MREN

MREN CA

CERTIFICATE POLICY
AND
CERTIFICATION PRACTICE STATEMENT

Table of Contents:

TABLE OF CONTENTS: 2

1. INTRODUCTION 7

1.1 OVERVIEW 7
1.2 DOCUMENT NAME AND IDENTIFICATION 8
1.3 PKI PARTICIPANTS 8
1.3.1 Certification authorities 8
1.3.2 Registration authorities 8
1.3.3 Subscribers 8
1.3.4. Relying parties 9
1.3.5 Other participants 9
1.4 CERTIFICATE USAGE 9
1.4.1 Appropriate certificate uses 9
1.4.2 Prohibited certificate uses 9
1.5 POLICY ADMINISTRATION 9
1.5.1 Organization administering the document. 9
1.5.2 Contact person 9
1.5.3 Person determining CPS suitability for the policy 10
1.5.4 CPS approval procedures 10
1.6 DEFINITIONS AND ACRONYMS 10

PUBLICATION AND REPOSITORY RESPONSIBILITIES 11

2.1 REPOSITORIES 11
2.2 PUBLICATION OF CERTIFICATION INFORMATION 11
2.3 TIME OR FREQUENCY OF PUBLICATION 11
2.4 ACCESS CONTROL ON REPOSITORIES 11

3 IDENTIFICATION AND AUTHENTICATION 12

3.1 NAMING 12
3.1.1 Types of names 12
3.1.2 Need for names to be meaningful. 12
3.1.3 Anonymity or pseudonmity of subscribers 12
3.1.4 Rules for interpreting various name forms 12
3.1.5 Uniqueness of names 12
3.1.6 Recognition, authentication, and role of trademarks 12
3.2 INITIAL IDENTITY VALIDATION 13
3.2.1 Method to prove possession of a key 13
3.2.2 Authentication of organization identity 13
3.2.3 Authentication of individual entity 13
3.2.4 Non-verified subscriber information 13
3.2.5 Validation of Authority 13
3.2.6 Criteria of interoperation 14
3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 14
3.3.1 Identification and authentication for routine re-key 14
3.3.2 Identification and authentication for re-key after revocation 14
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 14

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 14

4.1 CERTIFICATE APPLICATION 14
4.1.1 Who can submit a certificate application 14
4.2 CERTIFICATE APPLICATION PROCESSING 15
4.2.1 Performing identification and authentication functions 15

4.2.2 Approval or rejection of certificate applications *15*
4.2.3 Time to process certificate applications *15*
4.3 CERTIFICATE ISSUANCE 16
4.3.1 CA actions during certificate issuance *16*
4.3.2 Notification to subscriber by the CA of issuance of certificate *16*
4.4 CERTIFICATE ACCEPTANCE 16
4.4.1 Conduct constituting certificate acceptance *16*
4.4.2 Publication of the certificate by the CA *16*
4.4.3 Notification of certificate issuance by the CA to other entities *16*
4.5 KEY PAIR AND CERTIFICATE USAGE 17
4.5.1 Subscriber private key and certificate usage *17*
4.5.2 Relying party public key and certificate usage *17*
4.6 CERTIFICATE RENEWAL 17
4.6.1 Circumstance for certificate renewal *17*
4.6.2 Who may request renewal *17*
4.6.3 Processing certificate renewal requests *17*
4.6.4 Notification of new certificate issuance to subscriber *17*
4.6.5 Conduct constituting acceptance of a renewal certificate *17*
4.6.6 Publication of the renewal certificate by the CA *17*
4.6.7 Notification of certificate issuance by the CA to other entities *17*
4.7 CERTIFICATE RE-KEY 18
4.7.1 Circumstances for certificate re-key *18*
4.7.2 Who may request certification of a new public key *18*
4.7.3 Processing certificate re-keying requests *18*
4.7.4 Notification of new certificate issuance to subscriber *18*
4.7.5 Conduct constituting acceptance of a re-keyed certificate *18*
4.7.6 Publication of the re-keyed certificate by the CA *18*
4.7.7 Notification of certificate issuance by the CA to other entities *18*
4.8 CERTIFICATE MODIFICATION 18
4.8.1 Circumstances for certificate modification *18*
4.8.2 Who may request certificate modification *18*
4.8.3 Processing certificate modification requests *18*
4.8.4 Notification of new certificate issuance to subscriber *18*
4.8.5 Conduct constituting acceptance of modified certificate *19*
4.8.6 Publication of the modified certificate by the CA *19*
4.8.7 Notification of certificate issuance by the CA to other entities *19*
4.9 CERTIFICATE REVOCATION AND SUSPENSION 19
4.9.1 Circumstances for revocation *19*
4.9.2 Who can request revocation *19*
4.9.3 Procedure for revocation request *19*
4.9.4 Revocation request grace period *19*
4.9.5 Time within which CA must process the revocation request *19*
4.9.6 Revocation checking requirement for relying parties *19*
4.9.7 CRL issuance frequency *20*
4.9.8 Maximum latency for CRLs *20*
4.9.9 On-line revocation/status checking availability *20*
4.9.10 On-line revocation checking requirements *20*
4.9.11 Other forms of revocation advertisements available *20*
4.9.12 Special requirements re key compromise *20*
4.9.13 Circumstances for suspension *20*
4.9.14 Who can request suspension *20*
4.9.15 Procedure for suspension request *20*
4.9.16 Limits on suspension period *20*
4.10 CERTIFICATE STATUS SERVICES 20
4.10.1 Operational characteristics *20*
4.10.2 Service availability *20*
4.10.3 Optional features *20*
4.11 END OF SUBSCRIPTION 21
4.12 KEY ESCROW AND RECOVERY 21

4.12.1 Key escrow and recovery policy and practices *21*
4.12.2 Session key encapsulation and recovery policy and practices *21*

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 21

5.1 PHYSICAL CONTROLS 21
5.1.1 Site location and construction *21*
5.1.2 Physical access *21*
5.1.3 Power and Air Conditioning *21*
5.1.4 Water Exposures *21*
5.1.5 Fire Prevention and Protection *21*
5.1.6 Media storage *21*
5.1.7 Waste Disposal *22*
5.1.8 Off-site Backup *22*
5.2 PROCEDURAL CONTROLS 22
5.2.1 Trusted roles *22*
5.2.2 Number of persons required per task *22*
5.2.3 Identification and authentication for each role *22*
5.2.4 Roles requiring separation of duties *22*
5.3 PERSONNEL CONTROLS 22
5.3.1 Qualifications, experience and clearance requirements *22*
5.3.2 Background check procedures *22*
5.3.3 Training requirements *22*
5.3.4 Retraining frequency and requirements *22*
5.3.5 Job rotation frequency and sequence *22*
5.3.6 Sanctions for unauthorized actions *22*
5.3.7 Independent contractor requirements *22*
5.3.8 Documentation supplied to personnel *23*
5.4 AUDIT LOGGING PROCEDURES 23
5.4.1 Types of events recorded *23*
5.4.2 Frequency of processing log *23*
5.4.3 Retention period for audit log *23*
5.4.4 Protection of audit log *23*
5.4.5 Audit log backup procedures *23*
5.4.6 Audit collection system (internal vs. external) *23*
5.4.7 Notification to event-causing subject *23*
5.4.7 Notification to event-causing subject *23*
5.4.8 Vulnerability assessments *23*
5.5 RECORDS ARCHIVAL 24
5.5.1 Types of records archived *24*
5.5.2 Retention Period for Archive *24*
5.5.3 Protection of Archive *24*
5.5.4 Archive backup procedures *24*
5.5.5 Requirements for time-stamping of records *24*
5.5.6 Archive collection system (internal or external) *24*
5.5.7 Procedures to obtain and verify archive information *24*
5.6 KEY CHANGEOVER 24
5.7 COMPROMISE AND DISASTER RECOVERY 25
5.7.2 Computing resources, software, and/or data are corrupted *25*
5.7.3 Entity private key compromise procedures *25*
5.7.4 Business continuity capabilities after a disaster *25*
5.8 CA OR RA TERMINATION 25

6. TECHNICAL SECURITY CONTROLS 25

6.1 KEY PAIR GENERATION AND INSTALLATION 25
6.1.1 Key Pair Generation *25*
6.1.2 Private key delivery to subscriber *25*
6.1.3 Public key delivery to certificate issuer *26*
6.1.4 CA public key delivery to relying parties *26*

6.1.5 Key sizes........26
6.1.6 Public key parameters generation........26
6.1.7 Key usage purposes (as per X.509 v3 key usage field)........26
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS........26
6.2.1 Cryptographic module standards and controls........26
6.2.2 Private key (n out of m) multi-person control........26
6.2.3 Private key escrow........26
6.2.4 Private key backup........26
6.2.5 Private key archival........26
6.2.6 Private key transfer into or from a cryptographic module........26
6.2.7 Private key storage on cryptographic module........26
6.2.8 Method of activating private key........26
6.2.9 Method of deactivating private key........27
6.2.10 Method of destroying private key........27
6.2.11 Cryptographic Module Rating........27
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT........27
6.3.1 Public Key Archival........27
6.3.2 Certificate operational periods and key pair usage periods........27
6.4 ACTIVATION DATA........27
6.4.1 Activation data generation and installation........27
6.4.2 Activation data protection........27
6.4.3 Other aspects of activation data........27
6.5 COMPUTER SECURITY CONTROLS........28
6.5.1 Specific computer security technical requirements........28
6.5.2 Computer security rating........28
6.6 LIFE CYCLE TECHNICAL CONTROLS........28
6.6.1 System development controls........28
6.6.2 Security management controls........28
6.6.3 Life cycle security controls........28
6.7 NETWORK SECURITY CONTROLS........28
6.8 TIME STAMPING........28

7. CERTIFICATE, CRL AND OCSP PROFILES........28

7.1 CERTIFICATE PROFILE........28
7.1.1 Version Number........28
7.1.2 Certificate Extensions........28
7.1.3 Algorithm Object Identifiers........29
7.1.4 Name Forms........29
7.1.5 Name constraints........30
7.1.6 Certificate Policy Object Identifier........30
7.1.7 Usage of Policy Constraints extension........30
7.1.8 Policy qualifiers syntax and semantics........30
7.1.9 Processing semantics for the critical Certificate Policies extension........30
7.2 CRL PROFILE........30
7.2.1 Version number(s)........30
7.2.2 CRL and CRL entry extensions........30
7.3 OCSP PROFILE........30
7.3.1 Version number(s)........30
7.3.2 OCSP extensions........30

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS........31

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT........31
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR........31
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY........31
8.4 TOPICS COVERED BY ASSESSMENT........31
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY........31
8.6 COMMUNICATION OF RESULTS........31

9 OTHER BUSINESS AND LEGAL MATTERS........31

9.1 FEES......31
9.1.1 Certificate issuance or renewal fees......31
9.1.2 Certificate access fees......31
9.1.3 Revocation or status information access fees......31
9.1.4 Fees for other services......32
9.1.5 Refund policy......32
9.2 FINANCIAL RESPONSIBILITY......32
9.2.1 Insurance coverage......32
No stipulation.......32
9.2.2 Other assets......32
No stipulation.......32
9.2.3 Insurance or warranty coverage for end-entities......32
No stipulation.......32
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION......32
9.3.1 Scope of confidential information......32
No stipulation.......32
9.3.2 Information not within the scope of confidential information......32
No stipulation.......32
9.3.3 Responsibility to protect confidential information......32
No stipulation.......32
9.4 CONFIDENTIALITY......32
9.4.1 Types of information to be kept confidential......32
9.4.2 Types of information not considered confidential......32
9.4.3 Disclosure of certificate revocation/suspension information......33
9.4.4 Release to law enforcement officials......33
9.4.5 Release as part of civil discovery......33
9.4.6 Disclosure upon owner's request......33
9.4.7 Other information release circumstances......33
9.5 INTELLECTUAL PROPERTY RIGHTS......33
9.6 REPRESENTATIONS AND WARRANTIES......33
9.6.1 CA representations and warranties......33
9.6.2 RA representations and warranties......34
9.6.3 Subscriber representations and warranties......34
9.6.4 Relying party representations and warranties......35
9.6.5 Representations and warranties of other participants......35
9.7 DISCLAIMERS OF WARRANTIES......35
9.8 LIMITATIONS OF LIABILITY......35
9.9 INDEMNITIES......35
9.10 TERM AND TERMINATION......35
9.10.1 Term......35
9.10.2 Termination......35
9.10.3 Effect of termination and survival......36
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS......36
9.12 AMENDMENTS......36
9.12.1 Procedure for amendment......36
9.12.2 Notification mechanism and period......36
9.12.3 Circumstances under which OID must be changed......36
9.13 DISPUTE RESOLUTION PROVISIONS......36
9.14 GOVERNING LAW......36
9.15 COMPLIANCE WITH APPLICABLE LAW......36
9.16 MISCELLANEOUS PROVISIONS......36
9.16.1 Entire agreement......36
9.16.2 Assignment......36
9.16.3 Severability......37
9.16.4 Enforcement (attorneys' fees and waiver of rights)......37
9.16.5 Force Majeure......37
9.17 Other Provisions......37

1. INTRODUCTION

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

1.1 Overview

Montenegrin Research and Education Network (MREN) was established in June 2005.

Montenegrin Research and Education Network (MREN) is the name given to the collection of all networking services and facilities, which support the communication and information requirements of the education and research community in Montenegro.

MREN aims to create, promote, offer, participate in and preserve the requisite bases for effective use of modern telecommunication technologies in the education and research in Montenegro.

The main mission is to connect MREN to GEANT multi-gigabit pan-European data communications network, reserved specifically for research and education use, via fiber optic with high speed.

The MREN's target is to support the substantial use of the Pan-European and world research networks by Montenegrin researchers, scientists, lecturers and students, as well as to facilitate the integration of Montenegrin educational, research and cultural resources in the international information space.

MGI (**Montenegro GRID Initiative**) has been established on November 1st, 2006
The main focus of MGI is:

- coordinate efforts to further develop academic and high performance computing facilities and help them integrate into MGI
- organize dissemination and training activities and help Montenegrin research communities to develop and deploy applications that use MGI infrastructure
- coordinate fund raising efforts to improve MGI infrastructure and human resources;
- facilitate wider participation of MGI members in Framework 6, Framework 7, and other international GRID projects
- create a national GRID development policy.

Any additional information can be obtained at: http://www.mren.ac.me/mgi.php

In order to stregthen MGI infrastructure and facilitate its efficient usage by Montenegrian research community, 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 MREN Certification Authority. The MREN CA will provide security infrastructure needed for the operation of all MREN resources and authentication of all MREN users, hosts and services.

This document is a combined certification policy and certificate practice statement. It describes the set of procedures followed by the Certification Authority (CA) in issuing certificates as well as the responsibilities of the involved parties.

The CA is operated at the premises of University of Montenegro Center of Information System.

This document is structured according to RFC 2527.

This document was issued on May, 2011, and took effect on July 1, 2011.

1.2 Document name and Identification

Document title: MREN CA Certificate Policy and Certificate Practices Statement
Document version: Version 1.1
Document date: May, 2011
ASN.1 Object Identifier (OID): 1.3.6.1.4.1.29544.1.1.1.1
The next table describes the meaning of the OID:

1.3.6.1.4.1	Prefix for IANA private enterprises
29544	University of Montenegro registered identifier
1	Certification Authorities
1	CP/CPS
1.1	Major and minor CP/CPS number.

1.3 PKI Participants

1.3.1 Certification authorities

MREN Certificates are signed by MREN CA. MREN CA provides PKI services to the Montenegrin academics and research communities who participate in national or international Grid activities. The MREN 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 MREN CA website.

1.3.3 Subscribers

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

- Users and site administrators of Montenegro Research and Education Network (MREN)
- Computers used in activities of Montenegro Research and Education Network (MREN)

- Services or host applications which are running on computers used in Montenegro Research and Education Network (MREN).

1.3.4. Relying parties

Users of Grid computing infrastructures that are using the public keys, in certificates issued by the MREN CA for signature verification and/or encryption, receiving signed e-mail, or accessing SSL web server will be considered as relying parties.

1.3.5 Other participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Same as in section 4.5.1

1.4.2 Prohibited certificate uses

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

1.5 Policy Administration

1.5.1 Organization administering the document.

The MREN CP/CPS document was authored and is administered by the University Of Montenegro - Center of Information Systems.
The MREN CA address for operations issues is:
MREN Certification Authority
Center of Information Systems
University of Montenegro
Bul. Džordža Vašingtona bb
81000 Podgorica
Montenegro

Phone:	+382 20 414 282
Phone:	+382 20 414 286
Fax:	+382 20 414 281
E-mail:	mren-ca@ac.me

1.5.2 Contact person

Contact person for questions related to this document or any other MREN CA related issue is:
Lidija Milosavljević
Center of Information Systems
University of Montenegro
Bul. Džordža Vašingtona bb
81000 Podgorica
Montenegro

Phone:	+382 20 414 286
Phone:	+382 67 365 201
Fax:	+382 20 414 281
E-mail:	lidija@ac.me

1.5.3 Person determining CPS suitability for the policy

Same as in section 1.5.2.

1.5.4 CPS approval procedures

No stipulation.

1.6 Definitions and Acronyms

EUGridPMA	European Grid Policy Management Authority
MREN	Montenegro Research and Education Network
MGI	Montenegro Grid Initiative
GEANT	Pan-European Gigabit research network
ASN1	Abstract Syntax Notation One (http://asn1.elibel.tm.fr/)
CA	Certification Authority
CP/CPS	Certificate Policy/Certificate Practice Statement
CRL	Certificate Revocation List
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
TLS	Transport Layer Security
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Change
S/MIME	Secure / Multipurpose Internet Mail Extensions
SEE-GRID	South East European Grid-enabled e-Infrastructure Development
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
USB	Universal Serial Bus
DN	Distinguished Name
RDN	Relative Distinguished Name
DC	Domain Component
O	Organization
OU	Organizational Unit
CN	Common Name
EE	End Entity
RP	Relying Party
CD-ROM	Compact Disc read-only memory
ID	Identity

PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The MREN CA is obliged to maintain on-line repository that is available to all relaying parties through a web interface at: http://www.mren.ac.me or http://mren-ca.ac.me. And it contains:

- The MREN 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 MREN CA communication information for information regarding repositories is:

MREN Certification Authority
University of Montenegro Center of Information Systems
Bul. Džordža Vašingtona bb
81000 Podgorica
Montenegro

Phone:	+382 20 414 282
Phone:	+382 20 414 286
Fax:	+382 20 414 281
E-mail:	mren-ca@ac.me

2.2 Publication of Certification Information

Same as in section 2.1.

2.3 Time or Frequency of Publication

Same as in section 4.9.7.

2.4 Access Control on Repositories

The online repository is maintained on best effort basis and is available substantially on 24 hours per day, 7 days per week basis, subject to reasonable scheduled maintenance.

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

The MREN 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 pseudonymity of subscribers

MREN 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

Issuer:
DC=me, DC=ac, DC=MREN, CN=MREN-CA
Subject:
DC=me, DC=ac, DC=MREN, O=XXX, CN=Subject-name
Where XXX is the name or acronym of the institution.
DN for each certificate must be unambiguous and unique. The DN must be linked to one and only one EE, over the lifetime of the CA. To prevent name collisions between different entities, mainly in issuing personal certificates, a number or other allowed distinguishing characters can be added to the CN to ensure uniqueness. The “CN” field structure for the user or host/service are described in section 3.1.1. A current list of OU’s can be obtained at web repository defined in section 2.1.
Private keys must not be shared among end entities.
DNs cannot be recycled.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of a key

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

The MREN 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 MREN 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 MREN CA authenticates organizations by:

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

3.2.3 Authentication of individual entity

Certificate of a person:

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

Certificate of a host or service:

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

- The host must have a valid DNS name
- The administrator must already possess a valid personal MREN Certificate
- The administrator must provide a proof of his or her relation to the host itself.

The subscriber requesting service from the MREN CA must present valid documents for personal identification (ID-card, driving license or a passport), and a valid document proving host's or service's relation with an institute or organization. RA should ensure that the requester is appropriately authorized by the owner of the associated FQDN or the responsible administrator of the machine to use the FQDN identifiers asserted in the certificate

MREN CA or RA. should have documented evidence on retaining the same identity over time, photocopies of ID documents in case of user certificates and digitally signed e-mails in case of host or service certificates. The RA must communicate with the CA with secure and auditable methods (e.g. signed emails, voice conversations with a known person, personally, SSL protected private web pages).

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 MREN 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 re-key time. Re-key before expiration can be executed by stating a re-key request signed with the personal certificate of the requester. Re-key after expiration uses completely the same authentication procedure as new certificate. For the first time and after that once every 5 years, a subscriber must be authenticated by the RA or CA serving his/her location following the procedure described in section 3.2.3.

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

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate application can be submitted by eligible entities defined in section 1.3.3.

4.1.2 Enrolment process and responsibilities

The applicant must:

1. Read and adhere to all of the statements of this document

2. Generate a key-pair using a trustworthy method. The private key must be at least 1024 bits.
3. Use a strong pass phrase of at least 12 characters
4. **User certificate:** The submission of the certificate requests will be done via an SSL secured web form. A subscriber must follow the procedure described in section 3.2.3. If the subscriber wants to re-key his/her certificate, then he/she must follow the procedures described in section 4.7.
5. **Host or service certificate**: The administrator must follow the procedure described in section 3.2.3. 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 MREN CA certificate in the browser in order to be authenticated automatically by the MREN 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 administrator will have to send an e-mail signed via his/her MREN CA certificate to email address defined in 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 or CA, 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 MREN CA and RAs as stated in section 3.2.3 and 3.3.1. Upon successful authentication, the information included in the certificate request will be validated by RA or CA.

4.2.2 Approval or rejection of certificate applications

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

- The subscriber must be authenticated by RA
- The subject must be an acceptable subscriber entity, as defined by this Policy (section 1.3.3)
- The request must obey the MREN CA distinguished name scheme(section 7.1.4)
- The distinguished name must be unique
- Each applicant generates his/her own key by using OpenSSL
- Host and service certificate requests must be submitted via SSL protected HTTP transport or via e-mail signed by a valid MREN CA certificate
- User certificate requests must be submitted via SSL secured web form or via e-mail
- RA must validate the association of the certificate signing request.
- The 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 or CA to the subject with carbon copy to email address defined in 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

If the certificate was requested through RA, RA must validate the association of the certificate signing request as described in section 3.2.3, the CA will validate the RA signature and RA authority and then issue the certificate.

If the user requested the certificate from the CA, the user must be validated as described in section 3.2.3 and then the certificate will be issued.

CA transfers the certificate request to the dedicated CA machine by using removable media. Certificate is signed and transferred back to the web repository by using removable media.

Right after the subscriber’s certificate is issued, an e-mail will be sent to the relevant RA manager or to the subscriber itself informing him/her about the action.

Communication between CA and RA will be done via encrypted and digitally signed e-mails using S/MIME.

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 and subscriber; right after subscriber’s certificate is issued.

If the subscriber has requested a certificate through the CA, an e-mail will be sent to the subscriber itself informing him/her about the action.

4.4 Certificate Acceptance

4.4.1 Conduct constituting certificate acceptance

The subscriber must send an e-mail, within 5 working days from the day that his/her certificate was issued, in which he will be stating that:

- He or she has read this policy and accepts to adhere to it
- He or she accepts his/her certificate signed by the MREN CA
- He or she assumes the responsibility to notify the MREN CA immediately:
    - In case of possible private key compromise
    - When the certificate is no longer required
    - When the information in the certificate becomes invalid.

The e-mail which the user sends to the CA has to be signed with the key corresponding to the public key in certificate he or she received from the CA.

If the subscriber does not send the e-mail within 5 working days, the certificate becomes the subject for revocation.

If a user wants to reject a certificate, he or she must submit a revocation request (section 4.9).

4.4.2 Publication of the certificate by the CA

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

4.4.3 Notification of certificate issuance by the CA to other entities

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

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

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

- Email signing/verifying and encryption/decryption (S/MIME)
- Server authentication and encryption of communications
- General purpose authentication (e.g. web site authentication)
- User authentication.

4.5.2 Relying party public key and certificate usage

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

- Email encryption and signature verification (S/MIME)
- Server authentication and encryption of communications
- 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

MREN 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:

- Expiration of their certificate signed by the MREN CA
- Revocation of their certificate by the MREN CA.

4.7.2 Who may request certification of a new public key

Same as in section 4.1.1

4.7.3 Processing certificate re-keying requests

Expiration warnings will be sent to subscribers before it is re-key time.

Re-key before expiration can be executed by stating a re-key request signed with the private key corresponding to the public one in the valid personal certificate of the subscriber. The authentication procedure is defined in section 3.3.1.

Re-key after certificate expiration uses completely the same authentication procedure as that for the new certificate.

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

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 MREN 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.
  Subscribers must request revocation as soon as possible, but within one working day after detection of loss or compromise of the private key pertaining to the certificate, or if the data in the certificate is no longer valid.

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 MREN CA certificate. Otherwise authentication will be performed with the same procedure as described in section 3.2.3.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

MREN CA will process all revocation requests within 1 working day.

4.9.6 Revocation checking requirement for relying parties

Relying parts must download the CRL from the online-repository [section 2.2] at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL issuance frequency

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

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

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

4.9.10 On-line revocation checking requirements

Same as section 4.4.9.

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

MREN 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

MREN 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 MREN CA operates in a controlled and protected room located in University of Montenegro Center of Information Systems. At least one person employed by University of Montenegro Center of Information Systems will always be present on premises 24 hours per day, 7 days per week.

5.1.2 Physical access

Physical access to the MREN 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

University of Montenegro Center of Information Systems premises have a fire alarm system installed.

5.1.6 Media storage

Backups are to be stored in removable storage media (CD-ROM, Floppies and USB Flash) in a safe location in University of Montenegro Center of Information Systems premises.

.

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

MREN CA personnel are selected in mutual agreement between MREN Coordinator and the respective MREN CA operating organization (University of Montenegro Center of Information Systems).

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to MREN CA and RA operators.

5.3.4 Retraining frequency and requirements

If the results of the operational audit are not satisfactory, retraining will be considered.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

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 MREN 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
- Login/logout/reboot of the signing machine
- All e-mail messages of correspondence between RA and CA
- Identity validation records (section 3.2.3).

Each RA must archive log of the following:

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

5.5.2 Retention Period for Archive

Minimum retention period is three years.

5.5.3 Protection of Archive

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

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

The archive collection system is internal to the MREN 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 EE certificate lifetime 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

5.7.1 Incident and compromise handling procedures

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

1. Notify subscribers, RAs, Relying Parties and cross-certifying CAs
2. Terminate the issuance and distribution of certificates and CRLs
3. Notify relevant security contacts.

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 MREN CA terminates its services, it will:

- Inform the RA-s, subscribers and RP-es of which the CA is aware
- Make information of its termination available on its website
- Stop issuing certificates
- Annihilate all copies of private keys

Before the MREN RA terminates its services, it will:

- Make information of its termination available on it’s and CA websites
- Stop accepting certificate requests
- Securely transfers archive to CA.

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 MREN CA root certificate are generated on a dedicated machine, not connected to any type of network. The software used for key generation is OpenSSL.
Each subscriber must generate his/her own key pair.

6.1.2 Private key delivery to subscriber

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

6.1.3 Public key delivery to certificate issuer

Applicants can make user/host/service certificate requests as described in section 4.1.2.

6.1.4 CA public key delivery to relying parties

The MREN CA root certificate is available on the website as described in section 2.1.

6.1.5 Key sizes

For a user or host certificate the key size is 1024 or 2048 bits. The MREN 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)

Keys may be used for authentication, data encipherment, message integrity and session establishment. Certificates and CRLs are signed by the CA private key.

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 MREN 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

MREN CA does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

MREN 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 MREN 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

Old activation data are destroyed according to current best practices.

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

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

6.4 Activation Data

6.4.1 Activation data generation and installation

MREN 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. The private key **must** be protected with a strong pass phrase, i.e., at least 12 characters long and following current best practice in choosing high-quality passwords. Private keys pertaining to host and service certificate **may** be stored without a passphrase, but **must** be adequately protected by system methods if stored without passphrase.
MREN CA private key is protected by a pass phrase of at least 15 characters known by specified CA personnel.

6.4.2 Activation data protection

The subscriber is responsible to protect the activation data for his/her private key.
The MREN CA uses a pass phrase to activate its private key which is known only by the MREN CA Manager and the MREN 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 MREN CA Manager and Operators.

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

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

- X509v3 Basic Constraints: critical, CA:TRUE
- X509v3 Key Usage: critical, Certificate Sign, CRL Sign

- X509v3 Subject Key Identifier: <CA key ID>
- X509v3 Authority Key Identifier: keyid: <CA key ID>
- X509v3 Issuer Alternative Name: email: mren-ca@ac.me
- X509v3 Subject Alternative Name: email: mren-ca@ac.me.

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

- X509v3 Basic Constraints: critical, CA:FALSE
- X509v3 Key Usage: critical, Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
- 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: mren-ca@ac.me
- CSP X509v3 Certificates Policies: Policy: <OID of the effective CP/CPS>
- X509v3 CRL Distribution Points.

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

- X509v3 Basic Constraints: critical CA,FALSE
- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
- X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication
- X509v3 Subject Key Identifier: <subject key ID>
- X509v3 Authority Key Identifier:
    - keyid: <CA key ID>
- X509v3 Issuer Alternative Name: email: mren-ca@ac.me
- X509v3 Subject Alternative Name: DNS:FDQN
- CSP 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

All RDN components in DN MUST be compliant with [RFC4630] and in addition SHOULD be encoded as PrintableString. DN must consist of: ‘a’-‘z’, ‘A’-‘Z’, ‘0’-‘9’, and the characters: ‘(‘, ‘)’, ‘+’, ‘,’, ‘-‘, ‘.’, ‘:’, ‘?’, ‘ ‘, that is, upper and lower case alphanumeric (english alphabet), left and right parentheses, plus, comma, minus/hyphen, dot (period), colon, question mark, and space.

Additionally, in case of grid host certificate and service certificate character ‘/’ can be used. The maximal length of the CN is 128 characters for all types of certificates.

7.1.5 Name constraints

Subjects attribute constraints:

- Domain Component: must be “me”
- Organization: must be “MREN”
- Organization Unit: must be the acronym of the subject's institute.
- Common Name: first name and last name of the subject for user certificates, DNS FQDN for host or service certificates. In the last 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 format.

7.2.2 CRL and CRL entry extensions

The following extension is set in CRLs:

- X509v3 Authority Key Identifier=keyid.

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

MREN CA will perform operational audit of the CA/RA staff at least once per year. The MREN CA must be audited by other trusted CAs to verify its compliance with the rules and procedures specified in this document. Any costs associated with such an audit must be covered by the requesting party.

8.2 Identity/Qualifications of Assessor

No stipulation.

8.3 Assessor's Relationship to Assessed Entity

No stipulation.

8.4 Topics Covered by Assessment

No stipulation.

8.5 Actions Taken as a Result of Deficiency

No stipulation.

8.6 Communication of Results

No stipulation.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees shall be charged.

9.1.2 Certificate access fees

Same as section 9.1.1.

9.1.3 Revocation or status information access fees

Same as section 9.1.1.

9.1.4 Fees for other services

Same as section 9.1.1.

9.1.5 Refund policy

Same as section 9.1.1.

9.2 Financial Responsibility

MREN 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 Confidentiality

9.4.1 Types of information to be kept confidential

The only confidential information kept by MREN CA is a photocopy of the subscriber’s official document (ID-card, driving license or a passport) declaring that the subject is a valid end entity, or organization official document proving the relation of the subscriber with the organization.

9.4.2 Types of information not considered confidential

The MREN CA collects the following information that is not considered confidential:

- The subscriber’s full name
- The subscriber’s e-mail address
- The subscriber’s organization address
- The subscriber’s certificate request file
- The subscriber’s public key file.

The information included in issued certificates and CRLs is not considered confidential.
Under no circumstances will the MREN CA have access to the private keys of any subscriber to whom it issues a certificate.

9.4.3 Disclosure of certificate revocation/suspension information

The MREN CA will notify and inform the following entities:

- The subject of the personal certificate
- The requestor of the server or service certificate.

9.4.4 Release to law enforcement officials

The information collected by the MREN CA will be made available to the law enforcement officials upon their request.

9.4.5 Release as part of civil discovery

The information collected by the MREN CA will be subject to the law of the Republic of Montenegro.

9.4.6 Disclosure upon owner’s request

Same as section 9.4.5.

9.4.7 Other information release circumstances

Same as section 9.4.5.

9.5 Intellectual Property Rights

- RFC 3647;
- SEE-GRID CA CP/CPS;
- Hellas Grid CA Certificate Policy;
- AEGIS CA CP/CPS;
- MARGI CP/CPS;
- SRCE CA CP/CPS;
- ArmeSFo CA CP/CPS;

9.6 Representations and Warranties

9.6.1 CA representations and warranties

The MREN CA is solely responsible for the issuance and management of certificates referencing this CP/CPS. The MREN 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 CRLs
    - make certificate revocation information publicly available
    - Publish MREN CAs root of trust to a trust anchor repository defined by accrediting Policy Management Authority.

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 MREN 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 MREN 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 MREN 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 subscriber accept the restrictions to liability described in section 9.8
- By using the authentication procedures described in this CP/CPS subscriber accept the statements relating to confidentiality of information in section 9.4
- Generate a key pair using a trustworthy method
- Use at least 12 characters long pass phrase, 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 MREN 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 MREN 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

- MREN CA guarantees to control the identity of the certification requests according to the procedures described in this document
- MREN CA guarantees to control the identity of the revocation requests according to the procedures described in this document
- MREN CA is run on a best effort basis and does not give any guarantees about the service security or suitability
- MREN CA shall not be held liable for any problems arising from its operation or improper use of the issued certificates
- MREN 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

OID MUST change on every CP/CPS change.

9.13 Dispute Resolution Provisions

Legal disputes arising from the operation of the MREN CA will be resolved according to the Montenegrin Law.

9.14 Governing Law

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

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.