for certification from the SEE-GRID CA are :

1. people involved in the SEE-GRID project located in a country that has not established its own Certification Authority;
2. digital processing entities, capable of performing cryptographic operations, used in activities of the SEE-GRID project;
3. services running on digital processing entities, which are used in activities of the SEE-GRID project.

1.3.4 Relying parties

Users of Grid computing infrastructures that are using the public keys, in certificates issued by the SEE-GRID CA for 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 SEE-GRID certificate does not imply automatic access to any kind of resources.

1.4.1 Appropriate certificate uses

Certificates issued by the SEE-GRID CA are only valid in the context of Grid research 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 SEE-GRID CP/CPS was authored and is administered by the GridAUTH Operations Center, which operates in the context of the Network and Telecommunications Committee of the Aristotle's University of Thessaloniki.

The SEE-GRID CA address for operational issues is :

SEE-GRID Certification Authority
Department of Physics
Building 22d
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE

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

1.5.2 Contact Person

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

Kanellopoulos Christos
Department of Physics
Building 22d
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE

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

1.5.3 Person determining CPS suitability for the policy

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

Kanellopoulos Christos
Department of Physics
Buidling 22d

Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE

Phone: (+ 30)2310998223
Fax: (+ 30)2310999428

1.5.4 CPS approval procedures

No stipulation.

1.6 DEFINITIONS AND ACRONYMS

TBD.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

All the on-line and off-line repositories of the SEE-GRID CA are operated by the GridAUTH Operations Center, Aristotle University of Thessaloniki, which operates in the context of the Network and Telecommunications Committee of the Aristotle's University of Thessaloniki.

The SEE-GRID CA communication information for issues regarding the repositories is :

SEE-GRID Certification Authority
Department of Physics
Building 22d
Aristotle University of Thessaloniki
University Campus
54124 Thessaloniki
GREECE

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

2.2 Publication of certification information

The SEE-GRID CA is obligated to maintain a secure on-line repository that is available to all Relying Parties through a web interface at http://www.grid.auth.gr/pki/seegrid-ca and which contains:

1. the SEE-GRID CA certificate for its signing key;
2. valid issued certificates that reference this policy;
3. the latest CRL;
4. a copy of the current and all previous versions of this document which specifies the CP and CPS;
5. a list with the current operational Registration Authorities;
6. other relevant information relating to certificates that refer to this Policy.

2.3 Time or 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 SEE-GRID 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 4.9.7.

2.4 Access control on repositories

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

SEE-GRID CA may impose a more restricted access control policy to the repository at its discretion.

The SEE-GRID CA web site is maintained in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available 24x7.

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 persons 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 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 and must have a reasonable association with the authenticated name of the subscriber.

3.1.3 Anonymity or pseudonimity of subscribers

SEE-GRID CA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

See section 3.1.1.

3.1.5 Uniqueness of names

The subject name listed in a certificate shall be unambiguous and unique for all certificates issued by the SEE-GRID CA. In the case of user certificates, 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 SEE-GRID 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 SEE-GRID CA proves possession of the private key that is the companion to the SEE-GRID CA root certificate by issuing certificates and signing CRLs.

The SEE-GRID CA verifies the possession of the private 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 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 SEE-GRID CA will not generate the key pair for subscribers and will not accept or retain private keys generated by subscribers.

3.2.2 Authentication of organization identity

SEE-GRID CA authenticates organization by:

- checking that the organization is affiliated with the SEE-GRID project;

- contacting the person who represents the organization in the project.

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. The subject authentication is performed through the presentation of a valid photo ID document or passport.
- **Digital Processing Entity or Service:** The entity must already have a valid DNS entry

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 section 4.2.2.

3.2.5 Validation of Authority

The subscriber requesting service from the SEE-GRID CA must present valid documents stating his/her affiliation with the organization.

3.2.6 Criteria of interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

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. Re key after expiration follows the same authentication procedure as new certificate.

3.3.2 Identification and authentication for re-key after revocation

A revoked key will not be re-certified. The authentication of a new certificate request follows the rules specified in section 3.2.3.

3.4 Identification and authentication for revocation request

Certificate revocation requests should be submitted to seegrid-ca@grid.auth.gr via e-mail. In case the revocation request is for a user certificate, the e-mail must be signed by the private key corresponding to the certificate that is requested to be revoked, which must be a valid, non-expired, non-revoked SEE-GRID 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 e-mail is not an option, the request will be authenticated using the procedure described in section 3.1.6.3.

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 section 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;

4.1.2 Enrollment process and responsibilities

5. **user Certificate:** For the first time and after that once every 3 years, a subscriber must be authenticated by the RA serving his/her location following the procedure described in section 3.2.3. After successful authentication the RA will enter the requester's name, email address and affiliation to the SSL secured SEE-GRID CA portal and a random 10 digit number will be generated. The first 5 digits of this number will be given to the requester in written form and the rest 5 digits will be sent automatically by the SEE-GRID CA portal to his/her e-mail address. From that point the requester has 2 working days to submit his/her certificate request to the SEE-GRID CA.
   The submission of the certificate requests will be done via an SSL secured web form where the requester will have to provide the same data as those given at the RA (name, e-mail, affiliation) along with the 10 digit number that was generated for him/her.
   If the subscriber wants to re key his/her certificate, then he/she must follow the procedures described in section 4.7.

6. **Server or Service Certificate:** The subject must already have a valid SEE-GRID CA certificate before requesting a server or service certificate. The submission of the certificate request can be done either via a web interface or via e-mail.
   In the first case the subject will have first to import his/her SEE-GRID CA certificate in the browser in order to be authenticated automatically by the SEE-GRID CA 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 SEE-GRID CA certificate to seegrid-ra@grid.auth.gr 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 sections 4.2.1 and 4.2.2

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All the certificate application will be authenticated and validated by the SEE-GRID CA and RAs. In the case of a new user certificate, the request will be authenticated by checking if the 10 digit number [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 SEE-GRID 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 SEE-GRID CA are in order to be approved:

1. the certificate application must be authenticated first by the RA as described in section 4.2.1;
2. the subject must apply the certificate request within 2 working days after the successful authentication performed by the RA;
3. the subject must be an acceptable subscriber entity, as defined by this Policy;
4. the request must obey the SEE-GRID CA distinguished name scheme;
5. the distinguished name must unambiguous and unique;
6. the key must have at least 1024 bits.

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 seegrid-ca@grid.auth.gr.

4.2.3 Time to process certificate applications

Each certificate application will take no more that 3 working days to be processed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Right after the subscriber's certificate is issued, an email will be 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 will be sent to him/her with information on how to download his certificate from the SEE-GRID CA portal. In the same e-mail the subscriber will be requested to return an e-mail signed by his/her newly issued certificate, in which he will will be stating that (s)he accepts his/her certificate signed by the SEE-GRID CA and that (s)he adheres to the this policy.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber must send an e-mail, within 5 working days from the day that his/her certificate was issued, in which he will be stating that:

1. (s)he has read this policy and accepts to adhere to it;
2. (s)he accepts his/her certificate signed by the SEE-GRID CA;
3. (s)he assumes the responsibility to notify the SEE-GRID 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 SEE-GRID CA will be published in the on-line repository operated by

the SEE-GRID 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 SEE-GRID CA can be used for:

1. email signing/verifying and encryption/decryption (S/MIME);
2. server authentication and encryption of communications;
3. authentication purposes in Grid 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 encryption and signature verification (S/MIME);
2. server authentication and encryption of communications;
3. authentication purposes in Grid infrastructures.

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

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

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

4.6.2 Who may request renewal

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

4.6.3 Processing certificate renewal requests

SEE-GRID CA will 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

SEE-GRID CA will 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

SEE-GRID CA will 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

SEE-GRID CA will 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

SEE-GRID CA will 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 SEE-GRID CA;
2. revocation of their certificate by the SEE-GRID CA;
3. compromise of their private key.

4.7.2 Who may request certification of a new public key

Same as in section 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 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 section 4.3.2

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Same as in section 4.4.1

4.7.6 Publication of the re-keyed certificate by the CA

Same as in section 4.4.2

4.7.7 Notification of certificate issuance by the CA to other entities

Same as in section 4.4.3

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate will be revoked in the following circumstances:

1. the subject of the certificate 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 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. 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 SEE-GRID CA certificate. Otherwise authentication will be performed with the same procedure as described in section 3.2.3.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

SEE-GRID CA will process all revocation requests within 1 working day.

4.9.6 Revocation checking requirement for relying parties

Relying parts must download the CRL from the online-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

No stipulation.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation checking requirements

Currently there are no on-line revocation/status services offered by the SEE-GRID 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

SEE-GRID CA does not suspend certificates.

4.9.14 Who can request suspension

SEE-GRID CA does not suspend certificates.

4.9.15 Procedure for suspension request

SEE-GRID CA does not suspend certificates.

4.9.16 Limits on suspension period

SEE-GRID CA does not suspend certificates.

4.10 Certificate status services

4.10.1 Operational characteristics

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

4.10.2 Service availability

The on-line repository is maintained on best effort basis with intended availability of 24x7.

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.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The SEE-GRID CA is located at the Aristotle University of Thessaloniki, in the Department of Physics.

5.1.2 Physical access

Physical access to the SEE-GRID CA is restricted to authorized personnel only.

5.1.3 Power and air conditioning

The SEE-GRID 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 at appropriate level by air conditioning system.

5.1.4 Water exposures

Due to the location of the SEE-GRID CA facilities, floods are not expected.

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

1. The SEE-GRID 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 SEE-GRID 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.

5.2.2 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

SEE-GRID CA personnel is selected in mutual agreement by the SEE-GRID Coordinator (GRNET) and the respective SEE-GRID CA operating organization (GridAUTH Operations Center, Aristotle's University of Thessaloniki)

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to SEE-GRID CA/RA operators.

5.3.4 Retraining frequency and requirements

SEE-GRID 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, which is stored in safe storage.

5.4.6 Audit collection system (internal vs. external)

The audit log accumulation system is internal to the SEE-GRID 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 SEE-GRID 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

5.5.6 Archive collection system (internal or external)

The archive collection system is internal to the SEE-GRID CA.

5.5.7 Procedures to obtain and verify archive information

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

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

5.7.3 Entity private key compromise procedures

5.7.4 Business continuity capabilities after a disaster

5.8 CA or RA termination

Upon termination the SEE-GRID 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 as widely as possible the end of the service.

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 any other than the owner of the key pair. Each subscriber must generate his/her own key pair. SEE-GRID CA does not generate private keys on behalf of subscribers.

6.1.2 Private key delivery to subscriber

The SEE-GRID 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 SEE-GRID 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 SEE-GRID CA web site.

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 SEE-GRID 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)

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 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 SEE-GRID 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

SEE-GRID CA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

SEE-GRID CA does not use any kind of cryptographic module.

6.2.7 Private key storage on cryptographic module

SEE-GRID CA does not use any kind of cryptographic module.

6.2.8 Method of activating private key

The private key of the SEE-GRID CA is activated by using a pass phrase. See section 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

No stipulation.

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

All certificates issued to subscribers by the SEE-GRID CA will have a maximum lifetime of 1 year.

The lifetime of the SEE-GRID CA root certificate must be no more than 5 years and and no less than 2 years.

6.4 Activation data

6.4.1 Activation data generation and installation

SEE-GRID CA does not generate activation data for subscribers. It's upon the subscriber to generate a secure pass phrase, at least 12 charaters long, in order to be used as activation data for his/her private key.

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

6.4.2 Activation data protection

- **The subsriber** is responsible to protect the activation data for his/her private key.
- The SEE-GRID CA uses a pass phrase to activate it's private key, which is known

only by the SEE-GRID CA Manager and the SEE-GRID 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 SEE-GRID CA Manager and Operators. Old activation data are destroyed according to current best practices.

6.4.3 Other aspects of activation data

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.

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, Host and Service 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
  9. Netscape cert type

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

Issuer:

DC=ORG
DC=SEE-GRID,
CN=SEE-GRID CA

Subject:

DC=ORG
DC=SEE-GRID,
O=*INSTITUTE,*

OU=*[Hosts|People],*
CN=*SUBJECT NAME*

7.1.5 Name constraints

Subject attribute constraints:

DomainComponent:
Must be "ORG"

DomainComponent:
Must be "SEE-GRID"

OrganizationName:
Must be the name of the subject's institute.

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 service name separated with a '/' from the DNS FQDN.

7.1.6 Certificate policy object identifier

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

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

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

7.2.2 CRL and CRL entry extensions

7.3 OCSP profile

No stipulation.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

The SEE-GRID 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.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees shall be charged.

9.1.2 Certificate access fees

No fees shall be charged.

9.1.3 Revocation or status information access fees

No fees shall be charged.

9.1.4 Fees for other services

No fees shall be charged.

9.1.5 Refund policy

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

9.2 Financial responsibility

SEE-GRID CA denies any financial responsibilities for damages or impairments resulting from its operation.

9.2.1 Insurance coverage

9.2.2 Other assets

9.2.3 Insurance or warranty coverage for end-entities

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

9.3.2 Information not within the scope of confidential information

9.3.3 Responsibility to protect confidential information

9.4 Privacy of personal information

SEE-GRID CA does not collect any confidential or private information.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

SEE-GRID CA collects the following information which is not deemed as private:

1. subscriber's e-mail address;
2. subscriber's name;
3. subscriber's organization;
4. subscriber's certificate;

9.4.4 Responsibility to protect private information

SEE-GRID CA has not responsibility to protect private information as all the information it collects is public.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

1. RFC 3647;
2. HellasGrid CA Certificate Policy;
3. INFN Certificate Policy and Certificate Practice Statement;
4. NIKHEF Certificate Policy and Certificate Practice Statement;

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

No stipulation.

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 SEE-GRID 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.