

Company	<i>MERO CR, a.s Veltruska 748, Kralupy nad Vltavou</i>
Document	<i>SI-GŘ-113</i>
Type	<i>A</i>

Certification Policy

Version	<i>1.</i>	Developer by	<i>Ing. Jan Kotera</i>
Date	<i>1st. Feb. 2011</i>	Rewieved by	<i>Ing. Peter Kováč</i>
Updates against the previous version		Approved by	<i>Ing. Jaroslav Pantůček</i>
-		IMS Executive Representative	<i>JUDr. Ing. Mgr. Libor Lukášek, Ph.D..</i>
		Administrator	<i>Petra Klemptová</i>
		Copy	<i>0</i>
		Strana	<i>1/30</i>

Table of contents

1	Introduction	5
1.1	Overview	5
1.2	Terms and abbreviations	5
1.3	Document name and identification	6
1.4	Participants	6
1.4.1	Certification authorities (CA)	6
1.4.2	Registration authorities (RA)	7
1.4.3	Certificate holders that requested issuing a certificate and to whom a certificate was issued	7
1.4.4	Relying Parties	7
1.5	Certificate usage	7
1.5.1	Appropriate certificate usages	7
1.5.2	Certificates - restricted usage	8
1.6	Policy administration	8
1.6.1	Organization administering the certification policy / certification implementing guidelines - contact person	8
1.7	Information and documentation repositories	8
1.8	Publication of the information and documentation	8
1.8.1	Publication of certificates and CRL	8
1.8.2	Publication of details on the certification authority	8
1.9	Frequency of publication	8
1.10	Access control on each type of repository	9
2	Identification and authentication	9
2.1	Naming in certificates issued by Mero CA	9
2.1.1	Types of names	9
2.1.2	Uniqueness of names	9
2.2	Initial identity validation	9
2.2.1	Authentication of individual's identity	9
2.2.2	Non-verified information related to certificate holders	10
2.2.3	Criteria for interoperation	10
2.3	Identification and authentication in processing re-key requests	10
2.3.1	Certificate re-key identification and authentication	10
2.3.2	Identification and authentication for re-key after revocation	10
2.4	Identification and authentication in processing certificate revocation requests	10
3	Certificate life cycle requirements	11
3.1	Certificate application	11
3.1.1	Entities authorised to apply for issuing a certificate	11
3.1.2	Provider and applicant responsibilities	11
3.2	Certificate application processing	12
3.2.1	Identification and authentication in processing certificate applications	12
3.2.2	Approval or rejection of certificate applications	12
3.2.3	Time to process certificate applications	12
3.3	Certificate issuance	13
3.3.1	Notification of certificate issuance to certificate holders	13
3.3.2	Publication of the certificate by the provider	13
3.4	Cryptographic key and certificate usage	14
3.4.1	Private key and certificate usage by certificate holders	14
3.4.2	Relying party public key and certificate usage	14
3.5	Certificate renewal	14
3.6	Certificate re-key	14
3.7	Certificate modification	15
3.8	Certificate revocation	15
3.8.1	Circumstances for revocation	15
3.8.2	Entities that can request revocation	16
3.8.3	Certificate revocation requests	16
3.8.4	Procedure for revocation request	16
3.8.5	Revocation request grace period	16
3.8.6	Maximum time within which the provider must process the revocation request	17
3.8.7	Revocation checking requirements for relying parties	17
3.8.8	CRL issuance frequency	17
3.8.9	Maximum latency for CRLs	17
3.9	Certificate status checking	17

3.10	End of subscription for certificate holders.....	17
4	Management, operational and physical security.....	17
4.1	Physical security.....	18
4.1.1	Physical access.....	18
4.1.2	Power and air conditioning, water exposures and fire prevention.....	18
4.1.3	Media storage.....	18
4.1.4	Waste disposal.....	18
4.1.5	Off-site backup.....	18
4.2	Procedural security.....	18
4.3	Personal security.....	18
4.4	Audit logging procedures (logs).....	19
4.4.1	Types of events recorded.....	19
4.4.2	Log processing frequency.....	19
4.4.3	Retention period for audit logs.....	19
4.4.4	Protection of audit logs.....	19
4.4.5	Audit log backup procedures.....	19
4.4.6	Audit collection system (internal vs. external).....	19
4.4.7	Notification to event-causing subject.....	19
4.4.8	Vulnerability assessments.....	19
4.5	Storage of information and documentation.....	19
4.6	Replacement of data to verify electronic signatures contained in the superior certificate of the provider.....	20
4.7	Compromise and disaster recovery.....	20
4.7.1	Incident and compromise handling procedures.....	20
4.7.2	Computing resources, software, and/or data are corrupted.....	20
4.7.3	Provider's electronic signature production data compromise procedures.....	20
4.7.4	Business continuity capabilities after a disaster.....	21
4.8	CA termination.....	21
5	Technical security.....	21
5.1	Cryptographic key generation and installation.....	22
5.2	Private key protection and cryptographic module security.....	22
5.3	Other aspects of cryptographic key management.....	22
5.4	Computer and network security.....	23
6	Certificate, CRL and OCSP profiles.....	23
6.1	Certificate profile.....	23
6.1.1	Version number.....	23
6.1.2	Certificate extensions.....	23
6.1.3	Algorithm object identifiers („OID“).....	23
6.1.4	Name recording methods.....	23
6.1.5	Name constraints.....	23
6.1.6	Certificate policy OID.....	23
6.1.7	„Policy Constraints“ extension.....	24
6.1.8	Processing semantics for the critical "Certificate Policies" extension.....	24
6.2	CRL profile.....	24
6.2.1	Version number.....	24
6.2.2	CRL and CRL entry extensions.....	24
7	Compliance audit and other assessments.....	24
7.1	Frequency and circumstances of assessment.....	24
7.2	Identity/qualifications of assessor.....	24
7.3	Assessor's relationship to assessed entity.....	24
7.4	Topics covered by assessment.....	24
7.5	Actions taken as a result of deficiency.....	24
7.6	Communications of results.....	24
8	Other business and legal matters.....	25
8.1	Fees.....	25
8.2	Confidentiality.....	25
8.3	Limitations of liability.....	25
8.4	Term and termination.....	25
8.5	Term.....	25
8.5.1	Termination.....	25
8.5.2	Effect of termination and survival.....	25
8.6	Communications between participants.....	25
8.6.1	Communications with certification service providers.....	25
8.7	Amendments.....	25

8.8	<i>Dispute resolution</i>	26
8.9	<i>Miscellaneous provisions</i>	26
8.9.1	<i>Force majeure</i>	26
8.10	<i>Other provisions</i>	26
8.10.1	<i>Governing documents</i>	26
9	<i>Annex A</i>	26
9.1	<i>Certificate profiles</i>	26
9.2	<i>Certificate extensions</i>	27
9.3	<i>Profiles of revoked certificates</i>	29

1 Introduction

This document has been designed to set out rules and procedures when issuing certificates for PKI security services provided by Mero CR, plc, (Mero CR), which includes the following:

- Electronic signature;
- Electronic mail encryption;
- Mero CR internal use data storage encryption;
- External subject electronic signature;
- External subject electronic mail encryption;
- External subject data storage encryption; and
- Infrastructure component authentication.

This Certification policy shall describe registration methods, appropriate use of certificates and essential procedures that need to be applied in order to abide by the security standards adopted by Mero CR. Certificates under this Certification policy are issued to the following entities:

- Mero CR staff members;
- Any external subject that has entered into a legal relationship with Mero CR for which there is the necessity of providing secure data transfer under the relevant data classification procedure; and
- Infrastructure components, i.e. servers and certification authorities within the PKI hierarchy of Mero CR.

Mero CR certificate shall not be issued to any other entity, i.e. private/legal persons.

1.1 Overview

Mero CR provides certification services. Mero CR has created a two-level hierarchy of internal certification authorities consisting of Mero Root CA - the root certification authority and CA Mero - the issuing certification authority (hereinafter referred to as "Mero CR PKI hierarchy"). For more details on the Mero CR PKI hierarchy, refer to Section 1.3.1.

Mero CR is not an accredited provider of certification services and none of the certification authorities within Mero CR PKI hierarchy is a certification authority issuing qualified certificates in accordance with Act No 227/2000 Coll. on electronic signatures.

1.2 Terms and abbreviations

CA Certification Authority

CRL (Certificate Revocation List) A list of revoked certificates; it contains certificates that can no longer be considered valid, for instance as a result of disclosure of the corresponding private key of the subject. CRL is digitally signed by the issuer of certificates, i.e. the certification authority.

Certificate Holder Mero CR staff member / business partner, or technical equipment operated by Mero CR from the time of issuing the certificate.

HeliosGreen An information system providing technical support to IS/IT end users. To resolve a request, the request submitter shall contact the IT department through the HeliosGreen information system.

Qualified certificate Any certificate qualified under the Act (9.10.1).

Certificate re-key Any certificate issued as a replacement for the certificate already issued; this policy shall set out which details of the original certificate may be amended within the act of certificate re-key.

Mero Root CA A root certification authority that possesses a self-signed system certificate. Mero Root CA shall also issue system certificates for Mero CA, the subordinate certification authority, and sign CRL of that authority.

Mero CA A subordinate (issuing) certificate authority that possesses a system certificate signed by Mero Root CA, the root certification authority. Mero CA issues system certificates for Mero CR staff members, selected business partners and infrastructure components used within Mero CR.

Cryptographic keys Data for creating electronic signatures together with the corresponding data for the validation of electronic signatures (corresponding private and public keys).

PKI (Public Key Infrastructure) Public key management and distribution infrastructure, which allows, through trusted transmission, the use of external subject public keys and verifying electronic signatures, as well as encryption or authentication.

PKI hierarchy Hierarchy of certification authorities, which covers all of the certification authorities operated within the company.

Private key Collectively refers to data for creating electronic signatures, decryption, or authentication.

Certificate end user A person using a certificate issued by Mero CR, e.g. for encryption, to verify an electronic signature or provide other security services. Otherwise known as a Relying party.

Public key The collective term for data used to verify electronic signatures or make encryption.

Staff member A person employed with Mero CR for which a certificate can be issued.

Applicant A person having the right to request a certificate under a valid certification policy.

1.3 Document name and identification

Document name:	Mero CR Certification policy
Document identifier:	SI-GŘ
Version No.:	XXX
Date of release:	XXX

1.4 Participants

The entities participating under this Certification policy are as follows:

- Mero CR as the provider of certification services;
- Mero CR staff members acting as certificate holders (end users), i.e. Relying parties;
- External subjects - Mero CR business partners acting as certificate holders (end users), i.e. Relying parties; and
- Person in charge - any Mero CR staff member acting as a person in charge for external subjects. Each external subject is assigned one person in charge within Mero CR.

Certificate service provider identification and contact details are as follows:

Mero CR, plc

ID: 60193468, VAT ID: CZ60193468

Veltruska 748, Kralupy nad Vltavou

Telephone: +420 315 701 100

Email: info@mero.cz

1.4.1 Certification authorities (CA)

PKI hierarchy of internal certification authorities within Mero CR consists of a root and issuing or subordinate certification authority.

Mero Root CA

The certification authority Mero Root CA acts as the root certification authority of the PKI hierarchy within Mero CR. This authority serves to provide assurances of trustworthiness throughout the PKI hierarchy. Mero Root CA issues system certificates for all certification authorities within the PKI hierarchy of Mero CR.

Mero CA

The subordinate certification authority Mero CA issues and manages end-user certificates. Types of the certificates issued are as follows:

- Electronic signature certificates;
- Electronic mail encryption certificates;
- Mero CR internal use data storage encryption certificates;

- External subject electronic signature certificates;
- External subject electronic mail encryption certificates;
- External subject data storage encryption; and
- Infrastructure component authentication certificates.

1.4.2 Registration authorities (RA)

The certification service provider does not operate a special registration authority office. Registration authority services, particularly receiving requests for, passing along and revoking certificates, are provided by persons acting as Certificate Managers.

1.4.3 Certificate holders that requested issuing a certificate and to whom a certificate was issued

Certificate holders are at all times

- Mero CR staff members; or
- External subjects - Mero CR business partner staff members;
- Infrastructure components operated within Mero CR;

that has requested a certificate (for infrastructure components, this refers to any person acting as a Certificate Manager), successfully passed request-processing steps and received a certificate based on the latter.

1.4.4 Relying Parties

A relying party (certificate end user) is any entity relying on a certificate issued by any of the Mero CR certification authorities, as are typically Mero CR staff members and/or Mero CR business partners.

1.5 Certificate usage

1.5.1 Appropriate certificate usages

The following table gives an overview of the appropriate use of different types of certificates that are issued within the Mero CR PKI hierarchy and under this Certification policy. Other usage of certificates issued than that shall not be considered appropriate.

Electronic signature certificate

- Verifying electronic signatures
- Authentication (identity proof)

Electronic mail encryption certificate

- Email encryption

Mero CR internal use data storage encryption certificate

- Data encryption within data storage, laptop, desktop, CD etc. for internal use

External subject electronic signature certificate

- Verifying electronic signatures
- Authentication (identity proof)

External subject electronic mail encryption certificate

- Email encryption

External subject data storage encryption certificate

- Data storage encryption for external use, such as USB keys designed for delivery to business partners

Infrastructure component authentication certificate

- Authentication (identity proof) of infrastructure components, such as applications, network devices, servers, etc.

Certification authority system certificate

- Certification authority certificates electronic signatures and CRL signatures

1.5.2 Certificates - restricted usage

Any certificate issued under this certificate policy shall be possible to use only where appropriate and legal and in accordance with applicable laws.

1.6 Policy administration

CA Manager is responsible for initiating any amendments to the existing certification policy and/or development of a new certification policy. The existing version of the certification policy is available on the certification service provider website: <http://www.mero.cz/dokumenty-ke-stazeni/>

Organization administering the certification policy / certification implementing guidelines

The certification service provider, i.e. Mero CR - CA Manager in particular - is responsible for administering this Certification policy.

1.6.1 Organization administering the certification policy / certification implementing guidelines - contact person

CA Manager acts as the contact person administering this Certification policy. For more information, please refer to the certification service provider website: <http://www.mero.cz/>

Responsibility for publication and repository of information and documents

1.7 Information and documentation repositories

Mero CR as a provider of certification services operates and is responsible for operating each information and documentation repository, excluding that available on <http://www.mero.cz/> operated by Qwerton Formica Ltd based on an effective contract with Mero CR.

Mero CR as a provider of certification services is responsible for publication of the information.

1.8 Publication of the information and documentation

Certificates issued are stored in the database of the issuing certification authority.

Information on operation of certificate authorities within Mero CR PKI hierarchy, as well as security documentation of each certification authority is published to the extent given below.

1.8.1 Publication of certificates and CRL

Certificates issued by the Mero CR certificate authorities, as well as details of status of any certificate issued in form of Certificate Revocation List (CRL) are published on Mero CR website: <http://www.mero.cz/files/PKI>

In addition, the list can be accessed on the server of the issuing certification authority: http://pki_sub

1.8.2 Publication of details on the certification authority

The certification policy is available on Mero CR website: <http://www.mero.cz/dokumenty-ke-stazeni/>

Other important information (e.g. information on revocation of certification authority system certificates) or also emergency information is posted on the website of Mero CR.

1.9 Frequency of publication

Information is published in the following intervals:

- Certification policy, certification implementing guidelines (CPS) and System security policy are published (if designed for publication) upon approval and release of new versions, but always before the document becomes active;
- Information on the status of the certificate in the form of a Certificate Revocation List (CRL) is published immediately after the release, but not later before the last published list of invalid certificates becomes inactive, which in the event the issuing certification authority Mero CA is at least 72 hours, while in the case of the root certification authority Mero Root CA this is at least every 12 months;
- any important information is published without delay.

1.10 Access control on each type of repository

Certification policies, certificates of certification authorities, end-user certificates and Certificate Revocation Lists (CRLs) and other important information are accessible as read-only without any restrictions.

2 Identification and authentication

2.1 Naming in certificates issued by Mero CA

2.1.1 Types of names

The "Subject" field within the certificate is designed according to the X.501 standard and/or the follow-up X.520 standard. Details of the structure of certificates issued can be found in chapter 7.1.

The extension of the certificate contains an e-mail address for each person in the "Subject Alternative Name" field. For infrastructure component authentication certificates, the extension of the certificate contains the IP address of that device next to "Subject Alternative Name".

2.1.2 Uniqueness of names

Certificate holders are distinguished using the Subject field of the certificate. For certificates issued for external subjects, the uniqueness of the CN detail under the Subject certificate field is the responsibility of the person in charge of the relevant business partner.

2.2 Initial identity validation

2.2.1 Authentication of individual's identity

Authentication time for individuals (applicants for certificate) depends on the type of the certificate requested:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

The certificates above are issued to Mero CR staff members only. The certificate is issued automatically to a company staff member without prior verification of identity.

Infrastructure component authentication certificates

The person acting as a Certificate Manager bears the responsibility for the process of identification and authentication of the infrastructure component administrator requesting the certificate.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

The certificates above are issued to selected external subjects for whom ensuring secure transmission of documents is necessary. Each external subject is assigned a person in charge within Mero CR responsible for ensuring initial identity verification of that external subject.

Certification authority system certificates

System certificates of certification authorities within the Mero CR PKI hierarchy are issued through the key generation ceremony attended by the persons acting as selected PKI security roles. Ensuring and conducting the ceremony is the responsibility of the person acting as CA Manager.

2.2.2 Non-verified information related to certificate holders

The person acting as Certificate Manager is responsible for verifying the accuracy of information in the certificate issued to Mero CR staff members. Verifying the accuracy of information in external subjects' certificates is the responsibility of the person in charge.

2.2.3 Criteria for interoperation

Any cooperation with other certification service providers is possible only after the approval of CA Manager, under the contract and conditions defined by CA Manager.

2.3 Identification and authentication in processing re-key requests

2.3.1 Certificate re-key identification and authentication

Identification and authentication method depends on the type of certificate where re-key is requested:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

The certificates above are issued to Mero CR staff members only. Re-keyed certificates are issued automatically to a company staff member without prior verification of identity.

Infrastructure component authentication certificates

The person acting as Certificate Manager is responsible for the process of identification and authentication in the case of infrastructure component administrator requesting issuing the re-keyed certificate.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

The certificates above are issued to selected external subjects for whom ensuring secure transmission of documents is necessary. Each external subject is assigned a person in charge within Mero CR responsible for ensuring identity verification of that external subject in issuing re-keyed certificates.

Certification authority system certificates

Re-keyed certificates of certification authorities within the Mero CR PKI hierarchy are issued through the key generation ceremony attended by the persons acting as selected PKI security roles. Ensuring and conducting the ceremony is the responsibility of the person acting as CA Manager.

2.3.2 Identification and authentication for re-key after revocation

In the case certificate revocation, the same procedure for identification and authentication associated with the release of a new certificate is necessary as that for the initial verification of identity when issuing the initial certificate (see chapter 3.2.1).

2.4 Identification and authentication in processing certificate revocation requests

The methods of identification and authentication when revoking certificates vary by the type of certificate:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

The method of identity verification when applying for revocation corresponds to the standard identity verifying procedure within Mero CR.

Infrastructure component authentication certificates

Certificate Manager is responsible for the process of identification and authentication in the case of infrastructure component administrator requesting certificate revocation.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

A person in charge is responsible for verifying identity of the external subject in certificate revocation.

Certification authority system certificates

Request for certificate revocation in the case of root/subordinate CA can only be submitted by CA Manager.

3 Certificate life cycle requirements

3.1 Certificate application

3.1.1 Entities authorised to apply for issuing a certificate

Entities authorised to apply for issuing a certificate differ according to certificate types:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

Request for issue of the certificate types above may be made only by a Mero CR staff member.

Infrastructure component authentication certificates

Request for issuing the certificate type above may be made only by the administrator of the infrastructure component in question.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

Application for issue of the certificates above may be submitted by the Certificate Manager upon the request of the person in charge assigned to the external subject.

Certification authority system certificates

Applications for issuing system certificates of certification authorities within the Mero CR PKI hierarchy may be submitted only by a person acting as CA Manager.

3.1.2 Provider and applicant responsibilities

Applicants (end users)

Applicants shall in particular:

- Check whether the information provided in the certificate is correct;
- Treat the private key corresponding to the public key with due care, in such a manner so as to prevent its unauthorized use;
- Use both the private key and corresponding certificate solely for the purposes set out in this Certification policy;
- Immediately inform the certification service provider on facts leading to the certificate revocation, especially on any suspicion that the private key has been compromised, as well as request certificate revocation and stop using the private key in question;
- Become familiar with the certification policy, under which the certificate had been issued to them.

Provider

Certification service provider shall, in particular:

- Issue a certificate containing factually correct information on the basis of information that were available to CA at the time of issuing the certificate;
- Publish any certification policy under which certificates are issued on the company's website;
- Publish any system certificate of a certification authority within the Mero CR PKI hierarchy in such a manner that any person could check their identity;
- Pay due care to any activity associated with the provision of certification services, where such due care shall involve operating according to
 - Applicable laws
 - This Certification policy
 - Certification implementing guidelines
 - System security policy and
 - Other operational documentation

3.2 Certificate application processing

3.2.1 Identification and authentication in processing certificate applications

Methods of identification and authentication when applying for a certificate depend on the type of certificate for which it is applied:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

The certificates above are issued to Mero CR staff members only. The certificate is issued automatically to a company staff member without prior verification of identity.

Infrastructure component authentication certificates

The person acting as a Certificate Manager bears the responsibility for the process of identification and authentication of the infrastructure component manager seeking the certificate.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

The certificates above are issued to selected external subjects for whom ensuring secure transmission of documents is necessary. Each external subject is assigned a person in charge within Mero CR responsible for ensuring initial identity verification of that external subject.

Certification authority system certificates

System certificates of certification authorities within the Mero CR PKI hierarchy are issued through the key generation ceremony attended by the persons acting as selected PKI security roles. Ensuring and conducting the ceremony is the responsibility of the person acting as CA Manager.

3.2.2 Approval or rejection of certificate applications

Methods of approval of certificate application vary depending on the type of certificate that is subject to application:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

The certificates above are issued to Mero CR staff members only. The certificate application of a Mero CR staff member is approved automatically based on end user's classification into the domain group assigned.

Infrastructure component authentication certificates

The person acting as Certificate Manager performs the process of approval/rejection of certificate applications in the case of infrastructure component authentication.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

The certificates above are issued to selected external subjects for whom ensuring secure transmission of documents is necessary. The person in charge shall apply for any external subject certificate. Assessing the requirement for issuing an external subject certificate is the responsibility of the person acting as Certificate Manager.

Certification authority system certificates

Any approval/rejection of a system certificate of certification authorities within the Mero CR PKI hierarchy is the responsibility of the person acting as CA Manager.

3.2.3 Time to process certificate applications

Certificate application processing time varies depending on the type certificate that is subject to application:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

Processing and approval of applications for certification for a Mero CR staff member proceeds automatically immediately after the application is received. The act of approval of the application received is followed by issuing the certificate to the staff member in question.

Infrastructure component authentication certificates

Applications for issuing a certificate to authenticate an infrastructure component are processed within one working day upon receipt. Upon approval of the application accepted, the certificate is issued.

External subject electronic signature certificates
External subject electronic mail encryption certificates
External subject data storage encryption certificates

Request for issuing an external subject certificate is processed within three working days upon receipt.

Certification authority system certificates

Applications for issuing system certificates for certification authorities are processed through the key generation ceremony.

3.3 Certificate issuance

The process of issuing a certificate depends on the type of the certificate to be issued:

Electronic signature certificates
Electronic mail encryption certificates
Mero CR internal use data storage encryption certificates

The certificates above are issued automatically after approval of the issuance request. The certificate is automatically installed on terminal devices of the respective users.

Infrastructure component authentication certificates

After generating, the certificate is sent to the administrator of infrastructure component by the person acting as Certificate Manager via email.

External subject electronic signature certificates
External subject electronic mail encryption certificates
External subject data storage encryption certificates

After approval of the application received by Certificate Manager, a certificate is generated to the external subject. The certificate is handed personally based on the signed agreement to the terms of use of Mero CR certificates using a removable medium containing the external subject's certificate, the cryptographic keys as appropriate and a valid certification policy of Mero CR. When taking over the certificate, the external subject shall check the certificate data for accuracy and sign a proof of receipt of the certificate including that external subject's declaration of having been made familiar with the certification policy and being aware of the obligations arising to that external subject under this certificate policy.

Certification authority system certificates

Issuing system certificates for certification authorities within the Mero CR PKI hierarchy proceeds through the key generation ceremony.

3.3.1 Notification of certificate issuance to certificate holders

Methods of notification of certificate issuance to certificate holders depend on the type of certificate issued:

Electronic signature certificates
Electronic mail encryption certificates
Mero CR internal use data storage encryption certificates

Holders of certificates are not notified of the act of issuance of the certificates above afterwards.

Infrastructure component authentication certificates

Certificate Manager shall inform the infrastructure component administrator in question on issuing the certificate via email.

External subject electronic signature certificates
External subject electronic mail encryption certificates
External subject data storage encryption certificates

Information on the issuance of certificates is forwarded to the person in charge who then shall inform the external subject and ensure the safe delivery of the certificate and cryptographic keys to that external subject.

Certification authority system certificates

Notification of issuance of system certificates for certification authorities within the Mero CR PKI hierarchy proceeds through the certification service provider website.

3.3.2 Publication of the certificate by the provider

Certificates issued under this certificate policy are not published to the extent specified in chapter 2.2.

3.4 Cryptographic key and certificate usage

Key pairs corresponding to the certificates have the same duration as the certificates. Key pairs for which a certificate has been issued by the Mero CA / Mero Root CA certification authority cannot be reused.

3.4.1 Private key and certificate usage by certificate holders

Certificate holders shall:

- Treat their private keys corresponding to the public keys in the certificates issued under this Certification policy with due care, in such a manner so as to prevent unauthorized use;
- Immediately inform the certification service provider on loss, theft or suspicion that the private key has been compromised, as well as stop using the private key in question;
- Use their private keys and corresponding certificates issued under this Certification policy solely for the purposes set out therein, as listed in Chapter 1.4.1.

3.4.2 Relying party public key and certificate usage

Parties relying on certificates issued by certification authorities of Mero CR shall:

- Obtain their certificates from a safe source (<http://www.mero.cz/files/PKI>) and verify the fingerprint of these certificates;
- Verify certificate validity before using the certificate and subsequently also the validity of the terminal certificate, checking the certificates for the correct signature of the issuing authority as well as against the current CRL and the current time; this activity is usually performed by applications of the certificate users - relying parties);
- Adequately consider appropriateness of certificates issued pursuant to this Certification policy for the intended use.

3.5 Certificate renewal

Certificate renewal refers to the act of issuance of a new certificate without changing the public key, but a new duration of the certificate. This type of service is not provided as part of certification authorities operated by Mero CR.

3.6 Certificate re-key

Certificate rekey refers to the issuance of a certificate without amending the data in the "Subject" field, changed key pair and new certificate expiry details.

The certificate re-key issuing processes vary depending on the type of certificate for which re-key is sought:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

A certificate re-key application is generated to Mero CR staff members eight weeks before the expiry of the certificate. The application for certificate re-key shall follow automatically once the staff member logs into that member's domain. Processing and approval of applications for certification re-key for Mero CR staff members proceeds automatically immediately after the receipt. Upon approval of the application for certificate issuance received, the re-keyed certificate is issued to the applicant and automatically installed on their workstation.

Infrastructure component authentication certificates

Certificate Manager shall generate requests to issue a re-keyed certificate. Applications for issuing re-keyed certificates to authenticate infrastructure components are processed within one working day upon receipt by the person acting as Certificate Manager. Upon approval of the application accepted, the certificate is issued.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

Certificate re-key applications shall be filed by the person in charge by means of the HeliosGreen information system using the "User accounts" folder. The certificate re-key application is then processed by the person acting as Certificate Manager. After approval of the application received, the certificate is issued and handed over to the

person in charge for the external subject in question together with cryptographic keys. The person in charge shall ensure the safe delivery of the certificate to the applicant concerned. When receiving the certificate, the applicant shall check the information in the certificate for accuracy and sign a proof of receipt of the certificate.

Certification authority system certificates

Issuing re-keyed certificates for Mero Root CA / Mero CA certification authorities proceeds through the key generation ceremony.

3.7 Certificate modification

Any modified certificate may only be issued

- As a new certificate in accordance with the procedures specified in Section 4.3; or
- As a re-keyed certificate according to the procedures specified in chapter 4.6, unless replacement of the following data is required:
 - CN information in certificate "Subject" field
 - The "Subject Alternative Name" field in the certificate extension.

If any of the details provided within the current certificate has lost its accuracy, revocation of that existing certificate shall be sought in an appropriate manner (see Section 4.8). Following the revocation of the existing certificate, application for a new certificate shall be filed.

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

Certificate holders shall report the modified details of the current certificate to the person acting as Certificate Manager.

Infrastructure component authentication certificates

Administrator of the relevant infrastructure components shall report the modified details of the current certificate to the person acting as Certificate Manager.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

Certificate holders (external subjects) shall inform the person in charge concerned on the fact that the data contained in the certificate had been modified. Based on the reported modifications, the person in charge concerned shall inform, by means of the HeliosGreen information system using the "User accounts" folder, the person acting as Certificate Manager, who then shall assess the application.

Certification authority system certificates

Any modification to the details within the CA certificate shall require amendment of the certification policy and renewal of the key generation ceremony.

3.8 Certificate revocation

Validity of the certificate is terminated at the time of its revocation and publication on the Certificate Revocation List (CRL). If there is no need for certificate revocation throughout its validity, the certificate shall expire at the time point indicated in the certificate.

3.8.1 Circumstances for revocation

Reasons for revocation of system certificates of certification authorities are particularly as follows:

- Any suspects that there has been a compromise of the corresponding private key;
- Other reasons (the provider of certification services has ceased to exist; loss of accuracy of the information based on which the certificate had been issued).

Reasons for the end-user certificate revocation are chiefly as follows:

- Any suspects that there has been a compromise of the corresponding private key;
- Gross breach of obligations of the certificate holder deriving from this Certification policy;
- Relevant application by the holder, Certificate Manager, or CA Manager;

- Other reasons (death, termination of the employment of the holder at Mero CR / given business partner; loss of accuracy of the information on which the certificate had been issued).

3.8.2 Entities that can request revocation

The CA Manager can request revocation of certificates of Mero Root CA or Mero CA.

Revocation of the end-user certificates can be requested by

- Certificate holders;
- Persons in charge for business partners concerned; or
- Person acting as Certificate Manager / CA Manager.

3.8.3 Certificate revocation requests

The methods of requesting certificate revocation depend on the type of certificate where re-key is requested:

Electronic signature certificates

Electronic mail encryption certificates

Mero CR internal use data storage encryption certificates

The certificate holder can submit a request for certificate revocation using the "User accounts" folder within the HeliosGreen information system, by telephone or in person to Certificate Manager.

Infrastructure component authentication certificates

The infrastructure component administrator can submit a request for certificate revocation using the "User accounts" folder within the HeliosGreen information system, by telephone or in person to Certificate Manager.

External subject electronic signature certificates

External subject electronic mail encryption certificates

External subject data storage encryption certificates

The person in charge assigned to the business partner concerned can submit a request for certificate revocation using the "User accounts" folder within the HeliosGreen information system, by telephone or in person to Certificate Manager. The above shall be done based on prior external subject (certificate holder) request or of that person in charge own will, such as cases of terminated partnership with the external subjects concerned.

Certification authority system certificates

The person acting as CA Manager files the request for certificate revocation using the "User accounts" folder within the HeliosGreen information system, by telephone or in person to Certificate Manager.

3.8.4 Procedure for revocation request

The certificate revocation methods vary depending on the type of entity that has requested the revocation:

Certificate revocation request of certificate holder's own will

Certificate revocation applicants shall ask the person acting as Certificate Manager for revocation. The certificate shall be revoked by Certificate Manager within the CA system, which shall be recorded by the same person within the "User accounts" folder of the HeliosGreen information system. This revocation method is available within operating hours of the IT Department (Monday to Friday, 8 am to 4 pm) at the Mero CR headquarters in Kralupy nad Vltavou, on a phone number 420 315 701 111, or by emailing to „_IT_mero@mero.cz“

Certificate revocation request of certificate authority's own will

Certificate can also be revoked based upon decision by the certification service provider through Certificate Manager provided the certificate holder breaches the rules listed under the certification policy or terminates cooperation with Mero CR. In such case, a Mero CA representative shall inform the certificate holder on revocation of that holder's certificate giving the reasons for revocation of the certificate. The certificate is subsequently revoked by Certificate Manager.

3.8.5 Revocation request grace period

Certificate holders must request revocation of the certificate immediately upon having found the fact giving the reasons for revocation of the certificate.

3.8.6 Maximum time within which the provider must process the revocation request

Maximum time to pass from the receipt of the revocation request until publication of CRL including the revoked certificate is 72 hours. The above applies to any certificate issued by certification authorities within the PKI hierarchy of Mero CR.

3.8.7 Revocation checking requirements for relying parties

Users of certificates issued by certification authorities within the Mero CR PKI hierarchy (relying parties) shall proceed in accordance with the provisions of Chapter 4.4.2.

3.8.8 CRL issuance frequency

Certificate Revocation Lists (CRLs) is published immediately whenever a certificate revocation request has been processed. Subsequently upon such processing, CRL is published. CRL publication frequency is at least

- 12 months for CRLs issued by Mero Root CA
- 72 hours for CRLs issued by subordinate Mero CA

3.8.9 Maximum latency for CRLs

Maximum latency when issuing Certificate Revocation Lists (CRLs) shall not exceed the limit set under Chapter 0.

3.9 Certificate status checking

The certificate status can be checked using a Certificate Revocation List (CRL),

which is publicly available information. Certificate Revocation Lists is posted on the following websites:

- Mero CR site <http://www.mero.cz/files/PKI>
- Server of the issuing certification authority http://pki_sub/

The server of the issuing certification authority is the primary source of the current CRL. Certificate Revocation Lists are also available online.

3.10 End of subscription for certificate holders

The methods of terminating provision of certification services vary by the type of the certificate holder:

Mero CR staff members

Subscription for certificate holders - Mero CR staff members - shall end and the holder's certificate shall be revoked once

- The holder's employment at Mero CR has ended
- The holder has been redeployed to such a post that is not authorised to use any electronic certificate.

External subjects

Subscription for certificate holders - external subjects - shall end and the holder's certificate shall be revoked when

- End of external subject's employment at Mero CR's business partner
- Loss of the right of the external subject to apply for issuance of a certificate, such as due to organizational restructuring
- Termination of cooperation between Mero CR and the business partner concerned

4 Management, operational and physical security

The following PKI security documentation has been developed for Mero Root CA and Mero CA:

- System security policy outlining security principles in the physical, procedural and personal field
- Certification implementing guidelines (CPS)

- Certification policy (the present document)
- Nominating PKI security roles

The Certification implementing guidelines and System security policy documents are not available to the public.

4.1 Physical security

4.1.1 Physical access

Technical equipment of the certification authorities (servers, repositories, network infrastructure) within the Mero CR PKI hierarchy is located in protected areas in the company's headquarters in Kralupy nad Vltavou. Physical security of the technical equipment results from security standards listed in the System security policy document. Perimeters of protected areas in which keys of the certification authorities are generated or stored are clearly defined and protected from intrusion by mechanical means (security locks and bars). Staff members with allowed access to such premises are listed in the System security policy document.

4.1.2 Power and air conditioning, water exposures and fire prevention

Requirements for furnishing and installations within the premises containing technical equipment of the certification authorities are listed in the System security policy document.

4.1.3 Media storage

Requirements for media storage are listed in the System security policy document.

4.1.4 Waste disposal

Any data and details related to the certification authorities and services must be disposed of once not necessary in a safe manner as follows:

- Any replaceable media are physically discarded or adequate software used ensuring the medium has been completely erased
- Any hard copy is disposed of in a designated facility.

4.1.5 Off-site backup

The certification service provider have ensured secure storage of certification authority's critical data backup, which in particular applies to certification authority's private key backup outside the primary site.

4.2 Procedural security

The certification service provider has defined the PKI security roles responsible for safe operation and administration of certification authorities within the Mero CR PKI hierarchy. The System security policy document lays down the rules by which security roles are staffed, including requirements for separation of powers.

Activities requiring the presence of more than a single person have been defined. These in particular include activities within which private keys of certificate authorities are handled.

All access rights (at the level of physical access / access to the operating system) are linked to the PKI security roles. Each role player must identify and authenticate when accessing the CA software means. Any user playing a PKI security role is assigned unique identification within the technical resources of the certification authority.

4.3 Personal security

Only a credible person and a Mero CR employee can be appointed to fill a PKI security role. Penalties for violation of work rules are subject to organizational regulations of Mero CR. PKI security documents are available to every person appointed to the PKI security role.

Staff members involved in the operation, management and maintenance of Mero CR certificate authorities are trained to perform the roles assigned. The training includes instruction on the system security and behaviour in emergencies.

Any independent contractor that has access to the system of the certification authority is obliged to comply with the requirements defined in the PKI security documents.

4.4 Audit logging procedures (logs)

Any emergency control and auditing principles are described in the System security policy document, which is accessible to any person involved in ensuring control and audits. Audit records are created within the system for checking and potential analysis and to investigate emergency events, and serve to ensure potential evidence for sequence of operations performed and their assignment to persons invoking the operations.

4.4.1 Types of events recorded

Within the Mero CR certification authorities' environment, all the events associated with the certificate issuance, revocation, handling CA keys and certificates and other important events (e.g. termination of CA activities) are recorded.

4.4.2 Log processing frequency

The person acting as CA Auditor has the responsibility for evaluating audit logs. Such person is independent on PKI infrastructure operations and administration. In addition, audit logs are subject to in-house reviews.

4.4.3 Retention period for audit logs

Any audit log is retained in accordance with Mero CR in-house regulations.

4.4.4 Protection of audit logs

Audit logs are stored in such a manner ensuring protection from theft, modification and destruction, either intentional or spontaneous (i.e. fire, water, etc.).

4.4.5 Audit log backup procedures

All audit logs associated with the certificate issuance and revocation, handling Mero CR certification authorities' keys and certificates and other important events are backed up automatically as part of company's standard back up system.

Based on the rules defined under the Mero CR System security policy document, any audit logs in writing are only stored.

4.4.6 Audit collection system (internal vs. external)

Audit records in a digital form (log) are automatically created in the certification authority system environment and evaluated automatically as well as manually.

4.4.7 Notification to event-causing subject

Anywhere the event contained in the audit log has been evaluated as a safety incident, actions are taken in accordance with the relevant Mero CR in-house directive.

4.4.8 Vulnerability assessments

Audit logs are periodically checked and analysed for occurrence of non-standard events that may be deemed as attempts to attack security. In addition, procedures for possible actions in such events are defined. The person acting as CA Auditor has the responsibility for evaluating logs.

4.5 Storage of information and documentation

The certification service provider has described principles of audit log checking and archiving, as well as audit requirements under the System security policy document.

Mero CR, the certification service provider, archives the following audit logs created in connection with operation of Mero Root CA a Mero CA:

- Software and data, including certificates issued and CRLs;
- Any documentation related to certificate applications;
- Records on nominating PKI security roles;
- Security events (logs) created automatically by the certification authority system.

Data and software archives are located in designated premises. A logbook containing reports on handling the stored records has to be managed at each location of a safe.

4.6 Replacement of data to verify electronic signatures contained in the superior certificate of the provider

The validity of certificate authority keys within the PKI hierarchy of Mero CR is limited as follows:

- Mero Root CA - 20 years
- Mero CA - 10 years

Mero Root CA

In sufficient time in advance, but at least 2 years before the expiry of the certificate of Mero Root CA, the root certification authority, the ceremony of issuing a new certificate must be carried out. The ceremony above shall result in a new self-signed Root Certificate Authority certificate, which will be published in the manner described in chapter 0.

Mero CA

At least 2 years before the expiry of the certificate of Mero CA, the subordinate certification authority, issuing a new certificate signed by Mero Root CA, the root certification authority, must be requested.

Any changeover of keys of both root and subordinate certification authority must be notified to certificate holders no later than 6 months prior issuance of a new Mero Root CA / Mero CA certificate. Such notice including reasoning for certificate expiry will be posted on certification service provider website.

Once any need for using the original cryptographic data to generate electronic signatures has expired, Mero CR shall destroy any such data, taking a record of such destruction.

The procedure above shall also be used when changeover of cryptographic keys is necessary because of the inadequacy of the algorithm or algorithm parameters used (e.g. key size).

4.7 Compromise and disaster recovery

Mero CR has documents developed and in place describing handling crisis as well as procedures for subsequent recovery. The persons active in PKI security roles are duly instructed on how to proceed in case of emergency.

4.7.1 Incident and compromise handling procedures

Procedures for recovery of certification authority resources upon disaster or any other exceptional event have been elaborated under emergency plans.

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

Procedures for protection of certification authority information assets upon disaster or any other exceptional event have been elaborated under emergency plans.

4.7.3 Provider's electronic signature production data compromise procedures

Mero Root CA private key compromise procedures

In the case of a suspected compromise of private keys of Mero Root CA, the root certificate authority, all the holders of certificates issued by Mero CA, the subordinate certification authority, shall be informed of the extraordinary termination of this authority's activities, with a notice published on the Mero CR website, including the cause for termination of the CA certificate.

The certification service provider shall revoke the certificate of Mero Root CA as well as that of Mero CA, and all valid certificates issued by Mero CA. All revoked certificates will be immediately posted within the relevant CRL.

Subsequently, Mero CR shall provably destroy Mero Root CA private keys, with Mero CA taking a record of the act of destruction.

The procedure above shall also be used in cases where there is a sudden weakening of the algorithm used for creating electronic signatures, which calls into question the credibility of certificates issued and lists of certificates issued.

Mero CA private key compromise procedures

In the case of a suspected compromise of private keys of Mero CA, the certificate issuing authority, all the certificate holders shall be informed of the extraordinary termination of this authority's activities, with a notice published on the Mero CR website, including the cause for termination of the CA certificate.

The Mero CA certificate shall be immediately revoked by Mero Root CA. Mero CA, the subordinate certification authority, shall revoke all end-user certificates issued. All revoked certificates will be immediately posted within the relevant CRL.

Subsequently, the certificate service provider shall provably destroy the Mero CA private key that had served for signing the certificates issued and Certificate Revocation Lists, taking a record of the act of destruction.

The procedure above shall also be used in cases where there is a sudden compromise of the algorithm used for creating electronic signatures, which indisputably calls into question the credibility of certificates issued and lists of certificates issued.

4.7.4 Business continuity capabilities after a disaster

Procedures for business continuity are described in the Mero CR emergency plans. In the event of an accident, Mero CR shall ensure at least the CRL publication certificate revocation service.

In the case of major accidents (such as natural disaster, act of war), the recovery of CA activity shall be a matter of Mero CR management decisions. The management decision shall be notified to all certificate holders.

4.8 CA termination

Mero Root CA termination

Termination of activities of Mero Root CA must be notified to all holders of valid certificates issued by Mero CA and also published on the Mero CR website, at least two months before the closure of the authority. In the event that the termination of the authority's activities involves the expiry of the authority's certificate, such information must be contained in the notification, including the adequate grounds of termination.

As per the date of termination of the activities, Mero Root CA must revoke all certificates still valid and issue the last CRL. Subsequently, the Mero Root CA system certificate shall be revoked. Only then, the work of this authority may be terminated.

Subsequently, Mero CR shall provably destroy the private keys for creating electronic signatures used to sign certificates issued and Certificate Revocation Lists, taking a record of the act of destruction. Any such records are stored in accordance with provisions of this Certification policy listed in Chapter 0.

Mero CA termination

Termination of activities of Mero CA must be notified to all holders of valid certificates and also published on the Mero CR website, at least two months before the closure of the authority. The notification must include information on the expiry of the authority's certificate, as well as adequate grounds of termination.

As per the date of termination of the activities, Mero CA must revoke all certificates still valid and issue the last CRL. Subsequently, the Mero CA system certificate shall be revoked. Only then, the work of this authority may be terminated.

The revoked Mero CA system certificate will be published within the CRL of Mero Root CA until the time provided herein.

Subsequently, Mero CR shall provably destroy the private keys for creating electronic signatures used to sign certificates issued and Certificate Revocation Lists, taking a record of the act of destruction. Any such records is stored in accordance with provisions of this Certification policy listed in Chapter 0.

5 Technical security

5.1 Cryptographic key generation and installation

Keys of certification authorities

Generating keys of the root certification authority and issuing certification authority is carried out in secure areas of Mero CR. Generation of the key pairs is a controlled process (the key generation ceremony) overseen by CA Manager. Key pairs (public and private key) of Mero Root CA and Mero CA are generated and stored in software repositories within dedicated servers of the certification authorities. Private keys of the authorities are kept in encrypted form. The keys of certification authorities within the Mero CR PKI hierarchy are designed for the RSA algorithm. The Root CA Mero key has a module length of 4096 bits, while the key of Mero CA has a module length of 2048 bits.

End-user keys

End-user private keys are generated by CA Mero together with an application for a certificate. Private keys are stored in the software repository within the end-user computer workstation. The RSA algorithm with a key length of 2048 bits is used for user cryptographic keys.

In certificates for email and data repository encryption, end-user private keys are backed up within CA systems.

5.2 Private key protection and cryptographic module security

Private keys of certification authorities

Private keys of the root certification authority and subordinate certification authority are stored in secure areas of Mero CR. The private key of Mero Root CA is stored within the dedicated server file system. The server above is disconnected from the network and switched off by default, except for key generating ceremony and signing the CRL. The server disks are physically removed from the server and placed in a sealed envelope in a safe.

The private key of Mero CA is stored in an encrypted form in the software repository of the certification authority. Any access to the key repository of the private key is constantly recorded and evaluated using technical means. The person acting as CA Auditor has the responsibility for evaluating audit logs. Such person is independent on PKI infrastructure operations and administration. No hardware cryptographic modules are used within the environment of Mero CR.

The private keys of certification authorities within the Mero CR PKI hierarchy are archived as part of key generating ceremony. Archiving methods are described in the System security policy document.

End-user private key protection

End-user private keys are stored in encrypted form in the software repository within the end-user computer workstation.

In certificates for email and data repository encryption, end-user private keys are backed up within CA systems.

5.3 Other aspects of cryptographic key management

Public keys in the form of end-user / certification authority certificates are archived in accordance with the Mero CR System Security Policy document.

Key pairs corresponding to the certificates have the same duration as the certificates. Duration of different types of certificates issued under this certificate policy is as follows:

- Mero Root CA system certificate: 20 years;
- Mero CA system certificate: 10 years;
- Electronic signature certificates: 2 years;
- Electronic mail encryption certificates: 2 years;
- Mero CR internal use data storage encryption certificates: 2 years;
- External subject data storage encryption certificates: 2 years;
- External subject electronic signature certificates: 2 years;
- External subject electronic mail encryption certificates: 2 years;
- Infrastructure component authentication certificates: 3 years.

5.4 Computer and network security

Computer security

The operating system of the server of the issuing Mero Root CA is periodically updated according to the principles defined by the internal politics of Mero CR.

No requirements in terms of updates are placed on the operating system of the server of Mero Root CA (the root authority server is disconnected from the computer network and switched off by default).

Network security

Requirements for server network security within the Mero CR PKI hierarchy are listed in the System security policy document.

Antivirus protection

The operating system of the issuing Mero CA is protected using periodically updated antivirus software according to the relevant in-house directive.

No requirements in terms of antivirus system are placed on the operating system of the Mero Root CA server (the root authority server is disconnected from the computer network and switched off by default).

Usage of replaceable media

Any replaceable medium must be checked using an updated antivirus system and/or formatted before use.

6 Certificate, CRL and OCSP profiles

6.1 Certificate profile

Mero CA issues certificates according to the X.509 standard, version 3. Profiles of the certificates issued are listed in Appendix A, Chapter 9 herein.

6.1.1 Version number

Certification authorities as part of the Mero CR PKI infrastructure publish certificates according to the X.509 standard, version 3.

6.1.2 Certificate extensions

Any extensions used within the certificates issued are listed in Annex A, Chapter 9.2 herein.

6.1.3 Algorithm object identifiers („OID“)

Algorithms used within Mero CA are not assigned any OID. Within the hierarchy of the certification authorities operated by Mero CR, only commonly known algorithms are used.

6.1.4 Name recording methods

Name recording rules are listed in Chapter 2.

6.1.5 Name constraints

The names listed in the certificate must exactly match the data in the domain (for certificates issued to internal staff members or for authenticating infrastructure components) and/or data obtained from the person in charge for a business partner (for certificates issued to staff members of business partners).

6.1.6 Certificate policy OID

Each certificate issued by certification authorities within Mero CR PKI hierarchy contains a link to the certification policy according to which the certificate had been issued (policy OID).

6.1.7 „Policy Constraints“ extension

No certificates issued by Mero CA use the „Policy Constraints“ extension.

6.1.8 Processing semantics for the critical "Certificate Policies" extension

The method of processing semantics for the critical "Certificate Policies" extension is provided in Chapter 9.2.

6.2 CRL profile

6.2.1 Version number

Certification authorities as part of the Mero CR PKI infrastructure publish CRLs according to the X.509 standard, version 2.

6.2.2 CRL and CRL entry extensions

Revoked certificate profiles are listed in Annex A, Chapter 9.3 herein.

7 Compliance audit and other assessments

7.1 Frequency and circumstances of assessment

Within Mero CR, the internal audit department regularly checks the ICT systems operated for system security. These include checking compliance of the provision of certification services with PKI internal security documentation (certification policy, certification implementation guidelines, system security policy).

Any security incident related to the operation of Mero CR certification authorities are regularly evaluated by CA Auditor, which is a person independent of the operation and management of CA.

7.2 Identity/qualifications of assessor

The internal review is performed by staff members with good knowledge of PKI issues. External auditors can be only a person / company with good knowledge in PKI implementation and demonstrated expertise in the field.

7.3 Assessor's relationship to assessed entity

The internal review is performed by Mero CR staff members.

External auditors can be only a person / company independent of Mero CR.

7.4 Topics covered by assessment

Topics to be assessed within periodical internal / external checks are specified in the Certification implementing guidelines.

7.5 Actions taken as a result of deficiency

Any results of internal / external checks are delivered to CA Manager who shall ensure remedy of any deficiency observed.

7.6 Communications of results

A written report on each internal / external audit undertaken is produced and forwarded to CA Manager, who shall ensure distribution and discussion of the report.

In cases where the report includes a self-standing auditor's opinion, CA Manager may decide on disclosure of such opinion.

8 Other business and legal matters

8.1 Fees

Certification services provided by Mero Root CA and Mero CA are provided free of any charge.

8.2 Confidentiality

Mero CR ensures the protection of personal data, to which it gains access as part of the provision of certification services. Privacy Policy is contained in this Certification policy and Certification implementing guidelines and is based on the relevant provisions of Act No. 101/2000 Coll. on protection of personal data, as amended.

8.3 Limitations of liability

Mero CR is not responsible for damage caused by the use of the certificate, if the holder or relying person fails to comply with the permitted use of the certificate referred to in section 1.5 of this certificate policy.

Mero CR is not liable for damages resulting from the use of certificates in the period after the receipt of the revocation request provided Mero CR has respected the deadline for publication of the revoked certificate on the Certificate Revocation List (CRL) as provided in Chapter 0 of this Certification policy.

The provisions of this Article shall remain in force even after termination of this Certification policy.

8.4 Term and termination

8.5 Term

This Certification policy becomes effective upon the day set forth in Chapter 0 until revoked.

8.5.1 Termination

This document remains applicable until

- It is replaced by a newer version, or
- Until the provision of certification services at Mero CR is terminated.

8.5.2 Effect of termination and survival

All limitations and provisions listed in 0 concerning business and legal matters shall survive possible termination of this document as a result of termination of the provision of certification services.

8.6 Communications between participants

8.6.1 Communications with certification service providers

Any information that the provider of certification services wishes to communicate to its customers shall be published on its website. Any major information, such as suspected compromise of keys of a certification authority within the Mero CR hierarchy shall be communicated by the certification service provider on its website as well, while a warning shall be directed to the certificate holders.

Certificate holders - internal Mero CR staff members - shall communicate with the certification service provider in person, by telephone or using the "User accounts" folder within the HeliosGreen information system.

Certificate holders - external subjects - shall communicate with the provider of certification services through the person in charge.

8.7 Amendments

Any new certification policy released shall be announced via the Mero CR website.

In addition, Mero CR staff members shall be notified via email. External subjects using the Mero CR certification services shall be informed via the relevant person in charge.

8.8 Dispute resolution

If any dispute arises, the certificate holder shall contact CA Manager.

8.9 Miscellaneous provisions

8.9.1 Force majeure

Mero CR is not responsible for the breach of its obligations caused by acts of God such as large-scale natural disasters, strikes, civil unrest or hostilities.

8.10 Other provisions

8.10.1 Governing documents

When creating certification policies and the certification implementing guidelines, the following documents were in particular taken into account:

- Act No. 227/2000 Coll. on electronic signature, as amended;
- Act No. 101/2000 Coll. on protection of private information, as amended;
- CWA 14167-1:2003: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- CSN ISO/IEC 27001:2006 Information technology - Security techniques - Information safety management systems - Requirement;
- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

9 Annex A

9.1 Certificate profiles

The table below contains profiles of certificates issued within the Mero CR PKI hierarchy.

Table 1 Certificate profiles

Field name	Root certification authority certificate	Subordinate certification authority certificate	Electronic signature certificate, electronic signature for external subjects	Electronic mail encryption certificate, electronic mail encryption for external subjects	Internal use data storage encryption certificate	External subject data storage encryption certificate	Infrastructure component authentication certificate
Version	3	3	3	3	3	3	3
Serial number	A series number assigned by the root certification authority to each certificate issued	A series number assigned by the root certification authority to each certificate issued	A certificate series number assigned by the issuing certification authority	A certificate series number assigned by the issuing certification authority	A certificate series number assigned by the issuing certification authority	A certificate series number assigned by the issuing certification authority	A certificate series number assigned by the issuing certification authority
Signature Algorithm	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption
Issuer							
Country	CZ	CZ	CZ	CZ	CZ	CZ	CZ
Organization	Mero CR	Mero CR	Mero CR	Mero CR	Mero CR	Mero CR	Mero CR
CN	Mero Root	Mero Root	Mero CA	Mero CA	Mero CA	Mero CA	Mero CA

Field name	Root certification authority certificate	Subordinate certification authority certificate	Electronic signature certificate, electronic signature for external subjects	Electronic mail encryption certificate, electronic mail encryption for external subjects	Internal use data storage encryption certificate	External subject data storage encryption certificate	Infrastructure component authentication certificate
	CA	CA					
Validity							
Not before	Certificate issue date	Certificate issue date	Certificate issue date	Certificate issue date	Certificate issue date	Certificate issue date	Certificate issue date
Not after	20 years as of the date of issue	10 years as of the date of issue	2 years as of the date of issue	2 years as of the date of issue	2 years as of the date of issue	2 years as of the date of issue	3 years as of the date of issue
Subject							
Country	CZ	CZ	CZ	CZ	CZ	CZ	CZ
Organization	Mero CR	Mero CR	Mero CR	Mero CR	Mero CR	Mero CR	Mero CR
CN	Mero Root CA	Mero CA	Certificate applicant name	Certificate applicant name	Certificate applicant name	External subject name	Infrastructure component identifier
Subject Public Key Info							
Algorithm	RsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption
SubjectPublicKey	Root CA public key, size: 4096 bits	Subordinate CA public key, size: 2048 bits	Certificate public key, size: 2048 bits	Certificate public key, size: 2048 bits	Certificate public key, size: 2048 bits	Certificate public key, size: 2048 bits	Certificate public key, size: 2048 bits
Extensions	Certificate extension as per the table below	Certificate extension as per the table below	Certificate extension as per the table below	Certificate extension as per the table below	Certificate extension as per the table below	Certificate extension as per the table below	Certificate extension as per the table below
Signature Algorithm	Sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption
Signature Value	Electronic signature of the certificate by the root CA	Electronic signature of the certificate by the root CA	Electronic signature of the certificate by the issuing CA	Electronic signature of the certificate by the issuing CA	Electronic signature of the certificate by the issuing CA	Electronic signature of the certificate by the issuing CA	Electronic signature of the certificate by the issuing CA

9.2 Certificate extensions

The table below contains profiles of extensions of certificates issued within the Mero CR PKI hierarchy.

Table 2 Extension profiles

Extension name	Root certification authority (Mero Root CA)	Subordinate certification authority (Mero CA)	Electronic signature, electronic signatures for external subjects	Electronic mail encryption, electronic mail encryption for external subjects	Internal use data storage encryption	Data storage encryption for external subjects	Infrastructure component authentication
Authority Key Identifier							
Key Identifier	Unique public key identifier of the superior certification authority, i.e. Mero Root CA	Unique public key identifier of the superior certification authority, i.e. Mero Root CA	Unique public key identifier of the issuing certification authority. The identifier value must match that of the Subject Key Identifier within the issuing certification authority certificate.	Unique public key identifier of the issuing certification authority. The identifier value must match that of the Subject Key Identifier	Unique public key identifier of the issuing certification authority. The identifier value must match that of the Subject Key Identifier	Unique public key identifier of the issuing certification authority. The identifier value must match that	Unique public key identifier of the issuing certification authority. The identifier value must match that of the Subject Key Identifier within

				within the issuing certification authority certificate.	within the issuing certification authority certificate.	of the Subject Key Identifier within the issuing certification authority certificate.	the issuing certification authority certificate.
Authority Cert Issuer	The same fields and values as with the Subject field	The same fields and values as with the root certification authority certificate Subject field	The same fields and values as with the issuing certification authority certificate Subject field	The same fields and values as with the issuing certification authority certificate Subject field	The same fields and values as with the issuing certification authority certificate Subject field	The same fields and values as with the issuing certification authority certificate Subject field	The same fields and values as with the issuing certification authority certificate Subject field
Authority CertSerial Number	The same value as with the Serial Number field	The same value as with the root certification authority certificate Serial Number field	The same value as with the issuing certification authority certificate Serial Number field	The same value as with the issuing certification authority certificate Serial Number field	The same value as with the issuing certification authority certificate Serial Number field	The same value as with the issuing certification authority certificate Serial Number field	The same value as with the issuing certification authority certificate Serial Number field
Subject Key Identifier	Unique public key identifier. The identifier value must match the Key Identifier value within the Authority Key Identifier extension in every certificate issued by the root certification authority.	Unique public key identifier. The identifier value must match the Key Identifier value within the Authority Key Identifier extension in every certificate issued by the certification authority.	Unique public key identifier.	Unique public key identifier.	Unique public key identifier.	Unique public key identifier.	Unique public key identifier.
Subject Alternative Name			Certificate applicant email address	Certificate applicant email address	Certificate applicant email address	Certificate applicant (external subject) email address	Infrastructure component identification
Key Usage (critical extension)	KeyCertSign CRLSign Off-line CRL Sign Digital Signature	KeyCertSign, CRLSign Off-line CRL Sign	DigitalSignature, NonRepudatation, KeyEncipherment	KeyEncipherment	KeyEncipherment DataEncipherment	KeyEncipherment DataEncipherment	KeyEncipherment
Extended Key Usage			EmailProtection	EmailProtection	EFS	EFS	serverAuth
CRL Distribution Points							
URI	http://pki_sub/certsrv/	http://pki_sub/certsrv/	http://pki_sub/certsrv/	http://pki_sub/certsrv/	http://pki_sub/certsrv/	http://pki_sub/certsrv/	http://pki_sub/certsrv/
URI	http://www.mero.cz/files/PKI	http://www.mero.cz/files/PKI	http://www.mero.cz/files/PKI	http://www.mero.cz/files/PKI	http://www.mero.cz/files/PKI	http://www.mero.cz/files/PKI	http://www.mero.cz/files/PKI
Basic Constraints							
Ca	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
PathLenC	1	0	-	-	-	-	-

<i>onstraint</i>							
------------------	--	--	--	--	--	--	--

9.3 Profiles of revoked certificates

The table below contains profiles of revoked certificates issued within the Mero CR PKI hierarchy.

Table 3 CRL profiles

Field name	Root certification authority (Mero Root CA) CRL	Subordinate certification authority (Mero CA) CRL
Version	2	2
Signature Algorithm	sha256WithRSAEncryption	sha256WithRSAEncryption
Issuer		
Country	CZ	CZ
Organization	Mero CR	Mero CR
CN	Mero Root CA	Mero CA
This Update	Date and time of issue	Date and time of issue
Next Update	Date and time of issue + 365 days	Date and time of issue + 72 hours
Revoked Certificates		
User Certificate	Revoked certificate series number	Revoked certificate series number
Revocation Date	Date and time of certificate revocation	Date and time of certificate revocation
CRL Entry Extensions	CRL extensions as per the table below	CRL extensions as per the table below
CRL Extensions	CRL extensions as per the table below	CRL extensions as per the table below
Signature Algorithm	Sha1WithRSAEncryption	Sha1WithRSAEncryption
Signature Value	Electronic signature by the issuing CA	Electronic signature by the issuing CA