Macedonian Academic and Research Grid Initiative

MARGI CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Document O.I.D: 1.3.6.1.4.1.28430.10.1.1.0

Version 1.0

January, 2008

Table of Contents:

1. INTRODUCTION

This document describes the rules and procedures used by the MARGI Certification Authority.

1.1 Overview

MARGI (Macedonian Academic Research Grid Initiative) was established on April 15th, 2005 by University of Sts. Cyril and Methodius, Skopje. It is operated by MARNET (Macedonian Academic and Research Network) that also is hosted and managed by University of Sts. Cyril and Methodius team. The main focus of MARGI is:

- coordinate efforts to further develop academic and high performance computing facilities and help them integrate into MARNET;
- organize dissemination and training activities and help research communities from the former Yugoslav Republic of Macedonia to develop and deploy applications that use MARNET infrastructure;
- coordinate fund raising efforts to improve MARNET infrastructure and human resources;
- facilitate wider participation of MARNET members in Framework 7 and other international GRID projects;
- create a national GRID development policy;

Any additional information can be obtained at: http://www.margi.marnet.net.mk/
In order to strengthen MARGI infrastructure and facilitate its efficient usage by research community from FYR of Macedonia, as well as to allow full integration of our user community and computing resources into the pan-European and other Grid infrastructures, it was necessary to establish MARGI Certification Authority. The MARGI CA will provide security infrastructure needed for the operation of all of MARGI resources and authentication of all MARGI users, hosts and services.
This document is a combined certification policy and certificate practice statement. It describes the set of procedures followed by the MARGI Certification Authority (CA) in issuing certificates as well as the responsibilities of the involved parties.
The MARGI CA is operated at the premises of MARNET located in the rectorate building of University of Sts. Cyril and Methodius.
This document is structured according to RFC 3647.
This document was issued on 10 November 2007, and took effect on 14 January 2008.

1.2 Document name and identification

Document title: MARGI CA Certificate Policy and Certificate Practices Statement
Document version: Version 1.0
Document date: 10 November 2007
ASN.1 Object Identifier (OID): 1.3.6.1.4.1.28430.10.1.1.0
The next table describes the meaning of the OID:

1.3.6.1.4.1	Prefix for IANA private enterprises
28430	University of Cyril and Methodius 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

MARGI certificates are signed by MARGI CA. MARGI CA provides PKI services to the academics and research communities from FYR of Macedonia who participate in national or international Grid activities. The MARGI does not issue 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 MARGI CA website.

1.3.3 Subscribers

The MARGI CA issues user (personal), host and service certificates. Subscribers eligible for certification from MARGI CA are:
- Users and site administrators of Macedonian Academic Research Grid Initiative (MARGI).
- Computers used in activities of Macedonian Academic Research Grid Initiative (MARGI).
- Services or host applications which are running on computers used in Macedonian Academic Research Grid Initiative (MARGI).

1.3.4. Relying parties

Users of Grid computing infrastructures that are using the public keys, in certificates issued by the MARGI 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 personal certificates for email signing and user authentication using https.

1.4.2 Prohibited certificate uses

Notwithstanding the above, using certificates for purposes contrary to the law in FYR of Macedonia is explicitly prohibited.

1.5 Policy administration

1.5.1 Organization administering the document.

The MARGI CP/CPS document was authored and is administered by the Macedonian Academic Research and Education Network – MARNet.

The MARGI CA address for operations issues is:
MARGI Certification authority
Macedonian Academic Research and Education Network
bul. Krste Misirkov bb
Skopje 1000
FYR of Macedonia
Phone: (+389) 2 3293-294
Phone: (+389) 2 3293-295
Fax: (+389) 2 3293-299
e-mail: margi-ca@margi.marnet.net.mk

1.5.2 Contact person

Contact person for questions related to this document or any other MARGI CA related issue is:
Aleksandar Dimeski
Macedonian Academic Research and Education Network - MARNet
bul. Krste Misirkov bb
Skopje 1000
FYR of Macedonia
Phone: (+389) 2 3293-296
Fax: (+389) 2 3293-299
e-mail: A.Dimeski@ukim.edu.mk

1.5.3 Person determining CPS suitability for the policy

The person who determines the CPS suitability for the policy is the same person as in section 1.5.2.

1.5.4 CPS approval procedures

New versions of the Certification Practice Statement are reviewed internally in order to verify their suitability against the minimum requirements, which are defined by the IGTF. Internal approval is followed by the submission of the CPS to the EUGridPMA, in order to go through the EUGridPMA accreditation procedure.

1.6 Definitions and acronyms

MARGI	Macedonian Academic Research Grid Initiative
MARNet	Macedonian Academic Research and Education Network
ASN	Abstract Syntax Notation One (http://asn1.elibel.tm.fr/)
CA	Certification Authority
CN	Common Name
CP/CPS	Certificate Policy/Certificate Practice Statement
CRL	Certificate Revocation List

DN	Distinguished Name
DNS	Domain Name System
EUGridPMA	European Policy Management Authority for Grid Authentication
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
IGTF	International Grid Trust Federation
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Change
S/MIME	Secure / Multipurpose Internet Mail Extensions
SEE-GRID	South East European GRid-enabled eInfrastructure Development
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
USB	Universal Serial Bus

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The MARGI operates an on-line repository that contains:

- The MARGI root certificate
- All 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.
- Other relevant information

The MARGI CA communication information for information regarding repositories is:

MARGI Certification authority
Macedonian Academic Research and Education Network
bul. Krste Misirkov bb
Skopje 1000
FYR of Macedonia
Phone: (+389) 2 3293-294
Phone: (+389) 2 3293-295
Fax: (+389) 2 3293-299
Web: http://www.margi-ca.marnet.net.mk
e-mail: margi-ca@margi.marnet.net.mk

2.2 Publication of certification information

The MARGI CA is obliged to maintain on-line repository which is described in section 2.1.

2.3 Time or frequency of publication

- Certificates will be published as soon as they are issued.
- CRL publication frequency is defined in section 4.9.7.
- This CP/CPS will be published whenever it is updated.

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.
MARGI CA may impose a more restricted access control policy to the repository at its discretion.
The MARGI 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.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.

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

MARGI 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

Distinguished names for each certificate must be unambiguous and unique, and it must be

linked to one and only one entity over the entire lifetime of the CA. When essential, extra characters may be affixed to the original name to guarantee the uniqueness of the subject name. Single subscriber may have more than one associated distinguished name.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of a key

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

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

3.2.3 Authentication of individual entity

Certificate of a person:
The subject should personally meet the RA staff in order to validate his/her identity. The subject authentication is fulfilled by providing an official document with picture (ID-card, driving license or a passport) declaring that the subject is a valid end entity. Subjects affiliation must be proven by specific document issued by subjects organization. Upon subjects authentication the RA will make a photocopy of the ID document. The gathered photocopies will be forwarded to the CA for archival.

Certificate of a host or service:
Host certificates can only be requested by the administrator responsible for the particular host. The certificate requests are sent to RA by e-mail signed from the responsible administrator. In order to request a host certificate the following conditions must be met:

1. The host must have a valid DNS name.
2. The administrator must already possess a valid personal MARGI certificate.
3. The administrator must provide a proof of his or hers relation to the host itself.

The RA must archive all email requests for the approved host or service certificate requests.

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

The subscriber requesting service from the MARGI CA 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

Expiration warnings will be sent to subscribers before it is rekey time. Rekey before expiration can be executed by stating a rekey request signed with the personal certificate of the subscriber. Rekey after expiration uses completely the same authentication procedure as new certificate. Once every 5 years the subscriber has to be authenticated by the local RA.

3.3.2 Identification and authentication for re-key after revocation

The procedure for re-authentication 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 MARGI certificate.
- 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 from RA should be done by e-mail signed with a valid RA operator key.
- Revocation request from any other entity presenting evidence of revocation circumstances.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

4.1.1 Who can submit a certificate application

The applicant must:

1. be an acceptable subscriber as stated in section 1.3.3
2. read and adhere to all of the statements of this document
3. generate a key-pair using a trustworthy method. The private key must be at least 1024 bits.

4. use a strong passphrase of at least 12 characters

4.1.2 Enrollment process and responsibilities

1. **User certificate:** A subscriber must submit the certificate requests via the SSL secured web form or email to the serving RA. A subscriber must be authenticated by the RA serving his/her location following the procedure described in section 3.2.3. If the subscriber wants to rekey his/her certificate, then he/she must follow the procedures described in section 4.7.
2. **Host or service certificate**: The subject must already have a valid MARGI CA certificate before requesting a host or service certificate. The submission of the certificate request can be done either via a web interface or via e-mail. In the first case the subject will have first to import his/her MARGI CA certificate in the browser in order to be authenticated automatically by the MARGI CA portal. Upon successful authentication the user will be able to submit the certificate request via a web based form. In the second case the subject will have to send an e-mail signed via his/her MARGI CA certificate to e-mail from section 1.5.1 with the certificate requests attached and stating in the body of the e-mail that he is the person responsible for the host/service. In both cases the certificate request will be forwarded to the appropriate RA, who will approve or disapprove the request according to sections 4.2.1 and 4.2.2

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All the certificate applications will be authenticated and validated by the MARGI CA RAs as stated in section 3.2.3. A case of rekey is addressed in section 3.3.1. Upon successful authentication, the information included in the certificate request will be validated by CA.

4.2.2 Approval or rejection of certificate applications

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

1. the subscriber must be authenticated by RA;
2. the subject must be an acceptable subscriber entity, as defined by this Policy;
3. the subject must have a valid e-mail address;
4. the request must obey the MARGI CA distinguished name scheme;
5. the distinguished name must be unique;
6. the key must be at least 1024 bits;
7. each applicant generates his/her own key by using OpenSSL or similar software;
8. host and service certificate requests must be submitted via SSL protected HTTP transport or via e-mail signed by a valid MARGI CA certificate;
9. user certificate requests must be submitted via SSL protected HTTP transport;
10. requests for certification keys with exponent == 3 will be rejected.

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 the e-mail address from section 1.5.1.

4.2.3 Time to process certificate applications

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

After CA receives certificate request the request is transferred to the dedicated CA machine by using removable media. Certificate is signed and transferred back to the web repository by using removable media. After the subscriber's certificate is issued, an e-mail will be sent to the relevant RA manager and to the subscriber itself informing him/her about the action.

4.3.2 Notification to subscriber by the CA of issuance of certificate

If the subscriber has requested a certificate through the RA, an e-mail will be sent to the relevant RA manager right after subscriber's certificate is issued.

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.
If a user does not accept certificate within 5 working days of signing a certificate, the certificate will be revoked.

4.4.1 Conduct constituting certificate acceptance

The certificate acceptance e-mail will be stating that:
1. He or She has read this policy and accepts to adhere to it;
2. He or She accepts his/her certificate signed by the MARGI CA;
3. He or She assumes the responsibility to notify the MARGI CA immediately:
    - in case of possible private key compromise;
    - when the certificate is no longer required;
    - when the information in the certificate becomes invalid.

4.4.2 Publication of the certificate by the CA

All the certificates issued by the MARGI CA will be published in the on-line repository operated by the MARGI CA.

4.4.3 Notification of certificate issuance by the CA to other entities

Corresponding RA that has handled the communication with the requesting subscriber will be notified of the certificate issuance.
The RA will be informed about any certificate signatures and rekeys 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 key along with the certificates issued by the MARGI CA usage is defined in section 1.4.1.
The private key associated with any certificate must not be disclosed to or shared with end-entities other than the one to which the certificate was issued.

4.5.2 Relying party public key and certificate usage

Relying parties can use the public keys and certificates of the subscribers for:
1. email encryption and signature verification (S/MIME);
2. host authentication and encryption of communications;
3. user authentication.
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

MARGI 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

Same as in section 4.6.1.

4.6.3 Processing certificate renewal requests

Same as in section 4.6.1.

4.6.4 Notification of new certificate issuance to subscriber

Same as in section 4.6.1.

4.6.5 Conduct constituting acceptance of a renewal certificate

Same as in section 4.6.1.

4.6.6 Publication of the renewal certificate by the CA

Same as in section 4.6.1.

4.6.7 Notification of certificate issuance by the CA to other entities

Same as in section 4.6.1.

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 MARGI CA;
2. revocation of their certificate by the MARGI CA;
Subscribers can regenerate their key pair 30 days before certificate expiration.

4.7.2 Who may request certification of a new public key

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

4.7.3 Processing certificate re-keying requests

Expiration warnings will be sent to subscribers before it is rekey time. Rekey before expiration can be executed by stating a rekey request signed with the personal certificate of the

subscriber. Rekey after expiration uses completely the same authentication procedure as new certificate. As mentioned in section 3.3.1 once in the specified period the subscriber must go through the same authentication procedure.
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 Circumstances for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A certificate will be revoked when the information it contains or the implied assertions it carries are known or suspected to be incorrect, compromised or the Subscriber does not need the certificate any more. This includes situations where:

- The CA is informed that the Subscriber has ceased to be a member of or associated with a MARGI 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.
- Evidence presented from any other entity of revocation circumstances.

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 MARGI CA certificate. Otherwise authentication will be performed with the same procedure as described in section 3.2.3. Also if CA or RA can individually prove by performing individual analysis that evidence for revocation provided by third party is correct it will be accepted as valid request.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

MARGI CA will process all revocation requests within 1 working day after receiving a revocation request.

4.9.6 Revocation checking requirement for relying parties

Relying parts must download the CRL from the online-repository [section 2.2] 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 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

No stipulation.

4.9.9 On-line revocation/status checking availability
Currently there are no on-line revocation/status services offered by the MARGI CA.

4.9.10 On-line revocation checking requirements
Same as in section 4.9.9.

4.9.11 Other forms of revocation advertisements available
No stipulation.

4.9.12 Special requirements re key compromise
No stipulation.

4.9.13 Circumstances for suspension
MARGI CA does not suspend certificates.

4.9.14 Who can request suspension
Same as in section 4.9.13.

4.9.15 Procedure for suspension request
Same as in section 4.9.13.

4.9.16 Limits on suspension period
Same as in section 4.9.13.

4.10 Certificate status services

4.10.1 Operational characteristics
MARGI CA operates an on-line repository that contains all the CRLs that has been issued. Promptly following revocation, the CRL or certificate status database in the repository, as applicable, shall be 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
No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

The MARGI CA operates in a controlled and protected room located in University of Sts Cyril and Methodius Computer Center. At least one person employed by University of Sts Cyril and Methodius Computer Center always will be present on premises 24 hours per day, 7 days per week.

5.1.2 Physical access

Physical access to the MARGI 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

Ss. Cyril and Methodius University - Skopje have 24 hours per day, 7 days per week personal security.

5.1.6 Media storage

Backups are to be stored in removable storage media.

5.1.7 Waste Disposal

Removable storage media 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

MARGI CA personnel are selected in mutual agreement between MARGI Coordinator and the respective MARGI CA operating organization (University of Sts Cyril and Methodius Computer Center).

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to MARGI CA and RA operators.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

Documentation regarding all the operational procedures of the CA is supplied to personnel during the initial training period.

5.4 Audit logging procedures

5.4.1 Types of events recorded

CA must keep log of the following events:

- 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 MARGI 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
- login/logoff/reboot of the signing machine
- personal identification photocopies gathered by the RA

The CA recoded events will be logged on paper and archived by CA. and kept in a safe in the MARGI CA premises.

Each RA must archive log of the following events:

- 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.

The RA recorded events will be logged in electronic form and kept in premises of the RA with controlled access.

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 MARGI CA.

5.5.7 Procedures to obtain and verify archive information

No stipulation

5.6 Key changeover

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 maximum validity period for certificates as defined in section 6.3.2. 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;
- Generate a new CA certificate with a new key pair that will be soon available on the website.

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 MARGI 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

Before the MARGI RA terminates its services, it will:

- inform the CA it is aware of
- make information of its termination available on its and CA website
- 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 MARGI 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

Defined in 4.1.2.

6.1.4 CA public key delivery to relying parties

The MARGI CA root certificate is available on the website defined in section 2.1.

6.1.5 Key Sizes

For a user or host certificate the key size is at least 1024 bits. The MARGI 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)

MARGI Keys may be used for authentication, data encipherment, message integrity and session establishment.
MARGI CA private key will only be used to issue CRLs and new certificates.

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 MARGI CA private key is kept encrypted in multiple copies in USB flash drive and CD-ROM. 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

MARGI CA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

MARGI CA does not use any kind of cryptographic module.

6.2.7 Private key storage on cryptographic module

Same as in section 6.2.6.

6.2.8 Method of activating private key

The private key of the MARGI CA is activated by using a pass phrase. See section 6.4.1

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

After termination of the CA, all media that contain the private key of the CA will be securely and permanently destroyed, according to then best current practice.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

No stipulation.

6.3.1 Public Key Archival

Public keys of all issued certificates are archived as a part of certificate archival.

6.3.2 Certificate operational periods and key pair usage periods

MARGI CA root certificate has a validity of twenty years. For subscribers, the maximum validity period for a certificate is one year plus one month.

6.4 Activation Data

6.4.1 Activation data generation and installation

MARGI 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.
MARGI CA private key is protected by a passphrase of at least 15 characters. Pass phrase is regenerated every 180 days by one of MARGI CA operators.

6.4.2 Activation data protection

The subscriber is responsible to protect the activation data for his/her private key.
The MARGI CA uses a pass phrase to activate its private key which is known only by the MARGI CA Manager and the MARGI CA Operators. A copy in written form of the pass phrase is sealed in an envelope and kept in a safe. Access to the safe is restricted only to the MARGI CA Manager and Operators. Old activation data are destroyed according to current best practices.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical 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

MARGI CA supports and uses the following X.509 v3 Certificate extensions.
For CA root certificate the extensions are:

- X509v3 Basic Constraints: critical, CA:TRUE
- X509v3 Key Usage: critical, CRL Sign, Key Cert Sign
- X509v3 Subject Key Identifier: <CA key ID>
- X509v3 Authority Key Identifier:
    - keyid:<CA key ID>
- X509v3 Issuer Alternative Name: email:margi-ca@margi.marnet.net.mk
- X509v3 Subject Alternative Name: email:margi-ca@margi.marnet.net.mk

For user certificate the extensions are:

- X509v3 Basic Constraints: critical CA:FALSE
- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
- 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>

- X509v3 Subject Alternative Name: email:<user's email address>
- X509v3 Issuer Alternative Name: email:margi-ca@margi.marnet.net.mk
- X509v3 Certificates Policies:
    - Policy: <OID of the effective CP/CPS>
- X509v3 CRL Distribution Points

In case of host and service certificates the extensions are:

- 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, TLS Web Client Authentication
- X509v3 Subject Key Identifier: <subject key ID>
- X509v3 Authority Key Identifier:
    - keyid:<CA key ID>
- X509v3 Issuer Alternative Name: email:margi-ca@margi.marnet.net.mk
- X509v3 Subject Alternative Name: DNS:FDQN
- X509v3 Certificates Policies:
    - Policy: <OID of the effective CP/CPS>
- X509v3 CRL Distribution Points

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Issuer:
C=MK,O=MARGI,CN=MARGI CA
Subject:
C=MK,O=MARGI,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 the web page defied in section 2.1.
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.
The DN is encoded as PrintableString as defined in RFC2252.

7.1.5 Name constraints

Subject attributes constraints:
Country:
Must be “MK”
OrganizationName:
Must be “MARGI”
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)

All CRLs will be issued in X.509 version 2.

7.2.2 CRL and CRL entry extensions

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 MARGI CA must allow to be audited by EUGridPMA members 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.
MARGI CA will perform operational audit of the CA/RA staff at least once per year.

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

In case of a deficiency, the MARGI CA 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

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

Same as section in 9.1.1.

9.1.3 Revocation or status information access fees

Same as section in 9.1.1.

9.1.4 Fees for other services

Same as section in 9.1.1.

9.1.5 Refund policy

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

9.2 Financial responsibility

MARGI CA denies any financial responsibilities for damages or impairments resulting from its operation.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

The MARGI CA collects information about the subscribers.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

MARGI CA collects a photocopy of an ID document which is considered as private according to the “Law for protection of personal data” will be kept confidential.

9.4.3 Information not deemed private

MARGI CA collects the following information which is not deemed as private:
1. subscriber's e-mail address;
2. subscriber's name;
3. subscriber's organization;
4. subscriber's certificate;

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

MARGI CA has the responsibility to protect the private information defined in section 9.4.2. The photocopies of ID documents will be kept private in a safe by the CA and will be only used while the audit process. The data from the photocopied documents will not be processed for any other purposes.

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;
6. AEGIS CA Certificate Policy;
7. MAGRID CA Certificate Policy;

9.6 Representations and warranties

9.6.1 CA representations and warranties

The MARGI CA is solely responsible for the issuance and management of certificates referencing this CP/CPS. The MARGI CA shall:

- handle certificate requests and issue new certificates:
    - confirm certification requests from entities requesting a certificate according to the procedures described in this CP/CPS
    - issue certificates based on requests from authenticated entities
    - send notification of issued certificates to requesting entities and corresponding RA
    - make issued certificates publicly available
- handle certificate revocation requests and certificate revocation:
    - confirm revocation requests from entities requesting that a certificate be revoked according to the procedures described in this CP/CPS
    - issue CRL's
    - make certificate revocation information publicly available
    - publish MARGI CA's root of trust to a trust anchor repository defined by accrediting

9.6.2 RA representations and warranties

Each RA shall:

- accept conditions and adhere to the procedures described in this CP/CPS
- handle certificate requests
    - verify that the information provided in the certificate request is correct and check that the email address provided by the subscriber is correct
    - authenticate the identity of the person requesting a certificate
    - check that the subscriber knows and agrees to subscriber obligations as defined in 9.6.3.
    - approve and sign certificate requests
    - notify the MARGI CA that a certificate request is authenticated and approved
- handle certificate revocation requests
    - verify that the information provided in the certificate revocation request is correct
    - approve and sign revocation requests
    - notify the MARGI CA that the certificate revocation request is authenticated and approved

9.6.3 Subscriber representations and warranties

In requesting a certificate, subscribers agree to:

- accept conditions and adhere to the procedures described in this CP/CPS
- provide true and accurate information to the MARGI CA and only such information as he/she is entitled to submit for the purposes of this CP/CPS
- use the certificate exclusively for authorized and legal purposes, consistent with this CP/CPS
- by using the authentication procedures described in this CP/CPS subscribers accept the restrictions to liability
- by using the authentication procedures described in this CP/CPS subscribers accept the statements relating to confidentiality of information in section 9.3
- generate a key pair using a trustworthy method
- use at least 12 characters long passphrase, consisting of letters, number and signs, to protect private key of user certificate
- ensure that private key of host or service certificate is readable only by root or a restricted user account
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate
- notify the MARGI CA immediately in case a private key is lost or compromised.

9.6.4 Relying party representations and warranties

In using a certificate issued by the MARGI CA relying parties agree to:

- accept conditions and adhere to the procedures described in this CP/CPS
- verify the certificate revocation information before using a certificate
- use the certificate exclusively for authorized and legal purposes, consistent with this CP/CPS.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

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

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

Legal disputes arising from the operation of the MARGI CA will be resolved according to the FYR of Macedonia Law.

9.14 Governing law

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

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.