MD-Grid

CERTIFICATION AUTHORITY

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Version 1.0

March, 2008

Table of Contents:

1. INTRODUCTION

This document describes the rules and procedures used by the MD-Grid Certification Authority.

1.1 Overview

This document is organized according to the specifications proposed by the RFC 3647. It describes the procedure followed by MD-Grid (National Grid Initiative of Moldova) Certification Authority and is the combination of Certificate Policy and Certification Practice Statement (CP/CPS).
This document is a valid CP/CPS as of March 04, 2008, 09:00 UTC.

1.2 Document name and identification

Document title: MD-Grid Certification Authority Certificate Policy and Certification Practice Statement
Document version: 1.0
Document date: 04.03.2008.
ASN.1 Object Identifier (OID): **1.3.6.1.4.1.31194.10.1.1.0**
The next table describes the meaning of the OID:

1.3.6.1.4.1	Prefix for IANA private enterprises
31194	RENAM registered identifier
10	Certification Authorities
1	CP/CPS
1.0	Major and minor CP/CPS number.

1.3 PKI participants

1.3.1 Certification Authorities

MD-Grid CA provides PKI services to the Moldavian academics and research communities who participate in national or international Grid activities. The MD-Grid CA does not issue or sign certificates to subordinate CAs.

1.3.2 Registration authorities

The RA Operators are responsible for verifying Subscribers' identities and approving their certificate requests. RA Operators do not issue certificates. The list of RAs is available on the MD-Grid CA website. Each RA will have it's own web interface.

1.3.3 Subscribers

The MD-Grid CA issues user (personal), host and service certificates. Subscribers eligible for certification from MD-Grid CA are:

- Users (people).

- Computers (hosts).
- Services (host applications).

1.3.4. Relying parties

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

Personal certificates can be used to authenticate a user that would like to benefit from the Grid resources.
Host certificates can be used to identify computers that have special tasks related to the Grid activities.
Service certificates can be used to recognize the host applications and, data or communication encryption (SSL/TLS).
In addition, it is permissible to use certificates for email signing.

1.4.2 Prohibited certificate uses

Notwithstanding the above, using certificates for purposes contrary to Moldovian law is explicitly prohibited.

1.5 Policy administration

1.5.1 Organization administering the document.

MD-Grid Security Group at RENAM is in charge of the management of MD-Grid CA.

Phone: +373 22 739827 or +373 22 234635
Fax: +373 22 288006
e-mail: MD-Grid-CA@renam.md

Address:
5 Academiei str. of. 331
MD-2028, Chisinau
Moldova, Republic of

1.5.2 Contact person

The contact person that can deal with any questions related to this document or operational issues:
Valentin Pocotilenco
Address:
RENAM Association
5 Academiei str. of. 331

MD-2028, Chisinau
Moldova, republic of
Phone: +373 22 739827 or +373 22 234635
Fax: +373 22 288006 or +373 22 234635
e-mail: pvv@renam.md

1.5.3 Person determining CPS suitability for the policy

Alexei Altuhov
Address:
RENAM Association
5 Academiei str. of. 331
MD-2028, Chisinau
Moldova, republic of
Phone: +373 22 739827 or or +373 22 234635
Fax: +373 22 288006 or +373 22 234635
e-mail: alexx@renam.md

Website: http://www.grid.md/ca

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

RENAM	Research and Educational Networking Association of Moldova
ASN.1	Abstract Syntax Notation One (http://asn1.elibel.tm.fr/)
CA	Certification Authority
CP/CPS	Certificate Policy/Certification Practice Statement
CRL	Certificate Revocation List
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
S/MIME	Secure / Multipurpose Internet Mail Extensions
SEE-GRID	South East European GRid-enabled eInfrastructure Development
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
USB	Universal Serial Bus

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The MD-Grid CA operates an on-line repository that contains:

- The MD-Grid CA root certificate
- User, Host and Service certificates issued by the CA.
- Certificate Revocation Lists (periodically updated)
- A copy of the most recent version of this CP/CPS and all previous versions
- A list of current operational Registration Authorities.
- Links to all trust anchor repositories where MD-Grid CA info is published.
- Other relevant information http://www.grid.md/ca

The MD-Grid CA communication information for information regarding repositories is:

RENAM Certification authority
RENAM Association
5 Academiei str. of. 331
MD-2028, Chisinau
Moldova, republic of
Phone: +373 22 739827
Phone: +373 22 234635
Fax: +373 22 288006
e-mail: MD-Grid-CA@renam.md

2.2 Publication of certification information

See section 2.1

2.3 Time or frequency of publication

Certificates will be put to the MD-Grid CA website as soon as they are issued.

- CRL publication will be updated immediately after a revocation is issued 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 MD-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 online repository is maintained on best effort basis and is available substantially on a 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance.
MD-Grid CA may impose a more restricted access control policy to the repository at its discretion.
The MD-Grid CA does not impose any access control on its CP/CPS, 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.509.v3 RENAM registered identifier standard and compliant with RFC3280:

1. in case of user certificate the subject name must include the persons name in the CN field;
2. in case of host certificate the subject name must include the DNS FQDN in the CN field;
3. in case service certificate the subject name must include the service name and the DNS FQDN separated by a „/“ in the CN field.

3.1.2 Need for names to be meaningful.

The subject name must represent the subscriber in a way that is easily understandable by humans and must have a reasonable association with the authenticated name of the subscriber. Each host certificate must be linked to a single network entity.

3.1.3 Anonymity or pseudonimity of subscribers

MD-Grid CA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4 Rules for interpreting various name forms

See section 3.1.1.

3.1.5 Uniqueness of names

The subject name included in the CN part of a certificate must be unique for all certificates issued by the MD-Grid CA. These certificates belong to the same end entity. When essential, extra characters may be affixed to the original name to guarantee the uniqueness of the subject name.
Private keys must not be shared among end entities.
DNs cannot be recycled.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of a key

The MD-Grid CA proves possession of the private key that is the companion to the public key in MD-Grid CA root certificate by issuing certificates and signing CRLs.
The MD-Grid CA verifies the possession of the private key relating to certificates requests by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to 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 MD-Grid CA will not generate the key pair for subscribers and will not accept or retain private keys generated by subscribers.

3.2.2 Authentication of organization identity

The MD-Grid CA authenticates organizations by:

- Checking that organization is affiliated with RENAM Initiative;
- Contacting the person who represents the organization in the project.

3.2.3 Authentication of individual entity

Certificate of a person:
The subject should contact personally the RA or CA staff in order to validate his/her identity. The subject authentication is fulfilled by providing an official document for personal identification (ID-card, driving license or a passport), and a valid document proving subject's relation with an institute or organization, declaring that the subject is a valid end entity. In exceptional cases such as remote geographical location of the subject, identity validation may be performed by video conference. In this case, an authenticated photocopy of the required document (ID-card, driving license or a passport) must be delivered by mail or courier to the RA staff prior to this online meeting. Authenticated photocopy refers to the verification made by a legally accepted notary public under Moldavian law.

Certificate of a host or service:
Host or service certificates can only be requested by the administrator responsible for the particular host. In order to request a host or service certificate the following conditions must be met:

1. The host must have a valid FQDN.
2. The administrator must already possess a valid personal MD-Grid certificate.
3. The administrator must provide a proof of his or hers relation to the host itself.

The subscriber requesting service from the MD-Grid CA must present valid documents for personal identification (ID-card, driving license or a passport), and a valid document proving subject's relation with an institute or organization.

MD-Grid CA or RA will archive photocopies of ID documents in case of user certificates and digitally signed e-mails in case of host or service certificates.

3.2.4 Non-verified subscriber information

During the initial identity validation the requester's e-mail is not verified. This is done during the processing of the certificate application as described in section 4.2.2.

3.2.5 Validation of Authority

No stipulation.

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 stating a re-key request signed with the personal certificate of the subscriber but after 3 years face-to-face identity validation is required as described in 3.2.3. Re-key after expiration uses completely the same authentication procedure as new certificate.

3.3.2 Identification and authentication for re-key after revocation

The procedure for re-key after revocation is exactly the same with an initial registration.

3.4 Identification and authentication for revocation request

Certificate revocation requests should be authenticated in one of the following ways:

- By signing a revocation request e-mail via a valid personal key corresponding to the certificate that is requested to be revoked which must be a valid, non-expired and non-revoked RENAM certificate.
- For persons who do not have a valid RENAM certificate, but hold an evidence of a revocation circumstance: by personal authentication as described in 3.2.3
- If the revocation request is for a host or service certificate, then the e-mail must be signed by the private key corresponding to the certificate of the person responsible of the host or service. When e-mail is not an option, the request will be authenticated using the procedure described in section 3.2.3.
- Revocation request by the RA should be done by e-mail, signed with valid RA operator key.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

The essential procedures that must be conformed in a certificate application request are as follows:

- The subject must be appropriate to the specifications stated in this policy.
- The key length of a certificate must be 1024 or 2048 bits.
- Each applicant generates his/her own key by using OpenSSL or similar software.
- Maximum life time of a certificate is 1 year.
- Message digests of the certificates must be generated by SHA1 algorithm.
- Host and service certificate requests must be submitted via SSL protected HTTP transport or via e-mail signed by a valid MD-Grid CA certificate to the appropriate RA.

- For host and service certificates, the requester must be appropriately authorized by the owner of the FQDN.
- User certificate requests must be submitted via SSL protected HTTP transport.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All the certificate applications will be authenticated and validated by the MD-Grid CA and RAs as stated in section 3.2.3. In the cases of re-key of user certificate or request for host or service certificate, the authentication of the certificate application will take place by checking that the requester has a valid MD-Grid CA certificate. Upon successful authentication, the information included in the certificate request will be validated by RA or CA.

4.2.2 Approval or rejection of certificate applications

If the certificate request does not meet one or more of the criteria in 4.1.1, it will be rejected and the requester will be informed via e-mail.

4.2.3 Time to process certificate applications

Each certificate application will take no more that 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.

4.4 Certificate acceptance

If the user wants to accept the certificate, he or she must follow the procedure in section 4.4.1.
If a user wants to reject a certificate, he or she must submit a revocation request as described in section 4.9.

4.4.1 Conduct constituting certificate acceptance

Subscribers of MD-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 MD-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 section 9.4

- 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 MD-Grid CA in case private key is compromised or lost
- notifying MD-Grid CA in case of information change in the certificate
- notifying MD-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 the MD-Grid CA will be published in the on-line repository operated by the MD-Grid CA.

4.4.3 Notification of certificate issuance by the CA to other entities

If the RA has handled the communication with the subscriber, then it will be notified of the certificate issuance.
The RA will be informed about any certificate signatures and re-keys before expiration that were submitted through it.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscribers' private keys along with the certificates issued by the MD-Grid CA can be used for:

- email signing/verifying and encryption/decryption (S/MIME);
- server authentication and encryption of communications;
- authentication purposes in Grid Infrastructures.
    - non-repuditation

4.5.2 Relying party public key and certificate usage

Relying parties can use the public keys and certificates of the subscribers for:

- email encryption and signature verification (S/MIME);
- server authentication and encryption of communications;
- authentication purposes in Grid infrastructures.

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

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

MD-Grid CA will not renew subscribers’ certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.2 Who may request renewal

MD-Grid CA will not renew subscribers’ certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.3 Processing certificate renewal requests

MD-Grid CA will not renew subscribers’ certificates. Subscribers must follow the re-key

procedure as defined in section 4.7.

4.6.4 Notification of new certificate issuance to subscriber

MD-Grid CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.5 Conduct constituting acceptance of a renewal certificate

MD-Grid CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.6 Publication of the renewal certificate by the CA

MD-Grid CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.7 Notification of certificate issuance by the CA to other entities

MD-Grid CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.7 Certificate re-key

4.7.1 Circumstances for certificate re-key

Subscribers must regenerate their key pair in the following circumstances:

1. expiration of their certificate signed by the MD-Grid CA;
2. revocation of their certificate by the MD-Grid CA;

4.7.2 Who may request certification of a new public key

Every subscriber holding a valid MD-Grid CA certificate can request certificate re-key 1 day before expiration of the certificate.

4.7.3 Processing certificate re-keying requests

Expiration warnings will be sent to subscribers before it is re-key time.
a) Re-key before expiration can be executed by stating a re-key request signed with the private key corresponding to the public one in the valid personal certificate of the subscriber. The requester is not required to pass the authentication procedure described in section 3.2.3, if this does not contrast with c) or d).
b) Re-key after certificate expiration uses completely the same authentication procedure as that for the new certificate.
c) At least once every 3 years the subscriber must go through the same authentication procedure as the one described for a new certificate.
d) In case the request for a new certificate is due to revocation 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 Circumstances for certificate modification

MD-Grid CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.2 Who may request certificate modification

MD-Grid CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.3 Processing certificate modification requests

MD-Grid CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.4 Notification of new certificate issuance to subscriber

MD-Grid CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.5 Conduct constituting acceptance of modified certificate

MD-Grid CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.6 Publication of the modified certificate by the CA

MD-Grid CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.8.7 Notification of certificate issuance by the CA to other entities

MD-Grid CA does not modify certificates. In case a modification is required the revocation and re-key procedures should be followed.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate will be revoked in the following situations:

- The CA is informed that the Subscriber has ceased to be a member of or associated with a RENAM program or activity;
- The Subscriber's private key is lost or suspected to be compromised;
- The information in the Subscriber's certificate is wrong or inaccurate, or suspected to be wrong or inaccurate;
- The Subscriber violates his/her obligations.

- The Subscriber does not need the certificate any more.

In one of the conditions above, end entity must request revocation of the certificate as soon as possible but within one working day.

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

The entity requesting the certificate revocation is authenticated by signing the revocation request with a valid MD-Grid CA certificate. Otherwise authentication will be performed with the same procedure as described in section 3.2.3.

4.9.4 Revocation request grace period

MD-Grid CA will process the revocation request with the highest priority. The maximum time for revocation must not exceed 1 working day.

4.9.5 Time within which CA must process the revocation request

MD-Grid CA will process all revocation requests within 1 working day.

4.9.6 Revocation checking requirement for relying parties

Relying parts must download the CRL from the online-repository [section 2.1] at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL issuance frequency

1. CRLs will be published in the on-line repository as soon as issued and at least once every 23 days;
2. The maximum CRL lifetime is 30 days;
3. Each new CRL is issued at least 7 days before expiration of the previous CRL.

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation checking requirements

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

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

MD-Grid CA does not suspend certificates.

4.9.14 Who can request suspension

MD-Grid CA does not suspend certificates.

4.9.15 Procedure for suspension request

MD-Grid CA does not suspend certificates.

4.9.16 Limits on suspension period

MD-Grid CA does not suspend certificates.

4.10 Certificate status services

4.10.1 Operational characteristics

MD-Grid CA online repository contains list of valid certificates and list of revoked certificates (CRL). Both lists are continuously updated.

4.10.2 Service availability

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

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

MD-Grid CA will not accept any key escrow or recovery services and will not give keys on escrow as well.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The MD-Grid CA operates in a controlled and protected room located in Technical University of Moldova. At least one person employed by RENAM Association will always be present on premises 24 hours per day, 7 days per week.

The address is:
Technical University of Moldova
Chisinau
Moldova
Phone: +373 22 234635
E-mail: MD-Grid-CA@renam.md

5.1.2 Physical access

Physical access to the MD-Grid CA is restricted to authorized personnel only.

5.1.3 Power and Air Conditioning

Premises containing the CA machine are air conditioned.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

Technical University of Moldova premises have a fire alarm system installed.

5.1.6 Media storage

Backups are to be stored in removable storage media (CD-ROM, Floppies and USB Flash) in a safe location in Technical University of Moldova.

5.1.7 Waste Disposal

Floppy disks or CDs are physically destroyed before being trashed.

5.1.8 Off-site Backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

No stipulation.

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 MD-Grid CA Security Personnel who are staff in RENAM.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to MD-Grid CA and RA operators.

5.3.4 Retraining frequency and requirements

MD-Grid CA will perform operational audit of the CA/RA staff at least once per year. If the results of the operational audit are not satisfactory, retraining will be considered.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

Operational manual for CA and RA operators is supplied to the new MD-Grid CA personnel.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events are recorded by MD-Grid CA:

- certification requests
- issued certificates
- requests for revocation
- issued CRLs
- login/logout/reboot of the signing machine

Each RA must keep log of the following:

- for each approved request, how it was approved;
- for each rejected request, why it was rejected;
- for each approved revocation request, the reason for revocation;
- for each rejected revocation request, the reason for revocation and the reason the request was rejected.

5.4.2 Frequency of processing log

Audit logs will be processed at least once per month.

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

Only authorized CA personnel are allowed to view and process audit logs. Audit logs are kept in a safe storage in a room with limited access.

5.4.5 Audit log backup procedures

Audit logs are copied to an offline medium and kept in a safe storage in a room with limited access.

5.4.6 Audit collection system (internal vs. external)

Audit log collection system is internal to the MD-Grid CA.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

The following data and files are recorded and archived by the CA:

- certification requests
- issued certificates
- requests for revocation
- issued CRLs
- all e-mail messages of correspondence between RA and CA
- identity validation records (section 3.2.3)

Each RA must keep log of the following:

- for each approved request, how it was approved;
- for each rejected request, why it was rejected;
- for each approved revocation request, the reason for revocation;
- for each rejected revocation request, the reason for revocation and the reason the request was rejected.
- all e-mail messages of correspondence between RA and CA
- identity validation records (section 3.2.3)

5.5.2 Retention Period for Archive

Minimum retention period is three years.

5.5.3 Protection of Archive

Archives are kept in a safe storage in a room with limited access.

5.5.4 Archive backup procedures

All data and files are copied to an off-line medium.

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 MD-Grid CA.

5.5.7 Procedures to obtain and verify archive information

No stipulation

5.6 Key changeover

Lifetime of MD-Grid CA is 5 years and 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

If the CA's private key is (or is suspected to be) compromised, the CA will:

- Inform the EUgridPMA;
- Inform the Registration Authorities, Subscribers and Relying Parties of which the CA is aware;
- Conclude the issuance and distribution of certificates and CRLs;
- Make a new presentation of site security for CA re-accreditation.

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.

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

No stipulation.

5.7.3 Entity private key compromise procedures

No stipulation.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA Termination

Before the MD-Grid CA terminates its services, it will:

- Inform the Registration Authorities, Subscribers and Relying Parties of which the CA is aware;
- Make information of its termination available on it's website;
- Stop issuing certificates.
- Annihilate all copies of private keys.
- Audit logs will be kept for 3 years from CA or RA termination date.

Before the RENAM RA terminates its services, it will:

- Inform the CA and Relying Parties it is aware of.
- Make information of its termination available on it's and CA websites.
- Stop accepting certificate requests.

An advance notice of no less than 60 days will be given in the case of normal (scheduled) CA or RA termination.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Keys for the MD-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.

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

Applicants can make user/host/service certificate requests as described in section 4.1

6.1.4 CA public key delivery to relying parties

The MD-Grid CA root certificate is available on the website: http://www.grid.md/ca/

6.1.5 Key Sizes

For a user or host certificate the key size is 1024 or 2048 bits. The MD-Grid CA key size is 2048 bits.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

MD-Grid CA does not archive private keys apart from the private key corresponding to the root certificate of MD-Grid CA.
MD-Grid CA does not use cryptographic module.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

A backup of the MD-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

MD-Grid CA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

MD-Grid CA does not use any kind of cryptographic module.

6.2.7 Private key storage on cryptographic module

MD-Grid CA does not use any kind of cryptographic module.

6.2.8 Method of activating private key

MD-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 pass phrase, at least 12 characters long for the private key. Private key cannot be shared and it is subscriber 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

No stipulation.

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

MD-Grid CA root certificate has a validity of ten years.
End Entity certificates have maximum lifetime of 1 year plus 1 month.

6.4 Activation Data

6.4.1 Activation data generation and installation

MD-Grid CA does not generate activation data for subscribers. It's upon the subscriber to generate a secure pass phrase, at least 12 characters long, in order to be used as activation data for his/her private key.
MD-Grid CA private key is protected by a passphrase of at least 15 characters. Pass phrase is regenerated every 180 days by one of MD-Grid CA operators.

6.4.2 Activation data protection

The MD-Grid CA does not have access to or generate the private keys of a subscriber. The key pair is generated and managed by the client and it is subscriber's responsibility to keep the private key secure.
The passphrase for the private key of 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

Computers operating at MD-Grid CA meet the following requirements:

- Operating systems are maintained at a high level of security by applying in a timely manner all recommended and applicable security patches;
- Monitoring is done to detect unauthorized software changes;
- System services are reduced to the bare minimum.

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

Certificates are issued on a machine, not connected to any kind of network. Protection of other machines is provided by firewalls.

6.8 Time stamping

No stipulation.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3

7.1.2 Certificate Extensions

The values of extensions in case of CA certificate are following:

- X509v3 Basic Constraints: critical CA:TRUE
- X509v3 Key Usage: critical Certificate Sign, CRL Sign
- X509v3 Subject Key Identifier: <CA key ID>
- X509v3 Authority Key Identifier:
    - keyid:<CA key ID>
    - DirName:/C=MD/O=RENAM/CN=MD-Grid-CA
    - serial:<CA certificate serial>
- X509v3 Issuer Alternative Name: email: MD-Grid-CA@renam.md
- X509v3 Subject Alternative Name: email: MD-Grid-CA@renam.md
- X509v3 CRL Distribution Points
- Netscape Cert Type: SSL CA, S/MIME CA, Object Signing CA
- Netscape Comment: RENAM Certification Authority Root Certificate

The values of extensions in case of user certificates are following:

- X509v3 Basic Constraints: critical CA:FALSE
- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement, Non-Repuditation.
- X509v3 Extended Key Usage: TLS Web Client Authentication, E-mail Protection

- X509v3 Subject Key Identifier: <subject key ID>
- X509v3 Authority Key Identifier:
  - keyid:<CA key ID>
  - DirName:/C=MD/O=RENAM/CN=MD-Grid-CA
  - serial:<CA certificate serial>
- X509v3 Subject Alternative Name: email:<user's email address>
- X509v3 Issuer Alternative Name: email: MD-Grid-CA@renam.md
- X509v3 CRL Distribution Points
- Netscape Cert Type: SSL Client, S/MIME, Object Signing
- Netscape Comment: RENAM Certification Authority Policy: http://www.grid.md/ca/documents/MD-Grid-CP-CPS.doc

The values of extensions in case of host and service certificates are following:

- X509v3 Basic Constraints: critical CA:FALSE
- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
- X509v3 Extended Key Usage: TLS Web Server Authentication
- X509v3 Subject Key Identifier: <subject key ID>
- X509v3 Authority Key Identifier:
  - keyid:<CA key ID>
  - DirName:/C=MD/O=RENAM/CN=MD-Grid-CA
  - serial:<CA certificate serial>
- X509v3 Issuer Alternative Name: email:MD-Grid-CA@renam.md
- X509v3 Subject Alternative Name: DNS:FDQN
- X509v3 CRL Distribution Points
- Netscape Cert Type: SSL Server
- Netscape Comment: RENAM Certification Authority Policy: CP/CPS http://www.grid.md/ca/documents/MD-Grid-CP-CPS.doc

A current list of OU's can be obtained at http://www.grid.md/ca/documents/MD-Grid-CP-CPS.doc

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Issuer:
DC=MD, DC=RENAM, CN=MD-Grid-CA
Subject:
DC=MD, DC=RENAM, OU=XXX, CN=Subject-name

Where XXX is the name or acronym of the institution. The "CN" field structure for the user or host/service are described in section 1.3. A current list of OU's can be obtained at http://www.grid.md/ca/documents/MD-Grid-CP-CPS.doc

In case of person, the CN part of DN can contain only letters, numbers and following special characters: left round bracket (‘(’), right round bracket (‘)’), space (‘ ‘) and hyphen (‘-‘). In case of host and service, the CN part of DN can contain only letters, numbers and following special characters: dot (‘.‘) and hyphen (‘-‘). Additionally, in case of grid host certificate and service certificate character ‘/’ can be used. The maximal length of the CN is 128 characters for all types of certificates.

7.1.5 Name constraints

Subject attribute constraints:

Domain Component:
must be “MD”
Organization:
must be “RENAM”
OrganizationUnit:
Must be the name of the subject's institute.
CommonName:
First name and last name of the subject for user certificates, DNS FQDN for host or service certificates. In the latter case the DNS FQDN may be prefixed by the value 'host' or the service name separated with a '/' from the DNS FQDN.

7.1.6 Certificate Policy Object Identifier

See 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)

CRLs are in X.509 v2 format, compliant with RFC 3280. SHA1 algorithm is used to generate CRLs.

7.2.2 CRL and CRL entry extensions

The CRL extension Authority Key Identifier will be used in CRLs. CRL entry extensions used are: CRL Number and CRL Reason Code. They are described in the following sections.

7.2.2.1 Authority key identifier

Non-critical extension, a unique identifier for the CA key as defined in RFC 3280.

7.2.2.2 CRL Number

Non-critical extension, the number of current CRL as defined in RFC 3280.

7.2.2.3 CRL Reason Code

Non-critical extension, carrying the revocation reason code as specified in RFC3280, section 5.3.1.

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 MD-Grid CA must allow to be audited by other trusted CAs to verify its compliance with the rules and procedures specified in this document. Any costs associated with such an audit must be covered by the requesting party.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

No stipulation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees shall be charged.

9.1.2 Certificate access fees

No fees shall be charged.

9.1.3 Revocation or status information access fees

No fees shall be charged.

9.1.4 Fees for other services

No fees shall be charged.

9.1.5 Refund policy

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

9.2 Financial responsibility

MD-Grid CA denies any financial responsibilities for damages or impairments resulting from its operation.

9.2.1 Insurance coverage

9.2.2 Other assets

9.2.3 Insurance or warranty coverage for end-entities

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

9.3.2 Information not within the scope of confidential information

9.3.3 Responsibility to protect confidential information

9.4 Privacy of personal information

MD-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. MD-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

No stipulation.

9.4.3 Information not deemed private

MD-Grid CA collects the following information which is not deemed as private:

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

9.4.4 Responsibility to protect private information

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

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

1. RFC 3647;
2. HellasGrid CA Certificate Policy;
3. TR-Grid CA Certificate Policy;
4. UK e-Science CA Certificate Policy;
5. SEE-GRID CA Certificate Policy;

9.6 Representations and warranties

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

1. MD-Grid CA guarantees to control the identity of the certification requests according to the procedures described in this document;
2. MD-Grid CA guarantees to control the identity of the revocation requests according to the procedures described in this document;
3. MD-Grid CA is run on a best effort basis.
4. MD-Grid CA guarantees its service security.
5. MD-Grid CA shall not be held liable for any problems arising from its operation or improper use of the issued certificates ;
6. MD-Grid CA denies any kind of responsibilities for damages or impairments resulting from its operation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.12.1 Procedure for amendment

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 declared on the website as defined in section 2.3. Changes are published on the website as well.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

Legal disputes arising from the operation of the MD-Grid CA will be resolved according to the Moldovian Law.

9.14 Governing law

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

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

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