

<b>Společnost</b>	MERO ČR, a. s. Veltruská 748, Kralupy nad Vltavou
<b>Dokument</b>	SI-GŘ-113
<b>Skartační znak</b>	A

## Certifikační politika MERO ČR, a. s.

<b>Vydání</b>	1.	<b>Zpracoval</b>	Ing. Jan Kotera v. r.
<b>Datum</b>	1. února 2011	<b>Ověřil</b>	Ing. Peter Kováč v. r.
<b>Změny oproti předchozím vydání</b>		<b>Schválil</b>	Ing. Jaroslav Pantůček v. r.
		<b>Představitel vedení pro ISŘ</b>	JUDr. Ing. Mgr. Libor Lukášek, Ph.D. v.r.
		<b>Správce</b>	Petra Klemptová v. r.
		<b>Výtisk</b>	0
		<b>Strana</b>	1/31

## 1 Obsah

1	Obsah.....	2
2	Účel.....	5
2.1	Přehled.....	5
3	Rozsah působnosti.....	5
4	Přehled použitých pojmů a zkratk.....	5
4.1	Participující subjekty.....	6
4.1.1	Certifikační autority (dále „CA“).....	6
4.1.2	Registrační autority (dále „RA“).....	7
4.1.3	Držitelé certifikátů, kteří požádali o vydání certifikátu, a kterým byl certifikát vydán.....	7
4.1.4	Spoléhající se strany.....	7
4.2	Použití certifikátu.....	7
4.2.1	Přípustné použití certifikátu.....	7
4.2.2	Omezení použití certifikátu.....	8
4.3	Správa politiky.....	8
4.3.1	Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici.....	8
4.4	Úložiště informací a dokumentace.....	8
4.5	Zveřejňování informací a dokumentace.....	8
4.5.1	Zveřejňování certifikátů a CRL.....	8
4.5.2	Zveřejňování informací o certifikační autoritě.....	8
4.6	Periodicita zveřejňování informací.....	8
4.7	Řízení přístupu k jednotlivým typům úložišť.....	9
5	Identifikace a autentizace.....	9
5.1	Pojmenování u certifikátů vydaných certifikační autoritou MERO CA.....	9
5.1.1	Typy jmen.....	9
5.1.2	Jedinečnost jmen.....	9
5.2	Počáteční ověření identity.....	9
5.2.1	Ověřování identity fyzické osoby.....	9
5.2.2	Neověřené informace vztahující se k držiteli certifikátu.....	9
5.2.3	Kritéria pro interoperabilitu.....	10
5.3	Identifikace a autentizace při zpracování požadavků na výměnu veřejného klíče v certifikátu.....	10
5.3.1	Identifikace a autentizace při vydání následného certifikátu.....	10
5.3.2	Identifikace a autentizace při výměně kryptografických klíčů po zneplatnění certifikátu.....	10
5.4	Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu.....	10
6	Požadavky na životní cyklus certifikátu.....	11
6.1	Žádost o vydání certifikátu.....	11
6.1.1	Subjekty oprávněné podat žádost o vydání certifikátu.....	11
6.1.2	Odpovědnosti poskytovatele a žadatele.....	11
6.2	Zpracování žádosti o certifikát.....	12
6.2.1	Identifikace a autentizace při podání žádosti o vydání certifikátu.....	12
6.2.2	Přijetí nebo zamítnutí žádosti o certifikát.....	12
6.2.3	Doba zpracování žádosti o certifikát.....	12
6.3	Vydání certifikátu.....	13
6.3.1	Oznámení o vydání certifikátu držiteli certifikátu.....	13
6.3.2	Zveřejňování vydaných certifikátů poskytovatelem.....	13
6.4	Použití kryptografických klíčů a certifikátu.....	13
6.4.1	Použití soukromého klíče a certifikátu držitelem certifikátu.....	14
6.4.2	Použití veřejného klíče a certifikátu spoléhající se stranou.....	14
6.5	Obnovení certifikátu.....	14
6.6	Vydání následného certifikátu.....	14
6.7	Změna údajů v certifikátu.....	15
6.8	Zneplatnění certifikátu.....	15
6.8.1	Podmínky pro zneplatnění certifikátu.....	15
6.8.2	Subjekty oprávněné žádat o zneplatnění certifikátu.....	15
6.8.3	Požadavek na zneplatnění certifikátu.....	16
6.8.4	Postup při zneplatnění certifikátu.....	16
6.8.5	Doba odkladu požadavku na zneplatnění certifikátu.....	16
6.8.6	Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu.....	16
6.8.7	Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn.....	17
6.8.8	Periodicita vydávání seznamu zneplatněných certifikátů.....	17

6.8.9	Maximální zpoždění při vydávání seznamu zneplatněných certifikátů .....	17
6.9	Ověřování statutu certifikátu .....	17
6.10	Ukončení poskytování služeb pro držitele certifikátu .....	17
7	Management, provozní a fyzická bezpečnost .....	17
7.1	Fyzická bezpečnost .....	18
7.1.1	Fyzický přístup .....	18
7.1.2	Elektrina a klimatizace, vlivy vody a protipožární ochrana .....	18
7.1.3	Ukládání médií .....	18
7.1.4	Nakládání s odpady .....	18
7.1.5	Zálohy mimo budovu .....	18
7.2	Procesní bezpečnost .....	18
7.3	Personální bezpečnost .....	18
7.4	Auditní záznamy (logy) .....	19
7.4.1	Typy zaznamenávaných událostí .....	19
7.4.2	Periodicita zpracování záznamů .....	19
7.4.3	Doba uchování auditních záznamů .....	19
7.4.4	Ochrana auditních záznamů .....	19
7.4.5	Postupy pro zálohování auditních záznamů .....	19
7.4.6	Systém shromažďování auditních záznamů (interní nebo externí) .....	19
7.4.7	Postup při oznamování události subjektu, který ji způsobil .....	19
7.4.8	Hodnocení zranitelnosti .....	19
7.5	Uchování informací a dokumentace .....	19
7.6	Výměna dat pro ověřování elektronických podpisů v nadřazeném certifikátu poskytovatele .....	20
7.7	Obnova po havárii nebo kompromitaci .....	20
7.7.1	Postup v případě incidentu a kompromitace .....	20
7.7.2	Poškození výpočetních prostředků, softwaru nebo dat .....	20
7.7.3	Postup při kompromitaci dat pro vytváření elektronických podpisů poskytovatele .....	20
7.7.4	Schopnost obnovit činnost po havárii .....	21
7.8	Ukončení činnosti CA .....	21
8	Technická bezpečnost .....	21
8.1	Generování a instalace kryptografických klíčů .....	21
8.2	Ochrana soukromého klíče a bezpečnost kryptografických modulů .....	22
8.3	Další aspekty správy kryptografických klíčů .....	22
8.4	Počítačová a síťová bezpečnost .....	23
9	Profily certifikátu, seznamu zneplatněných certifikátů a OCSP .....	23
9.1	Profil certifikátu .....	23
9.1.1	Číslo verze .....	23
9.1.2	Rozšiřující položky v certifikátu .....	23
9.1.3	Objektové identifikátory (dále „OID“) algoritmů .....	23
9.1.4	Způsoby zápisu jmen a názvů .....	23
9.1.5	Omezení jmen a názvů .....	23
9.1.6	OID certifikační politiky .....	23
9.1.7	Rozšiřující položka „Policy Constraints“ .....	24
9.1.8	Způsob zápisu kritické rozšiřující položky „Certificate Policies“ .....	24
9.2	Profil seznamu zneplatněných certifikátů .....	24
9.2.1	Číslo verze .....	24
9.2.2	Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v CRL .....	24
10	Hodnocení shody a jiná hodnocení .....	24
10.1	Periodicita hodnocení nebo okolnosti pro provedení hodnocení .....	24
10.2	Identita a kvalifikace hodnotitele .....	24
10.3	Vztah hodnotitele k hodnocenému subjektu .....	24
10.4	Hodnocené oblasti .....	24
10.5	Postup v případě zjištění nedostatků .....	24
10.6	Sdělování výsledků hodnocení .....	24
11	Ostatní obchodní a právní záležitosti .....	25
11.1	Poplatky .....	25
11.2	Ochrana osobních údajů .....	25
11.3	Omezení odpovědnosti .....	25
11.4	Doba platnosti, ukončení platnosti .....	25
11.4.1	Doba platnosti .....	25
11.4.2	Ukončení platnosti .....	25
11.4.3	Důsledky ukončení a přetrvání závazků .....	25

11.5	Komunikace mezi zúčastněnými subjekty .....	25
11.5.1	Komunikace s poskytovatelem certifikačních služeb .....	25
11.6	Změny .....	26
11.7	Řešení sporů .....	26
11.8	Další ustanovení .....	26
11.9	Vyšší moc .....	26
11.10	Další opatření .....	26
11.11	Související dokumenty .....	26
12	Závěrečná ustanovení .....	26
13	Seznam příloh .....	26

## 2 Účel

Účelem tohoto dokumentu je stanovit pravidla a postupy pro vydávání certifikátů pro bezpečnostní služby PKI poskytované MERO ČR, a.s. Mezi poskytované bezpečnostní služby PKI patří:

- elektronický podpis,
- šifrování elektronické pošty,
- šifrování datových úložišť pro interní použití v MERO ČR, a.s.,
- elektronický podpis pro externí subjekt,
- šifrování elektronické pošty pro externí subjekt,
- šifrování datových úložišť pro externí subjekt,
- autentizace technických zařízení.

Tato certifikační politika popisuje způsoby registrace, přípustné použití certifikátů a nezbytné postupy, které je zapotřebí uplatňovat v zájmu dodržení přijatých bezpečnostních standardů MERO ČR, a.s. Certifikáty podle této certifikační politiky jsou vydávány následujícím subjektům:

- zaměstnanci MERO ČR, a.s.,
- externí subjekty, se kterými má MERO ČR, a.s. uzavřen smluvní vztah a u kterých je potřeba zajistit bezpečný přenos dat dle příslušného postupu pro klasifikaci dat,
- technická zařízení (servery, certifikační autority v rámci PKI hierarchie MERO ČR, a.s.).

Jiným subjektům (soukromé či právnické osoby) nejsou certifikáty MERO ČR, a.s. vydávány.

### 2.1 Přehled

MERO ČR, a.s. je poskytovatel certifikačních služeb. MERO ČR, a.s. vytvořilo dvouúrovňovou hierarchii interních certifikačních autorit, kterou tvoří kořenová certifikační autorita MERO Root CA a vydávající certifikační autorita MERO CA (dále jen „PKI hierarchie MERO ČR, a.s.“). Detaily o PKI hierarchii MERO ČR, a.s. jsou uvedeny v kapitole 4.1.1.

MERO ČR, a.s. není akreditovaným poskytovatelem certifikačních služeb a certifikační autority v rámci její PKI hierarchie nevydávají kvalifikované certifikáty ve smyslu zákona č. 227/2000 Sb., o elektronickém podpisu.

## 3 Rozsah působnosti

Tato směrnice je určena pro všechny uživatele výpočetních a komunikačních technologií ve správě IT oddělení společnosti MERO ČR, a. s.

## 4 Přehled použitých pojmů a zkratk

**CA** - Certifikační autorita.

**CRL (Certificate Revocation List)** – seznam zneplatněných certifikátů. Obsahuje certifikáty, které nadále nelze pokládat za platné například z důvodu prozrazení odpovídajícího soukromého klíče subjektu. CRL je digitálně podepsán vystavitelem certifikátů – certifikační autoritou.

**Držitel certifikátu** – zaměstnanec MERO ČR, a.s., její obchodní partner nebo technické zařízení provozované v MERO ČR, a.s. od okamžiku vydání certifikátu.

**HeliosGreen** – je informační systém poskytující technickou podporu koncovým uživatelům IS/IT. Zadavatel požadavku se prostřednictvím informačního systému HeliosGreen spojí s oddělením IT, které požadavek vyřeší.

**Kvalifikovaný certifikát** – kvalifikovaný certifikát ve smyslu zákona (**Chyba! Nenalezen zdroj odkazů.**).

**Následný certifikát** – certifikát vydaný jako náhrada za již vydaný certifikát; tato certifikační politika stanovuje, které údaje původního certifikátu mohou být v následném certifikátu změněny.

**MERO Root CA** – kořenová certifikační autorita, která má samopodepsaný systémový certifikát. MERO Root CA dále vydává systémové certifikáty pro podřízenou certifikační autoritu MERO CA a podepisuje její CRL.

**MERO CA** – podřízená (vydávající) certifikační autorita, která má systémový certifikát podepsaný kořenovou certifikační autoritou MERO Root CA. Tato autorita vydává systémové certifikáty pro zaměstnance MERO ČR, a. s., její vybrané obchodní partnery a technická zařízení používaná v rámci MERO ČR, a. s.

**Kryptografické klíče** – data pro vytváření elektronického podpisu spolu s odpovídajícími daty pro ověřování elektronického podpisu (odpovídající si soukromý a veřejný klíč).

**PKI (Public Key Infrastructure)** - infrastruktura správy a distribuce veřejných klíčů, která umožňuje pomocí přenosu důvěry používat cizí veřejné klíče a ověřovat jimi elektronické podpisy, šifrovat, nebo se autentizovat.

**PKI hierarchie** -Hierarchie certifikačních autorit, která zahrnuje všechny certifikační autority, které jsou ve společnosti provozovány.

**Soukromý klíč** – souhrnné označení dat pro vytváření elektronického podpisu, dešifrování nebo autentizaci.

**Uživatel certifikátu** – osoba, která užívá certifikát vydaný MERO ČR, a. s. například pro šifrování, pro ověření elektronického podpisu nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Osoba spoléhající se na certifikát.

**Veřejný klíč** – souhrnné označení dat pro ověřování elektronického podpisu nebo šifrování.

**Zaměstnanec** – osoba v zaměstnaneckém poměru k MERO ČR, a. s., pro kterou je umožněno vydání certifikátu.

**Žadatel** – osoba, která má právo žádat o certifikát dle platné certifikační politiky.

## 4.1 Participující subjekty

Participujícími subjekty pro tuto certifikační politiku jsou:

- MERO ČR, a. s., jako poskytovatel certifikačních služeb,
- zaměstnanci MERO ČR, a. s., jako držitelé (uživatelé) certifikátů (spoléhající se strany),
- externí subjekty – obchodní partneři MERO ČR, a. s., jako držitelé (uživatelé) certifikátů (spoléhající se strany),
- pověřené osoby – zaměstnanci MERO ČR, a. s., kteří vystupují jako kontaktní osoby pro externí subjekty. Každý externí subjekt má v MERO ČR, a. s. přidělenou jednu pověřenou osobu.

Identifikační a kontaktní údaje poskytovatele certifikačních služeb jsou:

MERO ČR, a. s.

IČ: 60193468, DIČ CZ60193468

Veltruská 748, Kralupy nad Vltavou

Telefon: +420 315 701 100

E-mail: [info@MERO.cz](mailto:info@MERO.cz)

### 4.1.1 Certifikační autority (dále „CA“)

PKI hierarchie interních certifikačních autorit v MERO ČR, a. s. je tvořena kořenovou a vydávající (rovněž podřízenou) certifikační autoritou.

#### MERO Root CA

Kořenem PKI hierarchie MERO ČR, a. s. je certifikační autorita MERO Root CA. Tato autorita slouží k zajištění důvěrnosti celé PKI hierarchie. MERO Root CA vydává systémové certifikáty všem certifikačním autoritám v rámci PKI hierarchie MERO ČR, a. s.

#### MERO CA

Podřízená certifikační autorita MERO CA vydává a spravuje certifikáty koncových uživatelů. Typy vydávaných certifikátů jsou následující:

- certifikáty pro elektronický podpis,
- certifikáty pro šifrování elektronické pošty,
- certifikáty pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.,
- certifikáty pro elektronický podpis pro externí subjekt,
- certifikáty pro šifrování elektronické pošty pro externí subjekt,

- certifikáty pro šifrování datových úložišť pro externí subjekt,
- certifikáty pro autentizaci technických zařízení.

#### 4.1.2 Registrační autority (dále „RA“)

Poskytovatel certifikačních služeb neprovozuje speciální pracoviště registrační autority. Služby registrační autority (zejména přijímání žádostí o certifikát, předání certifikátu, zneplatnění certifikátů) zajišťují osoby v rolích Správce certifikátů.

#### 4.1.3 Držitelé certifikátů, kteří požádali o vydání certifikátu, a kterým byl certifikát vydán

Držitelem certifikátu je vždy:

- zaměstnanec MERO ČR, a. s., nebo
- externí subjekt - zaměstnanec obchodního partnera MERO ČR, a. s.,
- technické zařízení provozované v rámci MERO ČR, a. s.,

který o certifikát požádal (v případě certifikátu pro technické zařízení je to osoba v roli Správce certifikátů), úspěšně prošel procesem zpracování žádosti a byl mu na základě tohoto procesu vydán certifikát.

#### 4.1.4 Spoléhající se strany

Spoléhající se stranou (uživatel certifikátu) je libovolný subjekt spoléhající se na certifikát vydaný některou z certifikačních autorit MERO ČR, a. s. Typicky se jedná o zaměstnance MERO ČR, a. s., případně o její obchodní partnery.

### 4.2 Použití certifikátu

#### 4.2.1 Přípustné použití certifikátu

Následující tabulka dává přehled o přípustném použití jednotlivých typů certifikátů, které jsou vydávány v rámci PKI hierarchie MERO ČR, a. s. podle této certifikační politiky. Jiné než toto použití vydávaných certifikátů není přípustné.

##### **Certifikát pro elektronický podpis**

- Ověřování elektronických podpisů,
- Autentizace (prokázání identity).

##### **Certifikát pro šifrování elektronické pošty**

- Šifrování e-mailů.

##### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

- Šifrování dat v datových úložištích, noteboocích, desktopech, CD apod. pro interní použití.

##### **Certifikát pro elektronický podpis pro externí subjekt**

- Ověřování elektronických podpisů,
- Autentizace (prokázání identity).

##### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

- Šifrování e-mailů.

##### **Certifikát pro šifrování datových úložišť pro externí subjekt**

- Šifrování dat v datových úložištích pro externí použití (např. USB klíč určený pro doručení obchodnímu partnerovi).

##### **Certifikát pro autentizaci technických zařízení**

- Autentizace (prokázání identity) technických zařízení (např. aplikací, síťových zařízení, serverů).

##### **Systémové certifikáty certifikačních autorit**

- Elektronický podpis certifikátů certifikačních autorit a podpis jejich CRL.

#### 4.2.2 Omezení použití certifikátu

Certifikáty vydané podle této certifikační politiky je možné využívat pouze v souvislosti s řádnými a legálními účely a v souladu s platnými právními předpisy.

#### 4.3 Správa politiky

Za iniciování změn v certifikační politice nebo inicializaci vytvoření nové certifikační politiky je odpovědný Manažer CA. Aktuální verze certifikační politiky je zveřejněna na webových stránkách poskytovatele certifikačních služeb <http://www.MERO.cz/dokumenty-ke-stazeni/>

Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici.

Za správu této certifikační politiky je odpovědný poskytovatel certifikačních služeb, tedy MERO ČR, a. s., konkrétně Manažer CA.

#### 4.3.1 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osobou spravující tuto certifikační politiku je Manažer CA. Další informace je možné získat na webových stránkách poskytovatele certifikačních služeb <http://www.MERO.cz/>

Odpovědnost za zveřejňování a úložiště informací a dokumentace.

#### 4.4 Úložiště informací a dokumentace

Jednotlivá úložiště informací a dokumentace provozuje a za jejich provoz odpovídá MERO ČR, a. s., jako poskytovatel certifikačních služeb.

Jedinou výjimkou je úložiště na adrese <http://www.MERO.cz/> provozované společností Qwerton Formica, spol. s r.o., na základě platné smlouvy s MERO ČR, a. s.

Za zveřejňování informací odpovídá MERO ČR, a. s., jako poskytovatel certifikačních služeb.

#### 4.5 Zveřejňování informací a dokumentace

Vydané certifikáty jsou uloženy v databázi certifikační autority, která je vydala.

Informace o provozu certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. a bezpečnostní dokumentace certifikačních autorit jsou zveřejňovány v níže uvedeném rozsahu.

#### 4.5.1 Zveřejňování certifikátů a CRL

Certifikáty certifikačních autorit MERO ČR, a. s. a informace o stavu vydaných certifikátů ve formě seznamu zneplatněných certifikátů (CRL) jsou zveřejňovány na webových stránkách MERO ČR, a. s.: <http://www.MERO.cz/files/PKI>

Dále pak i na serveru vydávající certifikační autority: [http://pki\\_sub](http://pki_sub)

#### 4.5.2 Zveřejňování informací o certifikační autoritě

Certifikační politika je zveřejněna na webových stránkách MERO ČR, a.s <http://www.MERO.cz/dokumenty-ke-stazeni/>

Další důležité informace (např. informace o zneplatnění systémového certifikátu certifikační autority) nebo informace o mimořádných událostech jsou zveřejňovány na webových stránkách MERO ČR, a. s.

#### 4.6 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

- certifikační politika, certifikační prováděcí směrnice (CPS) a systémová bezpečnostní politika jsou zveřejňovány (pokud jsou určeny ke zveřejnění) po schválení a vydání nové verze, vždy však před počátkem platnosti daného dokumentu,

- informace o stavu certifikátu ve formě seznamu zneplatněných certifikátů (CRL) jsou zveřejňovány neprodleně po jejich vydání, nejpozději však před koncem platnosti posledního zveřejněného seznamu zneplatněných certifikátů. V případě vydávající certifikační autority MERO CA je to alespoň jednou za 72 hodin a v případě kořenové certifikační autority MERO Root CA alespoň jednou za 12 měsíců, důležité informace jsou zveřejňovány neprodleně.

#### 4.7 Řízení přístupu k jednotlivým typům úložišť

Certifikační politiky, certifikáty certifikačních autorit, certifikáty koncových uživatelů a seznamy zneplatněných certifikátů (CRL) a další důležité informace jsou přístupné pro čtení bez jakéhokoliv omezení.

## 5 Identifikace a autentizace

### 5.1 Pojmenování u certifikátů vydaných certifikační autoritou MERO CA

#### 5.1.1 Typy jmen

Položka „Subject“ v certifikátu je konstruována podle standardu X.501 resp. návazného standardu X.520. Podrobnosti o struktuře vydávaných certifikátů lze nalézt v kapitole 9.1.

V rozšíření certifikátu v položce „Subject Alternative Name“ je u osob uvedena e-mailová adresa. V případě certifikátu pro autentizaci technických zařízení je v rozšíření certifikátu u „Subject Alternative Name“ uvedena IP adresa tohoto zařízení.

#### 5.1.2 Jedinečnost jmen

Rozlišení držitelů certifikátů je dáno položkou Subject certifikátu. V případě certifikátu vydaného externímu subjektu je za zaručení jednoznačnosti údaje CN v položce Subject certifikátu zodpovědná příslušná pověřená osoba daného obchodního partnera.

### 5.2 Počáteční ověření identity

#### 5.2.1 Ověřování identity fyzické osoby

Ověřování identity osoby (žadatele o certifikát) se liší podle typu certifikátu, o který je žádáno:

##### **Certifikát pro elektronický podpis**

##### **Certifikát pro šifrování elektronické pošty**

##### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Tyto certifikáty jsou vydávány výhradně zaměstnancům MERO ČR, a. s. Certifikáty jsou interním zaměstnancům vydávány automaticky bez předchozího ověření jejich identity.

##### **Certifikát pro autentizaci technických zařízení**

Osoba v roli Správce certifikátů odpovídá za identifikaci a autentizaci správce technického zařízení, který žádá o certifikát.

##### **Certifikát pro elektronický podpis pro externí subjekt**

##### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

##### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Tyto certifikáty jsou vydávány vybraným externím subjektům, u kterých je potřeba zajistit bezpečné předání dokumentů. Každý externí subjekt má v rámci MERO ČR, a. s. přidělenou pověřenou osobu, která zajistí počáteční ověření identity externího subjektu.

##### **Systémové certifikáty certifikačních autorit**

Systémové certifikáty certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. jsou vydávány na základě ceremonálu generování klíčů za účasti osob ve vybraných bezpečnostních rolích PKI. Odpovědnost za zajištění a průběh ceremonálu má osoba v roli Manažera CA.

#### 5.2.2 Neověřené informace vztahující se k držiteli certifikátu

Za ověření správnosti údajů v certifikátu vydávaného internímu zaměstnanci MERO ČR, a. s. je odpovědná osoba v roli Správce certifikátů. Za ověření správnosti údajů v certifikátu pro externí subjekt je odpovědná příslušná pověřená osoba.

### 5.2.3 Kritéria pro interoperabilitu

Případná spolupráce s jinými poskytovateli certifikačních služeb je možná až po schválení Manažerem CA, na základě uzavřené smlouvy a za podmínek definovaných Manažerem CA.

## 5.3 Identifikace a autentizace při zpracování požadavků na výměnu veřejného klíče v certifikátu

### 5.3.1 Identifikace a autentizace při vydání následného certifikátu

Způsob identifikace a autentizace se liší podle typu certifikátu, o jehož následný certifikát je žádáno:

#### **Certifikát pro elektronický podpis**

#### **Certifikát pro šifrování elektronické pošty**

#### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Tyto certifikáty jsou vydávány výhradně zaměstnancům MERO ČR, a. s. Následné certifikáty jsou interním zaměstnancům vydávány automaticky bez předchozího ověření jejich identity.

#### **Certifikát pro autentizaci technických zařízení**

Osoba v roli Správce certifikátů odpovídá za identifikaci a autentizaci správce technického zařízení, který žádá o vydání následného certifikátu.

#### **Certifikát pro elektronický podpis pro externí subjekt**

#### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

#### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Tyto certifikáty jsou vydávány vybraným externím subjektům, u kterých je potřeba zajistit bezpečné předání dokumentů. Každý externí subjekt má v rámci MERO ČR, a. s. přidělenou pověřenou osobu, která zajistí ověření identity externího subjektu při vydávání následného certifikátu.

#### **Systémové certifikáty certifikačních autorit**

Následné certifikáty certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. jsou vydávány na základě ceremonálu generování klíčů za účasti osob ve vybraných bezpečnostních rolích PKI. Odpovědnost za zajištění a průběh ceremonálu má osoba v roli Manažera CA.

### 5.3.2 Identifikace a autentizace při výměně kryptografických klíčů po zneplatnění certifikátu

V případě zneplatnění certifikátu je nutné při identifikaci a autentizaci spojené s vydáním nového certifikátu postupovat stejně jako v případě počátečního ověření identity při vydání prvního certifikátu (viz kapitola 5.2.1).

## 5.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Způsob identifikace a autentizace při zneplatnění certifikátu se liší podle typu certifikátu:

#### **Certifikát pro elektronický podpis**

#### **Certifikát pro šifrování elektronické pošty**

#### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Způsob ověřování identity při podávání žádosti o zneplatnění odpovídá standardnímu postupu pro ověřování identity v MERO ČR, a. s.

#### **Certifikát pro autentizaci technických zařízení**

Správce certifikátů odpovídá za identifikaci a autentizaci správce technického zařízení, který žádá o zneplatnění certifikátu.

#### **Certifikát pro elektronický podpis pro externí subjekt**

#### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

#### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Za ověření identity externího subjektu při zneplatnění certifikátu je odpovědná pověřená osoba.

#### **Systémové certifikáty certifikačních autorit**

Žádost o zneplatnění certifikátů kořenové nebo podřízené certifikační autority může podat pouze Manažer CA.

## 6 Požadavky na životní cyklus certifikátu

### 6.1 Žádost o vydání certifikátu

#### 6.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Subjekty oprávněné podat žádost o vydání certifikátu se liší podle typu certifikátu:

**Certifikát pro elektronický podpis**

**Certifikát pro šifrování elektronické pošty**

**Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Žádost o vydání těchto typů certifikátu mohou podat pouze zaměstnanci MERO ČR, a. s.

**Certifikát pro autentizaci technických zařízení**

Žádost o vydání tohoto typu certifikátů může podat správce příslušného technického zařízení.

**Certifikát pro elektronický podpis pro externí subjekt**

**Certifikát pro šifrování elektronické pošty pro externí subjekt**

**Certifikát pro šifrování datových úložišť pro externí subjekt**

Žádost o vydání těchto typů certifikátů může podat Správce certifikátů na základě požadavku od příslušné pověřené osoby pro daný externí subjekt.

**Systémové certifikáty certifikačních autorit**

Žádost o vydání systémového certifikátu certifikační autority v rámci PKI hierarchie MERO ČR, a. s. může podat pouze osoba v roli Manažer CA.

#### 6.1.2 Odpovědnosti poskytovatele a žadatele

##### Odpovědnost žadatele (držitele) certifikátu

Žadatel je povinen zejména:

- zkontrolovat, zda údaje uvedené v certifikátu jsou správné,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,
- užívat soukromý klíč a odpovídající certifikát pouze pro účely stanovené v této certifikační politice,
- neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče,
- seznámit se s certifikační politikou, podle které mu byl vydán certifikát.

##### Odpovědnost poskytovatele

Poskytovatel certifikačních služeb je zejména povinen:

- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu,
- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na webových stránkách společnosti,
- zveřejnit systémové certifikáty certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. tak, aby se každý mohl ujistit o jeho identitě,
- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
  - s platnými právními předpisy,
  - s touto certifikační politikou,
  - s certifikační prováděcí směrnicí,
  - se systémovou bezpečnostní politikou,
  - s ostatní provozní dokumentací.

## 6.2 Zpracování žádosti o certifikát

### 6.2.1 Identifikace a autentizace při podání žádosti o vydání certifikátu

Způsob identifikace a autentizace při podání žádosti o certifikát se liší podle typu certifikátu, o který je žádáno:

#### **Certifikát pro elektronický podpis**

#### **Certifikát pro šifrování elektronické pošty**

#### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Tyto certifikáty jsou vydávány výhradně zaměstnancům MERO ČR, a. s. Certifikáty jsou interním zaměstnancům vydávány automaticky bez předchozího ověření jejich identity.

#### **Certifikát pro autentizaci technických zařízení**

Osoba v roli Správce certifikátů odpovídá za identifikaci a autentizaci správce technického zařízení, který žádá o certifikát.

#### **Certifikát pro elektronický podpis pro externí subjekt,**

#### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

#### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Tyto certifikáty jsou vydávány vybraným externím subjektům, u kterých je potřeba zajistit bezpečné předání dokumentů. Každý externí subjekt má v rámci MERO ČR, a. s. přidělenou pověřenou osobu, která zajistí počáteční ověření identity externího subjektu.

#### **Systémové certifikáty certifikačních autorit**

Systémové certifikáty certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. jsou vydávány na základě ceremonie generování klíčů za účasti osob ve vybraných bezpečnostních rolích PKI. Odpovědnost za zajištění a průběh ceremonie má osoba v roli Manažera CA.

### 6.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Schvalování žádosti o certifikát se liší podle typu certifikátu, o který je žádáno:

#### **Certifikát pro elektronický podpis**

#### **Certifikát pro šifrování elektronické pošty**

#### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Tyto certifikáty jsou vydávány výhradně zaměstnancům MERO ČR, a. s. Schvalování žádosti o vydání certifikátu zaměstnanci MERO ČR, a. s., probíhá automaticky na základě příslušnosti uživatele v určené doménové skupině.

#### **Certifikát pro autentizaci technických zařízení**

Schvalování nebo zamítnutí žádosti o vydání certifikátu pro autentizaci technických zařízení provádí osoba v roli Správce certifikátů.

#### **Certifikát pro elektronický podpis pro externí subjekt**

#### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

#### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Tyto certifikáty jsou vydávány vybraným externím subjektům, u kterých je potřeba zajistit bezpečné předání dokumentů. Pověřená osoba podá požadavek na certifikát pro externí subjekt. Za posouzení požadavku na vydání certifikátu pro externí subjekt je odpovědná osoba v roli Správce certifikátů.

#### **Systémové certifikáty certifikačních autorit**

Za schválení či odmítnutí žádosti o systémový certifikát certifikační autority v rámci PKI hierarchie MERO ČR, a. s. je odpovědná osoba v roli Manažera CA.

### 6.2.3 Doba zpracování žádosti o certifikát

Doba zpracování žádosti o certifikát se liší podle typu certifikátu, o který je žádáno:

#### **Certifikát pro elektronický podpis**

#### **Certifikát pro šifrování elektronické pošty**

#### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Zpracování a schválení žádosti o vydání certifikátu pro zaměstnance MERO ČR, a. s., probíhá automaticky bezprostředně po jejím přijetí. Po schválení přijaté žádosti je danému zaměstnanci vydán certifikát.

#### **Certifikát pro autentizaci technických zařízení**

Žádost o vydání certifikátu pro autentizaci technických zařízení je zpracována do jednoho pracovního dne od jejího přijetí. Po schválení přijaté žádosti je vydán certifikát.

#### **Certifikát pro elektronický podpis pro externí subjekt**

#### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

**Certifikát pro šifrování datových úložišť pro externí subjekt**

Žádost o vydání certifikátu pro externí subjekt je zpracována do tří pracovních dnů od jejího přijetí.

**Systémové certifikáty certifikačních autorit**

Žádost o vydání systémového certifikátu pro certifikační autoritu je zpracována v rámci ceremoniálu generování klíčů.

**6.3 Vydání certifikátu**

Proces vydání certifikátu se liší podle typu vydávaného certifikátu:

**Certifikát pro elektronický podpis****Certifikát pro šifrování elektronické pošty****Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

K vydání těchto certifikátů dojde automaticky po schválení žádosti o jeho vydání. Příslušným uživatelům je certifikát automaticky instalován na jejich koncové zařízení.

**Certifikát pro autentizaci technických zařízení**

Po vygenerování certifikátu zasílá osoba v roli Správce certifikátů příslušnému správci technického zařízení certifikát prostřednictvím e-mailu.

**Certifikát pro elektronický podpis pro externí subjekt****Certifikát pro šifrování elektronické pošty pro externí subjekt****Certifikát pro šifrování datových úložišť pro externí subjekt**

Po schválení přijaté žádosti Správcem certifikátů je vygenerován externímu subjektu certifikát. Předání certifikátu probíhá na základě podepsaného souhlasu s podmínkami použití certifikátů MERO ČR, a. s. Předání probíhá osobně za pomoci vyměnitelného média, které obsahuje certifikát externího subjektu, příslušné kryptografické klíče a platnou certifikační politiku MERO ČR, a. s. Při převzetí certifikátu externí subjekt zkontroluje správnost údajů uvedených v certifikátu a podepíše doklad o převzetí certifikátu. Součástí dokladu o převzetí certifikátu je i prohlášení, že se seznámil s certifikační politikou a že si je vědom svých povinností, které pro něj z této certifikační politiky plynou.

**Systémové certifikáty certifikačních autorit**

Vydání systémových certifikátů certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. probíhá v rámci ceremoniálu generování klíčů.

**6.3.1 Oznámení o vydání certifikátu držiteli certifikátu**

Způsob oznámení o vydání certifikátu jeho držiteli se liší podle typu vydaného certifikátu:

**Certifikát pro elektronický podpis****Certifikát pro šifrování elektronické pošty****Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Držitelé certifikátů nejsou o vydání těchto certifikátů dodatečně informováni.

**Certifikát pro autentizaci technických zařízení**

Správce certifikátů informuje příslušného správce technického zařízení o vydání certifikátu prostřednictvím e-mailu.

**Certifikát pro elektronický podpis pro externí subjekt****Certifikát pro šifrování elektronické pošty pro externí subjekt****Certifikát pro šifrování datových úložišť pro externí subjekt**

Informace o vydání certifikátu je předána příslušné pověřené osobě, která informuje externí subjekt a zajistí bezpečné předání certifikátu a kryptografických klíčů externímu subjektu.

**Systémové certifikáty certifikačních autorit**

Oznámení o vydání systémových certifikátů certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. probíhá na webových stránkách poskytovatele certifikačních služeb.

**6.3.2 Zveřejňování vydaných certifikátů poskytovatelem**

Certifikáty vydané podle této certifikační politiky nejsou zveřejněny v rozsahu uvedeném v kapitole 4.5.

**6.4 Použití kryptografických klíčů a certifikátu**

Klíčové páry svázané s certifikáty mají stejnou dobu platnosti jako certifikáty. Klíčové páry, na základě kterých již byl vydán certifikát certifikačními autoritami MERO CA nebo MERO Root CA, nemohou být znovu použity.

### 6.4.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Držitel certifikátu:

- nakládá se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,
- v případě ztráty, odcizení nebo podezření na kompromitaci soukromého klíče neprodleně informuje poskytovatele certifikačních služeb a zároveň ukončí používání uvedeného soukromého klíče,
- užívá soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice, uvedené v kapitole 4.2.1.

### 6.4.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Strana spoléhající na certifikát vydaný certifikačními autoritami MERO ČR, a. s.:

- získá certifikáty z bezpečného zdroje (<http://www.MERO.cz/files/PKI>) a ověří otisk ("fingerprint") těchto certifikátů.
- před použitím certifikátu ověří platnost certifikátu a následně i platnost vydaného koncového certifikátu; kontrola se provádí na správnost podpisu vydávající autority a vůči příslušnému aktuálnímu CRL a aktuálnímu času (tuto činnost obvykle vykonává aplikace uživatele certifikátu – spoléhající se strany).
- dostatečně zváží, zda je certifikát vydaný podle této certifikační politiky vhodný pro účel, ke kterému jej chce použít.

### 6.5 Obnovení certifikátu

Pod službou obnovení certifikátu je myšleno vydání nového certifikátu se stejným veřejným klíčem a novou dobou platnosti. V rámci certifikačních autorit provozovaných MERO ČR, a. s. není tato služba poskytována.

### 6.6 Vydání následného certifikátu

Vydáním následného certifikátu je zamýšleno vydání certifikátu se stejnými údaji v položce „Subject“, se změněným klíčovým párem a novými údaji o platnosti certifikátu.

Proces vydání následného certifikátu se liší podle typu certifikátu, o jehož následující certifikát je žádáno:

#### **Certifikát pro elektronický podpis**

#### **Certifikát pro šifrování elektronické pošty**

#### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Zaměstnanci MERO ČR, a. s. je osm týdnů před vypršením platnosti jeho certifikátu vygenerována žádost o nový (tzv. následný) certifikát. Podání žádosti o vydání následného certifikátu proběhne automaticky při přihlášení daného zaměstnance do domény. Žádost o vydání následného certifikátu je zpracována automaticky bezprostředně po jejím přijetí a je automaticky schválena. Po schválení přijaté žádosti o vydání certifikátu je následný certifikát automaticky vydán žadateli a nainstalován na jeho pracovní stanici.

#### **Certifikát pro autentizaci technických zařízení**

Správce certifikátů vygeneruje požadavek o vydání následného certifikátu. Žádost o vydání následného certifikátu pro autentizaci technických zařízení je zpracována do jednoho pracovního dne od jejího přijetí osobou v roli Správce certifikátů. Po schválení přijaté žádosti je vydán certifikát.

#### **Certifikát pro elektronický podpis pro externí subjekt**

#### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

#### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Pověřená osoba podá prostřednictvím informačního systému HeliosGreen, pořadače „Účty uživatelů“, žádost o vydání následného certifikátu. Žádost o vydání následného certifikátu je poté zpracována osobou v roli Správce certifikátů. Po schválení přijaté žádosti je vydán certifikát, který je následně společně s kryptografickými klíči předán příslušné pověřené osobě pro daný externí subjekt. Pověřená osoba zajistí bezpečné předání certifikátu příslušnému žadateli. Při převzetí certifikátu žadatel zkontroluje správnost údajů v certifikátu a podepíše doklad o převzetí certifikátu.

#### **Systémové certifikáty certifikačních autorit**

Vydání následného certifikátu certifikačních autorit MERO Root CA nebo MERO CA probíhá v rámci ceremoniálu generování klíčů.

## 6.7 Změna údajů v certifikátu

Certifikát se změněnými údaji lze vydat pouze

- jako nový certifikát podle postupů uvedených v kapitole 6.3, nebo
- jako následný certifikát podle postupů uvedených v kapitole 6.6, pokud není požadována výměna následujících údajů:
  - údaj CN v položce „Subject“ certifikátu,
  - položku „Subject Alternative Name“ v rozšíření certifikátu.

Pokud pozbývá pravdivosti některý z údajů uvedených v aktuálním certifikátu, je nutné odpovídajícím způsobem požádat o zneplatnění aktuálního certifikátu (viz kapitola 6.8). Po zneplatnění aktuálního certifikátu dojde k podání žádosti o nový certifikát.

### **Certifikát pro elektronický podpis**

### **Certifikát pro šifrování elektronické pošty**

### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Držitel certifikátu nahlásí osobě v roli Správce certifikátů změnu údajů v aktuálním certifikátu.

### **Certifikát pro autentizaci technických zařízení**

Správce příslušného technického zařízení nahlásí osobě v roli Správce certifikátů změnu údajů v aktuálním certifikátu.

### **Certifikát pro elektronický podpis pro externí subjekt**

### **Certifikát pro šifrování elektronické pošty pro externí subjekt**

### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Držitel certifikátu (externí subjekt) informuje příslušnou pověřenou osobu, že došlo ke změně údajů, které jsou obsaženy v certifikátu. Příslušná pověřená osoba na základě nahlášených změn informuje prostřednictvím informačního systému HeliosGreen, pořadače „Účty uživatelů“, osobu v roli Správce certifikátů, která posoudí danou žádost.

### **Systémové certifikáty certifikačních autorit**

Změna údajů v certifikátu certifikační autority si vyžádá úpravu certifikační politiky a nový ceremoniál generování klíčů.

## 6.8 Zneplatnění certifikátu

Platnost certifikátu je ukončena v okamžiku jeho zneplatnění a zveřejnění na seznamu zneplatněných certifikátů (CRL). Pokud není certifikát po dobu jeho platnosti nutné zneplatnit, skončí jeho platnost v časovém okamžiku uvedeném v certifikátu.

### 6.8.1 Podmínky pro zneplatnění certifikátu

Důvody pro zneplatnění systémových certifikátů certifikačních autorit jsou především následující:

- jakékoliv podezření na kompromitaci odpovídajícího soukromého klíče,
- další důvody (zánik poskytovatele certifikačních služeb; pozbytí pravdivosti údajů, na jejichž základě byl certifikát vydán).

Důvody pro zneplatnění certifikátu koncového uživatele jsou především následující:

- jakékoliv podezření na kompromitaci odpovídajícího soukromého klíče,
- hrubé porušení povinností držitele certifikátu vyplývajících z této certifikační politiky,
- příslušná žádost držitele, Správce certifikátů nebo Manažera CA,
- další důvody (úmrtí, ukončení pracovně právního poměru držitele u MERO ČR, a. s., případně u daného obchodního partnera; pozbytí pravdivosti údajů, na jejichž základě byl certifikát vydán).

### 6.8.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu certifikační autority MERO Root CA nebo MERO CA může požádat Manažer CA.

O zneplatnění certifikátu koncového uživatele může požádat

- držitel certifikátu,
- pověřená osoba pro příslušného obchodního partnera, nebo
- osoba v roli Správce certifikátů nebo Manažer CA.

### 6.8.3 Požadavek na zneplatnění certifikátu

Možnosti podání požadavku na zneplatnění certifikátu se liší podle typu certifikátu, o jehož zneplatnění je žádáno:

#### **Certifikát pro elektronický podpis**

#### **Certifikát pro šifrování elektronické pošty**

#### **Certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s.**

Držitel certifikátu může podat žádost o zneplatnění certifikátu pomocí informačního systému HeliosGreen, pořadače „Účty uživatelů“, telefonicky nebo osobně Správci certifikátu.

#### **Certifikát pro autentizaci technických zařízení**

Správce technického zařízení může podat žádost o zneplatnění certifikátu pomocí informačního systému HeliosGreen, pořadače „Účty uživatelů“, telefonicky nebo osobně Správci certifikátu.

#### **Certifikát pro elektronický podpis pro externí subjekt**

#### **Certifikát pro šifrování elektronické pošty pro externí subjekt,**

#### **Certifikát pro šifrování datových úložišť pro externí subjekt**

Pověřená osoba pro příslušného obchodního partnera může podat žádost o zneplatnění certifikátu pomocí informačního systému HeliosGreen, pořadače „Účty uživatelů“, telefonicky nebo osobně u Správce certifikátů. Učiní tak na základě předchozí žádosti externího subjektu (držitele certifikátu) nebo z vlastní vůle, např. pokud byla ukončena spolupráce s daným externím subjektem.

#### **Systémové certifikáty certifikačních autorit**

Osoba v roli Manažer CA podává požadavek na zneplatnění systémového certifikátu pomocí informačního systému HeliosGreen, pořadače „Účty uživatelů“, telefonicky nebo osobně Správci certifikátu.

### 6.8.4 Postup při zneplatnění certifikátu

Postup při zneplatnění certifikátu se liší podle subjektu, který o zneplatnění požádal:

#### **Žádost o zneplatnění certifikátu z vůle držitele certifikátu**

Žadatel o zneplatnění certifikátu požádá osobu v roli Správce certifikátů o zneplatnění. Správce certifikátů v systému certifikační autority certifikát zneplatní a zaznamená daný požadavek v informačním systému HeliosGreen, pořadači „Účty uživatelů“. Tento způsob zneplatnění je dostupný v době pracovních hodin oddělení IT (pondělí – pátek od 8:00 – 16:00) v prostorech sídla MERO ČR, a. s., Veltruská 748, v Kralupech nad Vltavou a na telefonním čísle 315 701 111, nebo mailem na „[\\_IT\\_MERO@MERO.cz](mailto:_IT_MERO@MERO.cz)“

#### **Zneplatnění certifikátu z vůle certifikační autority**

O zneplatnění certifikátu může rozhodnout rovněž poskytovatel certifikačních služeb prostřednictvím Správce certifikátů, pokud držitel certifikátu porušuje pravidla uvedená v certifikační politice nebo ukončí spolupráci s MERO ČR, a. s. Zástupce certifikační autority MERO CA v takovém případě informuje držitele certifikátu o zneplatnění jeho certifikátu s udáním důvodu, proč byl certifikát zneplatněn. Správce certifikátů následně certifikát zneplatní.

### 6.8.5 Doba odkladu požadavku na zneplatnění certifikátu

Držitel certifikátu je povinen požádat o zneplatnění certifikátu neprodleně po zjištění skutečnosti, která je důvodem pro zneplatnění certifikátu.

### 6.8.6 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu

Maximální doba, která uplyne od přijetí žádosti o zneplatnění certifikátu do zveřejnění CRL obsahující i zneplatněný certifikát, je 72 hodin. To platí v případě všech certifikátů vydaných certifikačními autoritami v rámci PKI hierarchie MERO ČR, a. s.

### 6.8.7 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn

Uživatel certifikátu vydaného certifikačními autoritami v rámci PKI hierarchie MERO ČR, a. s. (spoléhající se strana) je povinen postupovat v souladu s ustanoveními kapitola 6.4.2.

### 6.8.8 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů (CRL) je vydáván vždy vzápětí po zpracování žádosti o zneplatnění certifikátu. Následně pak dojde k publikaci CRL. Periodicita publikace CRL je alespoň každých

- 12 měsíců v případě CRL vydávaného kořenovou autoritou MERO Root CA,
- 72 hodin v případě CRL vydávaných podřízenou autoritou MERO CA.

### 6.8.9 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Maximální zpoždění při vydávání seznamu zneplatněných certifikátů (CRL) nesmí překročit hodnotu uvedenou v kapitole 6.8.6.

## 6.9 Ověřování statutu certifikátu

Status certifikátu je možné ověřit na seznamu zneplatněných certifikátů (CRL).

Seznam zneplatněných certifikátů je veřejně přístupná informace. Seznam zneplatněných certifikátů je zveřejňován na následujících serverech:

- webové stránky MERO ČR, a. s. <http://www.MERO.cz/files/PKI>
- server vydávající certifikační autority [http://pki\\_sub/](http://pki_sub/).

Primárním zdrojem aktuálního CRL je server vydávající certifikační autority. Seznam zneplatněných certifikátů je rovněž dostupný z Internetu.

## 6.10 Ukončení poskytování služeb pro držitele certifikátu

Způsoby ukončení poskytování certifikačních služeb se liší dle typu držitele certifikátu:

### Držitel certifikátu - zaměstnanec MERO ČR, a. s.

Poskytování služeb pro držitele certifikátu končí a k zneplatnění certifikátu držitele dojde v případě:

- ukončení pracovně právního poměru s MERO ČR, a. s.,
- nebo jeho přeřazením na takovou pracovní pozici, která nemá oprávnění používat elektronické certifikáty.

### Držitel certifikátu – externí subjekt

Poskytování služeb pro držitele certifikátu končí a k zneplatnění certifikátu držitele dojde v případě:

- ukončení pracovně právního poměru externího subjektu s daným obchodním partnerem MERO ČR, a. s.,
- pozbytím práva externího subjektu žádat o vydání certifikátu, např. z důvodu organizačních změn,
- nebo ukončením spolupráce MERO ČR a. s. s daným obchodním partnerem.

## 7 Management, provozní a fyzická bezpečnost

Pro certifikační autority MERO Root CA a MERO CA byla vypracována následující bezpečnostní dokumentace PKI:

- Systémová bezpečnostní politika, popisující zásady bezpečnosti v oblasti fyzické, procedurální a personální,
- Certifikační prováděcí směrnice (CPS),
- Certifikační politika (tento dokument),
- Jmenování do bezpečnostních rolí PKI.

Dokumenty certifikační prováděcí směrnice a systémová bezpečnostní politika nejsou veřejně přístupné.

## 7.1 Fyzická bezpečnost

### 7.1.1 Fyzický přístup

Technické vybavení certifikačních autorit (servery, datová úložiště, síťová infrastruktura) v rámci PKI hierarchie MERO ČR, a. s. je umístěno v chráněných prostorách v sídle společnosti v Kralupech nad Vltavou. Fyzické zabezpečení technického vybavení vyplývá z bezpečnostních požadavků uvedených v dokumentu Systémová bezpečnostní politika. Chráněné prostory, ve kterých probíhá generování, či uložení klíčů certifikačních autorit mají jasně definovaný perimetr a jsou chráněny proti neoprávněnému vniknutí mechanickými prostředky (bezpečnostní zámky a mříže). V systémové bezpečnostní politice je definováno, kteří pracovníci mají do těchto prostor umožněn fyzický přístup.

### 7.1.2 Elektřina a klimatizace, vlivy vody a protipožární ochrana

Požadavky na vybavení prostor, v kterých se nachází technické vybavení certifikační autority, jsou uvedeny v dokumentu systémová bezpečnostní politika.

### 7.1.3 Ukládání médií

Požadavky na ukládání médií jsou uvedeny v dokumentu systémová bezpečnostní politika.

### 7.1.4 Nakládání s odpady

Informace související s certifikačními autoritami a certifikačními službami musí být poté, co nejsou zapotřebí, likvidována bezpečným způsobem:

- vyměnitelná média jsou fyzicky zlikvidována nebo je použit vhodný program zajišťující úplné smazání média,
- papírové dokumenty jsou zlikvidovány v zařízení k tomu určeném.

### 7.1.5 Zálohy mimo budovu

Poskytovatel certifikačních služeb má zajištěno bezpečné uložení záloh kritických dat certifikační autority (zejména zálohy soukromých klíčů certifikačních autorit) mimo primární lokalitu.

## 7.2 Procesní bezpečnost

Poskytovatel certifikačních služeb definoval bezpečnostní role PKI, které jsou zodpovědné za bezpečný provoz a správu certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. V dokumentu Systémová bezpečnostní politika jsou stanovena pravidla, podle kterých jsou tyto bezpečnostní role obsazovány, včetně požadavků na oddělení pravomocí.

Jsou definovány činnosti vyžadující přítomnost více než jedné osoby. Jedná se zejména o činnosti, při kterých se manipuluje se soukromými klíči certifikačních autorit.

Veškerá přístupová práva (na úrovni fyzického přístupu, na úrovni přístupu k operačnímu systému) jsou vázána na bezpečnostní role PKI. Představitel každé role se musí při přístupu k softwarovým prostředkům certifikační autority identifikovat a autentizovat. Uživatelé v bezpečnostních rolích PKI mají v rámci technických prostředků certifikační autority přidělenou jednoznačnou identifikaci.

## 7.3 Personální bezpečnost

Do bezpečnostních rolí PKI jsou jmenovány výhradně důvěryhodné osoby, které jsou zaměstnanci MERO ČR, a. s. Postihy za porušení pracovní kázně se řídí organizačními předpisy MERO ČR, a. s. Osoby jmenované do bezpečnostních rolí PKI mají k dispozici bezpečnostní dokumentaci PKI.

Každý pracovník, podílející se na provozu, správě a údržbě certifikačních autorit MERO ČR, a. s. je vyškolen pro výkon přidělené role. Součástí školení je i školení o bezpečnosti systému a o chování v havarijních situacích.

Externí dodavatelé, kteří mají přístup do systému certifikační autority, mají povinnost dodržovat požadavky definované v bezpečnostní dokumentaci PKI.

## 7.4 Auditní záznamy (logy)

Zásady kontroly bezpečnostních událostí a auditu jsou popsány v dokumentu Systémová bezpečnostní politika. Tento dokument je přístupný osobám, které se podílejí na zajištění kontroly a auditu. Auditní záznamy jsou v systému vytvářeny pro účel kontroly a případné analýzy a vyšetření mimořádných událostí. Slouží k zajištění možnosti prokázat sled provedených operací a jejich přiřazení osobě, která je vyvolala.

### 7.4.1 Typy zaznamenávaných událostí

V prostředí certifikačních autorit MERO ČR, a. s. jsou zaznamenávány všechny události spojené s vydáváním certifikátů, zneplatněním certifikátů, nakládání s klíči a certifikáty certifikačních autorit a dalších významných událostech (např. ukončení činnosti certifikační autority).

### 7.4.2 Periodicita zpracování záznamů

Odpovědnost za vyhodnocování auditních záznamů má osoba v roli Auditor CA, což je osoba nezávislá na provozu a správě PKI infrastruktury. Auditní záznamy dále podléhají interní kontrole.

### 7.4.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány v souladu s vnitřními předpisy MERO ČR, a. s.

### 7.4.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy tak, aby byly ochráněny proti krádeži, modifikaci a zničení úmyslnému i neúmyslnému (ohněm, vodou).

### 7.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy spojené s vydáváním certifikátů, zneplatněním certifikátů, nakládáním s klíči a certifikáty certifikačních autorit MERO ČR, a. s. a dalšími významnými událostmi jsou automaticky zálohovány v rámci standardních záloh společnosti.

Písemné auditní záznamy jsou pouze archivovány v souladu s pravidly definovanými v Systémové bezpečnostní politice MERO ČR, a. s.

### 7.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Auditní záznamy v elektronické podobě (logy) jsou automaticky vytvářeny v prostředí systému certifikační autority. Auditní záznamy jsou automaticky i manuálně vyhodnocovány.

### 7.4.7 Postup při oznamování události subjektu, který ji způsobil

V případě, že je událost z auditního logu vyhodnocena jako bezpečnostní incident, je postupováno v souladu s příslušnou interní směrnicí MERO ČR, a. s.

### 7.4.8 Hodnocení zranitelnosti

Auditní záznamy jsou v pravidelných intervalech kontrolovány a analyzovány na výskyt nestandardních událostí, které mohou znamenat pokus o narušení bezpečnosti. Dále jsou definovány procedury, jak v těchto případech dále postupovat. Odpovědnost za vyhodnocování logů má osoba v bezpečnostní roli Auditor CA.

## 7.5 Uchování informací a dokumentace

Poskytovatel certifikačních služeb má v dokumentu Systémová bezpečnostní politika popsány zásady kontroly auditních záznamů, zásady archivace auditních záznamů a požadavky na audit.

Poskytovatel certifikačních služeb, MERO ČR, a. s., archivuje následující auditní záznamy vytvořené v souvislosti s provozem certifikačních autorit MERO Root CA a MERO CA:

- programové vybavení a data, včetně vydaných certifikátů a CRL,
- veškerou dokumentaci související s žádostí o certifikát,
- záznamy o obsazování do bezpečnostních rolí PKI,

- bezpečnostní události (logy) automaticky vytvářené systémem certifikační autority.

Archivy dat a programového vybavení jsou umístěny v prostorách k tomu určených. V každé lokalitě, kde je umístěn trezor, musí být veden protokol o manipulaci s uloženými záznamy.

## 7.6 Výměna dat pro ověřování elektronických podpisů v nadřazeném certifikátu poskytovatele

Platnost klíčů certifikačních autorit v rámci PKI hierarchie MERO ČR, a. s. je omezena:

- MERO Root CA – 20 let, a
- MERO CA – 10 let.

### MERO Root CA

S dostatečným předstihem, avšak nejméně 2 roky před vypršením platnosti certifikátu kořenové certifikační autority MERO Root CA se musí uskutečnit ceremoniál vydání nového certifikátu. Výsledkem ceremoniálu bude vytvořený nový samo podepsaný certifikát kořenové certifikační autority, který bude zveřejněn způsobem popsáním v kapitole 0.

### MERO CA

Nejméně 2 roky před vypršením platnosti certifikátu podřízené certifikační autority MERO CA je nutno požádat o vydání následného certifikátu podepsaného kořenovou certifikační autoritou MERO Root CA.

Plánovaná výměna klíčů kořenové i podřízené certifikační autority musí být oznámena držitelům certifikátů nejpozději 6 měsíců před vydáním nového certifikátu MERO Root CA, resp. 3 měsíce před uskutečněním výměny certifikátu autority MERO CA. Toto oznámení bude (včetně důvodu ukončení platnosti certifikátu) zveřejněno na webových stránkách poskytovatele certifikačních služeb.

Po ukončení potřeby používání původních kryptografických dat pro vytváření elektronických podpisů MERO ČR, a. s. prokazatelně tato data zničí a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy bude nutné provést výměnu kryptografických klíčů z důvodu nedostatečnosti použitého algoritmu nebo jeho parametrů (např. velikostí klíče).

## 7.7 Obnova po havárii nebo kompromitaci

MERO ČR, a. s. má vypracovány dokumenty popisující zvládání krizových situací a postupy pro následnou obnovu. Osoby v bezpečnostních rolích PKI jsou řádně vyškoleny, jak postupovat v případě havárie.

### 7.7.1 Postup v případě incidentu a kompromitace

Postup obnovy prostředků certifikační autority po živelné katastrofě nebo jiné mimořádné události je rozpracován v havarijních plánech.

### 7.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Postup zabezpečení informačních aktiv certifikační autority po živelné katastrofě nebo jiné mimořádné události je rozpracován v havarijních plánech.

### 7.7.3 Postup při kompromitaci dat pro vytváření elektronických podpisů poskytovatele

#### Kompromitace soukromého klíče MERO Root CA

V případě podezření na kompromitaci soukromého klíče kořenové certifikační autority MERO Root CA informování všichni držitelé certifikátů vydaných podřízenou certifikační autoritou MERO CA o mimořádném ukončení činnosti této autority. Oznámení bude zveřejněno na webových stránkách MERO ČR, a. s. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

Poskytovatel certifikačních služeb zneplatní certifikát kořenové autority MERO Root CA, certifikát podřízené certifikační autority MERO CA a všechny jí vydané platné certifikáty. Všechny zneplatněné certifikáty budou neprodleně zveřejněny na příslušném CRL.

Následně MERO ČR, a. s., prokazatelně zničí soukromé klíče MERO Root CA a MERO CA o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických podpisů, které zpochybní důvěryhodnost vydávaných certifikátů a seznamů vydávaných certifikátů.

### **Kompromitace soukromého klíče MERO CA**

V případě podezření na kompromitaci soukromého klíče vydávající certifikační autority MERO CA budou informováni všichni držitelé certifikátů o mimořádném ukončení činnosti této autority. Oznámení bude zveřejněno na webových stránkách MERO ČR, a. s. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

MERO Root CA okamžitě zneplatní certifikát MERO CA. Podřízená certifikační autorita MERO CA zneplatní všechny vydané certifikáty koncových uživatelům. Zneplatněné certifikáty budou zveřejněny na příslušném CRL.

Poskytovatel certifikačních služeb následně prokazatelně zničí soukromý klíč MERO CA, který sloužil pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických podpisů, které nepopíratelně zpochybní důvěryhodnost vydávaných certifikátů a seznamů vydávaných certifikátů.

#### **7.7.4 Schopnost obnovit činnost po havárii**

Postupy obnovy činnosti po havárii jsou popsány v havarijních plánech MERO ČR, a. s. V případě havárie zajistí MERO ČR, a. s. alespoň službu zneplatnění certifikátů publikace CRL. V případě havárie velkého rozsahu (přírodní pohroma, válečný stav), je obnova činnosti certifikační autority věcí rozhodnutí vedení MERO ČR, a. s. O rozhodnutí vedení jsou informováni všichni držitelé certifikátů.

### **7.8 Ukončení činnosti CA**

#### **Ukončení činnosti MERO Root CA**

Ukončení činnosti kořenové certifikační autority MERO Root CA musí být oznámeno všem držitelům platných certifikátů vydaných podřízenou certifikační autoritou MERO CA a rovněž zveřejněno na webových stránkách MERO ČR, a. s., a to nejméně dva měsíce před ukončením činnosti autority. V případě, že součástí ukončení činnosti autority je i ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně příslušného důvodu ukončení platnosti.

K datu ukončení činnosti musí certifikační autorita MERO Root CA zneplatnit všechny dosud platné certifikáty a vydat poslední CRL. Následně dojde k zneplatnění systémového certifikátu MERO Root CA. Teprve poté může být činnost této autority ukončena.

Následně MERO ČR, a. s., prokazatelně zničí soukromé klíče pro vytváření elektronických podpisů, které sloužily pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů. O zničení soukromých klíčů je vytvořen záznam. Tyto záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole 7.4.

#### **Ukončení činnosti MERO CA**

Ukončení činnosti podřízené certifikační autority MERO CA musí být oznámeno všem držitelům platných certifikátů a rovněž zveřejněno na webových stránkách MERO ČR, a. s. a to nejméně dva měsíce před ukončením činnosti autority. Součástí oznámení musí být i informace o ukončení platnosti certifikátu autority včetně příslušného důvodu ukončení.

K datu ukončení činnosti musí certifikační autorita MERO CA zneplatnit všechny dosud platné certifikáty a vydat poslední CRL. Následně dojde k zneplatnění systémového certifikátu MERO CA. Teprve poté může být činnost této autority ukončena.

Zneplatněný systémový certifikát MERO CA bude zveřejněn na CRL kořenové certifikační autority MERO Root CA, a to do doby uvedené v této certifikační politice.

Následně MERO ČR, a. s., prokazatelně zničí soukromé klíče MERO CA, které sloužily pro podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů. O zničení soukromých klíčů se provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole 7.4.

## **8 Technická bezpečnost**

### **8.1 Generování a instalace kryptografických klíčů**

#### **Klíče certifikačních autorit**

Generování klíčů kořenové certifikační autority a vydávající certifikační autority je uskutečněno v zabezpečených prostorách MERO ČR, a. s. Generování těchto klíčových párů probíhá kontrolovaným procesem (tzv.

ceremoniálem generování klíčů), na jehož průběh dohlíží Manažer CA. Klíčové páry (soukromý a veřejný klíč) certifikačních autorit MERO Root CA a MERO CA jsou generovány a uchovávány na softwarových úložištích na dedikovaných serverech certifikačních autorit. Soukromé klíče autorit jsou uchovávány v šifrované podobě. Klíče certifikačních autorit v PKI hierarchii MERO ČR, a.s jsou vytvořeny pro algoritmus RSA. Klíč kořenové certifikační autority MERO Root CA má délku modulu 4096 bitů a klíč podřízené certifikační autority MERO CA má délku modulu 2048 bitů.

#### **Klíče koncových uživatelů**

Soukromé klíče koncových uživatelů jsou generovány společně s žádostí o certifikát podřízenou certifikační autoritou MERO CA. Soukromé klíče jsou uloženy na softwarové úložiště na počítačové stanici uživatele. Pro kryptografické klíče uživatelů je použit algoritmus RSA s délkou klíče 2048 bitů.

Soukromé klíče koncových uživatelů u certifikátů určených k šifrování e-mailů a šifrování datových úložišť jsou zálohovány na systémech certifikační autority.

## **8.2 Ochrana soukromého klíče a bezpečnost kryptografických modulů**

#### **Soukromého klíče certifikačních autorit**

Soukromé klíče kořenové certifikační autority i podřízené certifikační autority jsou uchovávány v zabezpečených prostorech MERO ČR, a. s. Soukromý klíč kořenové certifikační autority MERO Root CA je uchováván na souborovém systému dedikovaného serveru. Tento server je odpojený z počítačové sítě a standardně vypnutý (mimo ceremoniál generování klíčů a podpis CRL). Disky serveru jsou ze serveru fyzicky vyjmuty a jsou umístěny v zapečetěné obálce v trezoru.

Soukromý klíč podřízené certifikační autority MERO CA je uchováván v zašifrované podobě v softwarovém úložišti certifikační autority. Přístup k úložišti klíčů soukromého klíče je neustále zaznamenáván a vyhodnocován technickými prostředky. Odpovědnost za vyhodnocování logů má Auditor CA, což je osoba nezávislá na provozu a správě PKI infrastruktury. Hardwarové kryptografické moduly nejsou v prostředí MERO ČR, a. s. použity.

Soukromé klíče certifikačních autorit v PKI hierarchii MERO ČR, a. s. jsou archivovány při ceremoniálu generování klíčů. Způsob archivace je popsán v dokumentu Systémová bezpečnostní politika.

#### **Ochrana soukromých klíčů koncových uživatelů**

Soukromé klíče koncových uživatelů jsou uchovávány v šifrované podobě v softwarovém úložišti na počítačové stanici uživatele.

Soukromé klíče koncových uživatelů u certifikátů určených k šifrování (tj. šifrování e-mailů a šifrování datových úložišť) jsou zálohovány na systémech certifikační autority.

## **8.3 Další aspekty správy kryptografických klíčů**

Veřejné klíče ve formě certifikátů koncových uživatelů, certifikačních autorit jsou archivovány v souladu s dokumentem Systémová bezpečnostní politika MERO ČR, a. s.

Páry klíčů svázané s certifikáty mají stejnou dobu platnosti jako certifikáty. Doba platnosti různých typů certifikátů vydaných podle této certifikační politiky následující:

- Systémový certifikát kořenové certifikační autority MERO Root CA – 20 let,
- Systémový certifikát vydávající certifikační autority MERO CA – 10 let,
- certifikát pro elektronický podpis – 2 roky,
- certifikát pro šifrování elektronické pošty – 2 roky,
- certifikát pro šifrování datových úložišť pro interní použití v MERO ČR, a. s. – 2 roky,
- certifikát pro šifrování datových úložišť pro externí použití – 2 roky,
- certifikát pro elektronický podpis pro externí subjekt – 2 roky,
- certifikát pro šifrování elektronické pošty pro externí subjekt – 2 roky,
- certifikát pro autentizaci technických zařízení – 3 roky.

## 8.4 Počítačová a síťová bezpečnost

### Počítačová bezpečnost

Operační systém serveru vydávající kořenové certifikační autority MERO CA je v pravidelných intervalech aktualizován dle zásad definovaných příslušné interní politiky MERO ČR, a. s.

Na operační systém serveru kořenové certifikační autority MERO Root CA nejsou kladeny žádné nároky na jeho aktualizace (server kořenové autority je odpojený z počítačové sítě a standardně vypnutý).

### Síťová bezpečnost

Požadavky na síťovou bezpečnost serverů v rámci PKI hierarchie MERO ČR, a. s. jsou definovány v dokumentu Systémová bezpečnostní politika.

### Antivirová ochrana

Systém vydávající certifikační autority MERO CA je chráněn pravidelně aktualizovaným antivirovým software podle příslušné interní směrnice.

Na server kořenové certifikační autority MERO Root CA nejsou kladeny žádné nároky na antivirový systém (server kořenové autority je odpojený z počítačové sítě a standardně vypnutý).

### Používání vyměnitelných médií

Všechna vyměnitelná média musí být před použitím zkontrolována aktualizovaným antivirovým systémem nebo zformátována.

## 9 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

### 9.1 Profil certifikátu

Certifikační autorita MERO CA vydává certifikáty podle standardu X.509 verze 3. Profily vydávaných certifikátů jsou uvedeny v Příloze A v kapitole 0 této certifikační politiky.

#### 9.1.1 Číslo verze

Certifikační autority v rámci PKI infrastruktury MERO ČR, a. s. vydávají certifikáty podle standardu X.509 verze 3.

#### 9.1.2 Rozšiřující položky v certifikátu

Rozšiřující položky použité ve vydávaných certifikátech jsou uvedeny v Příloze A v kapitole **Chyba! Nenalezen zdroj odkazů.** této certifikační politiky.

#### 9.1.3 Objektové identifikátory (dále „OID“) algoritmů

Algoritmům používaným v MERO CA nejsou přiřazeny OID. V hierarchii certifikačních autorit provozovaných MERO ČR, a. s., se používají pouze obecně známé algoritmy.

#### 9.1.4 Způsoby zápisu jmen a názvů

Pravidla pro zápis jmen a názvů jsou uvedena v kapitole 5.1.

#### 9.1.5 Omezení jmen a názvů

Jména a názvy uvedené v certifikátu musí přesně odpovídat údajům v doméně (v případě certifikátu vydaného internímu zaměstnanci nebo certifikátu pro autentizaci technických zařízení) nebo údajům získaných od pověřené osoby obchodního partnera (v případě certifikátu vydaného zaměstnanci obchodního partnera).

#### 9.1.6 OID certifikační politiky

V každém certifikátu vydaném certifikační autoritou v rámci PKI hierarchie MERO ČR, a. s. je uveden odkaz na certifikační politiku, podle které byl certifikát vydán (OID politiky).

### 9.1.7 Rozšiřující položka „Policy Constraints“

V certifikátech vydaných certifikační autoritou MERO CA se rozšiřující položka „Policy Constraints“ nepoužívá.

### 9.1.8 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Způsob zápisu rozšiřující položky „Certificate Policies“ je uveden v kapitole **Chyba! Nenalezen zdroj odkazů.**

## 9.2 Profil seznamu zneplatněných certifikátů

### 9.2.1 Číslo verze

Certifikační autority v rámci PKI infrastruktury MERO ČR, a. s. vydávají seznamy zneplatněných certifikátů podle standardu X.509 verze 2.

### 9.2.2 Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v CRL

Profily zneplatněných certifikátů jsou uvedeny v Příloze A v kapitole **Chyba! Nenalezen zdroj odkazů.** této certifikační politiky.

## 10 Hodnocení shody a jiná hodnocení

### 10.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

V prostředí MERO ČR, a. s. jsou oddělením interního auditu pravidelně prováděny kontroly zabezpečení provozovaných ICT systémů. Součástí těchto kontrol je i kontrola souladu poskytování certifikačních služeb s interní bezpečnostní dokumentací PKI (certifikační politika, certifikační prováděcí směrnice, systémová bezpečnostní politika).

Bezpečnostní události související s provozem certifikačních autorit MERO ČR, a. s. jsou pravidelně vyhodnocovány Auditorem CA, což je osoba nezávislá na provozu a správě certifikační autority.

### 10.2 Identita a kvalifikace hodnotitele

Interní kontrolu provádějí pracovníci znalí problematiky PKI. Externím auditorem smí být pouze osoba nebo společnost znalá problematiky implementace PKI s dostatečnou zkušeností v této oblasti.

### 10.3 Vztah hodnotitele k hodnocenému subjektu

Interní kontrolu provádí zaměstnanci MERO ČR, a. s.

Externí kontrolu smí provádět pouze osoba nebo společnost nezávislá na MERO ČR, a. s.

### 10.4 Hodnocené oblasti

Oblasti hodnocené v rámci pravidelných interních i externích kontrol jsou specifikovány v Certifikační prováděcí směrnici.

### 10.5 Postup v případě zjištění nedostatků

Výsledky interních i externích kontrol jsou předávány Manažerovi CA, který zajistí nápravu zjištěných nedostatků.

### 10.6 Sdělování výsledků hodnocení

O provedení každé interní či externí kontroly je vypracována písemná zpráva, která je předána Manažerovi CA. Ten zajistí její distribuci a projednání.

V případě, kdy je součástí zprávy samostatný výrok auditora, může Manažer CA rozhodnout o jeho zveřejnění.

## 11 Ostatní obchodní a právní záležitosti

### 11.1 Poplatky

Certifikační služby poskytované certifikačními autoritami MERO Root CA i MERO CA jsou poskytovány bezplatně.

### 11.2 Ochrana osobních údajů

MERO ČR, a. s., zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy v této certifikační politice a v certifikační prováděcí směrnici a vycházejí z příslušných ustanovení zákona č. 101/2000 Sb. o ochraně osobních údajů ve znění pozdějších předpisů.

### 11.3 Omezení odpovědnosti

MERO ČR, a. s. neodpovídá za škodu způsobenou z použití certifikátu, pokud došlo ze strany držitele nebo spoléhající se osoby k nedodržení přípustného použití certifikátu uvedeného v kapitole 4.2.1 této certifikační politiky.

MERO ČR, a. s. neodpovídá za škodu vyplývající z použití certifikátu v období po přijetí žádosti o jeho zneplatnění, pokud MERO ČR, a. s. dodrží lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL), uvedenou v kapitole 0 této certifikační politiky.

Ustanovení tohoto článku zůstávají v platnosti i po ukončení platnosti této certifikační politiky.

### 11.4 Doba platnosti, ukončení platnosti

#### 11.4.1 Doba platnosti

Doba platnosti této certifikační politiky je od data uvedeného v kapitole **Chyba! Nenalezen zdroj odkazů.** do odvolání.

#### 11.4.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě

- jeho nahrazení novější verzí, nebo
- ukončení poskytování certifikačních služeb v MERO ČR, a. s.

#### 11.4.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu v důsledku ukončení poskytování certifikačních služeb zůstávají v platnosti omezení a ustanovení uvedená v kapitole 11, která se týkají obchodních a právních záležitostí.

### 11.5 Komunikace mezi zúčastněnými subjekty

#### 11.5.1 Komunikace s poskytovatelem certifikačních služeb

Veškeré informace, které chce poskytovatel certifikačních služeb sdělit zákazníkům, zveřejní na svých webových stránkách. Závažné informace, jako například podezření na kompromitaci klíče některé z certifikačních autorit hierarchie MERO ČR, a. s., sděluje poskytovatel certifikačních služeb opět na webových stránkách a současně upozorněním směřovaným na držitele certifikátů.

Držitel certifikátu – interní zaměstnanec MERO ČR, a. s. komunikuje s poskytovatelem certifikačních služeb osobně telefonicky nebo prostřednictvím informačního systému HeliosGreen, pořadače „Účty uživatelů“.

Držitel certifikátu – externí subjekt komunikuje s poskytovatelem certifikačních služeb prostřednictvím pověřené osoby.

## 11.6 Změny

Vydání nové certifikační politiky bude oznámeno na webových stránkách MERO ČR, a. s.

Interní zaměstnanci MERO ČR, a. s. budou rovněž informováni e-mailovou zprávou. Externí subjekty, které využívají certifikační služby MERO ČR, a. s., budou informováni příslušnou pověřenou osobou.

## 11.7 Řešení sporů

V případě vzniku sporu se držitel certifikátu obrátí na Manažera CA.

## 11.8 Další ustanovení

## 11.9 Vyšší moc

MERO ČR, a. s., nenese odpovědnost za porušení svých povinností způsobené zásahy vyšší moci, jako jsou například přírodní katastrofy velkého rozsahu, stávkový, občanský nepokoje nebo válečný stav.

## 11.10 Další opatření

## 11.11 Související dokumenty

Při tvorbě certifikačních politik a certifikační prováděcí směrnice bylo zejména přihlíženo k následujícím dokumentům:

- Zákon č. 227/2000 Sb. o elektronickém podpisu v platném znění,
- Zákon č. 101/2000 Sb. o ochraně osobních údajů v aktuálním znění,
- CWA 14167-1:2003: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- ČSN ISO/IEC 27001:2006 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky,
- RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

## 12 Závěrečná ustanovení

Tato směrnice je majetkem MERO ČR, a. s., a její předávání třetím osobám není bez předchozího souhlasu představitele vedení pro ISŘ MERO ČR, a. s., povoleno.

## 13 Seznam příloh

Příloha č. 1 – Profily certifikátů

Příloha č. 2 – Rozšiřující položky v certifikátu

Příloha č. 3 – Profily zneplatněných certifikátů

Příloha č. 4 - Rozdělovník

## Příloha č. 1 – Profily certifikátů

Následující tabulka obsahuje profily certifikátů, které jsou vydávány v rámci PKI hierarchie MERO ČR, a. s.

Název položky	Certifikát kořenové certifikační autority	Certifikát podřízené certifikační autority	Certifikát pro elektronický podpis, elektronický podpis pro externí subjekt	Certifikát pro šifrování elektronické pošty, šifrování elektronické pošty pro externí subjekt	Certifikát pro šifrování datových úložišť pro interní použití	Certifikát pro šifrování datových úložišť pro externí subjekt	Certifikát pro autentizaci technických zařízení
<b>Version</b>	3	3	3	3	3	3	3
<b>Serial number</b>	Kořenová certifikační autorita přiřazuje každému vydanému certifikátu sériové číslo	Kořenová certifikační autorita přiřazuje každému vydanému certifikátu sériové číslo	Sériové číslo certifikátu přidělené vydávající certifikační autoritou	Sériové číslo certifikátu přidělené vydávající certifikační autoritou	Sériové číslo certifikátu přidělené vydávající certifikační autoritou	Sériové číslo certifikátu přidělené vydávající certifikační autoritou	Sériové číslo certifikátu přidělené vydávající certifikační autoritou
<b>Signature Algorithm</b>	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption
<b>Issuer</b>							
<b>Country</b>	CZ	CZ	CZ	CZ	CZ	CZ	CZ
<b>Organization</b>	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.
<b>CN</b>	MERO Root CA	MERO Root CA	MERO CA	MERO CA	MERO CA	MERO CA	MERO CA
<b>Validity</b>							
<b>Not before</b>	Datum vydání certifikátu	Datum vydání certifikátu	Datum vydání certifikátu	Datum vydání certifikátu	Datum vydání certifikátu	Datum vydání certifikátu	Datum vydání certifikátu
<b>Not after</b>	20 let od data vydání	10 let od data vydání	2 roky od data vydání	2 roky od data vydání	2 roky od data vydání	2 roky od data vydání	3 roky od data vydání
<b>Subject</b>							
<b>Country</b>	CZ	CZ	CZ	CZ	CZ	CZ	CZ
<b>Organization</b>	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.	MERO ČR, a. s.
<b>CN</b>	MERO Root CA	MERO CA	Jméno žadatele o certifikát.	Jméno žadatele o certifikát.	Jméno žadatele o certifikát.	Jméno externího subjektu	Identifikátor technického zařízení
<b>Subject Public Key Info</b>							
<b>Algorithm</b>	RsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption	rsaEncryption
<b>SubjectPublicKey</b>	Veřejný klíč kořenové CA o velikosti 4096 bitů	Veřejný klíč podřízené CA o velikosti 2048 bitů	Veřejný klíč certifikátu o velikosti 2048 bitů	Veřejný klíč certifikátu o velikosti 2048 bitů	Veřejný klíč certifikátu o velikosti 2048 bitů	Veřejný klíč certifikátu o velikosti 2048 bitů	Veřejný klíč certifikátu o velikosti 2048 bitů
<b>Extensions</b>	Rozšíření certifikátů dle tabulky níže	Rozšíření certifikátů dle tabulky níže	Rozšíření certifikátů dle tabulky níže	Rozšíření certifikátů dle tabulky níže	Rozšíření certifikátů dle tabulky níže	Rozšíření certifikátů dle tabulky níže	Rozšíření certifikátů dle tabulky níže
<b>Signature Algorithm</b>	Sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption	sha1WithRSAEncryption
<b>Signature Value</b>	Elektronický podpis certifikátu kořenovou certifikační autoritou	Elektronický podpis certifikátu kořenovou certifikační autoritou	Elektronický podpis certifikátu vydávající certifikační autoritou	Elektronický podpis certifikátu vydávající certifikační autoritou	Elektronický podpis certifikátu vydávající certifikační autoritou	Elektronický podpis certifikátu vydávající certifikační autoritou	Elektronický podpis certifikátu vydávající certifikační autoritou

## Příloha č. 2 – Rozšiřující položky v certifikátu

Následující tabulka obsahuje profily rozšiřujících položek certifikátů, které jsou vydávány v rámci PKI hierarchie MERO ČR, a. s.

Název rozšiřující položky	Kořenová certifikační autorita (MERO Root CA)	Podřízená certifikační autorita (MERO CA)	Elektronický podpis, elektronický podpis pro externí subjekt	Šifrování elektronické pošty, šifrování elektronické pošty pro externí subjekt	Šifrování datových úložišť pro interní potřeby	Šifrování datových úložišť pro externí subjekt	Autentizace technických zařízení
<b>Authority Key Identifier</b>							
<b>Key Identifier</b>	Jednoznačný identifikátor veřejného klíče nadřazené certifikační autority, tj. MERO Root CA.	Jednoznačný identifikátor veřejného klíče nadřazené certifikační autority, tj. MERO Root CA.	Jednoznačný identifikátor veřejného klíče vydávající certifikační autority. Jeho hodnota musí být stejná jako hodnota Subject Key Identifier v certifikátu vydávající certifikační autority.	Jednoznačný identifikátor veřejného klíče vydávající certifikační autority. Jeho hodnota musí být stejná jako hodnota Subject Key Identifier v certifikátu vydávající certifikační autority.	Jednoznačný identifikátor veřejného klíče vydávající certifikační autority. Jeho hodnota musí být stejná jako hodnota Subject Key Identifier v certifikátu vydávající certifikační autority.	Jednoznačný identifikátor veřejného klíče vydávající certifikační autority. Jeho hodnota musí být stejná jako hodnota Subject Key Identifier v certifikátu vydávající certifikační autority.	Jednoznačný identifikátor veřejného klíče vydávající certifikační autority. Jeho hodnota musí být stejná jako hodnota Subject Key Identifier v certifikátu vydávající certifikační autority.
<b>Authority Cert Issuer</b>	Stejně položky a hodnoty jako v položce Subject	Stejně položky a hodnoty jako v položce Subject certifikátu kořenové certifikační autority	Stejně položky a hodnoty jako v položce Subject certifikátu vydávající certifikační autority	Stejně položky a hodnoty jako v položce Subject certifikátu vydávající certifikační autority	Stejně položky a hodnoty jako v položce Subject certifikátu vydávající certifikační autority	Stejně položky a hodnoty jako v položce Subject certifikátu vydávající certifikační autority	Stejně položky a hodnoty jako v položce Subject certifikátu vydávající certifikační autority
<b>Authority CertSerial Number</b>	Stejná hodnota jako v položce Serial Number	Stejná hodnota jako v položce Serial Number certifikátu kořenové certifikační autority	Stejná hodnota jako v položce Serial Number certifikátu vydávající certifikační autority	Stejná hodnota jako v položce Serial Number certifikátu vydávající certifikační autority	Stejná hodnota jako v položce Serial Number certifikátu vydávající certifikační autority	Stejná hodnota jako v položce Serial Number certifikátu vydávající certifikační autority	Stejná hodnota jako v položce Serial Number certifikátu vydávající certifikační autority
<b>Subject Key Identifier</b>	Jednoznačný identifikátor veřejného klíče. Jeho hodnota musí být stejná jako hodnota Key Identifier v rozšíření Authority Key Identifier všech certifikátů vydaných kořenovou certifikační	Jednoznačný identifikátor veřejného klíče. Jeho hodnota musí být stejná jako hodnota Key Identifier v rozšíření Authority Key Identifier všech certifikátů vydaných touto certifikační autoritou.	Jednoznačný identifikátor veřejného klíče.	Jednoznačný identifikátor veřejného klíče.	Jednoznačný identifikátor veřejného klíče.	Jednoznačný identifikátor veřejného klíče.	Jednoznačný identifikátor veřejného klíče.

	autoritou.						
<b>Subject Alternative Name</b>			Emailová adresa žadatele o certifikát	Emailová adresa žadatele o certifikát	Emailová adresa žadatele o certifikát	Emailová adresa žadatele (externího subjektu) o certifikát	Označení technického zařízení
<b>Key Usage (kritické rozšíření)</b>	KeyCertSign CRLSign Off-line CRL Sign Digital Signature	KeyCertSign, CRLSign Off-line CRL Sign	DigitalSignature, NonRepudation, KeyEncipherment	KeyEncipherment	KeyEncipherment DataEncipherment	KeyEncipherment DataEncipherment	KeyEncipherment
<b>Extended Key Usage</b>			EmailProtection	EmailProtection	EFS	EFS	serverAuth
<b>CRL Distribution Points</b>							
<b>URI</b>	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/
<b>URI</b>	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
<b>Basic Constraints</b>							
<b>Ca</b>	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
<b>PathLenConstraint</b>	1	0	-	-	-	-	-

## Příloha č. 3 – Profily zneplatněných certifikátů

Následující tabulka obsahuje profily zneplatněných certifikátů, které jsou vydávány v rámci PKI hierarchie MERO ČR, a. s.

Název položky	CRL kořenové certifikační autority MERO Root CA	CRL podřízené certifikační autority MERO CA
Version	2	2
Signature Algorithm	sha256WithRSAEncryption	sha256WithRSAEncryption
Issuer		
Country	CZ	CZ
Organization	MERO ČR, a. s.	MERO ČR, a. s.
CN	MERO Root CA	MERO CA
This Update	Datum a čas vydání	Datum a čas vydání
Next Update	Datum a čas vydání + 365 dnů	Datum a čas vydání + 72 hodin
Revoked Certificates		
User Certificate	Sériové číslo zneplatněného certifikátu	Sériové číslo zneplatněného certifikátu
Revocation Date	Datum a čas zneplatnění certifikátu	Datum a čas zneplatnění certifikátu
CRL Entry Extensions	Rozšíření CRL dle tabulky níže	Rozšíření CRL dle tabulky níže
CRL Extensions	Rozšíření CRL dle tabulky níže	Rozšíření CRL dle tabulky níže
Signature Algorithm	Sha1WithRSAEncryption	Sha1WithRSAEncryption
Signature Value	Elektronický podpis vydávající autoritou	Elektronický podpis vydávající autoritou

**Příloha č. 4 - Rozdělovník**

Evid. číslo	Držitel	Status
0	Petra Klemptová	Správce dokumentace