RomanianGRID CA

Certificate Policy

Certification Practice Statement

Version 2.2

January, 2019

Current status: Accredited

TABLE OF CONTENTS

1. Introduction

1.1. Overview

The RomanianGRID CA is a top level Certification Authority which provides PKI services for GRID activities to the Romanian research and academic communities.
The RomanianGRID CA was established and is operated by the Romanian Space Agency (ROSA), a public institution supervised by the Ministry of Research and Innovation in Romania.
This document describes the rules and procedures used by the RomanianGRID CA for issuing certificates. It is structured in accordance with RFC 3647.
This document shall be approved and subsequently audited by the EUGridPMA.

1.2. Document name and identification

Document name	**"RomanianGRID CA Certificate Policy and Certification Practice Statement"**
Version	**2.2**
Document date	**15.01.2019**
O.I.D.	**1.3.6.1.4.1.27103.9.1.2.1.2.2**

The structure of the OID:

1.3.6.1.4.1	.27103	.9	.1	.2	.1	.2	.2
Prefix for IANA private enterprises	**Romanian Space Agency (ROSA)**	**Information Systems and Security**	**PKI**	**RomanianGRID CA**	**cp/cps**	**Doc version - major**	**Doc version - minor**

1.3. PKI participants

1.3.1. Certification Authorities

RomanianGRID certificates are signed by the RomanianGRID CA. RomanianGRID CA does not issue certificates to subordinate Certification Authorities.
In IGTF acceptance, RomanianGRID CA is the only certification authority deserving the e-science community in Romania.

1.3.2. Registration Authorities

The RomanianGRID CA is supported by a network of Registration Authorities.

The procedures of verification of the Subscriber's identity and of approving their certificate requests are performed by trusted individuals – Registration Authorities (RA) – assigned by the RomanianGRID CA.
The current list of the valid Registration Authorities is available in an online repository as described in section 2.2.
RAs do not issue certificates.

1.3.3. Subscribers (end entities)

RomanianGRID CA issues certificates for natural persons, robots, digital processing entities and services running on digital processing entities, involved in GRID related activities of the Romania based research and academic communities.

1.3.4. Relying parties

Users of GRID computing infrastructure that are using the public keys in certificates issued by the RomanianGRID 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

The RomanianGRID certificates may be used for any application that is suitable for X.509 certificates such as e-mail signing and encryption, authentication and encryption of communications, authentication of users, hosts and services, etc.

1.4.2. Prohibited certificate uses

The certificates issued by the RomanianGRID CA must not be used for financial transactions. They must not be used for purposes that violate Romanian or international laws.

1.5. Policy administration

1.5.1. Organization administering the document

Romanian Space Agency is administering the RomanianGRID CA.
The RomanianGRID CA address for operational issues is:

RomanianGRID Certification Authority
Romanian Space Agency (ROSA)
21-25 Mendeleev
010362, Bucharest
ROMANIA

Phone: 00-40-21-3168722
Fax: 00-40-21-3128804
E-mail: grid-ca@rosa.ro

1.5.2. Contact Person

The contact person for questions related to this CP/CPS document is the CA manager:

Cosmin NISTOR
Romanian Space Agency
21-25 Mendeleev
010362, Bucharest
ROMANIA

Phone: 00-40-21-3168722
Fax: 00-40-21-3128804
E-mail: cosmin.nistor@rosa.ro

1.5.3. Person determining CPS suitability for the policy

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

Cosmin NISTOR
Romanian Space Agency
21-25 Mendeleev
010362, Bucharest
ROMANIA

Phone: 00-40-21-3168722
Fax: 00-40-21-3128804
E-mail: cosmin.nistor@rosa.ro

1.5.4. CPS approval procedures

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

1.6. Definitions and acronyms

T.B.D.

2. Publication and repository responsibilities

2.1. Repositories

All the on-line and the off-line repositories of the RomanianGRID CA are operated by the Romanian Space Agency (ROSA).
The online repositories are published at the URL http://www.romaniangrid.ro
The address for issues regarding the repositories is:

RomanianGRID Certification Authority
Romanian Space Agency
21-25 Mendeleev
010362, Bucharest
ROMANIA

Phone: 00-40-21-3168722
Fax: 00-40-21-3128804
E-mail: grid-ca@rosa.ro

The RomanianGRID CA online repository is maintained on a best effort basis with an intended availability of 24x7.

2.2. Publication of certification information

The RomanianGRID CA operates on-line repositories that contain:

- The RomanianGRID CA certificate:
  http://www.romaniangrid.ro/certs/root.pem
- The latest Certificate Revocation List (CRL) signed by the CA:
  http://www.romaniangrid.ro/crl/crl-v2.der
- The current and all previous versions of the CP/CPS:
  http://www.romaniangrid.ro/cpcps.htm
- All valid certificates:
  http://www.romaniangrid.ro/valcerts.htm
- A list with the current operational Registration Authorities:
  http://www.romaniangrid.ro/ra.htm
- Other relevant information relating to certificates that refer to this policy

The online repositories are published at the URL http://www.romaniangrid.ro

2.3. Time or frequency of publication

All information to be published in the repository shall be published promptly after such information is available to the CA. Information relating to the revocation of a certificate will be published as described in section 4.9.7.

2.4. Access control on repositories

RomanianGRID CA does not impose any access control restrictions to the information available at its website, which includes the CA certificate, latest CRL and the CP/CPS document.

3. Identification and authentication

3.1. Naming

3.1.1. Types of names

The subject name for the certificate applicants shall follow the X.500 standard.
The CN component has one of the following forms:

- In case of user certificate the subject name must include the persons first name, followed by a blank space, then last name (CN=Cosmin Nistor). The subject name may contain the affiliation of the subscriber to his organization (CN=Cosmin Nistor-ROSA).
- In case of host certificate the subject name must include the DNS FQDN in the CN field.
- In case of service certificate the subject name must include the service name and the DNS FQDN separated by a "/" in the CN field
- In case of robot certificate the subject name must start with the string "Robot" followed by a dash "-" then the "description of the grid function", a dash "-" and the "first name" followed by a blank space and then the "last name" of the subscriber responsible for the robot (CN=Robot - GridPortal - Cosmin Nistor).

3.1.2. Need for names to be meaningful

The subject name must represent the subscriber in a way that is easily understandable by humans and must have a reasonable association with the authenticated name of the subscriber.

3.1.3. Anonymity or pseudonimity of subscribers

RomanianGRID CA will neither issue nor sign pseudonymous or anonymous certificates.

3.1.4. Rules for interpreting various name forms

See section 3.1.1.

3.1.5. Uniqueness of names

The subject name listed in a certificate shall be unambiguous and unique for all entities certified by RomanianGRID CA. In case of user certificates, additional

numbers or letters may be appended to the real name to ensure the uniqueness of the name within the domain of certificates issued by the RomanianGRID CA.

3.1.6. Recognition, authentication, and role of trademarks

No stipulation.

3.2. Initial identity validation

3.2.1. Method to prove possession of key

RomanianGRID CA proves possession of the private key of its own root certificate by issuing certificates and signing CRLs.
RomanianGRID CA verifies the possession of the private key of certificate requests by out-of-band, non-technical means at the time of authentication. Such verification may take the form of a directly posed question to the requester. A cryptographic challenge-response exchange may be used to prove possession of the private key at any point in time before certification of the subscriber.
RomanianGRID CA will not generate the key pair for the subscribers and will not accept or retain private keys generated by the 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 RomanianGRID CA and it consents to the request.

3.2.3. Authentication of individual identity

The RA must have documented evidence of retaining the same identity over time in accordance with the identity vetting procedure.

- Natural person: the subject must contact personally an RA and authenticate himself by presenting a photo ID document or passport.
- Digital processing entity or service: the entity must already have a valid DNS entry. The requestor must send the request to the RA by a signed e-mail, confirming that he is responsible for the resource in question. The RA sends the request after verifying the correctness of the request.
- Robot: The requestor must send the request to the RA by a signed e-mail, confirming that he/she is responsible for the operations of the robot. The RA sends the request after verifying the correctness of the request.

3.2.4. Non-verified subscriber information

No stipulation.

3.2.5. Validation of Authority

The subscriber must present valid documents stating his/her affiliation with the organization.

3.2.6. Criteria of interoperation

No stipulation.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key

Re-key before the certificate expires can be done by sending a re-key request email signed with the current user certificate. Rekey after expiration follows the same authentication procedures as for a new certificate.
Certificates must only be re-keyed consecutively for a period of 5 years. After that, the user must follow the same authentication procedure as for a new certificate.

3.3.2. Identification and authentication for re-key after revocation

Re-key after revocation follows the same rules as an initial registration.

3.4. Identification and authentication for revocation request

Certificate revocation requests should be submitted via e-mail. In case the revocation request is for a user certificate, the e-mail must be signed by the private key, corresponding to the certificate that is requested to be revoked, which must be a valid, non-expired, non-revoked certificate, issued by RomanianGRID CA.
If the e-mail is not an option then the request will be authenticated following the procedure described in section 3.2.3. If the revocation request is for a host, service or robot certificate, then the e-mail must be signed by the private key corresponding to a valid, non-expired, nonrevoked RomanianGRID CA certificate of the person responsible for the given host, service or robot.

4. Certificate life-cycle operational requirements

4.1. Certificate application

4.1.1. Who can submit a certificate application

The subject must:

- Be an acceptable subscriber as defined in subsection 1.3.3;
- Read and adhere to the policies and procedures described in this document;
- Generate his/her own key pair with length of at least 2048 bits.
- Use a strong passphrase of at least 12 characters
- Follow the RomanianGRID CA distinguished name scheme, and the name must be unambiguous and unique

4.1.2. Enrollment process and responsibilities

For user certificate:

- The subject requests an appointment at the local RA (by email or in person). The authentication according to 1.3.3, 3.2.3 and 3.2.5 must be processed in a face to face meeting at the local RA
- During the face to face meeting, after a successful authentication the subject must provide the RA with a certificate signing request stored on a digital medium
- After verification the RA contacts the CA and forwards the request via signed email, which is then processed and signed by the CA

For digital processing entities and services:

- The certificate request is sent via email to the appropriate RA and the email must be signed by a valid RomanianGRID CA user certificate. The RA verifies the correctness of the request according to 1.3.3, 3.2.3 and 3.2.5. If the request is valid, the RA forwards the request to the CA via signed email.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

The certificate applications will be validated by the RA where the application was issued.
For new user certificate request the RA will authenticate the request according to sections 3.2.2 and 3.2.3.

For re-key of user certificate while still valid, and for digital processing entity or service certificate the applications will be authenticated on the proof of possession of a valid RomanianGRID CA certificate.

4.2.2. Approval or rejection of certificate applications

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

- The certificate application must be authenticated by the RA as described in section 4.2.1.
- The subject must be an acceptable subscriber entity as defined in section 1.3.3.
- The request must obey the RomanianGRID CA distinguished name scheme
- The distinguished name scheme must be unambiguous and unique
- The private key of the end entity must be at least 2048 bits long

If at least one of the above criteria is not fulfilled by the applicant, the request will be rejected and a signed notification e-mail will be sent by the RA to the applicant with cc to the RomanianGRID CA.

4.2.3. Time to process certificate applications

Each certificate application will take no more than 5 working days to be processes from the time RA approves the request.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

The certificate request will be transferred to the signing machine which is not connected to any network. Here the certificate is signed.

4.3.2. Notification to subscriber by the CA of issuance of certificate

Right after the issuance of the certificate the CA will send an e-mail to the subscriber with information on how to download the certificate from the RomanianGRID CA online server.
At the same time an e-mail will be sent to the appropriate RA informing about the certificate issuance.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

No stipulation.

4.4.2. Publication of the certificate by the CA

RomanianGRID CA will publish all valid certificates in an online repository available at the URL: http://www.romaniangrid.ro/valcerts.htm

4.4.3. Notification of certificate issuance by the CA to other entities

The appropriate RA will be notified about the certificate issuance.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

The certificates issued by the RomanianGRID CA shall be used according to section 1.4.:

- E-mail signing and decryption
- Server authentication and encryption of communications
- Authentication of users, hosts and services in research and educational infrastructures.

The certificates shall not be used for purposes described in section 1.4.2.
No user certificates may be shared.

4.5.2. Relying party public key and certificate usage

Relying parties can use the subscriber's public keys and certificates for:

- Validation of e-mail signature and decryption
- Server authentication and encryption of communications
- Authentication of users, hosts and services in research and educational infrastructures.

The relying party must consult the current CRL and implement its restrictions while validating certificates.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

RomanianGRID CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.2. Who may request renewal

RomanianGRID CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.3. Processing certificate renewal requests

RomanianGRID CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.4. Notification of new certificate issuance to subscriber

RomanianGRID CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.5. Conduct constituting acceptance of a renewal certificate

RomanianGRID CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.6. Publication of the renewal certificate by the CA

RomanianGRID CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.6.7. Notification of certificate issuance by the CA to other entities

RomanianGRID CA does not renew subscribers' certificates. Subscribers must follow the re-key procedures as described in section 4.7.

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

Subscribers must regenerate their key pair in the following circumstances:

- Expiration of their RomanianGRID CA signed certificate
- Revocation of their certificate by the RomanianGRID CA

4.7.2. Who may request certification of a new public key

Same as in section 4.1.1 under the circumstances given in section 4.7.1

4.7.3. Processing certificate re-keying requests

Re-key request before expiration of the user certificate can be accomplished by sending an email signed with the current user certificate.
Re-key request after expiration follows the same authentication procedure as for a new certificate.
Re-key request in case of revocation or compromise of the current certificate follows the same procedure as for a new certificate.
Certificates must only be re-keyed consecutively for a period of 5 years. After that, the user must follow the same authentication procedure as for a new certificate.

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

No stipulation.

4.7.6. Publication of the re-keyed certificate by the CA

RomanianGRID CA will publish all valid certificates in an online repository available at the URL: http://www.romaniangrid.ro/valcerts.htm

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

RomanianGRID 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

RomanianGRID 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

RomanianGRID 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

RomanianGRID 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

RomanianGRID 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

RomanianGRID 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

RomanianGRID 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

Subscribers must request revocation of its certificate as soon as possible, but within one working day, in the following circumstances:

- The subject of the certificate has ceased being an eligible end entity for certification as described in the Policy under which the certificate was signed;
- The subject does not require the certificate anymore;

- The private key has been lost or compromised;
- The data in the certificate is wrong, inaccurate, or no longer valid;
- The digital processing entity or service to which the certificate has been issued has been retired;
- The subject has failed to comply with the rules of this policy

4.9.2. Who can request revocation

The revocation of the certificate can be requested by:

- The certificate subscriber in case of user certificate
- The appropriate RA
- The CA
- Any other entity presenting proof of knowledge that the private key has been compromised or that the subscriber's data has been modified

4.9.3. Procedure for revocation request

The entity requesting revocation must present the proof of a compromised key:

- by a signed request with a valid RomanianGRID CA certificate
- if a signed request is not possible then the authentication of the requester must be done according to section 3.2.3.

4.9.4. Revocation request grace period

RomanianGRID 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

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

4.9.6. Revocation checking requirement for relying parties

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

4.9.7. CRL issuance frequency

RomanianGRID CA issues CRLs immediately after every certificate revocation or at least 7 days before the expiration of the previous one. The maximum lifetime for a CRL is 30 days.

4.9.8. Maximum latency for CRLs

CRLs will be published in the online repository as soon as issued.

4.9.9. On-line revocation/status checking availability

RomanianGRID CA issues CRLs immediately after every certificate revocation or at least 7 days before the expiration of the previous one. The maximum lifetime for a CRL is 30 days. The latest Certificate Revocation List (CRL) signed by the CA: http://www.romaniangrid.ro/crl/crl-v2.der

4.9.10. On-line revocation checking requirements

No stipulation.

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

RomanianGRID CA does not suspend certificates.

4.9.14. Who can request suspension

RomanianGRID CA does not suspend certificates.

4.9.15. Procedure for suspension request

RomanianGRID CA does not suspend certificates.

4.9.16. Limits on suspension period

RomanianGRID CA does not suspend certificates.

4.10. Certificate status services

4.10.1. Operational characteristics

The RomanianGRID CA operates as an online repository that contains all the CRLs that have been issued. Promptly following revocation the CRL in the repository shall be updated.

4.10.2. Service availability

The RomanianGRID CA online repository is maintained on a best effort basis with an 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 rekeyed before that date, or if the subscriber requests the revocation of the certificate.

4.12. Key escrow and recovery

4.12.1. Key escrow and recovery policy and practices

RomanianGRID 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 RomanianGRID CA is located at the Romanian Space Agency (ROSA) facility in the National Authority for Scientific Research building in Bucharest.
The address is:

Romanian Space Agency (ROSA)
21-25 Mendeleev
010362, Bucharest
ROMANIA

Phone: 00-40-21-3168722
Fax: 00-40-21-3128804
E-mail: grid-ca@rosa.ro

5.1.2. Physical access

The access to the RomanianGRID CA is restricted to the authorized personnel only. The signing machine is kept locked in a safe, being removed from there only when in use.

5.1.3. Power and air conditioning

Both the RomanianGRID CA online and offline machines are protected by uninterruptable power supplies and they operate in an air conditioning environment.

5.1.4. Water exposures

No stipulation.

5.1.5. Fire prevention and protection

No stipulation.

5.1.6. Media storage

The RomanianGRID CA private key is kept in several removable storage media in different safe places to which only the authorized personnel has access.

5.1.7. Waste disposal

Waste carrying potential confidential information is 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

The RomanianGRID CA personnel is selected by the Romanian Space Agency (ROSA)

5.3.2. Background check procedures

No stipulation.

5.3.3. Training requirements

Internal training is given to the RomanianGRID CA operators.

5.3.4. Retraining frequency and requirements

Retraining is mandatory when new software or features or new organizational procedures are introduced.

5.3.5. Job rotation frequency and sequence

No stipulation.

5.3.6. Sanctions for unauthorized actions

No stipulation.

5.3.7. Independent contractor requirements

No stipulation.

5.3.8. Documentation supplied to personnel

Documentation regarding the operational procedure is given to the personnel during training sessions.

5.4. Audit logging procedures

5.4.1. Types of events recorded

The following events will be recorded:

- System boots and shutdowns for the signing machine and repository server
- User logins and logouts for the signing machine
- Requests for certificates
- Requests for revocations
- Certificate issuing

- CRL issuing

5.4.2. Frequency of processing log

Audit logs will be analyzed once per month.

5.4.3. Retention period for audit log

Audit logs will be retained for at least 3 years.

5.4.4. Protection of audit log

The audit logs shall only be accessible by RomanianGRID CA authorized personnel.

5.4.5. Audit log backup procedures

Audit logs are copied on an offline medium.

5.4.6. Audit collection system (internal vs. external)

The audit collection system is internal to the RomanianGRID CA.

5.4.7. Notification to event-causing subject

No stipulation.

5.4.8. Vulnerability assessments

The CA must perform operational audits on CA and RA staff at least once per year.

5.5. Records archival

5.5.1. Types of records archived

CA:

- System boots and shutdowns for the signing machine and repository server
- User logins and logouts for the signing machine
- Requests for certificates
- Requests for revocations

- Certificate issuing
- CRL issuing
- Copy of subscribers photo IDs

RA:

- Requests for certificates
- Requests for revocations
- Copy of subscribers photo IDs

5.5.2. Retention period for archive

The minimum retention period is 3 years or at least as long as there are valid certificates based on such records.

5.5.3. Protection of archive

The archive shall only be accessible by RomanianGRID CA authorized personnel.

5.5.4. Archive backup procedures

Archive is copied to an offline 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.

5.5.7. Procedures to obtain and verify archive information

No stipulation.

5.6. Key changeover

The CA's private signing key is changed periodically. From that time on only the new key will be used for signing certificates. The overlap between the old key and the new one is for at least the validity period of a subscriber certificate. During that period the old key pair is used to verify old signatures and to sign the CRLs until all the certificates signed with the old key have expired or have been revoked.

The lifetime of subscriber certificates must be no longer than 400 days. The lifetime of the CA certificate is described in section 6.3.2.
Re-key of subscriber certificates is described in sections 3.3.1 and 4.7.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

If the RomanianGRID CA private key is compromised or destroyed, the CA will:

- Notify subscribers, RAs, relying parties
- Terminate the issuance and distribution of certificates and CRLs
- Notify relevant security contacts

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

Both public and private data are backed up every time they are changed.

5.7.3. Entity private key compromise procedures

For user certificate: The user must first inform the appropriate RA in order for that to ask for certificate revocation. After the certificate revocation the user can start the procedures for issuing a new certificate.
For digital processing entity: the administrator of the subject must ask for the revocation of the certificate. After the certificate revocation the administrator can start the procedures for issuing a new certificate.

5.7.4. Business continuity capabilities after a disaster

No stipulation.

5.8. CA or RA termination

Upon the permanent termination of its activity the RomanianGRID CA shall:

- Notify subscribers and RAs
- Terminate the issuance and distribution of certificates and CRLs
- Notify relevant security contacts
- Notify as widely as possible the termination of the service.
- In case of RA termination all the information related to this action will be published on the RomanianGRID CA website.

6. Technical security controls

6.1. Key pair generation and installation

6.1.1. Key pair generation

The key pair for the RomanianGRID CA is generated on a computer which is not connected to any kind of network by authorized CA staff only.
The key pairs for user certificates or for digital processing units certificates are generated by the requesting parties themselves on their systems.
The key material based on which a robot certificate is issued must be generated either:

1. Inside a secure hardware token
2. Locally on an appropriately secured computer system

a) of which the natural person responsible for the robot is the sole user and administrator, or

b) to which only those people responsible for the robots operation have access, and where the key material is generated using trustworthy cryptographic software.

6.1.2. Private key delivery to subscriber

Each subscriber must generate his/her own key pair. RomanianGRID CA does not generate private keys to subscribers.

6.1.3. Public key delivery to certificate issuer

The subscriber's public key is delivered to the CA in a way that ensures that it has not been altered.

6.1.4. CA public key delivery to relying parties

CA certificate (containing its public key) can be downloaded from the online RomanianGRID CA repository.
The online repository is published at the URL http://www.romaniangrid.ro

6.1.5. Key sizes

Keys of length less than 2048 bits are not accepted. RomanianGRID CA key length is 2048 bits.

6.1.6. Public key parameters generation and quality checking

No stipulation.

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

Keys may be used for authentication, data encryption, message integrity and session key establishment.
The CA' private key is only used for signing certificates and CRLs.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.2.3. Private key escrow

Private keys must not be escrowed.

6.2.4. Private key backup

The RomanianGRID CA private key is kept in encrypted form in media storage located in a safe place where access is restricted to authorized personnel only.
A copy in written form of the passphrase is kept in a sealed envelope in a safe. Access to the safe is restricted only to the RomanianGRID CA operators.

6.2.5. Private key archival

The RomanianGRID CA private key is kept in encrypted form in media storage located in a safe place where access is restricted to authorized personnel only.
A copy in written form of the passphrase is kept in a sealed envelope in a safe. Access to the safe is restricted only to the RomanianGRID CA operators.

6.2.6. Private key transfer into or from a cryptographic module

No stipulation.

6.2.7. Private key storage on cryptographic module

No stipulation.

6.2.8. Method of activating private key

The CA private key is protected by a strong passphrase of at least 15 characters long generated on the RomanianGRID CA signing machine, and known only to designated personnel of the CA.
All end entity private keys must be properly protected. The user private key must be protected by a strong passphrase of at least 12 characters, following current best practice in choosing high-quality passwords. Host and service private keys may be stored without a passphrase if adequately protected by system methods.

6.2.9. Method of deactivating private key

No stipulation.

6.2.10. Method of destroying private key

No stipulation.

6.2.11. Cryptographic Module Rating

No stipulation.

6.3. Other aspects of key pair management

6.3.1. Public key archival

The RomanianGRID CA archives all issued certificates on removable media stored in a secure place.

6.3.2. Certificate operational periods and key pair usage periods

The lifetime of the RomanianGRID CA root certificate is 20 years.

6.4. Activation data

6.4.1. Activation data generation and installation

The private key is protected by a strong passphrase of at least 15 characters long generated on the RomanianGRID CA signing machine.

6.4.2. Activation data protection

RomanianGRID CA uses a passphrase to activate its private key which is known only by the RomanianGRID CA operators. A copy in written form of the passphrase is kept in a sealed envelope in a safe. Access to the safe is restricted only to the RomanianGRID CA operators.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

- The security status of the operating systems of the RomanianGRID CA computers are maintained up to date by applying the relevant patches;
- Monitoring is performed to detect unauthorized software changes;
- CA systems configuration is reduced to the bare minimum;
- CA signing machine is a dedicated machine, running no other services than those needed for CA signing operations, and it is powered off and kept in a locked rack between uses;

6.5.2. Computer security rating

No stipulation.

6.6. Life cycle technical controls

6.6.1. System development controls

No stipulation.

6.6.2. Security management controls

No stipulation.

6.6.3. Life cycle security controls

No stipulation.

6.7. Network security controls

- The CA signing machine is not connected to any network and it is kept powered off between uses.
- The CA public server is protected by firewall.

6.8. Time-stamping

No stipulation.

7. Certificate, CRL and OCSP profiles

7.1. Certificate profile

7.1.1. Version number(s)

Version number of the RomanianGRID CA certificates is X.509 v3

7.1.2. Certificate extensions

User, Digital processing entity or Robot:

- Basic constrains (critical): Not a CA
- Key usage (critical): Digital signature, key encipherment, data encipherment
- Subject key identifier
- Authority key identifier
- Subject alternative name
- Issuer alternative name
- CRL distribution points
- Certificate policies: OIDs as in 7.1.6
- Netscape cert type

7.1.3. Algorithm object identifiers

No stipulation.

7.1.4. Name forms

Issuer:

- DC=RO
- DC=RomanianGRID
- O=ROSA
- OU=Certification Authority
- CN=RomanianGRID CA

Subject:

- DC=RO
- DC=RomanianGRID
- CN=Subject name

7.1.5. Name constraints

As described in sections 3.1.1, 3.1.2 and 7.1.4

7.1.6. Certificate policy object identifier

Subscriber certificates contain the following object identifiers:

- The Certificate Policy OID (as in section 1.2) valid at the time the certificate was issued: 1.3.6.1.4.1.27103.9.1.2.1.2.0
- The IGTF Classic Authentication Profile OID valid at the time this CP/CPS was issued (1.2.840.113612.5.2.2.1), in case of user or digital processing entity.
- The IGTF 1SCP "Policy on Automated Clients or Robot Entities" OID valid at the time this CP/CPS was issued (1.2.840.113612.5.2.3.3.1) in case of robot certificates.

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 will be issued in X.509 v2 format.

7.2.2. CRL and CRL entry extensions

No stipulation.

7.3. OCSP profile

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

No stipulation.

8. Compliance, audit and other assessments

8.1. Frequency or circumstances of assessment

RomanianGRID CA may be audited by other trusted CAs to verify its compliance with the rules and procedures described in this document. Any costs associated with such an audit must be covered by the requesting party. All records shall be made available to external auditors.

8.2. Identity/qualifications of assessor

No stipulation.

8.3. Assessor's relationship to assessed entity

No stipulation.

8.4. Topics covered by assessment

The audit will verify the compliance of the service provided by the RomanianGRID CA with its latest CP/CPS approved.

8.5. Actions taken as a result of deficiency

In case of deficiency the RomanianGRID CA will announce a timetable which includes the steps to be taken for solving the compliance problems.

8.6. Communication of results

The results will be made public on the CA website.

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 therefore there is no refund policy.

9.2. Financial responsibility

9.2.1. Insurance coverage

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

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

9.4.1. Privacy plan

RomanianGRID CA does not collect any confidential or private information.

9.4.2. Information treated as private

RomanianGRID CA does not collect any confidential or private information.

9.4.3. Information not deemed private

The following information is not deemed as private:

- Subscriber's name
- Subscriber's email address
- Subscriber's organization
- Subscriber's office phone number
- Subscriber's research domain
- Subscriber's department
- Subscriber's position
- Subscriber's certificate

9.4.4. Responsibility to protect private information

No stipulation.

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

- HellasGrid CA Certification Policy and Certification Practice Statement
- pkIRISGrid CA Certificate Policy (CP) and Certification Practice Statement (CPS)
- UK e-Science Certification Authority Certificate Policy and Certification Practices Statement
- DutchGrid and NIKHEF Medium-security X.509 Certification Authority Certification Policy and Practice Statement

9.6. Representations and warranties

9.6.1. CA representations and warranties

No stipulation

9.6.2. RA representations and warranties

No stipulation.

9.6.3. Subscriber representations and warranties

No stipulation.

9.6.4. Relying party representations and warranties

No stipulation.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7. Disclaimers of warranties

No stipulation.

9.8. Limitations of liability

RomanianGRID 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 accepted by a relying party.
RomanianGRID CA declines any liability for damages arising from the non-issuance of a requested certificate, or for revocation of a certificate initiated by the CA or the appropriate RA in conformity with this CP/CPS.

9.9. Indemnities

RomanianGRID CA declines any payment of indemnities for damages arising from the use or rejection of its issued certificates.

9.10. Term and termination

9.10.1. Term

This document becomes effective after its accreditation and publication on the RomanianGRID CA website.
No term is set for its expiration.

9.10.2. Termination

This document remains effective until it is superseded by a newer version.

9.10.3. Effect of termination and survival

No stipulation.

9.11. Individual notices and communications with participants

No stipulation.

9.12. Amendments

9.12.1. Procedure for amendment

The document must be changed whenever necessary. The amendments must be applied in accordance with section 1.5.

9.12.2. Notification mechanism and period

Subscribers will not be announced in advance about the CP/CPS changes. All previous versions of the document will be published on the RomanianGRID CA online repository. All new versions of the CP/CPS will be announced to the EUGridPMA. The most recent CP/CPS will be published as current CP/CPS as soon as EUGridPMA approves it.

9.12.3. Circumstances under which OID must be changed

The OID must be changed when the document suffered modifications. For minor modifications (rephrasing, small corrections, etc.) only the minor version of the OID must be changed. When there is a substantial amendment of the CP/CPS, the major version of the OID must be changed.

9.13. Dispute resolution provisions

No stipulation.

9.14. Governing law

The RomanianGRID CA and its operations are subject to the Romanian law.

9.15. Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of the RomanianGRID CA certificates must comply with the Romanian law.

9.16. Miscellaneous provisions

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.