SEE-GRID CA

CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT

1. INTRODUCTION

1.1. OVERVIEW

This document describes the Certification Policy and the Certificate Practice statement of the SEE-GRID Certification Authority.

SEE-GRID CA is a Certification Authority managed and operated by the GRNET S.A. In the period between July 2004 and April 2010, SEE-GRID CA had been operating in the context of the SEE-GRID Regional Grid Infrastructure project series (SEE-GRID-I 2004-2006, SEE-GRID-II 2006-2008, SEE-GRID-SCI 2008-2010) with the mandate to provide catch all PKI services to the wider region of South Eastern Europe in order to facilitate the needs of distributed computing and pave the way for the countries in the region to establish their own national Public Key Infrastructure and guide them through the IGTF accreditation process. Since May 2010, SEE-GRID CA provides Catch-All PKI services for the European Grid Initiative (EGI.eu).

1.2. DOCUMENT NAME AND IDENTIFICATION

Title: **SEE-GRID CA Certification Policy and Certificate Practice Statement**

Version: **3.0**

Document Date: **August 21, 2017**

O.I.D.: **1.3.6.1.4.1.16515.20.2.1.3.0**

1.3. PKI PARTICIPANTS

1.3.1. CERTIFICATION AUTHORITIES

SEE-GRID CA, issues certificates directly to End Entities and does not issue certificates to subordinate Certification Authorities. See section 10 for further information regarding the scope of the SEE-GRID CA.

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 CA. At any time the current list of valid Registration Authorities will be available at the SEE-GRID CA web site.

1.3.3. SUBSCRIBERS

SEE-GRID CA issues certificates to people collaborating with EGI.eu or GRNET in activities, which require access to the e-Infrastructures, and who are not able to get certificates from any of the other existing IGTF accredited CAs. SEE-GRID CA issues personal, host, service, and robot certificates.

1.3.4. RELYING PARTIES

Users or providers of Computing Infrastructure services that are using the certificates issued by the SEE-GRID CA for signature verification and/or encryption, are considered relying parties.

1.3.5. OTHER PARTICIPANTS

No stipulation.

1.4. CERTIFICATE USAGE

The ownership of a SEE-GRID certificate does not imply 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 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 SEE-GRID CP/CPS was authored and is administered by GRNET S.A. The SEE-GRID CA address for operational issues is:

SEE-GRID Certification Authority
GRNET S.A.
7, Kifisias Av.
11523 Athens
Greece

Phone: (+30)2107474274
Fax: (+30)2107474490
Email: see-grid-ca@hellasgrid.gr

1.5.2. CONTACT PERSON

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

Kostas Koumantaros
GRNET S.A.
7, Kifisias Av.
11523 Athens
Greece

Phone: (+30)2107474274
Fax: (+30)2107474490
Email: kkoum@grnet.gr

1.5.3. PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The persons who determine the CPS suitability for the policy are:

Kostas Koumantaros
GRNET S.A.
7, Kifisias Av.
11523 Athens
Greece

Phone: (+30)2107474274
Fax: (+30)2107474490
Email: kkoum@grnet.gr

1.5.4. CPS APPROVAL PROCEDURES

New versions of the Certification Practice Statement are reviewed internally in order to verify their compliance with the IGTF minimum requirements for "classic X.509 CAs with secure infrastructures". After a successful internal review, the CPS 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 Practice 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 SEE-GRID 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 tha an individual or organization under that name is in fact the named individual or organization.
IGTF	Interoperable Global Trust Federation
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	A recipient of a certificate who acts in reliance on that certificate and/or 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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

All the repositories of the SEE-GRID CA are operated by GRNET S.A. The SEE-GRID CA contact details for issues regarding the repositories is:

SEE-GRID Certification Authority
GRNET S.A.
56, Mesogion Av.
11527 Athens
Greece

Phone: (+30)2107474274
Fax: (+30)2107474490
Email: see-grid-ca@hellasgrid.gr

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The SEE-GRID CA maintains a secure on-line repository that is available to all Relying Parties through a web interface accessible at http://see-grid-ca.hellasgrid.gr 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

Information shall be published promptly to the repository after such information is available to the CA. Certificates issued by the SEE-GRID CA, will be published in a searchable repository after the requester has successfully accepted the terms and conditions written in this document. Information relating to the revocation of a certificate will be published as described in section 23.

2.4. ACCESS CONTROL ON REPOSITORIES

SEE-GRID CA does not impose any access control restrictions to the information available at its web site, namely the CA certificate, the latest CRL and all versions of this CP and CPS, under which SEE-GRID CA has issued End Entity certificates..

The SEE-GRID CA web site is maintained in a best effort basis. Excluding disruption of service due to scheduled maintenance and unforeseen failures the site should be available 24×7.

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

3.1.3. ANONYMITY OR PSEUDONIMITY OF SUBSCRIBERS

SEE-GRID CA neither issues nor signs pseudonymous or anonymous certificates.

3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS

See section 15.

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 SEE-GRID CA. In the case of personal or robot certificates, additional numbers or letters may be appended to the real name of the subscriber or robot, when necessary, in order 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 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 SEE-GRID 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

SEE-GRID CA authenticates organizations by:

- checking that the organization is affiliated with GRNET or EGI.eu;
- contacting the person who acts as liaison with GRNET or EGI.eu.

3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY

Physical Person: The subject must contact the RA in person, in order to have his/her identity vetted and to verify the validity of the request. The authentication of the subject is performed through the presentation of a valid photo ID document or passport. In cases where the subject resides in a remote geographical location and 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 (ID document or passport must be delivered by mail or courier service to the RA prior to this online meeting. Authenticated photocopy refers to the verification made by a legally accepted notary public under the law of the country where the RA operates.

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 [section 10]. The system administrator requesting the certificate must use his/her personal certificate, issued by an IGTF accredited CA, to authenticate to the SEE-GRID CA web portal or digitally sign the e-mail in order to submit the certificate request.

Robot: The entity must be an acceptable end entity as defined in this document [section 10]. 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 SEE-GRID CA web portal or digitally sign the e-mail in order to submit the certificate request.

3.2.4. NON-VERIFIED SUBSCRIBER INFORMATION

The telephone number of the user is not verified by SEE-GRID CA.

3.2.5. VALIDATION OF AUTHORITY

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

3.2.6. CRITERIA OF INTEROPERATION

SEE-GRID CA is a Certification Authority accredited by IGTF and as such the basic criterium for interoperation within the federation is the adherence to the IGTF minimum requirements

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Expiration warnings will be issued to subscribers when re key time arrives. Re key before expiration can be accomplished by sending a re key request via a digitally signed e-mail or by logging into the SEE-GRID CA web portal using the current user certificate and submitting re-key request. Re key after expiration follows the same authentication procedure as requesting a new certificate. Once every five years the user has to be authenticated by an RA.

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 16.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Certificate revocation requests should be submitted via e-mail or through the SEE-GRID 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 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 or submission through the SEE-GRID CA web portal is not an option, the request will be authenticated using the procedure described in section 16.

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 18

4.1.2. ENROLLMENT PROCESS AND RESPONSIBILITIES

Users can enroll to the SEE-GRID CA Identity Management System via the SEE-GRID 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 SEE-GRID CA System. It is the responsibility of the user to keep this information up to date. All users who have successfully enrolled with the SEE-GRID CA, are able to submit certificate applications.

User Certificate: The users can request to have their public keys signed via the SEE-GRID 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. For the first time and since then at least every 5 years, the subscriber must have his/her identity vetted by the RA serving his/her organization following the procedure described in section 16. After successfully completing the identity vetting procedure, the RA will approve the certificate request on the SEE-GRID 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 SEE-GRID 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 SEE-GRID 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 16. After successful authentication

the RA will approve the certificate request at the SEE-GRID CA web portal. If the subscriber requires to re key his/her certificate, then he/she must follow the procedures described in section 21.

All certificate applications 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 hash [see section 18] 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 18;
2. the subject must be an acceptable End Entity, as defined by this Policy;
3. the request must obey the SEE-GRID CA distinguished name scheme;
4. the distinguished name must be 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 signed notification e-mail will be sent by the RA to the subject with carbon copy to e-mail address of the CA.

4.2.3. TIME TO PROCESS CERTIFICATE APPLICATIONS

Each certificate application will take no more than 2 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/her certificate from the SEE-GRID CA online repository. In the same e-mail the subscriber will be requested to acknowledge his/her adherence to this policy.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The subscriber must log in the SEE-GRID CA web portal within 5 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. has read this policy and accepts to adhere to it;
2. accepts his/her certificate signed by the SEE-GRID CA;

3. 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.

Alternatively the subscriber may complete the certificate acceptance procedure by sending a signed e-mail with 5 working days from the day that his/her certificate was issued in which (s)he will stating what as described above.

4.4.2. PUBLICATION OF THE CERTIFICATE BY THE CA

All the certificates issued by the SEE-GRID CA and whose requesters have accepted the terms and conditions of this document, will be published in an on-line repository operated by the SEE-GRID CA, which will be accessible via a search web form.

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 and other Computing 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 and other Computing 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' certificates. Subscribers must follow the re-key procedure as defined in section 21.

4.6.2. WHO MAY REQUEST RENEWAL

SEE-GRID CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 21.

4.6.3. PROCESSING CERTIFICATE RENEWAL REQUESTS

SEE-GRID CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 21.

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 21.

4.6.5. CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

SEE-GRID CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 21.

4.6.6. PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

SEE-GRID CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 21.

4.6.7. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

SEE-GRID CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 21.

4.7. CERTIFICATE RE-KEY

4.7.1. CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Subscribers must generate a new key pair for each certificate they request to be signed by the SEE-GRID CA.

4.7.2. WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Same as in section 18.

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 on the SEE-GRID CA web portal with their personal certificates and submit 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. At least once every 5 years the subscriber must go through the same authentication procedure as the one described for a new certificate.

In case the request for re-key a personal 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 requesting a new certificate.

4.7.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Same as in section 19.

4.7.5. CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Same as in section 19.

4.7.6. PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Same as in section 20.

4.7.7. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Same as in section 20.

4.8. CERTIFICATE MODIFICATION

4.8.1. CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

SEE-GRID CA does not modify signed End Entity certificates.

4.8.2. WHO MAY REQUEST CERTIFICATE MODIFICATION

SEE-GRID CA does not modify signed End Entity certificates.

4.8.3. PROCESSING CERTIFICATE MODIFICATION REQUESTS

SEE-GRID CA does not modify signed End Entity certificates.

4.8.4. NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

SEE-GRID CA does not modify signed End Entity certificates.

4.8.5. CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

SEE-GRID CA does not modify signed End Entity certificates.

4.8.6. PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

SEE-GRID CA does not modify signed End Entity certificates.

4.8.7. NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

SEE-GRID CA does not modify signed End Entity certificates.

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 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.

4.9.2. WHO CAN REQUEST REVOCATION

The revocation of the certificate can be requested by:

1. the certificate owner;
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 revocation of a certificate is authenticated by logging on the SEE-GRID CA website using a valid SEE-GRID 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 16.

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 14] 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

SEE-GRID 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, as applicable, shall be updated.

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 section 23.

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 hosted at the Scientific Computing Center at the Aristotle University of Thessaloniki.

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 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 SEE-GRID CA facilities, floods are not expected.

5.1.5. FIRE PREVENTION AND PROTECTION

The Data Center where SEE-GRID 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 SEE-GRID CA private key is kept in several removable storage media;
2. Backup copies of CA related information may be kept in off-line media such as magnetic tape cartridges, floppies and CD-ROMs.

5.1.7. WASTE DISPOSAL

Waste carrying potential confidential information such as magnetic tape cartridges, floppies and CD-ROMs 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 NGIGRNET and the Grid & HPC Operations Center, at the Aristotle 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 along with the corresponding private key will be available in order to verify digital signatures and issue 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

No stipulation.

5.7.3. ENTITY PRIVATE KEY COMPROMISE PROCEDURES

No stipulation.

5.7.4. BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

No stipulation.

5.8. CA OR RA TERMINATION

Upon termination the 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 the 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 an End Entity 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 25. 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 31.

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 20 years 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 characters 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 characters long. Every 180 days the pass phrase is regenerated by one of the SEE-GRID CA Operators.

6.4.2. ACTIVATION DATA PROTECTION

- The subscriber 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 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 SEE-GRID CA Manager and Operators. Old activation data is 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;
5. the signing machine is not connected to any kind of networks.

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

CA certificate:

1. *Basic constraints (Critical): CA:TRUE.*
2. *Key usage (Critical): Certificate Sign, CRL Sign*
3. *Subject key identifier*
4. *Authority key identifier*

End Entity certificates:

1. *Basic constraints (Critical): Not a CA.*
2. *Key usage (Critical): Digital signature, key encipherment, data encipherment.*
3. *Extended Key Usage*
4. *Subject key identifier*
5. *Authority key identifier*
6. *Subject alternative name*
7. *CRL distribution points*
8. *Certificate policies*

7.1.3. ALGORITHM OBJECT IDENTIFIERS

1. Hash Function: 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:

DC=ORG
DC=SEE-GRID,
CN=SEE-GRID CA 2013

Subject:

DC=ORG DC=SEE-GRID, O=[Hosts|People|Services|Robots], O=INSTITUTE, CN=SUBJECT NAME	DC=EU DC=EGI, C=Country, O=[Hosts|People|Services|Robots], O=INSTITUTE, CN=SUBJECT NAME

7.1.5. NAME CONSTRAINTS

Subject attribute constraints:

- **DomainComponent 1**: Must be either “ORG” or “EU”
- **DomainComponent 2**: Must be “SEE-GRID” if DomainComponent 1 is “ORG” or “EGI” if DomainComponent 1 is “EU”
- **Country**: In case DomainComponent 1 is “EU” and DomainComponent 2 is “EGI, then the Country component must be the country of residence of the subscriber.
- **Organization**: Must be the name of the institution of the subject.
- **OrganizationalUnit**: Must be either “Hosts” or “People” or “Services” or “Robots”.
- **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. 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 (“:”).

7.1.6. CERTIFICATE POLICY OBJECT IDENTIFIER

SEE-GRID CA identifies this policy with the object identifier (O.I.D) specified in section 10. 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 X.509 version 2 format.

7.2.2. CRL AND CRL ENTRY EXTENSIONS

No stipulation

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

No stipulation.

9.2.2. OTHER ASSETS

No stipulation.

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

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;
5. subscriber's work phone number.

9.4.4. RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

SEE-GRID CA has no 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

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

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