SPRÁVA ZÁKLADNÍCH REGISTRŮ	POL008C-2013	
POLITIKA	SZR-498-14/Ř-2013	
	počet stran	37
	přílohy	0

Certifikační politika Správy základních registrů pro certifikáty vydávané pro AIS

Oblast působnosti:
zaměstnanci SZR, správci AIS

Gestor, podpis: Josef KNOTEK	**Nahrazuje:** POL008B-2013
Zpracovatel, podpis: Ota ZÁHORA	**Schvalovatel, podpis:** Ing. Michal PEŠEK
Odborný garant, podpis: -	**Schváleno dne:** 22. 01. 2019
Klasifikace: VEŘEJNÝ	**Účinnost od dne:** 01. 02. 2019

HISTORIE DOKUMENTU:

Verze	Datum	Autor	Popis
1.0	02. 04. 2012	SZR	Verze pro zahájení provozu základních registrů.
1.1	01. 08. 2012	SZR	Upřesněn proces odvolávání certifikátů.
A	01. 05. 2013	SZR	Povoleno použití certifikátů pro vzájemnou autentizaci AIS a ustavení šifrovaného spojení mezi AIS.
B	17. 08. 2015	SZR	Definice Validační autority. Povoleno využití certifikátů pro komunikaci se všemi systémy poskytujícími eGON služby. Specifikace podmínek, za kterých lze povolit přístup k soukromému klíči pro smluvní partnery držitelů certifikátů. Změny vyplývající ze Zákona o státní službě 234/2014 Sb. a ze Zákona o kybernetické bezpečnosti 181/2014 Sb.
C	17. 01. 2019	SZR	Celková revize a upřesnění dokumentu. Hlavní změny: používání aplikace pro RA SZR; změna podmínek, za jakých může mít AIS více certifikátů; upřesnění podmínek pro zneplatnění certifikátu; definice důvěryhodných rolí; změna profilu certifikátu (nový atribut SAN).

OBSAH

1. Úvod

Tato certifikační politika definuje podmínky pro vydávání certifikátů pro agendové informační systémy za účelem zabezpečení jejich komunikace s produkčním prostředím základních registrů České republiky, za účelem zabezpečení jejich komunikace s dalšími systémy, které poskytují eGON služby, a za účelem zabezpečení jejich vzájemné komunikace.

1.1 Název a jednoznačné určení dokumentu

Tento dokument má název:

CERTIFIKAČNÍ POLITIKA
SPRÁVY ZÁKLADNÍCH REGISTRŮ
PRO CERTIFIKÁTY VYDÁVANÉ PRO AIS

Zkratka názvu dokumentu je: CP CASZR AIS

OID dokumentu je: 1.2.203.72054506.2.10.1.4

1.2 Rozsah působnosti

Politika je závazná pro správce AIS a pro všechny zaměstnance SZR, kteří se podílejí na poskytování certifikačních služeb.

1.3 Zkratky a pojmy

Agendový informační systém (AIS) – informační systém podle § 2 písm. f zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

ASCII – American Standard Code for Information Interchange je znaková sada pro kódování znaků anglické abecedy v počítačích a jiných zařízeních.

CA – Certifikační autorita.

CA SZR – CA, která vydává certifikáty pro AIS ve smyslu § 5 odst. 3 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

Certifikační politika (CP) – množina pravidel, která definují podmínky pro vydávání určitých certifikátů certifikační autoritou a určují použitelnost certifikátů v rámci určité skupiny (domény) a/nebo v rámci třídy aplikací.

Certifikát veřejného klíče (certifikát) – je elektronický atest podepsaný certifikační autoritou, který spojuje veřejný klíč s určitou entitou a potvrzuje identitu této entity. Identifikace entity je uvedená v předmětu certifikátu.

CRL (Certificate Revocation List) – seznam sériových čísel zneplatněných certifikátů.

DN jméno – jméno, jehož tvar je definován normami řady X.500.

Držitel certifikátu – orgán veřejné moci nebo soukromoprávní uživatel údajů podle § 2 písm. c), d) a § 5 odst. 3, 4 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

eGON služba – služba, která poskytuje referenční údaje ze základních registrů, nebo zprostředkované údaje z jiných registrovaných AIS. Je publikovaná na vnějším rozhraní informačního systému základních registrů.

eGSB – eGON Service Bus.

Informační systém základních registrů (ISZR) – aplikace, která zprostředkovává přístup AIS k základním registrům.

Interní předpisy SZR – systémová bezpečnostní politika (Politika bezpečnosti informací SZR, Bezpečnostní politika ISMS, Politika ITSM), pracovní smlouvy, definice postupů a procesů.

IT – informační technologie.

JIP – jednotný identitní prostor základních registrů. Jde o adresář uživatelů.

Klíčový pár – párová data, tj. veřejný a soukromý klíč, které byly vytvořeny prostředky asymetrické kryptografie.

Kontrolní řád – zákon č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění zákona č. 183/2017 Sb.

Nařízení o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce – nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES.

Obecné nařízení o ochraně osobních údajů – nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

OCSP – Online Certificate Status Protocol je protokol pro online zjišťování platnosti certifikátu.

OID – Object Identifier je identifikace objektu v určitém prostoru jmen, zde je použitý pro jednoznačnou identifikaci dokumentů a kryptografických algoritmů.

Párová data – klíčový pár.

PKCS – Public Key Cryptography Standards.

PKI – Public Key Infrastructure, infrastruktura veřejného klíče je množina hardware, software, lidí a postupů vydávání, odvolávání a správy digitálních certifikátů založených na asymetrické kryptografii.

PKI SZR – Certifikační autorita SZR, Validační autorita SZR a Registrační autorita SZR určené pro vydávání a ověřování certifikátů pro zabezpečení komunikace AIS s produkčním prostředím ZR, pro zabezpečení komunikace AIS se systémy poskytujícími eGON služby a pro zabezpečení vzájemné komunikace mezi AIS.

Předmět certifikátu – jednoznačná identifikace entity, pro kterou byl certifikát vydaný. Identifikace je uvedená v atributu Subject vydaného certifikátu. V případě CA SZR je entitou AIS a identifikací entity označení AIS. Předmět certifikátu dále obsahuje označení správce AIS.

Registrační autorita (RA) – přijímá žádosti od uživatelů, ověřuje je, předává požadavky CA, přijímá výsledky od CA a distribuuje je žadatelům.

Služební zákon – zákon č. 234/2014 Sb., o státní službě, ve znění pozdějších předpisů.

Spoléhající se strana – je subjekt spoléhající se na certifikát vydaný CA SZR. V souladu s bodem 6 článku 3 nařízení o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce může být spoléhající se stranou pouze fyzická nebo právnická osoba, která se spoléhá na elektronickou identifikaci nebo službu vytvářející důvěru.

Správce AIS – subjekt, který je uveden v evidenci SZR, respektive v evidenci vedené mimo SZR orgánem státní správy, respektive pověřeným subjektem, jako správce příslušného AIS.

SZR – Správa základních registrů je správní úřad zřízený zákonem č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. SZR je podřízena Ministerstvu vnitra.

Validační autorita (VA) – poskytuje informace o platnosti certifikátů vydaných CA SZR.

Zaměstnanec – zaměstnanec SZR nebo osoba, která je vůči SZR v pracovněprávním či obdobném vztahu.

Zákoník práce – zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

Zákon o ochraně utajovaných informací – zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

ZR – základní registry, viz zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

1.4 Zúčastněné subjekty

1.4.1 Certifikační autority

Struktura CA provozovaných SZR je dvouúrovňová. Vrchol tvoří kořenová certifikační autorita SZR (Root CA SZR). Kořenová certifikační autorita vydává certifikáty pouze podřízeným certifikačním autoritám a vydala tedy i certifikát pro certifikační autoritu CA SZR, pro kterou je určena tato certifikační politika.

1.4.2 Registrační autorita

CA SZR poskytuje své služby správcům AIS prostřednictvím RA SZR.

RA SZR přijímá žádosti o vydání certifikátů, žádosti o zneplatnění certifikátů, ověřuje údaje požadované pro vydání a zneplatnění certifikátů a komunikuje s držiteli certifikátů.

RA SZR je provozována jako fyzický úřad zařazený do organizační struktury SZR.

Účast jiných registračních autorit se nepřipouští.

1.4.3 Validační autorita

CA SZR poskytuje služby ověřování platnosti certifikátů prostřednictvím VA SZR.

VA SZR poskytuje na vyžádání seznam odvolaných certifikátů (CRL).

1.4.4 Držitel certifikátu

Držitel certifikátu je správce AIS, kterému byl certifikát vydán na základě jeho žádosti. Správce AIS podáním žádosti o certifikát vyslovuje souhlas s touto certifikační politikou a s tím, že vydaný certifikát i jemu příslušející soukromý klíč bude používat v souladu s ní.

1.4.5 Spoléhající se strany

Spoléhající se strany jsou:

a) správci AIS;
b) správce ISZR;
c) správci dalších systémů, které poskytují eGON služby.

1.4.6 Jiné zúčastněné subjekty

RA SZR používá JIP k autentizaci a autorizaci žadatelů o certifikát a žadatelů o zneplatnění certifikátu.

1.5 Použití certifikátů

1.5.1 Přípustné použití certifikátů

ISZR může certifikáty používat pro identifikaci a autentizaci AIS a navazování šifrovaného spojení s nimi.

eGSB a další systémy, které poskytují eGON služby, mohou certifikáty používat pro identifikaci a autentizaci AIS a navazování šifrovaného spojení s nimi.

AIS mohou certifikáty používat pro identifikaci a autentizaci vůči jiným AIS a navazování šifrovaného spojení s nimi, pro identifikaci a autentizaci vůči ISZR a dalším systémům, které poskytují eGON služby, a navazování šifrovaného spojení s nimi.

Vzájemná autentizace AIS a navázání šifrovaného spojení mezi nimi s použitím certifikátů vydaných CA SZR je povolená, ale pro jejich skutečné použití vždy musí být zváženo, zda certifikáty vydané CA SZR pro AIS splňují požadavky důvěryhodnosti pro použití v konkrétní situaci.

1.5.2 Zakázané použití certifikátů

Certifikáty vydávané podle této CP nesmějí být používány k jinému účelu, než je uvedeno v kapitole 1.5.1.

Dalším omezením použití certifikátu je jeho nesprávné použití, například při operacích, kdy sice držitel má platný certifikát, ale AIS nemá právo jistou operaci uskutečnit.

1.6 Správa politiky

1.6.1 Organizace spravující certifikační politiku

Tuto certifikační politiku spravuje SZR.

1.6.2 Kontaktní osoby

Kontaktní osoby určuje vedoucí služebního úřadu SZR.

Aktuální kontaktní údaje jsou uvedeny na webových stránkách SZR http://www.szrcr.cz v sekci Kontakty.

Adresa pro komunikaci elektronickou poštou je podpora@szrcr.cz.

1.6.3 Odpovědná osoba

Osobou odpovědnou za tuto politiku a uplatňování jejích ustanovení je osoba určená vedoucím služebního úřadu SZR.

1.6.4 Postupy při schvalování

Osoba určená jako odpovědná za tuto CP je odpovědná za věcnou správnost jednotlivých ustanovení CP, za pravidelnou aktualizaci CP a za aktuálnost právě platné verze.

Nová verze certifikační politiky je před zveřejněním schválena vedoucím služebního úřadu SZR.

2. Odpovědnosti za zveřejňování a úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

Za úložiště informací a dokumentace PKI SZR odpovídá poskytovatel certifikačních služeb, tj. SZR.

SZR má neveřejné a veřejné úložiště informací a dokumentace.

2.2 Zveřejňování informací a dokumentace

Za zveřejňování informací a dokumentace o PKI SZR odpovídá SZR.

Veřejné informace, týkající se PKI SZR, včetně dokumentace musí být zveřejňovány pravidelně, správně a včas takovým způsobem, aby byla zajištěna jejich dostupnost jak všem uživatelům PKI SZR, tak i osobám, pro které jsou tyto informace důležité z hlediska spoléhání se na jejich pravdivost.

CA SZR zveřejňuje minimálně následující informace:

a) certifikační politiku v její aktuální verzi;
b) kontaktní místa RA SZR;
c) umístění VA SZR;
d) informace vztahující se k PKI SZR.

CA SZR zveřejňuje následující informace pro spoléhající se strany:

d) certifikát Root CA SZR a certifikát CA SZR;
e) seznam zneplatněných certifikátů (CRL) vydaných CA SZR.

Údaje jsou zveřejňovány buď přímo na webových stránkách SZR http://www.szrcr.cz, nebo je na těchto stránkách uveden odkaz na tyto údaje, nebo jsou distribuovány přímo uživatelům PKI SZR.

2.3 Periodicita zveřejňování informací

Certifikační politika je zveřejněna nejpozději v den, kdy vstoupí v platnost. Certifikáty jsou vydávány podle aktuálně platné verze CP.

Kontaktní místa RA SZR jsou zveřejněna při každé změně.

Umístění VA SZR je zveřejněno při každé změně.

Informace vztahující se k PKI SZR jsou uveřejňovány, když vstoupí v platnost nebo dříve.

Certifikáty certifikačních autorit jsou zveřejněny dříve, než je s jejich použitím vydán první certifikát.

Seznam zneplatněných certifikátů (CRL) je zveřejněn okamžitě po jeho vydání, a nejpozději před koncem platnosti posledního vydaného CRL.

2.4 Řízení přístupu k jednotlivým typům úložišť

Přístup k veřejným informacím týkajícím se PKI SZR poskytuje SZR bez omezení.

Přístup k neveřejným informacím týkajícím se PKI SZR je povolen pouze pro autorizované osoby.

3. Identifikace a autentizace

3.1 Pojmenování

3.1.1 Typy jmen

Všechny certifikáty vydávané CA SZR obsahují neprázdné označení předmětu certifikátu (Subject) a vydavatele certifikátu (Issuer) ve tvaru definovaném technickými standardy a normami.

3.1.2 Požadavky na významovost jmen

Význam položek certifikátů vydávaných CA SZR je definován v kapitole 7.

3.1.3 Anonymita držitele certifikátu a používání pseudonymů

Vydávání a používání anonymních certifikátů nebo používání pseudonymů se nepřipouští.

3.1.4 Pravidla pro interpretaci různých forem jmen

V certifikátech vydaných CA SZR lze používat pouze znaky ASCII, tj. není povoleno používání znaků s diakritickými znaménky.

Toto pravidlo se týká všech jmen, která poskytovatel certifikačních služeb umožňuje vložit do certifikátů, které vydává. Povolené tvary jmen jsou definovány v kapitole 7.

3.1.5 Jedinečnost jmen

V každém certifikátu vydaném CA SZR je v předmětu (Subject) uvedena identifikace AIS a identifikace správce AIS.

Za identifikaci AIS v žádostech o vydání certifikátu odpovídá žadatel o certifikát. RA i CA SZR považují všechny žádosti o vydání certifikátu pro AIS se stejnou identifikací AIS v předmětu certifikátu za žádosti pro tentýž AIS.

CA SZR zaručuje ve vydávaných certifikátech jedinečnost následujících jmen:

- označení vydavatele (Issuer) je jedinečné mezi všemi CA, které spravuje SZR;
- CA SZR nevydá certifikát se stejnou identifikací AIS dvěma různým žadatelům o certifikát.

CA SZR dále zaručuje, že nevydá dva certifikáty se stejným sériovým číslem.

3.1.6 Uznávání, ověřování a role ochranných známek

Certifikační politika nepředpokládá uvádění ochranných známek ve vydávaných certifikátech.

Pokud v některých položkách certifikátu žadatel o certifikát uvede ochrannou známku, je žadatel zodpovědný za její použití.

3.2 Počáteční ověření identity

3.2.1 Ověření vlastnictví soukromého klíče

Žádost o certifikát obsahuje veřejný klíč. Tato žádost je opatřena elektronickou pečetí, která byla vytvořena odpovídajícím soukromým klíčem. Tím je díky kryptografickému vztahu mezi veřejným a soukromým klíčem dokázáno, že žadatel vlastnil v okamžiku podpisu žádosti o certifikát obě části klíčového páru.

3.2.2 Ověřování identity žadatele

Aplikace RA SZR, která je určená pro příjem požadavků od žadatelů, používá k ověření identity žadatele JIP. Při ověřování identity fyzické osoby v JIP podle kap. 3.2.3 získá aplikace také informaci o identitě subjektu, ke kterému je fyzická osoba v JIP registrována.

V případě telefonicky nebo osobně podaného požadavku ověřují pracovníci RA SZR identitu žadatele podle interní evidence SZR.

3.2.3 Ověřování identity fyzické osoby

Aplikace RA SZR, která je určená pro příjem požadavků od žadatelů, používá k ověření identity fyzické osoby, která zastupuje žadatele, JIP. Tj. fyzická osoba se musí před podáním žádosti prostřednictvím aplikace identifikovat a autentizovat vůči JIP.

V případě telefonicky nebo osobně podaného požadavku na zneplatnění certifikátu ověřují pracovníci RA SZR identitu fyzické osoby, která zastupuje žadatele, podle osobní znalosti žadatele, nebo ověřují u osoby znalost hesla domluveného při vydání certifikátu, pokud bylo takové heslo domluveno.

3.2.4 Neověřované informace o držiteli certifikátu

RA ani CA SZR neověřuje následující položky, jejichž hodnoty jsou součástí vydávaných certifikátů:

a) existenci ani vlastnictví DNS jména domény, respektive serveru, uvedeného v atributu CN položky Subject, žadatelem;
b) existenci ani vlastnictví DNS jmen domén, respektive serverů, uvedených v Subject Alternative Name, žadatelem;
c) označení (jméno) žadatele;
d) adresu žadatele;
e) správnost označení země (státu), pokud je ale hodnota uvedena, kontroluje, že jde o povolený stát.

3.2.5 Ověřování specifických práv

SZR ověřuje, že žadatel je oprávněný k přístupu do základních registrů, viz kap. 4.1.1.

SZR ověřuje, že žadatel je správcem AIS, pro který žádá o přístup k základním registrům, a že tento AIS patří mezi informační systémy, které jsou oprávněny k přístupu do základních registrů, viz kap. 4.1.2.

3.2.6 Kritéria pro interoperabilitu

Spolupráce PKI SZR s jinými poskytovateli certifikačních služeb je možná až po schválení vedoucím služebního úřadu SZR.

3.3 Ověřování identity při požadavku na výměnu párových dat

3.3.1 Ověřování identity při požadavku na výměnu párových dat v době platnosti certifikátu

Při požadavku na změnu klíčového páru je třeba žádat o nový certifikát.

Identifikace a autentizace při vydávání druhého certifikátu a dalších certifikátů pro jeden AIS se provádí stejně jako při počátečním ověření identity způsobem popsaným v kapitole 3.2.

3.3.2 Ověřování identity při požadavku na výměnu párových dat po době platnosti certifikátu

Stejný postup jako v kap. 3.3.1.

3.4 Ověřování identity při požadavku na zneplatnění certifikátu

Identifikace a autentizace se provádí způsobem popsaným v kap. 3.2.2 a 3.2.3.

4. Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Požádat o certifikát může kterýkoli subjekt, který je podle platných a účinných právních předpisů oprávněný k přístupu do základních registrů a současně je správcem AIS, který je oprávněn k přístupu do základních registrů.

4.1.2 Registrační proces a odpovědnosti

RA SZR přebírá seznam subjektů oprávněných k přístupu do základních registrů a AIS (a jejich správců) oprávněných k přístupu do základních registrů z určených seznamů vedených orgány státní správy nebo vedenými z jejich pověření.

4.1.2.1 Uzavření smlouvy

SZR neuzavírá s žadateli o certifikáty žádné smlouvy o poskytování certifikačních služeb.

4.1.2.2 Odpovědnosti žadatele

a) Žadatel o certifikát je odpovědný za to, že splnil veškeré požadavky pro přístup do základních registrů.

b) Žadatel o certifikát je povinen se seznámit s touto certifikační politikou.

c) Žadatel o certifikát je povinen uvádět v žádostech o certifikát pravdivé údaje.

4.1.2.3 Odpovědnosti poskytovatele

a) Za ověření údajů poskytnutých žadatelem o certifikát je zodpovědná RA SZR.

b) CA SZR je povinna vydat certifikát, pokud je žádost o jeho vydání oprávněná a úplná a obsahuje správné údaje.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Žadatel o certifikát se identifikuje a autentizuje vůči RA SZR způsobem definovaným v kapitole 3.2.

4.2.2 Přijetí nebo zamítnutí žádosti

Žadatel podává žádost o certifikát zasláním vyplněného formuláře a žádosti ve formátu PKCS#10 prostřednictvím aplikace, kterou určila SZR.

RA SZR žádost o vydání certifikátu přijme a zaeviduje ji.

RA SZR zkontroluje údaje ve formuláři i v žádosti o certifikát. Pokud jsou údaje chybné nebo neúplné, RA SZR žádost o certifikát odmítne a pošle do datové schránky žadatele i do aplikace určené pro příjem žádostí o certifikáty informaci o důvodu odmítnutí žádosti.

Pokud jsou údaje úplné a správné, RA SZR předá žádost o certifikát na CA SZR.

4.2.3 Doba zpracování žádosti

Žádost o certifikát se zpracovává bez zbytečného odkladu, zpravidla do dvou pracovních dnů, maximálně do 30 kalendářních dnů.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

CA SZR provede následující činnosti:

a) zkontroluje obsah žádosti o certifikát z hlediska technických požadavků;
b) vydá certifikát, tj. vytvoří datovou strukturu certifikátu a opatří ji elektronickou pečetí vytvořenou soukromým klíčem CA SZR;
c) předá certifikát RA SZR.

Pokud některá z kontrol skončí negativně, CA SZR certifikát nevydá a tuto informaci předá RA SZR.

4.3.2 Oznámení o vydání certifikátu držiteli

Sdělení o vydání certifikátu zasílá RA SZR žadateli společně s certifikátem do jeho datové schránky a současně prostřednictvím aplikace, kterou určila SZR.

V případě nevydání certifikátu zasílá RA SZR žadateli informaci o důvodech nevydání do jeho datové schránky a současně prostřednictvím aplikace, kterou určila SZR.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Žadatel o certifikát zkontroluje obsah vydaného certifikátu a zejména se ujistí, že obsahuje údaje, které uvedl v příslušné žádosti o certifikát a že veřejný klíč v certifikátu je stejný jako veřejný klíč v žádosti o certifikát. Pokud zjistí odlišnosti, oznámí to bez zbytečného odkladu RA SZR. V opačném případě je žadatel povinen certifikát převzít.

Pokud žadatel certifikát nepřevezme, je o tom povinen bez zbytečného odkladu informovat RA SZR prostřednictvím aplikace, kterou určila SZR, nebo datovou schránkou.

Žadatel o certifikát se převzetím certifikátu stává držitelem certifikátu.

Žadatel nainstaluje certifikát do prostředí vlastní infrastruktury. Je povoleno nainstalovat certifikát na více serverů.

SZR doporučuje, aby žadatel provedl zálohu klíčového páru a certifikátu.

4.4.2 Zveřejňování vydaných certifikátů certifikační autoritou

CA SZR nezveřejňuje vydané certifikáty ani údaje o vydaných certifikátech.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

SZR neuveřejňuje žádné informace (mimo CRL) o certifikátech vydaných podle této CP.

4.5 Použití párových dat a certifikátů

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Držitel certifikátu smí klíčový pár a certifikát k veřejnému klíči používat pouze v souladu s touto CP a pouze pro ten AIS, pro který byl certifikát vydaný, a pouze po dobu, kdy je AIS v jeho správě. Nesmí soukromý klíč a k němu příslušející certifikát použít pro jiný AIS, i když jde o AIS v jeho správě.

Držitel certifikátu nesmí soukromý klíč poskytnout jinému subjektu s výjimkou subjektů, se kterými má smlouvu na zajištění provozu příslušného AIS. Smlouva musí obsahovat ustanovení o ochraně soukromého klíče, minimálně:

- Držitel certifikátu předává subjektu jednu kopii soukromého klíče a certifikátu odpovídajícího veřejného klíče. Tato kopie musí být chráněna heslem.
- Subjekt nepoužije soukromý klíč ani certifikát pro jiný účel než pro provoz příslušného AIS.
- Subjekt nainstaluje soukromý klíč a certifikát pouze na ta technická zařízení, která komunikují přímo s ISZR, nebo jiným systémem poskytujícím eGON služby, nebo s jiným AIS.
- Subjekt nebude vytvářet další kopie soukromého klíče (tj. mimo kopií uvedených v předcházejícím bodu).
- Soukromý klíč a certifikát budou na technických zařízeních uloženy tak, aby byla zabezpečena jejich důvěrnost maximálním způsobem, který dané technické zařízení a provoz AIS umožňují. To znamená, že přístup k soukromému klíči je chráněn technickými prostředky a je zablokována možnost exportu soukromého klíče ze zařízení.
- Uživatelské přístupy k soukromému klíči, případně k zařízením se soukromým klíčem a operace s ním jsou automaticky protokolovány technickými prostředky.
- Subjekt povolí přístup k soukromému klíči pouze nezbytnému okruhu osob a povede seznam osob, které mají k soukromému klíči přístup.
- Subjekt neprodleně nahlásí držiteli certifikátu zneužití soukromého klíče a podezření na zneužití soukromého klíče.

Jakákoli smluvní ustanovení nezbavují držitele certifikátu odpovědnosti za bezpečnost soukromého klíče.

Pokud se změní správce AIS, nesmí nový správce používat soukromý klíč ani certifikát vydaný pro původního správce, i když se jedná o stále stejný AIS. Pokud se mění správce AIS, je původní správce AIS povinen požádat o zneplatnění všech dosud platných certifikátů vydaných pro AIS.

Certifikát (a soukromý klíč) je tedy vázán na AIS a jeho správce.

Držitelé certifikátů mají dále za povinnost:

a) chránit a držet v utajení soukromý klíč;
b) v co nejkratší době uvědomit RA SZR o jakémkoli podezření z vyzrazení soukromého klíče;
c) dodržovat veškerá ustanovení, podmínky a omezení uložená touto certifikační politikou v souvislosti s užíváním soukromých klíčů a certifikátů;
d) podávat RA SZR přesné, pravdivé a úplné informace ve vztahu k vydanému certifikátu.

Držitelům certifikátů, kteří jsou usvědčeni z jednání, která jsou v rozporu s touto certifikační politikou a jejími nařízeními, může být jejich certifikát zneplatněn.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany mají za povinnost nakonfigurovat příslušné informační systémy tak, aby předtím, než použijí certifikát vydaný CA SZR pro AIS:

a) získaly certifikáty používané CA SZR a Root CA SZR při vydávání certifikátů z bezpečného zdroje a ověřily otisk těchto certifikátů;
b) ověřily platnost certifikátů CA SZR a Root CA SZR;
c) AIS navíc:
    - v případě komunikace s ISZR nebo jiným systémem poskytujícím eGON služby ověří platnost certifikátu vydaného CA SZR pro příslušný systém a ověří, že byl skutečně vydán pro příslušný systém;
    - v případě komunikace s jiným AIS ověří platnost certifikátu vydaného CA SZR pro jiný AIS a ověřil, že byl skutečně vydán pro příslušný AIS;
d) ISZR navíc:
    - ověří platnost certifikátu vydaného CA SZR pro AIS a že byl skutečně vydán pro příslušný AIS;
    - ověří, zda certifikát vydaný pro AIS nebyl dočasně zablokován, viz kapitolu 4.9.

4.6 Obnovení certifikátu

CA SZR neposkytuje službu obnovení certifikátu ve smyslu vydání nového certifikátu ke stejnému klíčovému páru a se stejnými parametry, jaké měl certifikát předchozí.

CA SZR neposkytuje službu obnovení certifikátu ve smyslu obnovení platnosti dříve zneplatněného (odvolaného) certifikátu.

4.6.1 Podmínky pro obnovení certifikátu

PKI SZR tuto službu neposkytuje.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

PKI SZR tuto službu neposkytuje.

4.6.3 Zpracování požadavku na obnovení certifikátu

PKI SZR tuto službu neposkytuje.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

PKI SZR tuto službu neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu držitelem

PKI SZR tuto službu neposkytuje.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

PKI SZR tuto službu neposkytuje.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

PKI SZR tuto službu neposkytuje.

4.7 Výměna veřejného klíče v certifikátu

Výměna veřejného klíče v certifikátu znamená vydání nového certifikátu k novému klíčovému páru v době platnosti certifikátu pro stejný AIS.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Žadatel o certifikát musí vygenerovat nový klíčový pár a postupovat stejně jako při vydání prvního certifikátu pro příslušný AIS podle kap. 4.1.

Je povoleno mít pro jeden AIS maximálně dva platné certifikáty maximálně po dobu 3 měsíců.

4.7.2 Subjekty oprávněné požadovat výměnu veřejného klíče v certifikátu

Platí stejná ustanovení, jako v kapitole 4.1.1.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Platí stejná ustanovení, jako v kapitole 4.2.

4.7.4Oznámení o vydání certifikátu s vyměněným veřejným klíčem držiteli

Platí stejná ustanovení, jako v kapitole 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Platí stejná ustanovení, jako v kapitole 4.4.1.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Platí stejná ustanovení, jako v kapitole 4.4.2.

4.7.7 Oznámení o vydání certifikátu s vyměněným veřejným klíčem jiným subjektům

Platí stejná ustanovení, jako v kapitole 4.4.3.

4.8 Změna údajů v certifikátu

CA SZR neumožňuje provést změnu údajů ve vydaném certifikátu. Pokud se některý údaj v dosud platném certifikátu změnil, je držitel certifikátu povinen tento fakt oznámit RA SZR a požádat o zneplatnění všech certifikátů, kterých se změna týká.

4.8.1 Podmínky pro změnu údajů v certifikátu

PKI SZR tuto službu neposkytuje.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

PKI SZR tuto službu neposkytuje.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

PKI SZR tuto službu neposkytuje.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

PKI SZR tuto službu neposkytuje.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji držitelem

PKI SZR tuto službu neposkytuje.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji certifikační autoritou

PKI SZR tuto službu neposkytuje.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

PKI SZR tuto službu neposkytuje.

4.9 Zneplatnění a pozastavení platnosti certifikátu

CA SZR poskytuje službu zneplatnění certifikátu, tj. ukončení jeho platnosti předtím, než uplyne jeho doba platnosti. Zneplatněný certifikát nemůže být obnoven.

CA SZR neposkytuje službu pozastavení platnosti certifikátu.

4.9.1 Podmínky pro zneplatnění certifikátu

Okolnosti, jejichž následkem může dojít ke zneplatnění certifikátů, jsou zejména tyto:

a) věcný obsah certifikátu nebo jeho část se stane neplatným před ukončením platnosti certifikátu;
b) držitel certifikátu porušil, respektive porušuje povinnosti uvedené v Certifikační politice, případně povinnosti vyplývající z této Certifikační politiky (viz zejména kapitoly 4.5.1 a 4.7.1), případně z jiných relevantních platných a účinných předpisů;
c) existuje důvodné podezření, že byl vyzrazen soukromý klíč;
d) držitel certifikátu požádá o zneplatnění certifikátu;
e) držitel certifikátu zanikl;
f) změnil se správce AIS;
g) dojde ke kompromitaci soukromého klíče některé certifikační autority podílející se na vydávání certifikátů, v tomto případě musí dojít k zneplatnění všech certifikátů, které byly vytvořeny s daným klíčem certifikační autority;
h) certifikát je použitý při útoku na bezpečnost základních registrů;
i) dojde k ukončení činnosti CA SZR;
j) RA SZR obdrží v žádosti o certifikát stejný veřejný klíč, který byl certifikován pro jiného držitele certifikátu, než je žadatel o certifikát (viz kapitolu 6.1.6);
k) pokrok v kryptoanalýze vedoucí k neakceptovatelnému riziku narušení bezpečnosti kryptografických prostředků, které byly použity při vydání certifikátu;
l) pokrok ve výpočetní technice vedoucí k neakceptovatelnému riziku narušení bezpečnosti kryptografických prostředků, které byly použity při vydání certifikátu;
m) nalezení zranitelnosti v technických nebo kryptografických prostředcích, které byly použity při vydání certifikátu a které mají za důsledek neakceptovatelné riziko narušení bezpečnosti certifikátu;
n) žadatel o certifikát odmítl převzít certifikát.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Subjektem oprávněným žádat o zneplatnění certifikátu je pouze:

a) držitel certifikátu;
b) SZR.

4.9.3 Zpracování požadavku na zneplatnění certifikátu

4.9.3.1 Zneplatnění certifikátu na základě žádosti držitele certifikátu

Držitel certifikátu může o zneplatnění certifikátu požádat jedním z následujících způsobů:
a) prostřednictvím aplikace, kterou určila SZR:
b) telefonicky nebo osobně, v tomto případě musí držitel certifikátu požadavek na zneplatnění certifikátu potvrdit zasláním žádosti prostřednictvím aplikace, kterou určila SZR.

RA SZR v každém případě vyžaduje sériové číslo certifikátu k zneplatnění a identifikaci držitele certifikátu.

Součástí žádosti o zneplatnění certifikátu může být také určení důvodu zneplatnění. V případech, kdy je zneplatnění certifikátu požadováno z důvodů vyzrazení klíče nebo existujícího podezření z neoprávněného použití klíče, musí tento důvod žadatel v žádosti o zneplatnění uvést.

RA SZR žádost o zneplatnění certifikátu přijme a zaeviduje ji.

RA SZR zkontroluje údaje o certifikátu. Žádost o zneplatnění certifikátu může být odmítnuta mj. z následujících důvodů:
- neplatné (neznámé) číslo certifikátu;
- certifikát nebyl vydán pro subjekt, který požaduje zneplatnění certifikátu;
- certifikát není platný – buď jeho platnost již uplynula, nebo byl již dříve zneplatněn.

Pokud jsou údaje chybné nebo neúplné, RA SZR provede jednu z následujících akcí:
- pokud SZR obdržela žádost o zneplatnění prostřednictvím aplikace, kterou určila SZR, pošle do datové schránky žadatele a do aplikace, kterou určila SZR, informaci o důvodu odmítnutí žádosti;
- pokud správce AIS žádá o zneplatnění certifikátu osobně nebo telefonicky, RA SZR odmítne žádost přijmout.

Pokud jsou údaje úplné a správné, RA SZR zablokuje přístup AIS k ZR (ale ne k eGSB, dalším systémům poskytujícím eGON služby a pro komunikaci s jinými AIS) s použitím dotyčného certifikátu (ale zatím ho nezneplatní) a provede jednu z následujících akcí:
- pokud SZR obdržela žádost o zneplatnění prostřednictvím aplikace, kterou určila SZR, předá certifikát CA SZR k zneplatnění;
- pokud SZR obdržela žádost o zneplatnění certifikátu osobně nebo telefonicky, čeká na zneplatnění do doby, než dostane žádost o zneplatnění certifikátu prostřednictvím aplikace, kterou určila SZR.

CA SZR požadavek co nejrychleji zpracuje, umístí identifikaci certifikátu do seznamu zneplatněných certifikátů (CRL) a výsledek sdělí RA SZR.

RA SZR sdělí výsledek žadateli datovou schránkou a prostřednictvím aplikace, kterou určila SZR.

4.9.3.2 Zneplatnění certifikátu z jiných důvodů

Pokud SZR potřebuje zneplatnit certifikát z jiných důvodů, než je žádost držitele certifikátu, postupuje takto:
a) pokud je nutné okamžitě zakázat používat certifikát pro přístup k ZR, zablokuje RA SZR použití certifikátu pro přístup do základních registrů (ale ne k eGSB, dalším systémům poskytujícím eGON služby a pro komunikaci s jinými AIS);
b) informuje držitele certifikátu o zahájení procesu zneplatnění zasláním zprávy do jeho datové schránky;
c) pokud důvody pro zneplatnění trvají i po případném vyjádření držitele certifikátu, RA SZR zablokuje použití certifikátu pro přístup k ZR (pokud již není zablokován), CA

SZR certifikát zneplatní a RA SZR odešle informaci o zneplatnění do datové schránky držitele certifikátu.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Subjekt oprávněný žádat o zneplatnění certifikátu je povinen o zneplatnění požádat bez zbytečného odkladu od chvíle, kdy se dověděl o důvodu pro zneplatnění certifikátu.

4.9.5 Doba zpracování požadavku na zneplatnění certifikátu

Certifikát, jehož zneplatnění je požadováno, je zneplatněn bez zbytečného prodlení, zpravidla během jednoho pracovního dne.

Maximální doba pro provedení zablokování certifikátu jsou 2 pracovní dny.

Maximální doba pro provedení zneplatnění certifikátu je 5 pracovních dní.

4.9.6 Povinnosti spoléhajících se stran při ověřování certifikátů

Spoléhající se strana je povinna ověřit, zda certifikát nebyl zneplatněn a zda nebyly zneplatněny certifikáty vydávajících CA, tedy CA SZR a Root CA SZR. Tato kontrola může proběhnout i automaticky, pokud je technicky taková kontrola možná nebo proveditelná. V případě, že toto ověření neproběhne a spoléhající se strana implicitně platnosti certifikátu (a tím platnosti elektronického podpisu) důvěřuje, není SZR odpovědná za případnou vzniklou škodu.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

CRL jsou vydávány pravidelně bez ohledu na změny v jejich obsahu. Aktuální CRL je vydáván standardně jedenkrát za 24 hodin. CRL mohou být vydávány i častěji.

V případě, že došlo ke zneplatnění certifikátu ISZR, je CRL vydán bezprostředně po zneplatnění certifikátu ISZR.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Zpoždění vydání CRL je přípustné pouze v důsledku technických omezení (havárie atp.). Maximální zpoždění může být 24 hodin a nový CRL by měl být publikován do 48 hodin od vydání předcházejícího CRL.

4.9.9 Dostupnost on-line služeb pro ověření stavu certifikátu

PKI SZR tuto službu neposkytuje.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

PKI SZR tuto službu neposkytuje.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

PKI SZR takovou službu neposkytuje.

4.9.12 Zvláštní postupy v případě kompromitace soukromého klíče

Držitel certifikátu je povinen kompromitaci soukromého klíče nahlásit při žádosti o zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

PKI SZR tuto službu neposkytuje.

4.9.14 Subjekty oprávněné žádat o pozastavení platnosti certifikátu

PKI SZR tuto službu neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

PKI SZR tuto službu neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

PKI SZR tuto službu neposkytuje.

4.10 Služby ověření stavu certifikátu

4.10.1 Funkční charakteristiky

CA SZR zveřejňuje seznam zneplatněných certifikátů (CRL) prostřednictvím VA SZR.

4.10.2 Dostupnost služeb

VA SZR poskytuje službu zveřejňování seznamu zneplatněných certifikátů (CRL) nepřetržitě. CRL je publikován na tolika místech, aby i v případě výpadku jedné lokality, ve které je jedna publikace, byl CRL dostupný na aspoň jednom místě.

4.10.3 Další charakteristiky služeb

Žádná opatření.

4.11 Ukončení poskytování služeb držiteli certifikátu

Pokud SZR ukončí činnost poskytovatele certifikačních služeb nebo jeho částí, bude SZR postupovat v souladu s ustanoveními článku 5.8.

Pokud je ukončení činnosti motivováno organizačními nebo jinými důvody, které nesouvisí s bezpečností CA SZR, pak lze certifikáty vydané CA SZR nadále používat. CA SZR ale nebude poskytovat služby spojené se zneplatňováním certifikátů.

4.12 Úschova a obnovení soukromého klíče

CA SZR neposkytuje služby úschovy soukromých klíčů, ani službu jejich obnovení.

Držitelé certifikátů jsou odpovědni za vytváření a uchovávání záloh svých soukromých klíčů. Jestliže dojde k vyzrazení soukromých klíčů držitelů certifikátů díky těmto kopiím, nese plnou odpovědnost za následky držitel certifikátu. RA ani CA SZR se žádným způsobem nepodílí na ukládání ani zálohování soukromých klíčů k vydávaným certifikátům.

CA SZR vytváří záložní kopie soukromých klíčů používaných v souvislosti s vydáváním certifikátů.

5. Správa, provozní a fyzická bezpečnost

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

PKI SZR je umístěna v lokalitách, které nejsou ohroženy záplavami ani nebezpečnými průmyslovými provozy. Konstrukce budov je přiměřeně odolná přírodním podmínkám. Prostory jsou vybaveny přiměřenou ochranou proti násilnému vniknutí a proti požárům.

5.1.2 Fyzický přístup

Prostory PKI SZR jsou chráněny před přístupem neoprávněných osob a zařízení v těchto prostorách jsou chráněna před neoprávněným použitím.

Prostory PKI SZR jsou rozděleny na zóny s různou úrovní zabezpečení, která odpovídá citlivosti zařízení a dat, která se v těchto zónách nacházejí.

5.1.3 Elektřina a provozní prostředí

Objekty, ve kterých jsou zařízení PKI SZR umístěna, jsou vybaveny zdroji elektrické energie a klimatizací dostatečnými k tomu, aby bylo možné vytvořit stabilní pracovní prostředí zajišťující bezchybné provádění certifikačních služeb.

Dodávky elektrické energie jsou zajištěny záložními napájecími zdroji anebo nepřerušitelnými zdroji napájení, které jsou schopny zajistit elektrickou energii po dobu nezbytně nutnou pro dokončení zpracování veškerých započatých činností a pro vytvoření permanentního záznamu o aktuálním stavu PKI SZR.

5.1.4 Vliv vody

Objekty, ve kterých jsou zařízení PKI SZR umístěna, jsou chráněny proti nežádoucím vlivům vody na provoz PKI SZR, a to podle ustanovení havarijní směrnice budovy, ve které jsou certifikační služby poskytovány.

5.1.5 Protipožární opatření a ochrana

Objekty, ve kterých jsou zařízení PKI SZR umístěna, jsou chráněny proti požárům, a to podle ustanovení požární směrnice budovy, ve které jsou certifikační služby poskytovány.

5.1.6 Ukládání médií

Média jsou uchovávána tak, aby nedošlo k jejich poškození či znehodnocení. Je zajištěna dostatečná spolehlivost paměťových médií, která jsou určena pro záznam a archivaci dat vzniklých při činnosti poskytovatele certifikačních služeb.

Média jsou ukládána tak, aby bylo zabráněno neoprávněnému přístupu k nim.

5.1.7 Nakládání s odpady

Fyzická média s neveřejnými informacemi jsou skartována odpovídajícím bezpečným způsobem včetně vymazání obsahu datových médií před jejich skartací.

5.1.8 Zálohy mimo budovu

Zálohování všech dat, která jsou vytvářena během poskytování certifikačních služeb, je prováděno pravidelně. Nejméně jedna záložní kopie je fyzicky uložena odděleně od ostatních kopií. Zálohy jsou uchovávány na místech, kde jsou uplatňovány fyzické a procedurální kontroly, které odpovídají požadovanému stupni ochrany.

5.2 Procedurální bezpečnost

5.2.1 Důvěryhodné role

Důvěryhodné role jsou:

- správce CA;
- operátor CA;
- správce RA;
- operátor RA;
- auditor PKI.

Osoby, které jsou pověřeny plněním těchto rolí, musí splňovat požadavky personální bezpečnosti, které jsou definovány v interních předpisech SZR.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Obvyklé činnosti v rámci certifikačních služeb jsou prováděny jednou osobou s tím, že složitější úlohy mohou být rozděleny na logické, vzájemně od sebe oddělitelné, navazující části, které vykonávají různé osoby.

V interních předpisech SZR jsou definovány činnosti, při kterých je vyžadována účast alespoň dvou osob. Jedná se o operace kritické pro důvěryhodnost poskytovatele certifikačních služeb a certifikátů vydávaných CA SZR.

5.2.3 Identifikace a autentizace pro každou roli

Každá osoba má povolen přístup pouze k aplikacím a do prostor, které jsou nezbytné pro výkon její činnosti.

Každá osoba má přiděleny identifikační a autentizační údaje a prostředky, za které je osobně zodpovědná.

5.2.4 Role vyžadující rozdělení povinností

Jakoukoli kombinaci následujících rolí nesmí vykonávat jedna osoba:

- správce CA;
- správce RA;
- auditor PKI.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Pracovníci PKI SZR zastávající důvěryhodné role musí splňovat:

- odborné předpoklady v oblasti IT, které vyplývají z jejich funkčního zařazení;
- občanskou bezúhonnost;
- další kritéria určená interními předpisy SZR.

5.3.2 Posouzení spolehlivosti osob

Řídí se interními předpisy SZR.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Veškerý personál zapojený do poskytování certifikačních služeb je dostatečně vyškolen.

Každá osoba, která bude zajišťovat certifikační služby, absolvuje před zahájením činnosti úvodní proškolení pro práci s programovým i hardwarovým vybavením poskytovatele certifikačních služeb, operační a bezpečnostní postupy a praktické uplatňování bezpečnostních a certifikačních politik a dalších předpisů.

5.3.4 Požadavky na opakování školení

SZR nevyžaduje ani nepořádá pravidelná školení pracovníků PKI SZR.

SZR zajišťuje seznámení pracovníků PKI SZR s novými relevantními předpisy.

SZR pořádá školení pracovníků PKI SZR v případě významných změn.

Významnými změnami v tomto smyslu jsou například změny programového nebo hardwarového vybavení, změny v požadavcích na bezpečnost, změny v procesech a pracovních postupech, případně další změny, které mají významný vliv na provádění certifikačních služeb.

5.3.5 Periodicita a posloupnost rotace zaměstnanců mezi různými rolemi

Žádná opatření.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Postihy za porušení pracovních povinností se řídí služebním zákonem, zákoníkem práce a interními předpisy SZR.

5.3.7 Požadavky na nezávislé dodavatele

Vztahy s dodavateli jsou upraveny smlouvami. Tyto smlouvy obsahují pouze ustanovení požadovaná nebo umožněná platnými a účinnými právními předpisy.

5.3.8 Dokumentace poskytovaná zaměstnancům

Dokumentace potřebná k provádění činností PKI SZR je poskytnuta všem osobám, kterých se týká a jejichž činnost definuje, nebo jiným způsobem ovlivňuje.

Zejména se jedná o následující dokumenty:

a) certifikační politika;
b) popis procesů a pracovních postupů;
c) technická dokumentace;
d) bezpečnostní dokumentace;
e) havarijní plány a plány kontinuity;
f) pokyny a postupy pro žadatele o certifikáty a pro žadatele o zneplatnění certifikátů.

5.4 Postupy pro zpracování záznamů o činnosti

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou tyto události:

a) příjem žádosti o vydání nebo zneplatnění certifikátu;
b) vydání nebo zneplatnění certifikátu;
c) odeslání sdělení o vydání nebo zneplatnění certifikátu;
d) nakládání s klíčovými páry CA;
e) generování a publikace CRL;
f) autentizační a autorizační události na systémech, na kterých je provozována CA SZR, a na systémech, na kterých je provozována RA SZR;
g) provedení zálohy a obnovy CA SZR;
h) start a zastavení CA SZR;
i) konfigurační změny CA SZR.

5.4.2 Periodicita zpracování záznamů

Četnost kontroly a vyhodnocování záznamů jsou definovány interními předpisy SZR. V případě bezpečnostního incidentu se vyhodnocují okamžitě.

5.4.3 Doba uchovávání záznamů

Záznamy se uchovávají po dobu stanovenou platnou a účinnou legislativou, minimálně ale pět let.

5.4.4 Ochrana záznamů

Záznamy jsou ukládány takovým způsobem, že jsou chráněny proti neoprávněnému přístupu, modifikaci a ztrátě vlivem technické chyby.

5.4.5 Postupy pro zálohování záznamů

Záznamy jsou zálohovány takovým způsobem, že je zajištěna jejich dostupnost, důvěrnost a integrita.

5.4.6 Systém shromažďování záznamů (interní nebo externí)

Systém shromažďování záznamů je z hlediska PKI SZR interní, tj. události se zaznamenávají v rámci prostředí PKI SZR.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

RA SZR oznamuje události a) - c) z kapitoly 5.4.1 příslušnému subjektu prostřednictvím aplikace, kterou určila SZR, anebo odesláním zprávy datovou schránkou.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti PKI SZR je prováděno jednak během periodicky prováděné analýzy rizik a za druhé operativně během vyhodnocování záznamů o činnosti PKI SZR.

5.5 Uchovávání informací a dokumentace

5.5.1 Typy informací a dokumentace, které se uchovávají

Následující informace jsou zaznamenány a uloženy do archivu na počátku fungování CA SZR:

a) vygenerování prvních klíčových párů pro CA SZR a Root CA SZR;
b) certifikační politika.

Následující skupiny informací jsou zaznamenány a archivovány po celou dobu provádění certifikačních služeb:

c) generování dalších klíčových párů pro CA SZR a Root CA SZR;
d) zničení klíčových párů pro CA SZR nebo Root CA SZR;
e) aktualizované dokumenty PKI SZR, především certifikační politika;
f) změny konfiguračních souborů programového vybavení certifikačních autorit;
g) dokumentace související s žádostmi o vydání nebo zneplatnění certifikátu;
h) vydané certifikáty;
i) vydané seznamy zneplatněných certifikátů (CRL).

5.5.2 Doba uchovávání informací a dokumentace

Záznamy o činnosti uvedené v kapitole **Chyba! Nenalezen zdroj odkazů.** jsou uchovávány po dobu uvedenou v kapitole 5.4.3.

Ostatní informace a dokumenty uvedené v kapitole 5.5.1 jsou uchovávány po celou dobu existence CA SZR. Při ukončení činnosti CA SZR bude rozhodnuto o jejich dalším uložení, nebo o jejich zničení.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Ochrana záznamů o činnosti i ostatních informací a dokumentace v elektronické formě je prováděna podle kapitoly 5.4.4, tj. jsou ukládány takovým způsobem, že jsou chráněny proti neoprávněnému přístupu, modifikaci a ztrátě vlivem technické chyby.

Neveřejné listinné záznamy a neveřejná dokumentace jsou ukládány v prostorách s kontrolou přístupu fyzických osob.

5.5.4 Postupy při zálohování informací a dokumentace

Zálohování záznamů o činnosti je prováděno podle kapitoly 5.4.5.

5.5.5 Požadavky na použití časových razítek při uchovávání informací a dokumentace

Každý archiv (tj. skupina informací archivovaná společně) je opatřena časovým údajem. Tzn., že jsou u něj uvedeny datum a čas, kdy byl archiv vytvořen.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní a externí)

Systém shromažďování informací a dokumentace je z hlediska PKI SZR interní, tj. informace a dokumentace se zaznamenávají v rámci prostředí PKI SZR.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Informace a dokumentace jsou zabezpečeny proti neoprávněnému přístupu.

Přístup mají pouze pověření zaměstnanci SZR. Jiné osoby pouze na základě písemného povolení vedoucího služebního úřadu SZR.

5.6 Výměna veřejného klíče

Soukromé (podepisovací) klíče CA SZR jsou obměňovány v přiměřených časových intervalech. Root CA SZR vydá v dostatečném předstihu před známým nebo plánovaným koncem platnosti klíče používaného CA SZR k podepisování vydávaných certifikátů nový certifikát. Nový certifikát CA SZR je zveřejněn.

Po ukončení platnosti je soukromý klíč CA SZR zničen a o zničení je proveden záznam.

5.7 Postupy při havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

Postup v případě incidentu a kompromitace je definován interními předpisy SZR pro zvládání bezpečnostních událostí a bezpečnostních incidentů.

5.7.2 Poškození výpočetních prostředků, software nebo dat

V případě, že dojde k poškození výpočetních prostředků, software nebo dat, zajistí CA SZR, respektive RA SZR kontinuitu činnosti podle plánů kontinuity.

Dále provede SZR obnovu stavu prostředků CA SZR, respektive RA SZR do původního stavu podle havarijních plánů.

5.7.3 Postup při kompromitaci soukromého klíče

V případě, že dojde ke kompromitaci podepisovacího klíče CA SZR nebo k důvodnému podezření z jeho kompromitace:

a) CA SZR ukončí vydávání certifikátů s použitím kompromitovaného klíče;
b) nadřízená certifikační autorita (tj. Root CA SZR) zneplatní podepisovací certifikát CA SZR.

Dalším krokem je zneplatnění všech aktuálně platných certifikátů, které byly podepsány kompromitovaným klíčem.

c) SZR informuje o zneplatnění držitele certifikátů vydaných s použitím kompromitovaného klíče;
d) CA SZR vygeneruje nový klíčový pár a požádá o certifikaci veřejného klíče nadřízenou autoritou (tj. Root CA SZR).

Následně se SZR pokusí zjistit způsob, jakým došlo k prozrazení soukromého klíče a přijme nápravná opatření.

Za kompromitaci podepisovacího klíče CA SZR se považuje i situace, kdy dojde k takovému pokroku v oblasti kryptoanalýzy nebo IT, že bude ohrožena bezpečnost vydávaných certifikátů.

5.7.4 Schopnost obnovit činnost po havárii

Platí ustanovení článků 5.7.1 a 5.7.2.

5.8 Ukončení činnosti CA nebo RA nebo VA

5.8.1 Ukončení činnosti CA

Pokud je ukončení činnosti CA SZR motivováno organizačními hledisky nebo jinými důvody, které nesouvisí s bezpečností CA SZR, pak lze certifikáty vydané CA SZR nadále používat (dle uvážení držitelů certifikátů). Držitelé certifikátů musí zejména vzít v úvahu, že CA nebude aktualizovat seznam odvolaných certifikátů (CRL).

SZR provede při ukončení činnosti CA SZR následující akce:

a) informuje o situaci na svých webových stránkách;
b) ukončí vydávání certifikátů;
c) ukončí vydávání nových CRL;
d) provede audit PKI SZR;
e) zničí soukromé klíče CA SZR a o zničení provede záznam;
f) archivuje veškeré relevantní informace.

5.8.2 Ukončení činnosti RA

Ukončení činnosti RA SZR znamená v případě PKI SZR i ukončení činnosti CA SZR. Postup je tedy stejný jako v kapitole 5.8.1.

5.8.3 Ukončení činnosti VA

SZR neukončí činnost VA SZR, dokud nebude ukončena činnost CA SZR. Činnost VA SZR může pokračovat i po ukončení činnosti CA SZR, po ukončení činnosti CA nebudou vydávány nové CRL.

V případě ukončení činnosti VA provede SZR následující akce:

a) informuje o situaci na svých webových stránkách;
b) informuje všechny držitele certifikátů;
c) uveřejní na svých webových stránkách poslední CRL a umožní jeho stažení.

6. Technická bezpečnost

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Tato certifikační politika nevylučuje žádný způsob generování dvojice klíčů, jestliže jsou dodrženy příslušné bezpečnostní požadavky. Předpokládá se, že klíče jsou generovány způsobem, který je pod kontrolou jejich budoucího držitele, nebo způsobem, který zajišťuje uchování soukromých klíčů v tajnosti.

Konkrétní postup pro generování dvojice klíčů na straně CA SZR pro podepisování vydaných certifikátů a popis použitých technických prostředků je uveden v technické dokumentaci PKI SZR.

6.1.2 Předání soukromého klíče držiteli certifikátu

Tato certifikační politika předpokládá, že soukromé klíče jsou generovány žadatelem o certifikát, tzn., že žádné doručování soukromých klíčů není prováděno.

6.1.3 Předání veřejného klíče poskytovateli certifikačních služeb

Veřejný klíč je RA SZR předáván žadatelem o certifikát elektronicky doručením souboru ve formátu PKCS#10 a kódování PEM prostřednictvím aplikace, kterou určila SZR.

6.1.4 Poskytování veřejných klíčů certifikační autoritou spoléhajícím se stranám

CA SZR neposkytuje veřejné klíče držitelů certifikátů spoléhajícím se stranám.

6.1.5 Délky klíčů

CA SZR používá algoritmus RSA a délky klíčů 2048 bitů a delší.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

CA SZR kontroluje veřejné klíče v žádostech o vydání certifikátu:

a) pokud obdrží klíč, který je již použitý v jiném certifikátu vydaném CA SZR, je žádost odmítnuta a žadatel je vyzván k podání nové žádosti s jiným veřejným klíčem;

b) pokud byl certifikát se stejným veřejným klíčem vydán jinému držiteli, než je žadatel o certifikát, je vydaný certifikát zneplatněn z iniciativy SZR a jeho držitel je o tom informován a vyzván k podání nové žádosti s jiným veřejným klíčem;

c) pokud byl certifikát se stejným veřejným klíčem vydán stejnému držiteli, jako je žadatel o certifikát, zůstane vydaný certifikát v platnosti.

6.1.7 Omezení pro použití veřejného klíče

Možná použití klíče jsou definována v kapitolách 7.1.2.4 a 7.1.2.5.

6.2 Ochrana soukromého klíče a bezpečnost kryptografického modulu

6.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat určených pro vydávání certifikátů CA SZR probíhá v prostředí, které splňuje požadavky standardu FIPS PUB 140-2 třídy 2.

6.2.2 Kontrola soukromého klíče více osobami (n z m)

Žádná opatření.

6.2.3 Úschova soukromého klíče

Soukromý klíč pro podepisování certifikátů vydávaných CA SZR je uchováván tak, aby bylo možné jeho použití, a je současně chráněn proti neoprávněnému přístupu.

6.2.4 Zálohování soukromého klíče

PKI SZR vytváří záložní kopie soukromých klíčů všech certifikačních autorit SZR. Uchovávání všech kopií splňuje stejné bezpečnostní požadavky jako uložení originálu. Zálohy klíčového páru jsou chráněny heslem, uloženy na bezpečném místě a přístup k nim je omezen na oprávněné osoby.

6.2.5 Archivace soukromého klíče

Soukromé klíče určené pro podepisování vydaných certifikátů nejsou CA SZR archivovány po uplynutí doby jejich platnosti. Naopak jsou zničeny všechny jejich kopie a je o tom vyhotoven protokol.

6.2.6 Transfer soukromého klíče do/z kryptografického modulu

Žádná opatření.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Žádná opatření.

6.2.8 Postup při aktivaci soukromého klíče

Žádná opatření.

6.2.9 Postup při deaktivaci soukromého klíče

Žádná opatření.

6.2.10 Postup při zničení soukromého klíče

Soukromý klíč je z kryptografického modulu vymazán a jsou fyzicky zničeny všechny jeho kopie.

6.2.11 Hodnocení kryptografických modulů

Hodnocení kryptografických modulů vychází z požadavků standardu FIPS PUB 140-2 level 2.

6.3 Další aspekty správy párových dat

6.3.1 Archivace veřejných klíčů

CA SZR archivuje vydané certifikáty po celou dobu činnosti PKI SZR.

6.3.2 Maximální doba platnosti certifikátu a párových dat

Doba platnosti certifikátu vydaného žadateli o certifikát je uvedena v kap. 7.1.1.5.

Doba platnosti klíčového páru je stejná jako doba platnosti certifikátu příslušného veřejného klíče.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Žádná opatření.

6.4.2 Ochrana aktivačních dat

Žádná opatření.

6.4.3 Ostatní aspekty aktivačních dat

Žádná opatření.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Veškeré programové vybavení CA SZR používá operační systém, který zabraňuje pokusům o obejití bezpečnostních mechanismů a zaznamenává je ve formě auditních záznamů. Operační systém vyžaduje identifikaci a autentizaci každého uživatele.

Technické vybavení CA SZR je určeno pouze pro provoz CA. Nejsou na něm provozovány žádné jiné aplikace.

6.5.2 Hodnocení počítačové bezpečnosti

SZR hodnotí počítačovou bezpečnost PKI SZR podle norem řady ČSN ISO/IEC 27000.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

PKI SZR byla implementována podle systémové bezpečnostní politiky a podle téže politiky je prováděn i další rozvoj PKI SZR.

6.6.2 Kontroly řízení bezpečnosti

Kontroly řízení bezpečnosti provádí SZR jako součást auditů systému řízení bezpečnosti SZR.

6.6.3 Řízení bezpečnosti životního cyklu

Bezpečnost životního cyklu PKI SZR je řízena na základě procesního přístupu. Veškeré změny v PKI SZR jsou zhodnoceny z hlediska bezpečnosti před jejich implementací.

6.7 Síťová bezpečnost

Servery CA SZR jsou umístěny v zabezpečeném segmentu počítačové sítě a přístup k nim je řízen a kontrolován na síťové úrovni. Na serverech CA SZR je aktivní pouze takový síťový software, který je nutný pro provoz CA.

Síťová bezpečnost se řídí systémovou bezpečnostní politikou.

6.8 Časová razítka

CP neřeší problematiku časových razítek. CA SZR takovou službu nenabízí.

7. Profily certifikátů, seznamu zneplatněných certifikátů a OCSP

7.1 Profil certifikátu

7.1.1 Položky certifikátu

7.1.1.1 Version

„0x2“
Hodnotu definuje CA SZR.
CA SZR vydává certifikáty podle normy X.509 verze 3.

7.1.1.2 Serial number

Unikátní číslo certifikátu v rámci vydávající CA.
Hodnotu definuje CA SZR.

7.1.1.3 Signature algorithm

„sha256RSA“
Hodnotu definuje CA SZR.

7.1.1.4 Issuer

Identifikace CA, která certifikát vydala.
CN = „ISZR AIS CA“
O = „SZR CR“
L = „Praha“
C = „CZ“
Hodnotu definuje CA SZR.

7.1.1.5 Validity

Doba platnosti certifikátu.

Not before - CA SZR dosadí čas vydání certifikátu.

Not after - CA SZR dosadí čas vydání certifikátu plus 3 roky. CA SZR při vydávání certifikátu nepřekročí dobu platnosti použitého podepisovacího klíče CA.

7.1.1.6 Subject

Předmět certifikátu. Identifikuje držitele certifikátu a AIS, pro který byl certifikát vydaný.

CN = Označení serveru.
CA SZR dosadí hodnotu z žádosti o certifikát.
Položka je nepovinná.
Maximální povolená délka je 64 znaků.

O = Označení (identifikace) žadatele o certifikát.
CA SZR dosadí hodnotu z žádosti o certifikát.
Položka je povinná. Musí být uvedeno IČO správce AIS.
Maximální povolená délka je 64 znaků.

OU = Označení (identifikace) AIS.
CA SZR dosadí hodnotu z žádosti o certifikát.
Položka je povinná. Musí být uveden identifikátor AIS z příslušného seznamu vedeného orgány státní správy nebo vedeného z jejich pověření.
Maximální povolená délka je 64 znaků.

ST = Označení (jméno) žadatele o certifikát.
CA SZR dosadí hodnotu z žádosti o certifikát.
Položka je nepovinná.
Maximální povolená délka je 128 znaků.

L = Adresa žadatele o certifikát.
CA SZR dosadí hodnotu z žádosti o certifikát.
Položka je nepovinná.
Maximální povolená délka je 128 znaků.

C = Země.
Položka je nepovinná. Pokud je uvedená, musí obsahovat platný kód povolené země.
CA SZR dosadí hodnotu z žádosti o certifikát.

7.1.1.7 Subject Public key info

Informace o veřejném klíči.

Algorithm – CA SZR dosadí hodnotu rsaEncryption.

SubjectPublicKey – CA SZR dosadí veřejný klíč RSA z žádosti o certifikát.

7.1.1.8 Signature

CA SZR dosadí podpis vydaného certifikátu provedený s použitím soukromého klíče CA SZR.

7.1.2 Rozšiřující položky certifikátu

7.1.2.1 Authority key identifier

Identifikace klíče CA SZR.
Obsah pole ‘Subject key identifier’ certifikátu, kterým CA SZR certifikát podepsala.
Hodnotu definuje CA SZR.

7.1.2.2 Subject key identifier

Identifikace předmětu, pro který byl certifikát vydán.
Hodnotu definuje CA SZR.

7.1.2.3 CRL Distribution Points

Distribuční místa seznamu odvolaných certifikátů. Definuje URL, na kterých lze CRL získat.
Hodnotu definuje CA SZR.

7.1.2.4 Key usage

Použití klíče.
„Digital Signature“ – autentizace pomocí digitálního podpisu.
„Key Encipherment“ – šifrování klíčů pro navázání bezpečného spojení.
Hodnotu definuje CA SZR.

7.1.2.5 Enhanced key usage

Rozšířené použití klíče.
„Server Authentication“ – autentizace serveru.
„Client Authentication“ – autentizace klienta.
Hodnotu definuje CA SZR.

7.1.2.6 Authority information access

Distribuční místa certifikátů CA, které se podílely na vydání certifikátu. Definuje URL, na kterých lze certifikát získat.
Hodnotu definuje CA SZR.

7.1.2.7 Certificate template name

Označení šablony, podle které byl certifikát vydán.
Hodnotu definuje CA SZR.

7.1.2.8 Application policies

Politiky aplikování.
„Server Authentication“ – autentizace serveru.
„Client Authentication“ – autentizace klienta.
Hodnotu definuje CA SZR.

7.1.2.9 Subject Alternative Name

Alternativní označení předmětu certifikátu.
Položka je nepovinná.
Maximální povolená délka je 64 znaků.
CA SZR dosadí hodnotu z žádosti o certifikát.

7.1.3 Objektové identifikátory algoritmů

Pro vydávání certifikátů se používá schéma sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11).

7.1.4 Způsoby zápisu jmen a názvů

Všechny názvy a texty se uvádí bez diakritiky. Viz kapitolu 3.1.4.

7.1.5 Omezení jmen a názvů

Omezení pro jméno subjektu jsou popsána v kapitole 3.1.5.

7.1.6 Objektový identifikátor Certifikační politiky

OID je uvedeno v kapitole 1.1.

V certifikátech vydávaných CA SZR se nepoužívá.

7.1.7 Rozšíření „Policy Constraints“

V certifikátech vydávaných CA SZR se nepoužívá.

7.1.8 Syntaxe a schémata rozšíření „Policy Qualifiers“

V certifikátech vydávaných CA SZR se nepoužívá.

7.1.9 Zpracování kritického rozšíření „Certificate Policies“

V certifikátech vydávaných CA SZR se toto rozšíření nepoužívá.

7.2 Profil CRL

7.2.1 Položky CRL

7.2.1.1 Version

„2“
Hodnotu definuje CA SZR.

7.2.1.2 Signature algorithm

„sha256RSA“
Hodnotu definuje CA SZR.

7.2.1.3 Issuer

Identifikace CA, která CRL vydala.
CN = „ISZR AIS CA“
O = „SZR CR“
L = „Praha“
C = „CZ“
Hodnotu definuje CA SZR.

7.2.1.4 This update

CA SZR dosadí čas vydání CRL.

7.2.1.5 Next update

CA SZR dosadí předpokládaný čas vydání příštího CRL.

7.2.1.6 Revoked certificates

CA SZR dosadí seznam zneplatněných certifikátů. Může být prázdný.

7.2.2 Rozšiřující položky CRL a záznamů v CRL

7.2.2.1 Authority key identifier

Hash, tj. obsah pole ‘Subject key identifier’ certifikátu, kterým vydávající CA CRL podepsala.

Hodnotu definuje CA SZR.

7.2.2.2 CRL number

Pořadové číslo seznamu zneplatněných certifikátů.
Hodnotu definuje CA SZR.

7.2.2.3 Delta CRL indicator

Rozšíření informuje o tom, že jde o rozdílový seznam zneplatněných certifikátů.
Hodnotu dosadí CA SZR v případě, že jde o rozdílový seznam zneplatněných certifikátů.

7.2.3 Rozšiřující položky záznamů v CRL

Jde o nepovinná rozšíření k jednotlivým zneplatněným certifikátům. Nemusí být uvedena.

7.2.3.1 Reason code

Může obsahovat důvod zneplatnění certifikátu.

7.2.3.2 Invalidity date

Může obsahovat čas, kdy RA SZR byla nahlášena kompromitace soukromého klíče, příslušejícího ke zneplatněnému certifikátu.

7.3 Profil OCSP

7.3.1 Číslo verze

Služba OCSP není poskytována.

7.3.2 Rozšiřující položky OCSP

Služba OCSP není poskytována.

8. Hodnocení shody a jiná hodnocení

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

O provedení auditu PKI SZR rozhoduje vedoucí služebního úřadu SZR. Provádí se v případě vážného bezpečnostního incidentu, v případě významných změn v oblasti kryptografie, v případě významných změn uvnitř SZR a dále podle potřeby.

8.2 Identita a kvalifikace hodnotitele

Auditor musí mít prokazatelnou praxi a kvalifikaci v oblasti bezpečnosti informačních technologií.

8.3 Vztah hodnotitele k hodnocenému subjektu

V případě interního hodnotitele se hodnotitel nesmí žádným způsobem podílet na provozu PKI SZR.

V případě externího hodnotitele nesmí být hodnotitel v žádném organizačním vztahu se SZR.

8.4 Hodnocené oblasti

Hodnocenými oblastmi jsou zejména:

a) certifikační politika;
b) ostatní navazující dokumentace;
c) uplatňování ustanovení CP a ostatní bezpečnostní dokumentace;
d) technické aspekty provozu PKI SZR;
e) generování klíčových párů pro podepisování vydávaných certifikátů;
f) nakládání s klíčovými páry pro podepisování vydávaných certifikátů (export, import, záloha);
g) všechny činnosti, související s životním cyklem certifikátů;
h) generování, publikace a update CRL;
i) všechny procesní záležitosti, aktualizace dokumentace;
j) identifikační, autentizační a autorizační mechanismy pro přístup k PKI SZR.

8.5 Postup v případě zjištění nedostatků

Pokud hodnotitel zjistí během auditu zvlášť závažné nedostatky, které podle jeho názoru bezprostředně ohrožují bezpečnost PKI SZR, je jeho povinností to sdělit vedoucímu služebního úřadu SZR a povinností vedoucího služebního úřadu SZR je rozhodnout, zda mají být certifikační služby přerušeny až do doby provedení nápravných opatření.

Výše uvedené i ostatní nedostatky uvede hodnotitel v závěrečné zprávě, viz kapitolu 8.6.

8.6 Sdělování výsledků hodnocení

Výsledek hodnocení je sdělován formou písemné závěrečné zprávy vedoucímu služebního úřadu SZR bez zbytečného prodlení po ukončení hodnocení. Procesní lhůty upravuje kontrolní řád.

Vedoucí služebního úřadu SZR zajistí projednání zprávy uvnitř SZR a zajistí realizaci případných nápravných opatření.

9. Ostatní obchodní a právní náležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Žadatelům o certifikát ani žadatelům o obnovení certifikátu SZR neúčtuje žádné poplatky.

9.1.2 Poplatky za přístup k certifikátu

SZR neúčtuje za přístup k certifikátům žádné poplatky.

9.1.3 Poplatky za zneplatnění certifikátu a za přístup k informacím o stavu certifikátu

Žadatelům o zneplatnění certifikátu SZR neúčtuje žádné poplatky.

SZR neúčtuje žádné poplatky za přístup k informacím o stavu certifikátu.

9.1.4 Poplatky za další služby

SZR neúčtuje za PKI služby žádné poplatky.

9.1.5 Jiná ustanovení týkající se poplatků

Žádná opatření.

9.2 Finanční odpovědnost

SZR není finančně nijak odpovědná uživatelům certifikátů vydaných CA SZR.

9.2.1 Krytí pojištěním

Žádná opatření.

9.2.2 Další aktiva a záruky

Žádná opatření.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Žádná opatření.

9.3 Ochrana citlivých a důvěrných informací

9.3.1 Výčet citlivých informací

Za citlivé informace SZR považuje zejména:

a) soukromé klíče všech certifikačních autorit SZR používané při vydávání certifikátů;
b) technickou dokumentaci PKI SZR;
c) interní předpisy SZR;
d) havarijní plány a plány kontinuity;
e) záznamy o činnosti PKI SZR;
f) záznamy o provedených hodnoceních PKI SZR;
g) veškeré osobní údaje.

9.3.2 Informace mimo rámec citlivých informací

SZR dále považuje za důvěrné (v obecném smyslu, nikoli podle zákona o ochraně utajovaných informací):

a) žádosti o vydání certifikátů;
b) žádosti o zneplatnění certifikátů;
c) sdělení o vydání certifikátů;
d) sdělení o zneplatnění certifikátů.

9.3.3 Odpovědnost za ochranu citlivých a důvěrných informací

Za ochranu citlivých a důvěrných informací je zodpovědný každý, kdo se z pověření SZR podílí na provozu PKI SZR.

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

Politika ochrany osobních údajů se řídí platnými a účinnými právními předpisy a příslušnými interními předpisy SZR.

9.4.2 Osobní údaje

Definice osobních údajů vychází z platných a účinných právních předpisů.

9.4.3 Údaje, které nejsou považovány za osobní údaje

Údaje, které nejsou osobními údaji dle platných a účinných právních předpisů.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je zodpovědný každý, kdo se z pověření SZR podílí na provozu PKI SZR.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Řídí se platnými a účinnými právními předpisy a příslušnými předpisy SZR.

9.4.6 Poskytování osobních údajů pro soudní nebo správní účely

Řídí se platnými a účinnými právními předpisy a příslušnými předpisy SZR.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

Řídí se platnými a účinnými právními předpisy a příslušnými předpisy SZR.

9.5 Práva na ochranu duševního vlastnictví

Certifikáty CA SZR a root CA SZR a jim odpovídající soukromé klíče, Certifikační politika a veškeré dokumenty související s provozem PKI jsou chráněny autorskými právy.

Autorskými právy jsou chráněny i veřejně dostupné informace publikované SZR v souvislosti s provozem PKI SZR, např. obsah příslušných webových stránek.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA SZR

CA SZR zastupuje vedoucí služebního úřadu SZR a osoby jím určené.

SZR zaručuje, že CA SZR bude vydávat a odvolávat certifikáty v souladu s touto certifikační politikou.

9.6.2 Zastupování a záruky RA SZR

RA SZR zastupuje vedoucí služebního úřadu SZR a osoby jím určené.

SZR zaručuje, že RA SZR bude postupovat v souladu s touto certifikační politikou.

9.6.3 Zastupování a záruky držitele certifikátu

Držitele certifikátu zastupuje statutární zástupce správce předmětného AIS.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle této CP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Žádná opatření.

9.7 Zřeknutí se záruk

Žádná opatření.

9.8 Omezení odpovědnosti

Odpovědnost SZR je vymezena platnými a účinnými právními předpisy a touto CP.

9.9 Odpovědnost za škodu, náhrada škody

Odpovědnost SZR je vymezena platnými a účinnými právními předpisy a touto CP.

9.10 Doba platnosti a ukončení platnosti

9.10.1 Doba platnosti

Doba platnosti CP je od data uvedeného na titulní straně tohoto dokumentu minimálně do doby platnosti posledního certifikátu, který byl podle ní vydaný, nebo do doby ukončení platnosti podle kapitoly 9.10.2.

CA SZR vydává certifikáty podle aktuálně platné verze CP.

Držitelé certifikátů a spoléhající se strany jsou povinné se řídit aktuálně platnou verzí CP.

9.10.2 Ukončení platnosti

Ukončení platnosti této certifikační politiky nastává:

a) rozhodnutím vedoucího služebního úřadu SZR;
b) ukončením činnosti PKI SZR.

9.10.3 Důsledky ukončení a přetrvávání závazků

Po ukončení platnosti této CP nebude CA SZR nadále vydávat certifikáty podle této CP.

Po ukončení platnosti této CP přetrvávají z ní vyplývající závazky SZR až do doby ukončení platnosti posledního certifikátu, který podle ní CA SZR vydala.

9.11 Komunikace mezi zúčastněnými subjekty

Pro komunikaci se subjekty, které využívají služeb PKI SZR, se používají jednak aplikace, kterou určila SZR, datové schránky, osobní jednání, e-mail, telefon a portál SZR.

9.12 Změny CP

9.12.1 Postup při změnách

Změna CP je řízený proces definovaný v interní dokumentaci SZR.

9.12.2 Postup při oznamování změn

Nová verze CP bude oznámena a publikována na webových stránkách SZR http://www.szrcr.cz.

9.12.3 Okolnosti, za kterých musí být změněn OID

V případě vydání nové verze CP jí musí být přiděleno nové OID.

9.13 Řešení sporů

Držitelé certifikátů se v případě sporů obrátí na RA SZR.

9.14 Rozhodné právo

Ustanovení CP a jejich výklad a platnost se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Činnost PKI SZR se řídí platnými a účinnými právními předpisy České republiky.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Žádná opatření.

9.16.2 Postoupení práv

V případě ukončení činnosti CA SZR bude řešeno postoupení práv k vydávání certifikátů podle platné legislativy.

9.16.3 Oddělitelnost ustanovení

Tato CP platí jako celek a oddělitelnost jednotlivých jejích ustanovení je možná pouze na základě rozhodnutí soudu nebo veřejnoprávního orgánu, který je k takovému rozhodnutí oprávněn podle platné legislativy.

9.16.4 Zřeknutí se práv

Žádná opatření.

9.16.5 Vyšší moc

SZR neodpovídá za porušení svých povinností vyplývajících z této CP způsobených událostmi, které není v moci SZR odvrátit, a proti jejímž negativním účinkům by byla protiopatření neúměrně nákladná.

Jedná se zejména o přírodní katastrofy velkého rozsahu, o válečné situace, společenský rozvrat, rozsáhlé epidemie, rozsáhlé výpadky zásobování elektřinou, rozsáhlé výpadky elektronických komunikací.

9.17 Další opatření

Žádná opatření.

10. Závěrečná ustanovení

Tato certifikační politika je platná od data účinnosti, které je uvedeno na titulní straně. Počínaje dnem účinnosti vydává a odvolává CA SZR certifikáty podle této politiky. Tento dokument je veřejný a je v platné verzi uložen také na webových stránkách SZR.