National Center for Scientific
and Technical Research

Certification Authority

MaGrid CA

Certificate Policy
and
Certification Practice Statement

Document OID: 1.3.6.1.4.1.26529.10.1.1.0

Version 1.1.0

January 10, 2007.

CONTENTS

1 INTRODUCTION

This document is structured according to RFC 3647. Not all sections of RFC 3647 are used. Sections that are not included have a default value of " No stipulation" . This document describes the set of rules and procedures established by CNRST (Centre National pour la Recherche Scientifique et Technique) for the operations of the Moroccan Gird Certification Authority (MaGrid CA) service. The data center housing the MaGrid CA server is located in Rabat.

This document will include both the Certificate Policy and the Certification Practice Statement for the MaGrid CA. The general architecture is a single certification authority and several registration authorities. The certification authority is a stand-alone self signed CA.

1.1 OVERVIEW

MaGrid is the infrastructure to support e-science activities provided by the CNRST according the Moroccan National Grid Initiative.

This document describes the set of rules and operational practices that shall be used by the MaGrid CA, the Certification Authority (CA) for MaGrid, for issuing certificates. This and any subsequent CP/CPS document can be found on its web site http://www.magrid.ma/ca/

1.2 DOCUMENT NAME AND IDENTIFICATION

Title:		MaGrid CA Certificate Policy (CP) and Certification Practice Statement (CPS)
Version:		1.1.0, January 10, 2007
Expiration:		This document is valid until further notice.
OID assigned:		1.3.6.1.4.1.26529.10.1.1.0
OID structure:		
	1.3.6.1.4.1	**IANA**
		Iso(1). org(3). dod(6). internet(1). private(4). enterprise(1)
	26529	CNRST
	10	MaGrid CA
	1	CP/CPS
	1	Major CP/CPS version number
	0	Minor CP/CPS version number

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

The MaGrid CA does not certificate to subordinate Certification Authorities.

1.3.2 Registration Authorities

The MaGrid CA does not perform the role of RA.

Each participant in MaGrid may appoint an individual who will act as RA for its own members and servers. It's also possible that one RA can manage members and servers for other participants in MaGrid if no RA exists for these users.

The list of RAs for the MaGrid is available from the MaGrid website

http://www.magrid.ma/ca/

1.3.3 Subscribers

Subscribers eligible for certification from the MaGrid CA are:

a) Moroccan academic organizations (e.g. public and private universities and educational institutes);

b) Moroccan academic research centers (either public or private, non-profit ones);

c) Other organizations with research and development (R&D) affiliations with one of the above classes of organization.

The subject entities for certificates are of the following types:

a) Employees, researchers and students related with the above organizations; or,

b) Computer systems and services related with the above organizations;

1.3.4 Relying parties

Relying parties may be:

- natural persons receiving signed e-mails, or accessing hosts or services
- host to which certificate owners login or send processes or jobs
- services called by owners of a certificate

1.3.5 Other participants

No stipulation.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate certificate uses

CA certificate may only be used to issue certificates and for checking certificates that claim to be issued by the MaGrid CA.

The end-entity certificate may be used for any application that is suitable for X.509 certificates, in particular:

- authentication of users, hosts and services
- authentication and encryption of communications
- authentication of signed e-mails
- authentication of signed objects

They may only be used or accepted for actions authorized by the certificate keys.

1.4.2 Prohibited certificate uses

The certificates issued by MaGrid CA must not be used for financial transactions.

They must not be used for purposes that violate Moroccan law or the law of the country in which the target entity (i.e. application or host to use, addressee of an e-mail) is located.

1.5 POLICY ADMINISTRATION

1.5.1 Organization administering the document

The MaGrid CP/CPS was authored and is administered by MARWAN/MaGrid department of CNRST, located in Rabat (Morocco).

CNRST is responsible for registration, maintenance, and interpretation of this CP/CPS. It is reachable at:

CNRST
52, Av Omar Ibn AlKhattab BP 8027.Agdal -10102
Rabat
Morocco
Phone : +212 37 68 62 33/34
Fax : +212 37 68 62 35
E-mail : magrid@cnrst.ma
Home page : http://www.cnrst.ma

1.5.2 Contact Person

The CA manager (contact person for questions related to this policy document) is:

Redouane Merrouch
CNRST-MaGrid,
52, Av Omar Ibn AlKhattab BP 8027.Agdal 10102
Rabat
Morocco.
Phone : +212 37 68 62 23
Fax : +212 37 68 62 35
E-mail : merrouch@cnrst.ma

1.5.3 Person determining CPS suitability for the policy

The manager of the MaGrid CA (see 1.5.2) is responsible for determining the CPS suitability for the policy.

1.5.4 CPS approval procedures

The approved document shall be submitted to EUGridPMA for acceptance and accreditation.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

The key words " MUST" , " MUST NOT" , " REQUIRED" , " SHALL" , " SHALL NOT" , " SHOULD" , " SHOULD NOT" , " RECOMMENDED" , " MAY" , and " OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Activation Data

Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (i.e., a PIN, a passphrase, or a manually-held key share).

Authentication

The process of establishing that individuals, organizations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organization which applies for or seeks access to something under a certain name is, in fact, the proper individual or organization. This process corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service providing assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.

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. That entity / system issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA)

Certificate Policy (CP)

A named set of rules indicating 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.

Certification Practice Statement (CPS)

A statement of the practices, which a certification authority employs in issuing certificates.

Community RM

One or more RMs that serve multiple, low request rate, sites / Virtual Organizations.

Host Certificate

A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine. Host Certificates are used internally by the PKI service and are not issued to other sites/VOs

Identification

The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organization corresponds to a real world identity of an individual or organization, and (2) establishing that an individual or organization applying for or seeking access to something under that name is, in fact, the named individual or organization.

A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.

Issuing Certification Authority (Issuing CA)

In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Person Certificate

A certificate used for authentication to establish a Grid Person Identity. It will represent an individual person.

Policy Qualifier

The Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Point of Contact

The member of a site/VO RA that has been chosen to handle all communications about policy matters with the Grid manager.

Private RM

RMs that serve high certificate request rate sites / Virtual Organizations, and that are operated by the site/VO.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Registration Agent (RAg) or " Agent"

RAg is the entity that interacts with the RM in order to cause the CA to issue certificates.

Registration Manager (RM)

The RM is a front-end Web server for the CA that provides a Web user interface for CA subscribers and agents. The RM forwards certificate signing requests to the actual CA to issue X.509 certificates.

Relying Party

A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Repository

A storage area, usually on-line, which contains lists of issued certificates, CRLs, policy documents, etc.

Service Certificate

A certificate for a particular service running on a host. It will represent a single service on a single host.

Subscriber

Or sometimes called End Entity is a person or server to whom a digital certificate is issued.

Virtual Organization (VO)

An organization that has been created to represent a particular research or development effort independent of the physical sites that the Scientist or Engineers work at. (i.e. PPDG, FNC, EDG, etc).

1.6.2 Acronyms

C	Country
CA	Certification Authority
CN	Common Name
CDROM	Compact Disc Read Only Memory
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguish name
EUgridPMA	The European Grid Authentication Policy Management Authority in e-Science, http://www.eugridpma.org/
MaGrid CA	Moroccan Grid Certification Authority
MARWAN	Moroccan Academic and Research Network
CNRST	National Center for Scientific and Technical Research
LDAP	Lightweight Directory Access Protocol
MIME	Multi-purpose Internet Mail Extensions
NTP	Network Time Protocol
O	Organization
OU	Organizational Unit
PKI	Public Key Infrastructure
RA	Registration Authority
SSL	Secure Sockets Layer
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier
URL	Universal Resource Locator
OID	Object Identifier
FQDN	Fully Qualified Domain Name

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The online repository of information from the MaGrid CA is accessible at the URL

http://www.magrid.ma/ca/

2.2 PUBLICATION OF CA INFORMATION

The MaGrid CA will operate a secure online repository that contains:

1. The MaGrid CA' s certificate, and all previous ones necessary to check still valid certificates,
2. The certificates issued by the PKI,
3. A Certificate Revocation List,
4. A copy of the most recent version of this policy and all previous versions,
5. The official contact e-mail address and physical contact address,
6. Other information deemed relevant to the MaGrid CA service.

2.3 TIME OR FREQUENCY OF PUBLICATION

All information published shall be up-to-date.

Certificates will be published to the MaGrid CA repository as soon as issued.

The certificate revocation list (CRL) shall have a lifetime of at most 30 days. The MaGrid CA must issue a new CRL at least 7 days before expiration or immediately after having processed a revocation, whichever comes first. A new CRL must be published immediately after its issuance.

This CP/CPS will be published whenever it is updated.

2.4 ACCESS CONTROL ON REPOSITORIES

The online repository is maintained on a best effort basis and is available substantially on a 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance. Outside the period 08:30-16:30 Monday-Friday it may run unattended "at risk"

The MaGrid CA does not impose any access control on its CP/CPS, its certificate, issued Certificates or CRLs.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of names

The subject names for the certificate applicants shall follow the X.500 standard:

1. in case of user certificate the subject name must include the persons name in the CN field;

2. in case of host certificate the subject name must include the DNS FQDN in the CN field;

3. in case service certificate the subject name must include the service name and the DNS FQDN separated by a / in the CN field.

Any name under this CP/CPS is in the form of "C=MA, O=MaGrid, OU=unit". The following part is the "CN" which is distinguished for each person or each host.

Illustration of a full subject distinguished name for a user:
C=MA, O=MaGrid, OU=Marwan, CN=Nabil Talhaoui

Illustration of a full subject distinguished name for a host:
C=MA, O=MaGrid, OU=Marwan, CN=host1.marwan.ma

Illustration of a full subject distinguished name for a service:
C=MA, O=MaGrid, OU=Marwan, CN=ldap/ldap.marwan.ma

3.1.2 Need for names to be meaningful

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber. Subscribers must choose a representation of their names in the permitted character set (see 3.1.1). The name must not refer to a role. Subscribers can neither be anonymous nor pseudonymous.

3.1.3 Anonymity or pseudonimity of subscribers

No natural person certificates shall be issued to roles or functions, only to named and identified persons.

3.1.4 Rules for interpreting various name forms

See section 3.1.1.

3.1.5 Uniqueness of names

The Distinguished Name must be unique for each subject name certified by the MaGrid CA service. The MaGrid does this task before request is generated.

In this policy two names are considered identical if they differ only in case. In other words, case must not be used to distinguish names.

If necessary, extra characters may be affixed to the original name to guarantee the uniqueness of the subject name.

Certificates must apply to unique individuals or resources.

Subscribers must not share certificates.

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

The MaGrid CA proves possession of the private key that is the companion to the MaGrid CA root certificate by issuing certificates and signing CRLs.

The MaGrid CA verifies the possession of the private relating to certificates requests by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to requester. A cryptographic challenge-response exchange may be used to prove possession of the private key at any point in time before certification of subscriber.

The MaGrid CA will not generate the key pair for subscribers and will not accept or retain private keys generated by subscribers.

3.2.2 Authentication of organization identity

The RA shall verify that the requesting party's organization or a unit of an organization is entitled (see 1.3.3) to get a certificate from the MaGrid CA and that it consents to the request.

An organization/unit that wants to get a certificate for a natural person, a server or a service, has to announce this officially to the appropriate RA. The RA has to ascertain that the organization or organizational unit exists and is entitled to request an MaGrid certificate. It must also get competent information on who is entitled to sign on behalf of the institution.

3.2.3 Authentication of individual identity

In order to enable the RA to authenticate the individual's identity the latter must meet in person with the RA and present an officially recognized document proving the requesting party's identity. Only documents accepted by Moroccan law (Moroccan national identity card, driving license or passport) will be accepted.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of Authority

Any organization or unit willing to apply for MaGrid certificates shall appoint one or more representatives who are entitled to request server or service/application certificates and answer all questions related to natural-person certificate requests.

These representatives shall be the first in their organization/unit to request individual certificates according to the provisions outlined in 3.2.3. The signatures of these individuals with the private

key associated with the certified public key shall be sufficient for all future information exchanges with or requests from that organization/unit.

When the organization/unit rescinds the individual's authorization it has to inform the RA and the MaGrid CA in the same way as it has made the authorization known.

3.2.6 Criteria of interoperation

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and authentication for routine re-key

Expiration warnings will be issued to subscribers when re key time arrives.

Rekey before the certificate expires can be done using a secure web interface. After expiration of the certificate no rekey is possible; a new application for initial registration must be made instead.

3.3.2 Identification and authentication for re-key after revocation

After revocation of a key, no re-key is possible. A new application for initial registration must be made.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Unless the revocation request originates from the MaGrid CA because it has independently verified that a key compromise has occurred, the revocation request has to be verified and the requesting party has to be authenticated.

Such a request coming from an RA must be made in a signed transfer sent to the CA. Before revoking a certificate the MaGrid CA has to authenticate the source of the request as it did for the request for certification.

In case of emergency the revocation can be initiated via oral communication with the appropriate RA or the MaGrid CA. The RA or the MaGrid CA have to use their best effort to authenticate the request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Who can submit a certificate application

The MaGrid CA issues certificates to members of MaGrid for:

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

4.1.2 Enrollment process and responsibilities

The requesting party generates the key pair with a size of at least 1024 bit on their system through the form provided at the MaGrid CA web site. After the form has been completed the encrypted private key will be stored on the system where the browser runs, in a file only accessible to the requester (if the operating system allows such a restriction), and the CSR will be stored in the LDAP system.

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 strong passphrase of at least 15 characters;
    - (Personal certificates) protecting the passphrase from others;
    - Notifying immediately the MaGrid CA and any relying parties if the private key is lost or compromised;

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing identification and authentication functions

For the natural persons the RA operator must authenticate the individual's identity (see 3.2.3). In the case of a server/service request it must also check that the user is a representative (see 3.2.5) of the organization or unit responsible for the host.

4.2.2 Approval or rejection of certificate applications

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

1. the certificate application must be authenticated first by the RA as described in section 4.2.1;

2. the subject must apply the certificate request within 2 working days after the successful authentication performed by the RA;

3. the subject must be an acceptable subscriber entity, as defined by this Policy;
4. the request must obey the MaGrid CA distinguished name scheme;
5. the distinguished name must be unambiguous and unique;
6. the key must have at least 1024 bits.

If the certificate request does not meet one or more of the above criteria, it will be rejected and signed notification e-mail will be sent by the RA to the subject with carbon copy to magrid-ra@magrid.ma

4.2.3 Time to process certificate applications

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

4.3 CERTIFICATE ISSUANCE

4.3.1 CA actions during certificate issuance

The CSR shall be transfered to the computer which holds the private key of MaGrid CA and which is not connected to any network. On this system the certificate is created and signed. The signed certificate shall then be transfered back to the MaGrid online server.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The MaGrid system shall then send a mail to the requesting party with the URL of the certificate download page. It shall also send an acknowledgment of the issuance to the appropriate RA.

A certificate will be valid for one year from the date of issuance or less than one year in specific cases (i.e. if the applicant's affiliation to the organization/unit is known to be less than one year).

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct constituting certificate acceptance

The requesting party shall notify the MaGrid CA of the rejection of a certificate, explaining the MaGrid CA and the RA the reasons for the rejection. Certificates whose rejection have not been received by the MaGrid CA within a week shall be considered accepted.

4.4.2 Publication of the certificate by the CA

The MaGrid CA will publish on its web server certificates as soon as they are issued.

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

Certificates issued by the MaGrid CA and their associated private keys must only be used according to the permissions and prohibition stated in section 1.4. They must only be used

according to the key usage fields of the certificate. When a certificate is revoked or has expired the associated private key shall not be used anymore.

4.5.2 Relying party public key and certificate usage

A relying party must, upon being presented with a certificate issued by the MaGrid CA check

- its validity by
  - checking that it trusts the CA that issued the certificate,
  - checking that the certificate hasn't expired,
  - consulting the MaGrid CA CRL in effect at the time of use of the certificate.
- the appropriate usage as outlined in the CP pointed to by the certificate and in the usage keys included in the certificate.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for certificate renewal

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

4.6.2 Who may request renewal

See 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

Subscribers must regenerate their key pair in the following circumstances:

1. expiration of their certificate signed by the MaGrid CA;
2. revocation of their certificate by the MaGrid CA;
3. compromise of their private key.

4. change in the certificate parameters.

4.7.2 Who may request certification of a new public key

Same as in section 4.1.1

4.7.3 Processing certificate re-keying requests

Expiration warnings will be issued to subscribers when re key time arrives. Re key before expiration can be accomplished by sending a re key request signed with the current user certificate. Re key after expiration follows the same authentication procedure as for a new certificate. At least once every 3 years the subscriber must go through the same authentication procedure as the one described for a new certificate.

In case the request for a new certificate is due to revocation or compromise of certificate the subscriber must follow the same procedure as the one described in for a new one.

4.7.4 Notification of new certificate issuance to subscriber

Same as in section 4.3.2

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Same as in section 4.4.1

4.7.6 Publication of the re-keyed certificate by the CA

Same as in section 4.4.2

4.7.7 Notification of certificate issuance by the CA to other entities

Same as in section 4.4.3

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstance for certificate modification

Certificates must not be modified. The old certificate must be revoked, and a new key pair must be generated and a request for the modified certificate contents must be submitted with the new public key.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for revocation

A certificate will be revoked in the following circumstances:

1. the subject of the certificate has ceased being an eligible end entity for certification, as described in this policy;
2. the subject does not require the certificate any more;
3. the private key has been lost or compromised;
4. the information in the certificate is wrong or inaccurate;
5. the system to which the certificate has been issued has been retired;
6. the subject has failed to comply with the rules of this policy.

4.9.2 Who can request revocation

A certificate revocation can be requested by

1. the owner of the certified key
2. the MaGrid CA or any RA that has proof of a compromise
3. the organization that wants to revoke its consent to its inclusion in the certificate
4. the Registration Authority which authenticated the holder of the certificate;
5. the holder of the private key;
6. any person presenting proof of knowledge that the subscriber's private key has been compromised or that the subscriber' s data have changed.

4.9.3 Procedure for revocation request

Unless the MaGrid CA acts on its own a revocation request must be made by:

1. the owner of the certificate, properly authenticated, using the online revocation facilities. In case of emergency, the owner of the certificate must go to the RA as soon as possible and ask the appropriate RA to request revocation.
2. the RA administrator using a secure web interface

Before revoking a certificate the MaGrid CA shall authenticate the source of the request by using signed e-mails.

4.9.4 Revocation request grace period

There is no grace period defined for a revocation request. The MaGrid CA shall process the authenticated request with priority and publish the revocation as fast as possible.

4.9.5 Time within which CA must process the revocation request

The MaGrid CA must process all revocation requests without delay within 1 working day.

4.9.6 Revocation checking requirement for relying parties

Before using a certificate the relying party must validate it against the CRL most recently published in the MaGrid CA repository.

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 30 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

The CRL shall be copied to a removable device immediately after creation on the offline CA system and transfered without delay to the on-line repository.

4.9.9 On-line revocation/status checking availability

The latest CRL is always available from the MaGrid web site. The MaGrid CA shall publish the CRL in effect in its repository (see 2.1). No other on-line checking is available now.

4.9.10 On-line revocation checking requirements

Relying parties must check the CRL before they use and trust a certificate. No access control shall limit the possibility to check the CRL.

4.9.11 Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available. Except for informing the owner of a newly revoked certificate and the appropriate RA of the issued revocation, no advertisement of a new CRL other than its publication in the MaGrid CA repository will be made.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

MaGrid 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

The MaGrid CA shall store in its public repository and make them available via its web site:

- the root CA certificate
- all valid certificates, and
- the most up-to-date CRL

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

The subscription ends with the expiry of the certificate if it is not renewed before that date. A subscription may end earlier if the subscriber requests a revocation of it's certificate.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key escrow and recovery policy and practices

No key escrow or recovery services are provided. The key owner must take all steps to prevent a loss.

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

The MaGrid CA is located at the MARWAN/MaGrid Department of the CNRST in Rabat.

The MaGrid CA is offline at all times and in a safe when not in use. CNRST maintains a limited access procedure to the system. All accesses to the server are limited to the MaGrid CA staff and Marwan staff.

The MaGrid CA is run on Scientific Linux system.

5.1.1 Site location and construction

The MaGrid CA is located at the following address:

CNRST
52, Av Omar Ibn AlKhattab BP 8027.Agdal -10102
Rabat
Morocco

5.1.2 Physical access

The CA operates in a controlled environment, where access is restricted to authorized people and logged. The machine hosting it is kept locked in a safe and the private key is locked in a different safe.

5.1.3 Power and air conditioning

The online machine operates in an air conditioned environment and is not rebooted or power-cycled except for essential maintenance.

The signing machine is switched off between signing operations and operates in an air conditioned environment.

The MaGrid CA signing machine and the online machine are both protected by uninterruptable power supplies

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

MaGrid CA facilities adhere to the Moroccan law regarding fire prevention and protection in public buildings.

5.1.6 Media storage

1. The MaGrid CA private key is kept in several removable storage media;

2. Backup copies of CA related information are kept in magnetic tape cartridges, floppies and CD-ROM.

3. Removable media are stored in locked safe places to which only authorized personnel have access

5.1.7 Waste disposal

Waste containing data to be protected (cryptographically relevant data like private keys or passphrases, or personal data) shall be disposed off in a way to guarantee that the information may not be re-used.

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 MaGrid 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

One person per task.

5.2.3 Identification and authentication for each role

No stipulations.

5.2.4 Roles requiring separation of duties

No stipulations.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, experience, and clearance requirements

All MaGrid CA personnel shall have system administrator or analyst experience.

5.3.2 Background check procedures

- All access to the servers and applications that comprise the MaGrid service is limited to MARWAN/MaGrid staff.
- The RA Manager must be an employee of the Physical Organization hosting that Registration Authority and must be appointed by an Authority responsible for a Department within that physical organization. The RA Manager has to be a member of that Department. The Authority will make a declaration to the CA Manager in writing on the organization's headed note paper. The information that must be contained in this letter is defined by the CA Manager.

- The RA Operator must be an employee of the site hosting that Registration Authority and will be appointed by the RA Manager concerned. The RA Manager will make a declaration to the CA Manager in writing on the organization's headed note paper. If the RA Operator is appointed in a different department from the RA Manager then the letter must be countersigned by an authority for the department in which the Operator is appointed. The information that must be contained in this letter is defined by the CA Manager. RA Operators must have certificates and must adhere also to the subscribers' Obligations.
- An RA Manager may appoint himself/herself as an RA Operator.
- An RA Manager may appoint any number of RA Operators.

5.3.3 Training requirements

Internal training is given to MaGrid CA/RA operators

5.3.4 Retraining frequency and requirements

Retraining shall be mandatory when new software or features, as well as new organizational procedures are introduced.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

In the event of unauthorized actions, abuse of authority or unauthorized use of entity systems by the CA or RA Operators, the CA manager may revoke the privileges concerned.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

All MaGrid CA personnel shall be provided with all documentation required for successfully performing their task.

- It is the responsibility of the CA Manager to provide the CA Operators with a copy of the "MaGrid CA Operator's Procedure".
- It is the responsibility of the CA Manager to provide the RA Manager with a copy of the "MaGrid RA Manager's Procedure".
- It is the responsibility of the RA Manager to provide the RA Operator with a copy of the "MaGrid RA Operator' s Procedure"

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of events recorded

The following events shall be recorded:

- MaGrid CA host
    - login / logout / reboot
    - creation and signing of certificates
    - revocation of certificates
    - CRL issues
- MaGrid web online server
    - receipt of certificate request
    - issued certificates
    - receipt of certificate revocation request
    - validation of certificate request from RA
    - export of CSR from RA
    - revocation of certificate
    - CRL issues

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

The minimal retention period for the audit logs is 3 years.

5.4.4 Protection of audit log

The audit logs shall only be accessible to the MaGrid CA operators and managers. The protection shall be state-of-the-art best effort.

5.4.5 Audit log backup procedures

The audit logs shall be backed-up on a removable medium every night except on weekends and holidays when no activity happens on the offline host and only read access to the online repositories happens on the online server.

5.4.6 Audit collection system (internal vs. external)

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

5.4.7 Notification to event-causing subject

Not defined

5.4.8 Vulnerability assessments

Not defined

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

See 5.4.1

5.5.2 Retention period for archive

The minimum retention period is 3 years.

5.5.3 Protection of archive

The archive shall be accessible to the MaGrid CA operation and management personnel only.

5.5.4 Archive backup procedures

Records shall be backed up on removable media, which shall be stored in a room with restricted access.

5.5.5 Requirements for time-stamping of records

All event records shall bear a time-stamp.

5.5.6 Archive collection system (internal or external)

The archive collection system is internal to the MaGrid CA.

5.5.7 Procedures to obtain and verify archive information

Not defined.

5.6 KEY CHANGEOVER

To avoid interruption of validity of subordinate keys, the new ca private key is generated one year before the expiration of the old key. The new public key is available on the on-line repository, and new certifactes can be issued.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and compromise handling procedures

- If the keys of an end entity are lost or compromised due to corruption of their computing basis, the appropriate RA must be informed immediately in order to start the certificate revocation process.
- If an 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.
- If the CA' s private key is (or suspected to be) compromised, the CA will:
    - Inform the Registration Authorities, subscribers, relying parties, and cross-certifying CAs of which the CA is aware
    - Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key

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

The CA will take best effort precautions to enable recovery.

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 any part of the running system is corrupted, a functioning hardware shall be loaded with the latest state of the software and data backed-up on a readonly medium and estimated to be uncorrupted. If not all encrypted copies of the MaGrid CA private key are destroyed or lost, and are not compromised, the operation shall be re-established as soon as possible 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 b informed by the owner of the key.

In case the private key of the MaGrid 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 MaGrid CA repository.

5.7.4 Business continuity capabilities after a disaster

The MaGrid CA is located inside a building that is part of governmental facilities for research and higher education. The plans for business continuity and disaster recovery for governmental activities related to research and education are applicable.

5.8 CA OR RA TERMINATION

Before MaGrid CA terminates its services, it will:

- Inform the Registration Authorities, subscribers and relying parties the CA is aware;
- Inform the EUGridPMA;
- Make information of its termination widely available;
- Stop issuing certificates

- Revoke all certificates
- Issue an publish CRL
- Destroy its private keys and all copies

An advance notice of no less than 60 days will be given in the case of normal (scheduled) termination. The CA Manager at the time of termination shall be responsible for the subsequent archival of all records as required in section 5.5.2.

The CA Manager may decide to let the CA issue CRLs only during the last year (i.e. the maximal lifetime of a subscriber certificate) before the actual termination; this will allow subscribers' certificates to be used until they expire. In that case notice of termination is given no less than one year and 60 days prior to the actual termination, i.e. no less than 60 days before the CA ceases to issue new certificates.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key pair generation

The key pair for the MaGrid CA is generated by authorized CA staff on a computer which is not connected to the network. The keys are generated by software using OpenSSL.

The key pairs for natural-person (including RA agents), host or service certificates are generated by the requesting parties themselves on their system (web interface).

6.1.2 Private key delivery to subscriber

Each subscriber must generate his/her own key pair using the MaGrid web interface. The CA does not generate private keys for its subscribers.

6.1.3 Public key delivery to certificate issuer

Subscribers public keys are delivered to the issuing CA by the SSL protected HTTP protocol via the MaGrid web interface.

6.1.4 CA public key delivery to relying parties

The CA certificate (containing its public key) is delivered to subscribers by online transaction from the MaGrid online web server. It can be downloaded from the repository (see 2.1).

6.1.5 Key sizes

Keys of length less than 1024 bits are not accepted. The MaGrid CA key is of length 2048 bits.

6.1.6 Public key parameters generation and quality checking

Not defined.

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 an end-entity certificate for
    - authentication
    - non-repudiation
    - data and key encipherment
    - message integrity
    - session establishment
    - proxy creation and signing
- With the self-signed CA certificate
    - certificate signing
    - CRL signing

- Certificate revokation

The CA's 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

End entities shall use the web form available on the MaGrid web site for key and CSR generation.

The MaGrid CA private key is generated using OpenSSL.

Each CA operator shall have his/her own personal copy of the CA private key encrypted with a passphrase of at least 15 characters and only known to him/her. These encrypted private keys shall be stored on the offline computer of the MaGrid CA.

An extra instance of the private key encrypted with a randomly generated passphrase of at least 15 characters shall be stored on removable media which must be deposited in a safe and locked up place; the passphrase shall be stored on a different removable media or written down, and the media or paper shall be placed in a sealed envelop and stored in a secure place.

No instance of the private CA key (plain or encrypted) shall reside on the permanent disc of any computer that is online.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

Private keys must not be escrowed.

6.2.4 Private key backup

All backup copies of the CA private key are kept at least as secure as the one used for signing (i.e. encrypted, and on media locked in a safe). The passphrase for activating the backup is locked in a different safe from the one containing the encrypted key.

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

The CA private key is activated by a passphrase which, for emergencies, is kept in a sealed envelope in a safe. The safe which contains the passphrase does not contain any copy of the private key.

6.2.8 Method of activating private key

The CA private key is activated is done by providing the passphrase.

6.2.9 Method of deactivating private key

The plain private key shall only be stored in RAM and erased when the activity for which it is needed is finished.

6.2.10 Method of destroying private key

See 6.2.9.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public key archival

The CA archives all issued certificates on removable media that is stored offline in a secure vault.

6.3.2 Certificate operational periods and key pair usage periods

There is no stipulation as to the validity of the generated key pair. Only the validity of the certificate issued by the MaGrid CA is defined by this CP/CPS document.

Subscribers' certificates have a validity period of one year or less if the affiliation of the requesting party to the group participating in MaGrid is less than one year.

The CA certificate has a validity period of 10 years.

6.4 ACTIVATION DATA

6.4.1 Activation data generation and installation

Each private key are protected by a strong passphrase consisting of at least 15 characters.

6.4.2 Activation data protection

All MaGrid CA Operators know the activation data for the CA private key. No other person knows the activation data. However, the activation data for the CA private key is also kept in a sealed envelope in a safe in a separate location from the safes containing the private key and its backup copies.

6.4.3 Other aspects of activation data

Not defined.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

The server hosting the CA product is run on a Scientific Linux system.

No other services or software are loaded or operated on the CA server. The server will receive occasional patches and other adjustments if the security risk warrants, in the judgment of MARWAN/MaGrid staff.

6.5.2 Computer security rating

Not defined.

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 Certification authority will never be connected to a computer network under any circumstances (It has not any network adapter). Certificates are generated on a machine not connected to any kind of network, located in a secure environment and managed by a suitably trained person.

The public machine is protected by a suitably configured firewall.

6.8 TIME-STAMPING

All time stamping of entries created on the online servers at the MaGrid CA is based on the network time provided by the time server of CNRST, synchronized with the official providers of time signals.

The hardware clock of the offline system for the certificate and CRL signing, which determines the time stamping of the certificates and the CRLs, will be synchronized manually by the operator whenever the host starts.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

All certificates issued by the MaGrid CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280.

7.1.1 Version number(s)

Only X.509 version 3 certificates are issued by the MaGrid CA.

7.1.2 Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in the MaGrid CA certificates are:

For natural person certificates:

- Basic Constraints: critical, ca: false
- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage: critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
- Extended Key Usage clientAuth, emailProtection, codeSigning timeStamping
- Netscape Cert Type: SSL Client, S/MIME, Object Signing
- Netscape Comment: STRING
- CRL Distribution Points: URI
- Certificate Policies: OID

For server/services certificates:

- Basic Constraints: critical, ca: false
- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage: critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
- Extended Key Usage serverAuth, clientAuth, emailProtection, codeSigning timeStamping
- Netscape Cert Type: SSL Server, SSL Client, S/MIME, Object Signing

- Netscape Comment: STRING
- CRL Distribution Points: URI
- Certificate Policies : OID

For CA certificates:

- Basic Constraints: critical, ca: true
- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage: critical, digitalSignature, nonRepudiation, KeyCertSign, cRLSign
- Extended Key Usage timeStamping
- Netscape Cert Type: SSL Certification authority, Email Certificate, Authority Object Signing
- Netscape Comment: STRING
- CRL Distribution Points: URI
- Certificate Policies: OID

7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by the MaGrid CA are according to:

a)	hash function:	id-sha	1 1.3.14.3.2.26
b)	encryption:	rsaEncryption	1.2.840.113549.1.1.1
c)	signature:	sha1WithRSAEncryption	1.2.840.113549.1.1.5

7.1.4 Name forms

Each entity has a unique and unambiguous Distinguished Name (DN) in all the certificates issued to the same entity by the MaGrid CA. The DN shall be structured as defined in ITU-T Standards Recommendation X.501.

CNRST prefers that organizations use domain component naming.

Issuer:

C=MA, O=MaGrid, CN=MaGrid CA

Subject:

C=MA, O=MaGrid, OU=string, CN=name surname

C=MA, O=MaGrid, OU=string, CN=FQDN

The subject field contains the Distinguished Name of the entity with the following attributes:

MA	Top-level domain (Morocco)
MaGrid	MaGrid domain
[string]	[Organization string]
name [surname]	CommonName
[service " /"] FQDN	

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

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

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version number(s)

The MaGrid CA creates and publish X.509 v2 CRLs.

7.2.2 CRL and CRL entry extensions

The MaGrid CA shall issue complete CRLs for all certificates issued by itself independently of the reason for the revocation. The reason for the revocation shall not be included in the individual CRL entries.

The CRL shall include the date by which the next CRL shall be issued. A new CRL shall be issued before this date if new revocations are issued.

The CRL extensions that shall be included are:

- The Authority Key Identifier
- The CRL Number

The CRL entry extensions that will be included are:

- CRL Reason Code
- Invalidity Date

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 MaGrid 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.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

Not defined

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The assessments are made by personnel of the MaGrid CA or members of the MaGrid community.

An external audit can be performed by any Moroccan government department or academic institution.

If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of MaGrid CA's personnel and infrastructure.

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

In case of a deficiency, the MaGrid CA Manager will announce the steps that will be taken to remedy the deficiency. This announcement will include a timetable.

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 shall be revoked immediately.

8.6 COMMUNICATION OF RESULTS

The CA Manager will make the result publicly available on the CA web site with as many details of any deficiency as (s)he considers necessary.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

No fees are charged for the certification service for the CNRST constituency and therefore there are no financial encumbrances.

9.1.1 Certificate issuance or renewal fees

See 9.1.

9.1.2 Certificate access fees

See 9.1.

9.1.3 Revocation or status information access fees

See 9.1.

9.1.4 Fees for other services

No fees shall be charged.

9.1.5 Refund policy

See 9.1.

9.2 FINANCIAL RESPONSIBILITY

No Financial responsibility is accepted for certificates issued under this policy.

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

The MaGrid CA service collects information about the subscribers. Information included in issued certificates and CRLs is not considered confidential.

The MaGrid CA collects a subscriber' s name, work telephone numbers and e-mail address. Additionally, for RA Managers and Operators, personal contact information is kept by the CA (work telephone number, work address).

Under no circumstances will the MaGrid CA have access to the private keys of any subscriber to whom it issues a certificate.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

The subscriber's e-mail address will be kept confidential unless the subscriber decides to make it public. The information provided by the subscriber to verify his/her identity will be kept confidential

9.4.3 Information not deemed private

Information included in issued certificates and CRLs is not considered confidential. RA contact information is not considered confidential since this information is generally available from the web pages of the RA's employer.

Statistics regarding certificates issuance and revocation don't contain any personal information and is not considered confidential.

9.4.4 Responsibility to protect private information

The responsibility to protect private information rests with the MaGrid CA and all its accredited RAs.

9.4.5 Notice and consent to use private information

If the MaGrid CA or any of its accredited RAs wants to use private information, it must ask the subscriber for a written consent. No subscriber shall be under the impression that he/she has an obligation to agree.

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 law enforcement officials who exhibit regular warrant.

9.4.7 Other information disclosure circumstances

Disclosure upon owner's request is done according to the Data Protection Law. Specifically, information is released to the subscriber if the CA has received a signed e-mail from the subscriber requesting the information. The CA charges no fee for this.

The CA will recognize requests in writing for the release of personal information from a subscriber provided the subscriber can be properly authenticated

9.5 INTELLECTUAL PROPERTY RIGHTS

The MaGrid CA does not claim any IPR on certificates which it has issued.

Parts in this document are inspired or even copied (in no particular order) from the :

- pkIRISGrid CA
- SeeGrid CA
- TR-Grid CA

and may be indirectly from documents they draw from.

Anybody may freely copy from any version of the MaGrid CA's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of the source.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA representations and warranties

The MaGrid CA guarantees to issue certificates only to subscribers identified by requests received from RAs via secure routes. The MaGrid CA will revoke a certificate only in response to an authenticated request from the subscriber, or the RA which approved the subscriber's request, or if it has itself reasonable proof that circumstances for revocation are fulfilled.

The MaGrid CA does not warrant its procedures, nor takes responsibility for problems arising from its operation or the use made of the certificates it provides and gives no guarantees about the security or suitability of the service.

The CA only guarantees to verify subscriber's identities according to procedures described in this document.

The CA does not accept any liability for financial loss, or loss arising from incidental damage or impairment, resulting from its operation. No other liability, implicit or explicit, is accepted

9.6.2 RA representations and warranties

All accredited RAs shall perform their task of identification of the requesting parties as described in 3.2.3 and 3.2.2 to the best of their knowledge. No other warranties are accepted.

An RA can conclude, at its strictly own risk, a more stringent agreement with its subscribers, but this shall never commit the MaGrid CA nor any of its other accredited RAs.

It is the RA's responsibility to request revocation of a certificate if the RA is aware that circumstances for revocation are satisfied.

9.6.3 Subscriber representations and warranties

By requesting an MaGrid CA certificate a subscriber commits itself to use and protect the certificate and the certified keys according to the stipulations of the CP/CPS document in effect at the date of issuance of the said certificate. (S)he may however apply more stringent observances.

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 Law)
- 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 Strong Passphrase;
    - (Personal certificates) protecting the passphrase from others;
    - Notifying immediately the MaGrid 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.

In case of a breach of stipulations of the CP/CPS document that the subscriber has agreed to by requesting the MaGrid CA certificate the certificate shall be revoked immediately. No further warranties are required from the subscriber.

9.6.4 Relying party representations and warranties

A relying party should accept the subscriber's certificate for authentication purposes if:

- The relying party is familiar with the CA' s CP and the CPS that generated the certificate before drawing any conclusion on trust of the subscriber' s certificate; and
- The reliance is reasonable and in good faith in light of all circumstances known to the relying party at the time of reliance; and
- The certificate is used for permitted purposes only; and
- The relying party checked the status of the certificate to their own satisfaction prior to reliance.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

The MaGrid 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

Also the MaGrid 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

Except if explicitly dictated otherwise by the Moroccan law the MaGrid CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party.

It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP/CPS.

9.9 INDEMNITIES

The MaGrid CA declines any payment of indemnities for damages arising from the use or rejection of certificates it issues.

End entities shall indemnify and hold harmless the MaGrid CA and all appropriate RAs operating under this CP/CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CP/CPS document.

9.10 TERM AND TERMINATION

9.10.1 Term

This document becomes effective after its publication on the Web site of the MaGrid CA starting at the date announced there.

There is no term 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

All e-mail communications between the CA and its accredited RAs must be signed with a certified key.

All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.

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 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are not considered amendments.

9.12.2 Notification mechanism and period

The amended CP/CPS document shall be published on the MaGrid CA Web pages at least 2 weeks before becoming effective.

The MaGrid CA will inform its subscribers and all relying parties it knows of by means of an e-mail.

9.12.3 Circumstances under which OID must be changed

Substantial changes shall cause the OID to be changed. The decision is made by the manager of the MaGrid CA and submitted to the EUGridPMA for approval.

9.13 DISPUTE RESOLUTION PROVISIONS

Disputes arising out of the CP/CPS shall be resolved by the Manager of the MaGrid CA.

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

All activities relating to the request, issuance, use or acceptance of a MaGrid CA certificate have to comply with the Moroccan law.

Activities initiated from or destined for another country than Morocco 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 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 stipulation.

9.16.5 Force Majeure

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

9.17 OTHER PROVISIONS

No stipulation.

10 REFERENCES

- S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, " Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" , RFC 3647, November 2003 [replaces RFC 2527]
  http://www.ietf.org/rfc/rfc3647.txt
- S. Chokani and W. Ford, " Internet X.509 Infrastructure Certificate Policy andCertification Practices Framework" , RFC 2527, March 1999
  http://www.ietf.org/rfc/rfc2527.txt
- R. Housley, W. Polk, W. Ford and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" , RFC 3280, April 2002
  http://www.ietf.org/rfc/rfc3280.txt
- R. Housley, W. Ford, W. Polk and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and CRL Profile" , RFC 2459,January 1999
  http://www.ietf.org/rfc/rfc2459.txt
- Certification Authority pkIRISGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.1, February 2006
  http://www.irisgrid.es/pki/policy/1.3.6.1.4.1.7547.2.2.4.1.1.1/pkIRISGridCA_CP_CPS_1_1_1.pdf
- Certification Authority SeeGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.1, September 2004
  http://www.grid.auth.gr/pki/seegrid-ca/documents/cps/SeeGridCA-CPS-1.1.pdf

- Certification Authority TR-Grid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.1.0, June 2005
  http://www.grid.org.tr/ca/policy/cpcps.pdf

11 LIST OF CHANGES

- January 10, 2007. Initial release CP/CPS