EG-GRID

Certification Authority

Certificate Policy
And
Certification Practice Statement

Document OID: 1.3.6.1.4.1.38589.1.1.0
Version 1.0

Table of Contents

1. INTRODUCTION

1.1 Overview

This document is organized according to the specifications proposed by the RFC 3647. It describes the procedure followed by National Grid Initiative of Egypt Certification Authority (EG-GRID CA) and is the combination of Certificate Policy and Certification Practice Statement (CP/CPS). The EG-Grid project is an initiative of Egyptian Universities Network (EUN), Supreme Council of Universities - Ministry for Higher Education, to set up a Grid infrastructure and Grid computing.

1.2 Document Name and Identification

Document Title

EG-GRID CA Certificate Policy and Certification Practice Statement

Document Version
1.0

Document Date
January, 2012

OID assigned: 1.3.6.1.4.1.38589.1. 1.0

OID structure:

- IANA: 1.3.6.1.4.1
- ISO(1).org(3).dod(6).internet(1).private(4).enterprise(1)
- EUN: 38589
- EG-GRID CA: 1
- Version of this CP/CPS: 1.0

1.3 PKI Participants

1.3.1 Certification Authorities

The EG-GRID CA is a stand-alone self-signed CA and 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 RAs), appointed by the EG-GRID CA.
Based on this CP/CPS document, RAs are not allowed to issue certificates.

1.3.3 Subscribers

EG-GRID CA provides PKI services to meet the requirements of Egyptian academics and research communities including national and international Grid activities.
EG-GRID CA issues certificates to the following entities:

- Users (people)

- Computers (hosts)
- Services

1.3.4. Relying Parties

All entities that use public keys of certificates, issued by EG-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

1.4.1 Appropriate Certificate Uses

- CA certificates may only be used to issue certificate and generate CRLs.
- User certificates can be used to authenticate a user that would like to benefit from the academic resources, services and activities including Grid resources.
- Host certificates can be used to identify computers that have special tasks related to the Grid or other academic activities.
- Service certificates can be used to recognize the host applications and, data or communication encryption (SSL/TLS).

In addition, user certificates can be used for e-mail signing and encryption (S/MIME). User certificates must not be shared.

1.4.2 Prohibited Certificate Uses

Any other kind of usage such as financial transactions is strictly forbidden.

Using certificates for purposes contrary to Egyptian law is explicitly prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Egyptian Universities Network (EUN) is responsible for the management, registration, maintenance and interpretation of EG-GRID CA. It is reachable at:

Egyptian Universities Network (EUN),
Supreme Council of Universities Building,
Cairo University Campus,
Giza 12613 - P.O. Box: 268 Orman,
Egypt.
Home page: www.eun.eg
EG-GRID CA Home page: www.grid.eun.eg
E-mail: ca@grid.eun.eg
Phone: +202 377 423 48

Fax: +202 357 064 71

1.5.2 Contact person

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

Ayman Bahaa
Egyptian Universities Network Director and EG-GRID CA Manager

Egyptian Universities Network (EUN),
Supreme Council of Universities Building,
Cairo University Campus,
Giza 12613 - P.O. Box: 268 Orman,
Egypt.

e-mail: aymanbahaa@eun.eg
Phone: +202 377 423 48 ext: 1111
Fax: +202 357 064 71

Deputy contact:

Dina Barakat
Egyptian Universities Network Vice Director

Egyptian Universities Network (EUN),
Supreme Council of Universities Building,
Cairo University Campus,
Giza 12613 - P.O. Box: 268 Orman,
Egypt.

e-mail: dina@eun.eg
Phone: +202 377 423 48 ext: 1002
Fax: +202 357 064 71

1.5.3 Person determining CPS suitability for the policy

Dina Barakat
Egyptian Universities Network Vice Director

Egyptian Universities Network (EUN),
Supreme Council of Universities Building,
Cairo University Campus,
Giza 12613 - P.O. Box: 268 Orman,
Egypt.

e-mail: dina@eun.eg
Phone: +202 377 423 48 ext: 1002
Fax: +202 357 064 71

1.5.4 CPS Approval Procedures

The CP/CPS document and all CPS modifications should be approved by the EUGridPMA before being applied.

1.6 Definitions and Acronyms

Activation Data: Data values, different from keys, that are required to operate cryptographic modules and that need to be protected such as a pin or a passphrase.

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.

CA – Certification Authority: The entity / system that signs X.509 identity certificates**.**

CP – Certificate Policy: 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.

CPS – Certification Practice Statement: A statement for the practices that a certification authority applies in its operations.

CRL – Certificate Revocation List: A time stamped list displaying revoked certificates that are signed by a CA and made freely available in a public repository.

PKI – Public Key Infrastructure: IT infrastructure that enables users of a basically unsecure public network (such as the Internet) to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

Private Key: In secure communication, an algorithmic pattern used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to decrypt messages that were encrypted by the corresponding public key.

Public Key: The pattern used to confirm "signatures" on incoming messages or to encrypt a file or message so that only the holder of the private key can decrypt the file or message.

RA – Registration Authority: An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

Relying Party: A recipient who accepts a digital certificate and digital signature.

Subscriber: In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

EG-GRID CA will maintain a secure on-line repository at http://www.grid.eun.eg that includes:

- The EG-GRID CA root certificate in CRT, PEM, DER, CER and text format
- User and host certificates issued by the CA
- A periodically updated DER, PEM and text Certificate Revocation List (CRL)

- All versions (current and past) of its approved CP/CPS document
- An official contact e-mail address
- A physical contact address
- Other information that can be regarded as relevant to EG-GRID CA

The on-line repository runs on best-effort basis with an availability of 24x7, liable to reasonable scheduled maintenance.

2.2 Publication of Certification Information

See section 2.1.

2.3 Time or Frequency of Publication

- Certificates will be put to the EG-GRID CA website as soon as they are issued.
- CRL is updated immediately after a revocation is done and it will be updated at least 7 days before the expiration date of the CRL where CRL life time is 30 days.
- New versions of all EG-GRID CA documents will be published on the website as soon as they are updated.
- New versions of this CP/CPS document will be published soon after they are validated and former versions will be kept as a record in the repository.

2.4 Access Control on Repositories

The on-line repository is available on a 24x7 basis, liable to reasonable scheduled maintenance. EG-GRID CA does not impose any access control restrictions to the information available at its website, which includes the CA certificate, latest CRL and a copy of the CP/CPS document.

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:

- in case of **user** certificate the subject name must include the person's name in the CN field;
- in case of **host** certificate the subject name must include the FQDN (Fully Qualified Domain Name) as registered to DNS in the CN field;
- in case of **service** certificate the subject name must include the FQDN separated by a "/" in the CN field.

The common names must be encoded as Printable Strings according with RFC 1778 and RFC 2252. The characters allowed in the common names of personal certificates are as follows:

' ' (space), '(', ')' and '-';

'0' – '9';

'a' – 'z' and 'A' – 'Z'.

In addition, the characters '.' (period) and '/' (slash) are allowed in host and service certificates. The period must be used to separate the DNS host name components and the slash must be used to separate the service name.

3.1.2 Need for Names to be Meaningful

The Subject Name in a certificate must represent the subscriber; preferably, it can be the actual name of the user. If it is a host certificate, the CN must be stated as the fully qualified domain name (FQDN). Each host certificate must be linked to a single network entity.

3.1.3 Anonymity or Pseudonimity of Subscribers

EG-GRID CA does not issue pseudonymous or anonymous certificates. No user certificates shall be issued to roles or functions, only to named and identified persons.

3.1.4 Rules for Interpreting Various Name Forms

The CN component of the subject name in a certificate for a user must contain the first and the family name as it appears in the authentication document proving the name of the subscriber.

The CN entry for a host must be the fully qualified domain name (FQDN) that can be universally used to access that host.

The CN entry for a service must be the name of the application followed by a slash (/) followed by the FQDN of the host on which the application is executed.
See section (3.1.1)

3.1.5 Uniqueness of Names

The subject name included in the CN part of a certificate must be unique for all certificates issued by the EG-GRID CA. When essential, extra characters may be affixed to the original name to guarantee the uniqueness of the subject name.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Requests are submitted via SSL protected HTTP transport, either in PKCS10 or SPKAC format. Host or service certificate requests can be submitted by signed e-mail. In all cases, signature is verified by the CA.

3.2.2 Authentication of Organization Identity

The first time an organization/unit entity wants to get a certificate for a user, a server or a service, it has to announce this officially to the RA or the EG-GRID CA. The RA has to ascertain that the organization or organizational unit exists and is entitled to request a EG-GRID certificate. It must also get competent information on who is entitled to sign on behalf of the institution.

3.2.3 Authentication of Individual Entity

Certificate of a user:

- The subject should contact personally the RA staff in order to validate his/her identity.
- The subject authentication is fulfilled by providing an official document (ID-card, driving license or a passport) declaring that the subject is a valid end entity.

The RA shall send via a secure communication channel or in a signed e-mail to the EG-GRID CA the following information:

- The type, identification number and name in the identification document presented by the subject to be authenticated;
- A contact e-mail and phone number of the requester;
- The date, time and place of the authentication.

Certificate of a host:

Host certificates can only be requested by the administrator responsible for the particular host. The host administrator must already have a valid personal EG-GRID certificate, required for requesting host certificate.

In the case of a host/service request the RA should ensure that the requestor is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate (see section 3.2.5).

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

The requester provides documentation for the organizational name that should be included in the certificate. The wording of the organizational name that should be included in the certificate needs to be identical to the wording in the documentation provided.

The RA should have document evidence on retaining the same identity over time.

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 sent to subscribers before it is re-key time. Re-key before expiration can be executed by sending a re-key e-mail request signed with the current personal certificate of the subscriber. Re-key after expiration uses completely the same authentication procedure as new certificate (specified in section 3.2.3).

3.3.2 Identification and Authentication for Re-key after Revocation

A revoked certificate shall not be renewed. The procedure for re-authentication is exactly the same with an initial registration (specified in section 3.2.3).

3.4 Identification and Authentication for Revocation Request

Personal certificate revocation request should be authenticated in one of the following ways:

- by issuing a revocation request from the public interface.
- by personal authentication as described in 3.2.3.

If the revocation request is for a host or service certificate the e-mail must be signed by the certificate of the administrator responsible for the particular host or service.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a Certificate Application

The EG-GRID CA issues certificates to eligible organizations, i.e. entities that are connected to the academic and research network, for:

- users affiliated to eligible organization for which they take full responsibility,
- hosts administered by the requesting eligible organization, and
- services provided on a host that is administered by an eligible organization.

Procedures are different if the subject is a user or a host/service. In every case the subject has to generate his own key pair. Minimum key length is 2048 bits.

User

The minimum key length for all certificates is 2048 bits. The maximum validity period is one year. Each applicant must generate its own key pair using OpenSSL or any other similar software.

Hosts and Services

Certificate requests are sent by e-mail to the RA and must be signed by a valid EG-GRID certificate belonging to a user. The RA verifies the right of the requestor to obtain the certificate and then forwards the request to the EG-GRID CA by a signed e-mail. Also certificate requests can be done via the EG-GRID CA secure website.

See section (4.1.2)

4.1.2 Enrollment Process and Responsibilities

User Certificate

For user certificates, request can be submitted as follow:

User certificate requests is submitted by an online procedure on EG-GRID CA secure website (https://www.grid.eun.eg), using a web browser.

The key pairs are generated by the web browser locally on the user's machine. When submitting a request to the CA, the Subscriber types a PIN – a personal string known only to the Subscriber.

The certificate request will be verified by the appropriate RA, who will approve or disapprove the request according to sections 4.2.1 and 4.2.2.

If the request is approved by the RA, the requester will then receive an e-mail, containing information needed to download the certificate using a browser by a secure URL on the EG-GRID CA website.
The certificate (public key signed by the CA) can only be downloaded using the same browser, including the key pair, on the same machine, by a secure URL from EG-GRID CA website.

Host or Service Certificate

The host or service administrator creates key pair and certificate request file using OpenSSL packages. The private key is kept by the host or service administrator. The subscriber submit certificate request file to the EG-GRID CA by signed e-mail or by uploading the request through the EG-GRID CA secure website (https://www.grid.eun.eg). In this last case, the Subscriber types a PIN – a personal string known only to the Subscriber. The certificate request will be verified by the appropriate RA, who will approve or disapprove the request according to sections 3.2.3, 4.2.1 and 4.2.2. If the request is approved by the RA, the requester will then receive an e-mail, containing his/her certificate or information needed to download using a browser by a secure URL on the EG-GRID CA website.

Subscribers Obligations:
Subscribers must:

- Read and adhere to the procedures published in this document
- Use the certificate for the permitted purposes only
- Authorize the processing and conservation of personal data (as required under the data protection regulations)
- Take every precaution to prevent any loss, disclosure or unauthorized access to or use of the private key associated with the certificate, including:
    - (Personal certificates) selecting a passphrase in accordance with the currently approved version of the "Guidelines on Private Key Protection";
    - (Personal certificates) protecting the passphrase from others;
    - Notifying immediately the EG-GRID CA and any relying parties if the private key is lost or compromised;
    - Requesting revocation if the subscriber is no longer entitled to a certificate, or if information in the certificate becomes wrong or inaccurate.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

For a certificate to be issued, the subject authentication must be successful and proper as specified in this document (see section 3.2.3 and 3.2.5). Applicants will be informed about the status of their certificate whether it is issued or rejected.
Identification and authentication functions are done by the RA.
For user certificate the RA operator must authenticate the individual's identity (see section 3.2.3).
In the case of a host/service the RA should ensure that the requestor is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate (see section 3.2.5).

When submitting a request to the CA, the Subscriber types a PIN – a personal string known only to the Subscriber. When the Subscriber verifies his or her identity to the RA Operator, the Operator can

check the PIN to ensure that the request he or she is about to approve was the one made by the Subscriber. Only one-way hashes of the PINs are processed by the CA and seen by the RA Operator (unless the Subscriber chooses to reveal it to the RA Operator). 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 EG-GRID CA certificate. Upon successful authentication, the certificate request 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

If the certificate request does not meet one or more of the following criteria, it will be rejected and the requester will be informed via e-mail.

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 EG-GRID CA distinguished name scheme;
5. the distinguished name must be unambiguous and unique;
6. the key must have at least 2048 bits.

4.2.3 Time to Process Certificate Applications

Each certificate application will take no more than 5 working days to be processed.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

CA will check that identity validation is properly performed as described in 3.2.3.
CA will ensure secure communication with RAs by signed e-mails, SSL protected private web pages and voice conversations with a known person.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Applicants will be notified via e-mail when the certificate is issued and the issued certificate will be hosted at the online CA repository. The RA will receive an acknowledgment of the issuance.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Subscribers of EG-GRID CA are required to agree with the following issues:

- acknowledgment of conditions and loyalty to the procedures interpreted in this document
- permanent provision of correct information to the EG-GRID CA and avoidance of unnecessary information out of purposes of this document
- use of the certificate for only authorized purposes that are stated in this document
- admission of restrictions to liability defined in section 9.8
- admission of statements about confidentiality of information emphasized in section9.4

- key pair (public key and private key) generation using a secure method
- acceptable precautions against loss, disclosure or illegal use of the private key
- notifying EG-GRID CA in case private key is compromised or lost
- notifying EG-GRID CA in case of information change in the certificate
- notifying EG-GRID CA in case the subscriber requests to revoke the certificate

4.4.2 Publication of the Certificate by the CA

All the certificates issued by EG-GRID CA will be published at the on-line CA repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

See section 4.3.2.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers may use their certificate as stated in section 1.4. They shall:

- Use certificate issued by EG-GRID CA exclusively for legal and authorized intended purposes
- Only use certificate issued by EG-GRID CA on behalf of the person, entity, or organization listed as the subject of such a certificate
- The subscriber must discontinue use of the private key along with the certificate following the expiration or revocation of the certificate.
- Certificates must apply to unique individuals or resources.
- Subscribers must not share certificates.

4.5.2 Relying Party Public Key and Certificate Usage

Relying party shall:

- Be held responsible to understand the proper use of certificates
- Read and agree to all terms and conditions of this CP/CPS
- Verify the validity of the certificate by consulting the EG-GRID CA CRL

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

EG-GRID CA will not renew subscribers' certificate. Subscribers must follow the re-key procedure described in section 3.3.1 and section 4.7.

4.6.2 Who may Request Renewal

See section 4.6.1.

4.6.3 Processing Certificate Renewal Requests

See section 4.6.1.

4.6.4 Notification of New Certificate Issuance to Subscriber

See section 4.6.1.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See section 4.6.1.

4.6.6 Publication of the Renewal Certificate by the CA

See section 4.6.1.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See section 4.6.1.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

The following circumstances require certificate re-key:

- expiration of subscriber's certificate,
- revocation of subscriber's certificate.
- the subscriber need to do change in the certificate parameter

4.7.2 Who may Request Certification of a New Public Key

Any subscriber holding a valid EG-GRID CA certificate can request certificate re-key. If the certificate has already expired, a certificate request procedure as described for an initial certificate request must be followed.

4.7.3 Processing Certificate Re-keying Requests

Upon receipt of the request endorsed by the appropriate RA, the EG-GRID CA will process the re-keying as it processes an initial certification request as described in section 3.3.1. The main exception is that the documentation which is valid and present at the RA does not need to be represented when requesting a new certificate through re-keying.

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 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

The same procedure will be followed as described in section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

The same procedure will be followed as described in section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

The same procedure will be followed as described in section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The same procedure will be followed as described in section 4.4.3.

4.8 Certificate Modification

Certificates must not be modified. In case of changes, the old certificate must be revoked and new certificate with new key pair must be requested as described in section 4.1

4.8.1 Circumstances 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 situations:

- the subscriber does not need the certificate any more.
- the subscriber has not obeyed the stated obligations.
- the information in the certificate is incorrect.
- the private key of a certificate is lost, compromised or suspected to be compromised.

4.9.2 Who can Request Revocation

The CA, RA, subscriber of the certificate or any other entity holding evidence of a revocation circumstance about that certificate can request revocation.

4.9.3 Procedure for Revocation Request

Revocation requests should be submitted in one of the following ways:

- by email sent to ca@grid.eun.eg

- personally at the RA/CA

All revocation requests should be properly authenticated as described in 3.4.
EG-GRID CA informs the owner of a revoked certificate and the appropriate RA of the issued revocation.

4.9.4 Revocation Request Grace Period

All revocation requests shall be issued and executed without delay but within one working day after detection of loss or compromise of the private key pertaining to the certificate.

4.9.5 Time within which CA must Process the Revocation Request

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

4.9.6 Revocation Checking Requirement for Relying Parties

A relying party must verify the certificate that it uses considering the most recently issued CRL.

4.9.7 CRL Issuance Frequency

See section 2.3.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/status Checking Availability

At present, no on line service for this purpose is available.

4.9.10 On-line Revocation Checking Requirements

See section 4.9.9.

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

EG-GRID CA does not suspend certificates.

4.9.14 Who can Request Suspension

See section 4.9.13.

4.9.15 Procedure for Suspension Request

See section 4.9.13.

4.9.16 Limits on Suspension Period

See section 4.9.13.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

EG-GRID CA online repository contains the root CA certificate, list of valid certificates and list of revoked certificates (CRL). All of them are continuously updated.

4.10.2 Service Availability

The on-line repository is available on a 24x7 basis, liable to reasonable scheduled maintenance.

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

EG-GRID CA keys are not given on escrow.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

See section 4.12.1.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The EG-GRID CA operates in a controlled Data Center at the Egyptian Universities Network Location. The details of the address are in section 1.5.1.

5.1.2 Physical Access

Physical access is only granted to authorized personnel of the EG-GRID CA.

5.1.3 Power and Air Conditioning

The building has an air condition system and the CA machines are connected to a UPS system.

5.1.4 Water Exposures

The building is in a zone not subject to floods.

5.1.5 Fire Prevention and Protection

The Data Center has a fire alarm system.

5.1.6 Media Storage

Backups are to be stored in removable storage media. Removable media are kept in locked safe places to which only authorized personnel have access.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural Controls

5.2.1 Trusted Roles

Personnel which include system and network administrators, operators and executives who are designed to oversee the CA's operations shall, for purpose of this policy, be considered as serving in trusted role.

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

Access to servers and applications is limited to the EG-GRID CA Security Personnel, who are working as Egyptian Universities Network staff.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Internal training is available and applied to the EG-GRID CA and RA operators.

5.3.4 Retraining Frequency and Requirements

EG-GRID CA will perform operational audit of the CA and RA operators once a year. Retraining is applied if the audit results are not satisfactory.

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

Operational manual for CA and RA operators is supplied to the personnel for successfully performing their task.

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

Certificate management functions:

- Certificate request
- Revocation request
- Certificate download
- CRL issuing
- All issued certificates

System management functions:

- Boot/reboot and shutdown
- Login/logout
- Backup and restore the CA database

5.4.2 Frequency of Processing Log

The log files shall be analyzed once a month, or after a potential security breach is suspected or known; whichever comes first.

5.4.3 Retention Period for Audit Log

Identity validation records must be kept at least as long as there are valid certificates based on such a validation.

5.4.4 Protection of Audit Log

Only authorized EG-GRID CA personnel are 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 kept in removable storage media in a safe place with restricted access.

5.4.6 Audit Collection System (Internal vs. External)

Audit log collection system is internal to EG-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 EG-GRID RA will archive the following items:

- Application data (certificate and revocation requests)
- Issued certificates
- Issued CRLs
- All e-mail messages correspondence with EG-GRID CA and RA
- The login/logout/reboot information of the issuing machine

5.5.2 Retention Period for Archive

Minimum retention period is three years.

5.5.3 Protection of Archive

Only authorized CA personnel are allowed to view and process records archived. All records archive are stored on off line medium.

5.5.4 Archive Backup Procedures

All archive data are copied to removable storage media.

5.5.5 Requirements for Time-stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

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

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation

5.6 Key Changeover

Lifetime of end entity certificates is 1 year. The CA's private key is changed periodically; from that

time on, the new key will be valid in order to sign new certificates or CRL lists of new certificates. The overlap of the old and new key must be at least one year. The older but still valid certificate must be available to verify old signatures and its private key must be used to sign CRLs until all the certificates signed using the associated key have expired or been revoked.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

1. If the CA private key is compromised or destroyed in some way, the CA will perform the following tasks:
    - Inform the EUGridPMA
    - Inform all the nodes, RAs and other relying parties
    - Conclude the issuance and distribution of certificates and CRLs
    - Generate a new CA certificate with a new key pair that will be soon available on the website.
2. If the RA Operator's private key is compromised or suspected to be compromised, the RA Operator or Manager must inform the CA and request the revocation of the RA Operator's certificate.
3. If the key of an end entity is lost or compromised, the RA has to be informed immediately in order to start the certificate revocation process.

5.7.2 Computing Resources, Software, and/or Data are corrupted

In order to be able to resume operation as fast as possible after the compute basis of the CA is corrupted, the following steps shall be performed:

- All CA software shall be backed-up on removable media after a new release of any of its components is installed.
- All data files of the offline CA shall be backed-up on a removable medium after each change, before the session is closed.
- If the hardware or software of the signing machine becomes corrupt, the status shall be diagnosed and suitably repaired. If there is any doubt about the extent of the damage involved, this shall imply rebuilding the machine from scratch, using original supplied parts and software distributions.

If needed, the EG-GRID CA private key stored in external media, will be restored according restore procedures (see section 6.2.4). Therefore operations should restart without need to revoke all issued certificates.

5.7.3 Entity Private Key Compromise Procedures

In case the key of an end entity or an RA is compromised, the corresponding certificate must be revoked. All relying parties known to accept the key should be informed by the owner of the key.

In case the private key of the EG-GRID CA is compromised (or suspected to be) the CA shall:

- make every reasonable effort to notify subscribers and RAs,

- terminate issuing and distributing certificates and CRLs,
- request revocation of the compromised certificate,
- generate a new CA key pair and certificate and publish the certificate in the repository,
- revoke all certificates signed using the compromised key, and
- publish the new CRL on the CA repository.

5.7.4 Business Continuity Capabilities after a Disaster

No stipulation.

5.8 CA or RA Termination

EG-GRID CA will do the following tasks before it terminates its Grid-related services:

- Inform all the subscribed users, RAs and relying parties
- Stop to issue certificates and CRLs
- Revoke all certificates
- Notify the relevant security contacts
- Declare its termination on the website
- Destroy all copies of private keys

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Keys for the EG-GRID CA root certificate are generated on a dedicated machine, not connected to any type of network. The software used for key generation is OpenSSL.
Each subscriber must generate his/her own key pair. EG-GRID CA does not generate private keys for its end-entities.

6.1.2 Private Key Delivery to Subscriber

As each applicant generates his/her own key pair, CA has no access to subscribers' private keys.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber's public key must be transferred to the EG-GRID CA in a secure manner: by online transaction from a secure web server for personal certificates or by signed e-mail for host and service certificates.

6.1.4 CA Public Key Delivery to Relying Parties

The EG-GRID CA root certificate can be downloaded from the EG-GRID CA website: http://www.grid.eun.eg

6.1.5 Key Sizes

For a user, host or service certificate the key size is 2048 bits and it is an RSA key.

The EG-GRID CA key size is 8192 bits and it is an RSA key.

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)

The keys may be used according to the type of certificate:

With a subscriber certificate for:

- Authentication
- Data and key encipherment
- Message integrity
- Session establishment
- Proxy creation and signing

With an RA certificate for:

- All activities needed for the work of an RA agent

With the CA certificate for:

- Certificates signing
- CRLs signing

The EG-GRID CA private key is the only key that can be used for signing certificates and CRLs.

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

EG-GRID CA keys are not given on escrow.

6.2.4 Private Key Backup

A backup of the EG-GRID CA private key is kept encrypted in multiple copies in USB flash drive and CD-ROM in a safe location. The password for the private key is kept separately in paper form with an access control. Only authorized CA personnel have access to the backups.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

No stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

EG-GRID CA private key is protected by a passphrase of at least 15 characters and only known by authorized CA personnel.
The subscriber is required to generate a secure passphrase, at least 12 characters long for the private key. Private Key cannot be shared and it is subscriber's responsibility to protect the private key properly.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

As a part of the certificate archival, the public key is archived.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

EG-GRID CA root certificate has a validity of twenty years. For subscribers, the maximum validity period for a certificate is one year.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

EG-GRID CA does not generate activation data for subscribers. The subscriber is required to generate a secure pass phrase, at least 12 characters long as activation data for the private key. EG-GRID CA private key is protected by a passphrase of at least 15 characters.

Host and service certificate may be stored without a passphrase. The private key is protected by the file system access control, in such a way only privileged users can access it. The key may be stored in a system-user account, provided no non-privileged users can read the key from that account.

6.4.2 Activation Data Protection

The EG-GRID CA does not have access to or generate the private keys of a subscriber. The key pair is generated and managed by the subscriber and it is subscriber's responsibility to keep the

private key secure.

The passphrase for the private key of EG-GRID CA root certificate is kept separately in paper form with an access limited to CA personnel.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

- The operating systems of CA/RA servers are protected at a high degree of security by applying all the relevant patches.
- Monitoring is performed to detect unauthorized software changes.
- System configuration is reduced to minimum.
- Machines used for RA are protected by a suitably configured firewall.
- The machine used for signing certificates is not connected to any kind of network and it is dedicated for the CA operations.

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

The signing machine is kept offline. All other CA machines are protected by a firewall and/or by removing all unnecessary services.

6.8 Time Stamping

All time stamping of entries created on the online servers at the EG-GRID CA is based on the network time provided by the time server of the EUN.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3

7.1.2 Certificate Extensions

EG-GRID CA supports and uses the following X.509 v3 certificate extensions:

For user certificates:

- Basic Constraints: CA : false
- Subject Key Identifier : hash
- Authority Key Identifier : keyid
- Key Usage : critical, digital Signature, key Encipherment
- Extended Key Usage : TLS Web Client Authentication, E-mail Protection
- CRL Distribution Points: URI
- Certificate Policies: OID
- Subject alternative name: Subscriber's E-mail address
- Netscape Cert Type : SSL Client, S/MIME
- Netscape Comment : (User role) of EG-GRID

For servers/services certificates:

- Basic Constraints: critical, ca: false
- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage: Critical, Digital Signature,key Encipherment, data Encipherment
- Extended Key Usage: ServerAuth, ClientAuth
- Netscape Comment: (Type of Server/Service) of EG-GRID
- CRL Distribution Points: URI
- Certificate Policies: OID
- Subject alternative name: Server's DNS FQDN host name

For CA certificate:

- Basic Constraints: critical, ca: true
- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage: Critical, keyCertSign, CRLSign
- CRL Distribution Points:URI

7.1.3 Algorithm Object Identifiers

The OIDs for algorithms used for signatures for certificates issued by the EG-GRID CA are according to:

- Hash Function: id-sha1 1.3.14.3.2.26
- RSA Encryption: rsaEncryption 1.2.840.113549.1.1.1
- Signature Algorithm: sha1WithRSAEncryption 1.2.840.113549.1.1.5

7.1.4 Name Forms

The subject name is of the X.500 name type. It has one of the following forms:

Issuer (EG-GRID CA)

"C=EG, O= EG-GRID, CN= EG-GRID Certification Authority ".

- **User**

  "C=EG, O=EG-GRID, OU=Users, CN=commonName",
  where the commonName must be the Forename and the Surname of the subject.

- **Host**

  "C=EG, O=EG-GRID, OU=Host, CN=commonName",
  where the commonName must be the DNS FQDN of the host.

- **Service**

  "C=EG, O=EG-GRID, OU=Service, CN=commonName",
  where the commonName must be the application followed by the FQDN.

The Distinguished Name must be unique for each subject certified by the EG-GRID CA. If the name presented by the subscriber is not unique, additional numbers or letters are appended to the commonName to ensure uniqueness.
The canonical name in the certificate subject must be obtained from the real subject name.
Certificates must apply to unique individuals or resources. Subjects must not share certificates.

7.1.5 Name Constraints

There are no other name constraints than those that are to be derived from the stipulations in 7.1.4, 3.1.2 and 3.1.1.

7.1.6 Certificate Policy Object Identifier

The OID of this CP/CPS is: 1.3.6.1.4.1.38589.1. 1.0

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)

The EG-GRID CA must create and publish X.509 version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The EG-GRID CA will issue complete CRLs for all certificates issued by itself independently of the reason for the revocation. The reason for the revocation will not be included in the individual CRL entries.
The CRL must include the date by which the next CRL will be issued. A new CRL must be issued before this date if new revocations are issued.
The CRL extensions that must be included are:

- the authority key identifier
- the CRL number

7.3 OCSP Profile

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 EG-GRID CA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.
The CA shall at least once a year assess the compliance of the procedures of each RA with the CP/CPS document in effect.
The CA accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document.

8.2 Identity/qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

8.5 Actions Taken as a Result of Deficiency

The EG-GRID CA must take immediate action if the assessment reveals a deficiency related to provisions of the CP/CPS document. If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem should be revoked immediately.

8.6 Communication of Results

No stipulation.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

For any service supplied, EG-GRID CA charges no fee.

9.1.2 Certificate Access Fees

See section 9.1.1.

9.1.3 Revocation or Status Information Access Fees

See section 9.1.1.

9.1.4 Fees for Other Services

See section 9.1.1.

9.1.5 Refund Policy

See section 9.1.1.

9.2 Financial Responsibility

EG-GRID CA rejects any financial or any other sort of responsibility for damages arising from its operations.

9.2.1 Insurance Coverage

Not applicable.

9.2.2 Other Assets

Not applicable.

9.2.3 Insurance or Warranty Coverage for End-entities

Not applicable.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Not applicable.

9.3.2 Information not within the Scope of Confidential Information

Not applicable.

9.3.3 Responsibility to Protect Confidential Information

Not applicable.

9.4 Privacy of Personal Information

EG-GRID CA does not collect any confidential or private information except for the case when CA or RA archives copies of ID documents for identity validation of a user certificate request. EG-GRID CA guarantees that this personal information will not be used for any other purposes.

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

The information provided by the subscriber to verify his/her identity will be kept confidential.

9.4.3 Information not Deemed Private

Information stated in issued certificates and CRLs is not considered to be confidential. EG-GRID CA collects the following information, which is not deemed as private, from the subscriber:

- subscriber's name,
- subscriber's e-mail address,
- subscriber's organization,
- subscriber's certificate.

9.4.4 Responsibility to Protect Private Information

The responsibility to protect private information rests with EG-GRID CA and all its accredited RAs.

9.4.5 Notice and Consent to Use Private Information

No stipulation.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA will not disclose confidential information to any third party unless authorized to do so by the subscriber or when required by Egyptian law enforcement officials who exhibit regular warrant.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Parts of this document are inspired by:

- RFC 3647
- CERN CA Policy
- TR-GRID CP/CPS
- INFN CP/CPS
- HIAST CP/CPS

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

No stipulation.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

The EG-GRID CA uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness.
The EG-GRID CA cannot be held responsible for any misuse of its certificate by a subscriber or any other party who got in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.
Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

9.8 Limitations of Liability

Based on this document, EG-GRID CA accepts neither explicit nor implicit liability for its actions. EG-GRID CA does not guarantee the security or appropriateness of a service that is identified by a EG- GRID certificate. The certification service is run with an optimum level of security and it tries to supply the best-effort conditions. It assures its procedures described in this document, but it will take no responsibility for the improper use of the issued certificates.
EG-GRID CA rejects any financial or any other sort of responsibility for damages arising from its operations.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This document becomes effective after its publication on the website of EG-GRID CA starting at the date announced there. No term is set for its expiration.

9.10.2 Termination

This CP/CPS remains effective until it is superseded by a newer version.

9.10.3 Effect of Termination and Survival

Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see section 1.5.4).

9.12.2 Notification Mechanism and Period

Subscribers will not be informed in advance if the CP/CPS document is changed. Changes are announced to EUGridPMA and get approved before the new CP/CPS is published on the website. Changes are published on the website as well.

9.12.3 Circumstances under which OID must be changed

OID must change whenever the CP/CPS document is updated.

9.13 Dispute Resolution Provisions

Disputes arising out of the CP/CPS shall be resolved by the manager of EG-GRID CA.

9.14 Governing law

The EG-GRID CA and its operation are subject to the Egyptian law. All legal disputes arising from the content of this CP/CPS document, the operation of the EG-GRID CA and its published RAs, the use of their services, the acceptance and use of any certificate issued by EG-GRID CA shall be treated according to law of Egypt.

9.15 Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of EG-GRID CA certificate must comply with the Egyptian law. Activities initiated from or destined for another country than Egypt must also comply with that country's law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS document supersedes any prior agreements, written or oral, between the parties covered by this present document.

9.16.2 Assignment

No provisions.

9.16.3 Severability

Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see section 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No provisions.

9.16.5 Force Majeure

Events that are outside the control of the EG-GRID CA will be dealt with immediately by the EUGridPMA.

9.17 Other provisions

No stipulation.