

Certifikační politika

**Interní certifikační autorita PRE
Vydávající CA II**

Obsah

OBSAH	2
1 ÚVOD.....	3
1.1 ÚPOZORNĚNÍ PRO UŽIVATELE CERTIFIKÁTU	3
1.2 PŘEHLED	3
1.3 ZÚČASTNĚNÉ STRANY A OBLAST POUŽITÍ.....	4
1.4 OBLAST POUŽITÍ.....	5
1.5 SPRÁVA CERTIFIKAČNÍ POLITIKY	5
1.6 POUŽITÉ ZKRATKY A POJMY	5
2 ZVEŘEJŇOVÁNÍ A UCHOVÁVÁNÍ INFORMACÍ	6
2.1 ÚLOŽENÍ DAT, JEJICH SPRÁVA A ZÁSADY ZVEŘEJŇOVÁNÍ.....	6
2.2 ZVEŘEJŇOVÁNÍ CERTIFIKÁTŮ A CRL	6
2.3 ZVEŘEJŇOVÁNÍ INFORMACÍ O CERTIFIKAČNÍ AUTORITĚ	6
2.4 PERIODICITA ZVEŘEJŇOVÁNÍ.....	6
2.5 ŘÍZENÍ PŘÍSTUPU K INFORMACÍM.....	6
3 IDENTIFIKACE A AUTENTIZACE.....	7
3.1 REGISTRACE ŽÁDOSTI O CERTIFIKÁT	7
3.2 REGISTRACE ŽÁDOSTÍ O ZNEPLATNĚNÍ CERTIFIKÁTŮ	7
3.3 REGISTRACE ŽÁDOSTÍ O VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU	7
3.4 JEDNOZNAČNOST JMEN.....	7
3.5 ZNAKOVÁ SADA	7
4 PROVOZNÍ POŽADAVKY.....	8
4.1 ŽÁDOST O CERTIFIKÁT, VYDÁNÍ CERTIFIKÁTU A JEHO PŘEDÁNÍ	8
4.2 VYDÁNÍ NÁSLEDNÉHO CERTIFIKÁTU	8
4.3 ZNEPLATNĚNÍ CERTIFIKÁTU	8
4.4 INFORMACE O STAVU CERTIFIKÁTU	10
4.5 KONEC PLATNOSTI CERTIFIKÁTU	10
5 BEZPEČNOST FYZICKÁ, PROCEDURÁLNÍ A PERSONÁLNÍ	11
5.1 UKONČENÍ ČINNOSTI SUB CA.....	11
5.2 PODEZŘENÍ NA KOMPROMITACI SOUKROMÉHO KLÍČE SUB CA	11
6 TECHNICKÁ BEZPEČNOST	11
6.1 OCHRANA KLÍČŮ AUTORITY	11
6.2 OCHRANA KLÍČŮ DRŽITELŮ CERTIFIKÁTŮ	12
7 PROFILY CERTIFIKÁTŮ.....	12
7.1 CERTIFIKÁT CERTIFIKAČNÍ AUTORITY SUB CA	12
7.2 UŽIVATELSKÝ CERTIFIKÁT PRO EXTERNÍHO UŽIVATELE.....	13
8 KONTROLA PROVOZU.....	13
8.1 KONTROLA PROVOZU SUB CA	13
8.2 ZÁZNAM UDÁLOSTÍ	13
8.3 ARCHIVACE ZÁZNAMŮ	14
9 OBECNÉ ZÁSADY	14
9.1 POPLATKY ZA SLUŽBY	14
9.2 POVINNOSTI.....	14

1 Úvod

1.1 Upozornění pro uživatele certifikátu

Před použitím certifikátu vydaného podle této certifikační politiky pozorně pročtěte tento dokument a ujistěte se, že jste mu řádně porozuměli.

1.2 Přehled

Společnost Pražská energetika, a.s. (dále také PRE) ustanovila dvouúrovňovou hierarchii certifikačních autorit (dále PKI PRE) za účelem zabezpečení výměny dat a posílení autentizace uživatelů jak v rámci systémů PRE, tak i mimo tyto systémy. Kořenem hierarchie je kořenová certifikační autorita (dále Root CA), která vydala certifikát pro podřízenou vydávající certifikační autoritu (dále Sub CA), která vydává certifikáty koncovým subjektům – uživatelům nebo technickým komponentám.

Certifikační politiky popisují pravidla, podle kterých vydává podřízená certifikační autorita certifikáty uživatelů a technických komponent.

Vydávající certifikační autorita vydává následující typy uživatelských certifikátů:

- » uživatelské certifikáty pro zabezpečení emailu (šifrování a elektronický podpis),
- » uživatelské certifikáty pro autentizaci (např. do VPN spojení),
- » externí uživatelské certifikáty pro autentizaci k externě přístupným aplikacím (velkoodběratelé a dodavatelé),
- » certifikáty technických komponent – WWW serverů nebo aktivních prvků.

U podřízené certifikační autority jsou používány následující způsoby registrace:

- » registrace na zákaznickém registračním místě (obchodní místo – certifikáty externích uživatelů),
- » registrace na interním pracovišti centrální registrační autority (certifikáty komponent nebo autentizační certifikáty) nebo
- » registrace pomocí autoenrollmentu pro uživatele registrované v Active Directory (certifikáty pro zabezpečení emailu).
- » Certifikační autority provozované v rámci PKI PRE nevydávají kvalifikované certifikáty ve smyslu zákona 227/2000 Sb.

Tento dokument (tato certifikační politika) upravuje vydávání certifikátů pro koncové externí uživatele (zástupce dodavatelů a velkoodběratelů společnosti PRE).

1.2.1 Certifikační služby poskytované Sub CA

Sub CA nabízí tyto certifikační služby:

- » vydání certifikátu podle existujících certifikačních politik,
- » zneplatnění certifikátu, vydání CRL a jeho zveřejnění,
- » informace o službách poskytovatele certifikačních služeb.

1.2.2 Identifikace politiky

Identifikace politiky	Název politiky	Certifikační politika vydávající certifikační autority společnosti PRE pro koncového externího uživatele
	Verze politiky	1.0
	Stav	platná
	Datum vydání	1.8.2008
	Doba platnosti	do odvolání

1.3 Zúčastněné strany a oblast použití

1.3.1 Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb je společnost Pražská energetika, a.s. kontaktní údaje:

Pražská energetika, a. s.

IČO: 60193913

Na Hroudě 1492/4, Praha 10 - 100 05

Česká republika

S dotazy a požadavky spojenými s provozem PKI PRE, například připomínkami k provozu a nabízeným službám, je možné se obracet na obchodního zástupce PRE.

1.3.2 Kořenová certifikační autorita

Root CA tvoří kořen hierarchie certifikačních autorit PRE. Jejím úkolem je především vydávat a spravovat certifikáty certifikačních autorit působících v rámci PKI PRE.

1.3.3 Vydávající certifikační autorita Sub CA

Vydávající certifikační autorita je určena pro vydávání certifikátů zaměstnancům, zákazníkům a partnerům PRE, případně i technickým komponentám ve správě PRE (např. WWW serverům). Tato certifikační autorita vlastní certifikát vydaný kořenovou certifikační autoritou Root CA.

Hlavním úkolem Sub CA je vydávat a spravovat certifikáty koncových subjektů – uživatelů nebo technických komponent v souladu s definovanými certifikačními politikami.

1.3.4 Registrační autority

Žadatelé o certifikát, kteří chtějí vydat certifikát podle této politiky, musí požádat o vydání certifikátu obchodní místo, které zároveň plní i roli registrační autority.

Žadatelé o certifikát, kteří chtějí zneplatnit libovolný certifikát vydaný podle této politiky, kontaktují obchodní místo v roli registrační autority. Zde je provedeno ověření jejich identity, přijata žádost o zneplatnění certifikátu a požadavek zpracován.

1.3.5 Klienti podřízené certifikační autority

Klientem vydávající podřízené certifikační autority Sub CA je pro certifikáty vydané podle této certifikační politiky externí uživatel – smluvní partner PRE. Osoby žádající o certifikát (uživatelé) jsou v rámci této certifikační politiky označovány jako žadatelé o certifikát a po obdržení certifikátu i jako držitelé certifikátů.

1.4 Oblast použití

Certifikáty vydané podle této certifikační politiky mohou být použity pouze pro autentizaci klienta v rámci SSL spojení a pro výměnu šifrovacích klíčů pro toto spojení.

Všechny certifikáty vydané Sub CA jsou určeny pro použití v prostředí PRE nebo pro komunikaci mezi PRE a identifikovaným subjektem (smluvním partnerem). Certifikáty vydané Sub CA nejsou určeny pro širokou veřejnost.

1.5 Správa certifikační politiky

Za obsahovou správnost a další správu této certifikační politiky odpovídá manažer PKI.

Nové verze certifikační politiky vznikají podle potřeby zejména však:

- » při vzniku nového typu certifikátu,
- » při takové změně PKI PRE (např. změně postupů), která ovlivní obsah těchto dokumentů.

Platnost tohoto dokumentu není časově omezena, reálně je však ukončena dnem ukončení platnosti posledního certifikátu vydaného podle této certifikační politiky.

Tento dokument byl schválen manažerem PKI PRE.

1.5.1 Kontaktní informace

Správa certifikátů

Telefon: 267 053 181 (Hotline PRE)

E-mail: sprava_certifikatu@pre.cz

1.6 Použité zkratky a pojmy

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/nahrazení novým certifikátem. CRL je digitálně podepsán vystavitelem certifikátů – certifikační autoritou
Držitel certifikátu	uživatel soukromého klíče odpovídajícího veřejnému klíči uvedenému v certifikátu od okamžiku převzetí certifikátu (koncový subjekt)
PRE	společnost Pražská energetika, a. s.
Root CA	kořenová certifikační autorita nabízející své služby v rámci PKI PRE
Sub CA	vydávající certifikační autorita nabízející své služby v rámci PKI PRE a vydávající certifikáty koncovým subjektům
PKI PRE	Public Key Infrastructure PRE – souhrnné označení struktury certifikačních a registračních autorit vydávající certifikáty pro potřeby PRE. Službu zajišťuje pracovní skupina Správa certifikátů.
RA (registrační autorita)	pracoviště zabezpečující správu certifikátů (např. vydání a zneplatnění certifikátů)
Uživatel	zaměstnanec PRE nebo osoba, která je s PRE ve smluvním vztahu a využívá systémy nebo jiná ICT aktiva PRE
Žadatel	osoba, která má právo žádat u PKI PRE o certifikát podle některé z platných certifikačních politik

2 Zveřejňování a uchování informací

2.1 Uložení dat, jejich správa a zásady zveřejňování

Vydané certifikáty jsou uloženy v databázi certifikační autority.

Informace o vydaných certifikátech a seznamech zneplatněných certifikátů jsou poskytovány prostřednictvím WWW stránek autority a jsou tedy dostupné pouze v rámci interní sítě PRE.

Vně PRE, tedy z Internetu, jsou dostupné pouze informace o certifikační autoritě a stavu certifikátu – jsou dostupné certifikáty certifikačních autorit a seznamy zneplatněných certifikátů.

2.2 Zveřejňování certifikátů a CRL

Certifikáty vydané Sub CA jsou určeny pro zveřejnění pouze v systémech PRE, a proto nejsou vně PRE volně přístupné.

Certifikát certifikační autority je dostupný na adrese:

[http://pki.pre.cz/Interni CA - Vydavajici CA II.crt](http://pki.pre.cz/Interni_CA_-_Vydavajici_CA_II.crt)

CRL je přístupné na adrese:

[http://pki.pre.cz/Interni CA - Vydavajici CA II.crl](http://pki.pre.cz/Interni_CA_-_Vydavajici_CA_II.crl)

2.3 Zveřejňování informací o certifikační autoritě

Informace o Sub CA (včetně této certifikační politiky) jsou dostupné na adrese

<http://www.pre.cz/pre/technicka-pomoc/prace-s-certifikaty.html>

a na registračních autoritách (obchodním místech).

2.4 Periodicita zveřejňování

Certifikáty uživatelů jsou neprodleně po vydání dostupné ke stažení z interní sítě PRE.

Certifikáty uživatelů jsou žadatelům o certifikát předávány neprodleně po vydání včetně soukromého klíče.

Seznamy zneplatněných certifikátů (CRL) jsou generovány a zveřejňovány jednou za 10 dní. Platnost každého vydaného CRL je 14 dní.

Nové certifikační politiky a revize stávajících politik Sub CA jsou po schválení manažerem PKI a jejich vydání zveřejňovány na

<http://www.pre.cz/pre/technicka-pomoc/prace-s-certifikaty.html>

a na registračních autoritách (obchodních místech).

2.5 Řízení přístupu k informacím

Certifikační politiky, certifikáty certifikačních autorit, certifikáty vydané Sub CA a seznamy zneplatněných certifikátů jsou přístupné v rámci PRE pro čtení bez jakéhokoliv omezení.

Vně PRE je dostupný certifikát a aktuální seznam zneplatněných certifikátů autority Sub CA.

Modifikace zveřejněných údajů je povolena pouze autorizované obsluze a procesům certifikační autority.

3 Identifikace a autentizace

3.1 Registrace žádosti o certifikát

Registrace žádosti o vydání uživatelského certifikátu je součástí procesu zavedení externího uživatele do systému PKI.

Žadatel – pracovník nebo zástupce externího partnera musí být oprávněn jednat za externího partnera, který musí mít podepsaný dodatek smlouvy* a žádost o vydání certifikátu (podepsané oprávněnou osobou nebo pověřenou osobou).

Ověření oprávnění žadatele jednat za externího partnera je založeno na předchozím prokázání tohoto oprávnění obchodníkovi PRE.

3.2 Registrace žádostí o zneplatnění certifikátů

Žádost o zneplatnění certifikátu podává držitel certifikátu oprávněný jednat za externího partnera osobně, vzdáleně emailem nebo telefonicky.

Při podání žádosti o zneplatnění emailem musí být doména emailu, z něhož byla žádost odeslána, shodná s doménou emailu uvedeného v certifikátu, o jehož zneplatnění je žádáno. Při podání žádosti o zneplatnění telefonicky je identita žádajícího adekvátně ověřena operátorem CA. O zneplatnění certifikátu může požádat operátor CA v z důvodu viz bod. 4.3 Certifikát vydaný Sub CA PRE může být zneplatněn i z vůle provozovatele PRE. V takovém případě je oprávněným žadatelem o zneplatnění manažer PKI.

3.3 Registrace žádostí o vydání následného certifikátu

Před vypršením platnosti certifikátu je držitel certifikátu informován o končící platnosti stávajícího certifikátu a o potřebě žádat o nový certifikát (21 dní před koncem platnosti stávajícího certifikátu).

Podmínky pro registraci žádosti o vydání následného certifikátu jsou shodné s podmínkami pro vydání prvotního certifikátu.

3.4 Jednoznačnost jmen

U uživatelských certifikátů je jednoznačnost jmen zaručena kombinací údajů uvedených v certifikátu a zejména jednoznačností použitého emailu, za kterou odpovídá žadatel.

Jednomu subjektu může být vydáno více certifikátů se stejným jménem.

3.5 Znaková sada

V certifikátech vydávaných Sub CA jsou podporovány pouze následující znakové sady:

US ASCII (PrintableString) a Unicode (UTF8String).

* Smlouva o sdružených službách dodávky elektřiny / Smlouva o dodávce elektřiny / Smlouva o poskytnutí distribuce

4 Provozní požadavky

4.1 Žádost o certifikát, vydání certifikátu a jeho předání

Generování klíčových párů a certifikátů zajišťuje osoba v roli operátor registrační autority (dále operátor RA) na obchodním místě. Operátor RA přistupuje na WWW rozhraní certifikační autority, přičemž se k tomuto rozhraní identifikuje a autentizuje.

Registrace žádosti o vydání certifikátu dávkovým zpracováním je podmíněna zavedením uživatele do systému PKI. Proces obsahuje následující kroky:

- » Oprávněný zástupce zákazníka (velkoobtěratele nebo dodavatele) se dostaví na příslušné obchodní místo.
- » Zástupce zákazníka předloží podepsaný dodatek smlouvy o elektronických komunikacích (podepsanou statutárním zástupcem) a žádost o vydání certifikátu (podepsanou statutární osobou nebo pověřenou osobou).
- » Zaměstnanec PRE odpovědný za komunikaci se zákazníkem (operátor RA) přistoupí na WWW rozhraní certifikační autority.
- » Operátor RA zavede resp. vyhledá zástupce zákazníka a zadá resp. upraví údaje se zástupcem zákazníka spojené.
- » Operátor RA vygeneruje v aplikaci klíčový pár, certifikát a vytvoří soubor PKCS12.
- » Operátor RA v aplikaci vytvoří a následně vytiskne protokol o vydání certifikátu, který spolu se zástupcem zákazníka podepíše.
- » Operátor RA v aplikaci vytvoří a následně vytiskne heslo k PKCS12 souboru, které předá zástupci zákazníka.
- » Operátor RA předá PKCS12 soubor zástupci zákazníka.
- » Operátor RA uloží podepsaný protokol do složky zákazníka.

4.2 Vydání následného certifikátu

Vydání následného certifikátu probíhá stejně jako vydání prvotního certifikátu bez nutnosti předkládání dodatku ke smlouvě a papírové žádosti o vydání certifikátu.

4.3 Zneplatnění certifikátu

4.3.1 Důvody zneplatnění certifikátu

Držitel certifikátu je zejména v případě podezření na odcizení resp. prozrazení soukromého klíče, který je svázán s certifikátem vydaným Sub CA, povinen požádat o zneplatnění tohoto certifikátu. Důvody pro zneplatnění certifikátu vydávající CA jsou především následující:

- » jakékoliv podezření na kompromitaci příslušného soukromého klíče,
- » změna důležitých údajů uvedených v certifikátu,
- » ukončení používání certifikátu (a soukromého klíče).

O zneplatnění certifikátu vydaného Sub CA z vůle provozovatele Sub CA může dále žádat příslušný operátor, který certifikát vydal, obchodní zástupce PRE a operátor PKI, zejména v případě, kdy držitel certifikátu neplní povinnosti dané touto certifikační politikou nebo používání certifikátu není v souladu s potřebami a cíli PRE.

4.3.2 Zneplatnění certifikátu osobní návštěvou

Zneplatnění certifikátů emailem je prováděno v následujících krocích:

- 1) Žadatel (typicky držitel certifikátu) se dostaví na obchodní místo (registrační autoritu) a požádá o zneplatnění certifikátu, přičemž sdělí:
 - » sériové číslo nebo Subjekt certifikátu, který chce zneplatnit,
 - » důvod pro zneplatnění a
 - » identifikaci držitele certifikátu a případně i identifikaci obchodního partnera.Operátor RA ověří identitu a právo držitele žádat o zneplatnění certifikátů.
- 2) Po ověření práva žadatele žádat o zneplatnění nahlášeného certifikátů operátor RA zašle údaje potřebné k zneplatnění centrálnímu operátorovi RA prostřednictvím hotline PRE.
- 3) Centrální operátor RA provede zneplatnění certifikátu a informuje žádajícího operátora RA
- 4) Žadatel o zneplatnění certifikátu od operátora RA dostane emailem nebo telefonicky potvrzení o zneplatnění certifikátu.

4.3.3 Zneplatnění certifikátu emailem

Zneplatnění certifikátů emailem je prováděno v následujících krocích:

- 1) Žadatel (typicky držitel certifikátu) vytvoří emailovou zprávu, kterou zašle na emailovou adresu přiděleného obchodníka (operátora RA), ve které požádá o zneplatnění. Zpráva bude obsahovat:
 - » sériové číslo nebo Subjekt certifikátu, který chce zneplatnit, a
 - » důvod pro zneplatnění a
 - » identifikaci držitele certifikátu a případně i identifikaci obchodního partnera.

Zpráva musí přijít z domény shodné s doménou emailu uvedeného v certifikátu.

- 2) Operátor RA ověří identitu a právo držitele žádat o zneplatnění certifikátů -
 - » žadatel zná identifikaci držitele certifikátu a identifikaci obchodního partnera,
 - » žadatel zná sériové číslo nebo Subjekt certifikátu, který chce zneplatnit,
- 3) operátor RA zašle emailovou zprávu na emailovou adresu uvedenou v certifikátu žádost o potvrzení žádosti o zneplatnění a počká na odpověď.
- 4) Po ověření práva žadatele žádat o zneplatnění nahlášeného certifikátů operátor RA zašle údaje potřebné k zneplatnění centrálnímu operátorovi RA elektronicky podepsaným emailem.
- 5) Centrální operátor RA provede zneplatnění certifikátu a informuje žádajícího operátora RA
- 6) Žadatel o zneplatnění certifikátu od operátora RA dostane emailem potvrzení o zneplatnění certifikátu.

4.3.4 Zneplatnění certifikátu vzdáleně telefonicky

Zneplatnění certifikátů telefonicky je prováděno v následujících krocích:

- 1) Žadatel (typicky držitel certifikátu) zavolá na telefonní číslo u přiděleného obchodníka (operátora RA) a požádá o zneplatnění certifikátu.
- 2) Operátor RA provede zpětné volání na telefon držitele podle seznamu partnerů, kterým ověří identitu držitele. Poté operátor RA požádá žadatele o sdělení:

- » sériového čísla nebo části Subjektu certifikátu, který chce držitel zneplatnit,
 - » důvodu pro zneplatnění,
 - » identifikaci držitele certifikátu a případně i identifikaci obchodního partnera a
 - » kontaktního telefonu.
- 3) Operátor RA ověří právo žádat o zneplatnění certifikátů -
- » žadatel zná identifikaci držitele certifikátu a identifikaci obchodního partnera,
 - » žadatel zná sériové číslo nebo Subjekt certifikátu, který chce zneplatnit,
 - » žadatel byl zastížen na telefonním čísle v rámci zpětného volání.
- 4) Po ověření práva žadatele žádat o zneplatnění nahlášeného certifikátů operátor RA zašle údaje potřebné k zneplatnění centrálnímu operátorovi RA elektronicky podepsaným emailem.
- 5) Centrální operátor RA provede zneplatnění certifikátu a informuje žádajícího operátora RA.
- 6) Žadatel o zneplatnění certifikátu od operátora RA dostane telefonicky potvrzení o zneplatnění certifikátu.

4.3.5 Zneplatnění certifikátu z vůle provozovatele Sub CA (PRE)

- 1) Zneplatnění uživatelského certifikátu zástupcem PRE se skládá z následujících kroků:
- 2) Manažer PKI zašle údaje potřebné k zneplatnění centrálnímu operátorovi RA elektronicky podepsaným emailem.
- 3) Centrální operátor RA provede zneplatnění certifikátu a informuje manažera PKI.
- 4) Manažer PKI informuje držitele certifikátu o zneplatnění certifikátu z vůle provozovatele PRE včetně důvodu pro zneplatnění.

4.3.6 Časová prodleva od přijetí žádosti o zneplatnění

Doba od přijetí žádosti o zneplatnění certifikátu a ověření práva žádat o zneplatnění do zveřejnění CRL obsahujícího i zneplatněný certifikát nepřesáhne 2 pracovní dny.

4.4 Informace o stavu certifikátu

Seznam zneplatněných certifikátů (CRL) je zveřejňován na adresách

[http://pki.pre.cz/Interni CA - Vydavajici CA II.crl](http://pki.pre.cz/Interni_CA_-_Vydavajici_CA_II.crl)

CRL je vydáváno jednou za 10 dní s přesahem platnosti 4 dni.

Sub CA neposkytuje informace o stavu certifikátu protokolem OCSP.

4.5 Konec platnosti certifikátu

Platnost certifikátu je ukončena v okamžiku jeho zneplatnění.

Pokud není certifikát po dobu jeho platnosti nutné zneplatnit, skončí jeho platnost v časovém okamžiku uvedeném v certifikátu.

5 Bezpečnost fyzická, procedurální a personální

Fyzická, procedurální a personální bezpečnost Sub CA se řídí platnými předpisy PRE.

5.1 Ukončení činnosti Sub CA

V případě ukončení činnosti Sub CA (například z důvodu nepotřebnosti služeb této certifikační autority) oznámí PRE tuto skutečnost všem držitelům platných certifikátů a kořenové certifikační autoritě nejméně jeden měsíc před ukončením činnosti.

Při vlastním procesu ukončení činnosti budou zneplatněny všechny platné certifikáty a bude vydáno CRL s délkou platnosti delší než je konec platnosti všech vydaných certifikátů. Toto CRL bude zveřejněno běžným způsobem. Následně bude zneplatněn certifikát Sub CA a příslušné CRL bude umístěno na obvyklé místo u kořenové certifikační autority Root CA (kde bude vystaveno minimálně po dobu předpokládané platnosti všech vydaných certifikátů). Po zneplatnění certifikátu Sub CA bude vymazán soukromý klíč certifikační autority a zničeny všechny jeho zálohy.

5.2 Podezření na kompromitaci soukromého klíče Sub CA

V případě podezření na kompromitaci soukromého klíče Sub CA budou emailem informováni všichni držitelé certifikátů o mimořádném ukončení činnosti této autority. Součástí oznámení bude i důvod ukončení platnosti certifikátu této certifikační autority.

Administrátor Sub CA ihned informuje kořenovou certifikační autoritu Root CA a požádá jí o zneplatnění certifikátu Sub CA. Po zneplatnění certifikátu Sub CA bude vymazán soukromý klíč certifikační autority a zničeny všechny jeho zálohy.

Po zveřejnění informace o mimořádném ukončení činnosti končí platnost všech certifikátů vydaných Sub CA.

6 Technická bezpečnost

PRE věnuje náležitou péči ochraně párových dat certifikační autority.

6.1 Ochrana klíčů autority

Soukromý klíč certifikační autority je generován a uložen v softwarovém kryptografickém modulu a je chráněn prostředky hostitelského operačního systému Sub CA (minimálně mechanizmy kontroly přístupu vztahující se k identifikovanému a autentizovanému subjektu).

Délka klíče pro algoritmus RSA je 2048 bitů.

Záloha soukromého klíče je uložena v zašifrovaném tvaru. Přístup k záloze soukromého klíče je možný pouze po zadání správného hesla. V případě, kdy toto není technicky možné, musí být taková záloha uložena na médiu uloženém v zapečetěné obálce v úschovném objektu s omezeným přístupem osob.

Přístup k záloze soukromého klíče je možný po schválení manažera PKI a nebo při obnově Sub CA po havárii.

6.2 Ochrana klíčů držitelů certifikátů

Soukromé klíče držitelů certifikátů musí být založené na algoritmu RSA o minimální délce modulu 1024 bitů.

Přístup k uloženému soukromému klíči musí být minimálně chráněn mechanismy kontroly přístupu vztahující se k identifikovanému a autentizovanému subjektu.

Žadatelé nebo držitelé certifikátů s přístupem k soukromým klíčům mají právo vytvářet zálohy (pokud je to technicky možné) pouze pro svou osobní potřebu. Přístup k zálohám musí být možný pouze po zadání hesla.

7 Profily certifikátů

7.1 Certifikát certifikační autority Sub CA

Basic Certificate Fields	
Version	v3
Serial Number	<i>Jednoznačné sériové číslo certifikátu</i>
Signature Algorithm	sha1RSA
Issuer	C=CZ, O=Pražska energetika a.s., CN= Interni CA - Root CA II
Valid From	27. 6. 2008
Valid To	27. 6. 2014
Subject	C=CZ, O= O=Pražska energetika a.s., CN=Interni CA - Vydavajici CA II
Public Key	rsaEncryption (2048 bit)
Critical Extensions	
Basic Constraints	Subject Type = CA, Path Length Constraint = None
Certificate Extensions	
Subject Key Identifier	<i>používá se</i>
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
MS Certificate Services CA Version	<i>používá se</i>
MS Certificate Type Extension	SubCA
Authority Key Identifier	<i>používá se</i>
CRL Distribution Points	URL=http://pki.pre.cz/Interni%20CA%20-%20Root%20CA%20II.crt
Authority Info Access caIssuers	URL=http://pki.pre.cz/Interni%20CA%20-%20Root%20CA%20II.crt

7.2 Uživatelský certifikát pro externího uživatele

Basic Certificate Fields	
Version	v3
Serial Number	<i>Jednoznačné sériové číslo certifikátu</i>
Signature Algorithm	sha1RSA
Issuer	C=CZ, O= O=Prazska energetika a.s., CN=Interni CA - Vydavajici CA II
Valid From	<i>datum a čas vydání certifikátu</i>
Valid To	<i>datum a čas vydání + 2 roky</i>
Subject	E = <i>email uživatele</i> CN = <i>jméno a příjmení uživatele</i> OU = <i>název společnosti</i> O = <i>IČO společnosti</i> L = <i>typ certifikátu (ECAV – pro odběratele/ECAD – pro dodavatele)</i> C = CZ
Public Key	RSA (1024 Bits)
Critical Extensions	
Basic Constraints	Subject Type = NON-CA
Certificate Extensions	
Subject Key Identifier	<i>používá se</i>
Authority Key Identifier	ID klíče=27 d7 60 60 c5 14 01 3b 59 19 e8 52 09 3c e7 9f e4 3a ed e3
CRL Distribution Points	URL=http://pki.pre.cz/Interni%20CA%20-%20Vydavajici%20CA%20II.crl
Key Usage	Digitální podpis, Zakódování klíče (a0)
MS Certificate Template	PRE External User

8 Kontrola provozu

8.1 Kontrola provozu Sub CA

Kontrola provozu podřízené certifikační autority je prováděna v rámci obecných kontrol provozu IT služeb v PRE.

Nálezy z kontroly jsou zaznamenány do provozního deníku Sub CA.

V rámci následné revize musí příslušná osoba zkontrolovat a zhodnotit odstranění nálezů předchozí kontroly.

8.2 Záznam událostí

Součástí provozu Sub CA je ukládání záznamů o důležitých událostech spojených se správou certifikátů koncových uživatelů a nebo provozem či správou systémů Sub CA.

8.3 Archivace záznamů

Záznamy o vydávání certifikátů jsou archivovány po dobu uvedenou v certifikační prováděcí směrnici, minimálně však dobu 1 roku po ukončení životnosti certifikační autority Sub CA.

8.3.1 Typy uchovávaných archivních záznamů

O činnosti Sub CA jsou archivovány zejména následující záznamy:

- » záznamy o vydání nebo zneplatnění certifikátu,
- » záznamy o jmenování osob do rolí (administrátor Sub CA, operátor RA, operátor obnovy klíče) a o rušení jejich jmenování,
- » provozní deníky,
- » logy OS a procesu CA,
- » veškeré programové vybavení, vydané certifikáty a CRL a
- » zprávy o provedení kontrol.

9 Obecné zásady

9.1 Poplatky za služby

Služby certifikační autority jsou poskytovány bezplatně.

9.2 Povinnosti

9.2.1 Povinnosti provozovatele Sub CA

Provozovatel certifikačních služeb je povinen:

- » věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb (náležitá péče zahrnuje provoz v souladu s platnými právními předpisy, s touto certifikační politikou, interními předpisy společnosti PRE);
- » posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán, a o tomto rozhodnutí informovat žadatele;
- » vydat certifikát vyhovující standardu X.509 a splňující požadavky žadatele a této politiky;
- » informovat žadatele o tom, že mu byl vydán certifikát a předat mu vydaný certifikát;
- » zneplatnit certifikát podle pravidel popsanych v certifikační politice;
- » informovat držitele certifikátu o skutečnosti, že byl zneplatněn certifikát z vůle provozovatele Sub CA;
- » provést zneplatnění certifikátu v co nejkratší době po podání žádosti o zneplatnění certifikátu;
- » zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na www serveru poskytovatele certifikačních služeb;
- » prověřit podezření, že došlo k prozrazení soukromého klíče v rámci působnosti Sub CA, což by mohlo vést ke ztrátě důvěryhodnosti certifikační autority;
- » provádět kontrolu provozu Sub CA;

- » informovat držitele platných certifikátů o zneplatnění certifikátu Sub CA;
- » zveřejnit certifikát Sub CA tak, aby se každý mohl ujistit o jeho identitě.

9.2.2 Povinnosti žadatele

Žadatel resp. držitel certifikátu je povinen:

- » poskytovat pravdivé a úplné informace při procesu registrace žádosti o certifikát;
- » nakládat 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;
- » užívat soukromý klíč, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky a odpovídající certifikát pouze pro účely stanovené v certifikační politice;
- » neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, a požádat o zneplatnění certifikátu;
- » seznámit se s certifikační politikou, podle které mu byl vydán certifikát.

9.2.3 Povinnosti spoléhajících se stran a ostatních uživatelů

Uživatel certifikátu vydaného Sub CA musí zejména:

- » získat certifikát kořenové certifikační autority (Root CA) z bezpečného zdroje (www server poskytovatele certifikačních služeb) a ověřit otisk („fingerprint“) tohoto certifikátu;
- » ověřit platnost certifikátu Sub CA; kontrola se provádí na správnost podpisu kořenové autority a proti příslušnému aktuálnímu CRL;
- » ověřit platnost uživatelského certifikátu vydaného Sub CA (kontrola se provádí na správnost podpisu vydávající autority Sub CA a proti příslušnému aktuálnímu CRL);
- » dostatečně zvážit (zejména na základě znalosti příslušné certifikační politiky), zda je certifikát vydaný Sub CA podle této politiky vhodný pro účel, ke kterému jej chce použít.