DIGITÁLNÍ A INFORMAČNÍ AGENTURA_	DIAPX003C615 prvotní identifikátor	
	DIA- 17112-2/OKŘ-2024	
	POL010B-2023	
POLITIKA	počet stran	38
	přílohy	0

Certifikační politika Digitální a informační agentury pro certifikáty vydávané pro AIS

Oblast působnost: zaměstnanci DIA, správci AIS

Gestor: Ing. Radovan PÁRTL	**Nahrazuje:** POL010A-2023
Zpracovatel: RNDr. Ota ZÁHORA	**Klasifikace:** VEŘEJNÝ
Odborný garant: -	**Schváleno dne:** *datum uvedeno v doložce elektronického podpisu*
Schvalovatel: *podepsáno elektronicky* Ing. Martin MESRŠMÍD	**Účinnost ode dne:** 01. 09. 2024

HISTORIE DOKUMENTU:

Verze	Datum	Autor	Popis
-	25. 03. 2023	RNDr. Ota ZÁHORA	Vznik nového dokumentu
A (1.1)	25. 04. 2024	RNDr. Ota ZÁHORA Ing. Ondřej PROKŮPEK	• Změny z důvodu přechodu na novou CA DIA (kapitoly 6.1.5, 7.1.1.3, 7.1.1.4, 7.1.3, 7.2.1.2 a 7.2.1.3). • Přidání informací o systému CAAIS (kapitoly 1.4.6, 3.2.2 a 3.2.3).
B (1.2)	18. 07. 2024	RNDr. Ota ZÁHORA Ing. Ondřej PROKŮPEK	• Doplnění SSVÚ do rozsahu působnosti (kapitola 1). • Upřesnění jedinečnosti jmen ve vydávaných certifikátech (kapitola 3.1.5). • Úpravy požadavků na zabezpečení soukromých klíčů na straně AIS (kapitoly 4.4 a 4.5). • Upřesnění zabezpečení CA DIA (kapitola 6.5). • Úpravy profilu vydávaných certifikátů (kapitoly 7.1.1.6 a 7.1.2.9).

OBSAH

Veřejný řídicí dokument.
“Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.”

1. Úvod

Tato certifikační politika definuje podmínky pro vydávání certifikátů pro agendové informační systémy a soukromoprávní systémy pro využívání údajů za účelem zabezpečení jejich komunikace se systémy, které poskytují služby referenčního rozhraní veřejné správy, a za účelem zabezpečení jejich vzájemné komunikace.

Pokud je v dokumentu uvedeno "AIS", myslí se tím jak AIS tak SSVÚ.

1.1 Název a jednoznačné určení dokumentu

Tento dokument má název:

CERTIFIKAČNÍ POLITIKA
DIGITÁLNÍ A INFORMAČNÍ AGENTURY
PRO CERTIFIKÁTY VYDÁVANÉ PRO AIS

Zkratka názvu dokumentu je: CP CADIA AIS

OID dokumentu je: 1.2.203.17651921.2.10.1.2

1.2 Rozsah působnosti

Politika je závazná pro správce AIS, pro správce systémů, které tvoří referenční rozhraní veřejné správy, a pro všechny zaměstnance DIA, kteří se podílejí na poskytování certifikačních služeb.

1.3 Zkratky a pojmy

AIS - Agendový informační systém (AIS) je informační systém, který má podle zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů přístup do základních registrů.

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

CA – Certifikační autorita.

CAAIS - Centrální autentizační a autorizační informační systém. Jde o adresář uživatelů, který postupně nahradí JIP.

CA DIA – CA, která vydává certifikáty pro AIS.

CP - Certifikační politika je množina pravidel, která definuje 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 elektronická datová struktura podepsaná certifikační autoritou, která spojuje veřejný klíč s určitou entitou a potvrzuje identitu této entity. Identifikace entity je uvedená v předmětu certifikátu.

CRL - Certificate Revocation List je seznam sériových čísel zneplatněných certifikátů.

DIA - Digitální a informační agentura.

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

Držitel certifikátu – orgán veřejné moci nebo soukromoprávní uživatel údajů podle zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů.

FAIS - Formulářový agendový informační systém je informační systém určený ke zpracování formulářových dotazů zadávaných prostřednictvím systému datových schránek.

FQDN - **Fully Qualified Domain Name**. Plně specifikované doménové jméno.

ISSS - **Informační systém sdílené služby** je unifikované rozhraní pro sdílení údajů mezi AIS. Dříve eGSB.

ISZR - **Informační systém základních registrů** je aplikace, která zprostředkovává přístup AIS k základním registrům.

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

IT – informační technologie.

JIP – jednotný identitní prostor. 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, tj. soukromý a veřejný klíč.

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 DIA – Certifikační autorita DIA, Validační autorita DIA a Registrační autorita DIA určené pro vydávání a ověřování certifikátů.

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

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

RPP - **Registr práv a povinností**. Jeden ze základních registrů.

Referenční rozhraní veřejné správy - komunikační rozhraní pro poskytování a využívání služeb poskytovaných nebo zprostředkovaných ISZR, ISSS a FAIS.

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 DIA. 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 DIA, respektive v evidenci vedené mimo DIA orgánem státní správy, respektive pověřeným subjektem, jako správce příslušného AIS.

SSVÚ - soukromoprávní systém pro využívání údajů. Informační systém, který splňuje požadavky pro přístup do základních registrů anebo do ISSS a jeho správcem je soukromoprávní subjekt, např. banka.

VA - Validační autorita poskytuje informace o platnosti certifikátů vydaných CA DIA.

Webové stránky DIA - Sekce SZR, www.szrcr.cz

Zaměstnanec – zaměstnanec DIA nebo osoba, která je vůči DIA 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 DIA je dvouúrovňová. Vrchol tvoří kořenová certifikační autorita DIA (Root CA DIA). Kořenová certifikační autorita vydává certifikáty pouze podřízeným certifikačním autoritám a vydala tedy i certifikát pro certifikační autoritu CA DIA, pro kterou je určena tato certifikační politika.

1.4.2 Registrační autorita

CA DIA poskytuje své služby prostřednictvím RA DIA.

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

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

Účast jiných registračních autorit se nepřipouští.

1.4.3 Validační autorita

PKI DIA poskytuje služby ověřování platnosti certifikátů prostřednictvím VA DIA.

VA DIA poskytuje seznam odvolaných certifikátů (CRL).

1.4.4 Držitel certifikátu

Držitel certifikátu je správce AIS, kterému byl certifikát vydaný. 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) správce ISSS;
d) správci dalších systémů, které jsou součástí referenčního rozhraní veřejné správy.

1.4.6 Jiné zúčastněné subjekty

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

1.5 Použití certifikátů

1.5.1 Přípustné použití certifikátů

ISZR, ISSS a další systémy, které jsou součástí referenčního rozhraní veřejné správy, 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 jsou součástí referenčního rozhraní veřejné správy, a navazování šifrovaného spojení s nimi.

Vzájemná autentizace AIS a navázání šifrovaného spojení mezi nimi s použitím certifikátů vydaných CA DIA je povolená, ale pro jejich skutečné použití vždy musí být zváženo, zda certifikáty vydané CA DIA 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 DIA.

1.6.2 Kontaktní osoby

Kontaktní osoby určuje ředitel DIA.

Aktuální kontaktní údaje jsou uvedeny na webových stránkách DIA.

Adresa pro komunikaci elektronickou poštou je podpora@dia.gov.cz.

1.6.3 Odpovědná osoba

Osobou odpovědnou za tuto politiku a uplatňování jejích ustanovení je osoba určená ředitelem DIA.

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 ředitelem DIA.

2. Odpovědnosti za zveřejňování a úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

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

DIA má neveřejné a veřejné úložiště informací a dokumentace.

2.2 Zveřejňování informací a dokumentace

Za zveřejňování informací a dokumentace o PKI DIA odpovídá DIA.

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

CA DIA zveřejňuje minimálně následující informace:

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

CA DIA zveřejňuje následující informace pro spoléhající se strany:

a) certifikát Root CA DIA a certifikát CA DIA;
b) seznam zneplatněných certifikátů (CRL) vydaných CA DIA.

Údaje jsou zveřejňovány buď přímo na webových stránkách DIA, nebo je na těchto stránkách uveden odkaz na tyto údaje, nebo jsou distribuovány přímo uživatelům PKI DIA.

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 DIA jsou zveřejněna při každé změně.

Umístění VA DIA je zveřejněno při každé změně.

Informace vztahující se k PKI DIA 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 předchozího vydaného CRL.

2.4 Řízení přístupu k jednotlivým typům úložišť

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

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

3. Identifikace a autentizace

3.1 Pojmenování

3.1.1 Typy jmen

Všechny certifikáty vydávané CA DIA 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 DIA 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 DIA 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 DIA 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 DIA považují všechny žádosti o vydání certifikátu pro AIS se stejnou identifikací AIS v předmětu certifikátu za žádosti pro tentýž AIS.

CA DIA zaručuje ve vydávaných certifikátech jedinečnost následujících jmen:

- označení vydavatele (Issuer) je jedinečné mezi všemi CA, které spravuje DIA;
- CA DIA nevydá dvěma různým žadatelům certifikát se stejným předmětem (Subject, viz 7.1.1.6).

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

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

3.2.3 Ověřování identity fyzické osoby

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

V případě telefonicky nebo osobně podaného požadavku na zneplatnění certifikátu ověřují pracovníci RA DIA 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 DIA 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

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

DIA 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 DIA s jinými poskytovateli certifikačních služeb je možná až po schválení ředitelem DIA.

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 DIA 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

DIA 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 DIA.

b) CA DIA 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 DIA 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 DIA.

RA DIA žádost o vydání certifikátu přijme a zaeviduje ji.

RA DIA zkontroluje údaje ve formuláři i v žádosti o certifikát. Pokud jsou údaje chybné nebo neúplné, RA DIA 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 DIA předá žádost o certifikát na CA DIA.

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 DIA 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 DIA;
c) předá certifikát RA DIA.

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

4.3.2 Oznámení o vydání certifikátu držiteli

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

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

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 DIA. V opačném případě je žadatel povinen certifikát převzít.

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

Žadatel o certifikát se převzetím certifikátu stává držitelem certifikátu.

Žadatel nainstaluje certifikát do prostředí vlastní infrastruktury.

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

4.4.2 Zveřejňování vydaných certifikátů certifikační autoritou

CA DIA nezveřejňuje vydané certifikáty ani údaje (mimo CRL) o vydaných certifikátech s výjimkou certifikátů vydaných pro ISZR a ISSS.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

DIA neuveřejňuje žádné informace (mimo CRL) o certifikátech vydaných podle této CP s výjimkou certifikátů vydaných pro ISZR a ISSS.

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 proti neoprávněnému přístupu (např. heslem).
- Subjekt nepoužije soukromý klíč ani certifikát pro jiný účel než pro provoz příslušného AIS.
- Subjekt nainstaluje soukromý klíč a certifikát pouze na ta zařízení, která jsou nezbytná pro zajištění komunikace AIS s ISZR, nebo s jiným systémem poskytujícím služby referenčního rozhraní veřejné správy, nebo s jiným AIS.
- Subjekt nebude vytvářet další kopie soukromého klíče (tj. mimo kopií uvedených v předcházejícím bodu).
- Soukromý klíč a certifikát budou na zařízeních uloženy tak, aby byla zabezpečena jejich důvěrnost. To znamená, že přístup k soukromému klíči je chráněn technickými nebo programovými prostředky.
- Uživatelské přístupy k soukromému klíči, případně k zařízením se soukromým klíčem, a operace s ním jsou automaticky protokolovány technickými nebo programovými 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 DIA 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 DIA 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 DIA:

a) získaly certifikáty používané CA DIA a Root CA DIA při vydávání certifikátů z bezpečného zdroje a ověřily otisk těchto certifikátů;
b) ověřily platnost certifikátů CA DIA a Root CA DIA;
c) AIS navíc:
    - v případě komunikace s ISZR nebo jiným systémem poskytujícím služby referenčního rozhraní veřejné správy ověří platnost certifikátu vydaného

CA DIA pro příslušný systém a ověří, že byl skutečně vydán pro příslušný systém;
- v případě komunikace s jiným AIS ověří platnost certifikátu vydaného CA DIA pro jiný AIS a ověřil, že byl skutečně vydán pro příslušný AIS;

d) ISZR navíc:
- ověří platnost certifikátu vydaného CA DIA pro AIS a že byl skutečně vydán pro příslušný AIS;
- ověří, zda certifikát vydaný pro AIS nebyl dočasně zablokován, viz kapitolu 4.9.

e) ISSS navíc:
- ověří platnost certifikátu vydaného CA DIA pro AIS a že byl skutečně vydán pro příslušný AIS.

4.6 Obnovení certifikátu

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

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

4.6.1 Podmínky pro obnovení certifikátu

PKI DIA tuto službu neposkytuje.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

PKI DIA tuto službu neposkytuje.

4.6.3 Zpracování požadavku na obnovení certifikátu

PKI DIA tuto službu neposkytuje.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

PKI DIA tuto službu neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu držitelem

PKI DIA tuto službu neposkytuje.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

PKI DIA tuto službu neposkytuje.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

PKI DIA 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.

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

4.8.1 Podmínky pro změnu údajů v certifikátu

PKI DIA tuto službu neposkytuje.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

PKI DIA tuto službu neposkytuje.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

PKI DIA tuto službu neposkytuje.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

PKI DIA tuto službu neposkytuje.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji držitelem

PKI DIA tuto službu neposkytuje.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji certifikační autoritou

PKI DIA tuto službu neposkytuje.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

PKI DIA tuto službu neposkytuje.

4.9 Zneplatnění a pozastavení platnosti certifikátu

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

PKI DIA 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 DIA;
j) RA DIA 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) DIA.

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 DIA:
b) telefonicky nebo osobně, v tomto případě musí držitel certifikátu požadavek na zneplatnění certifikátu potvrdit zasláním žádosti prostřednictvím aplikace, kterou určila DIA.

RA DIA 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 DIA žádost o zneplatnění certifikátu přijme a zaeviduje ji.

RA DIA 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 DIA provede jednu z následujících akcí:

- pokud DIA obdržela žádost o zneplatnění prostřednictvím aplikace, kterou určila DIA, pošle do datové schránky žadatele a do aplikace, kterou určila DIA, informaci o důvodu odmítnutí žádosti;
- pokud správce AIS žádá o zneplatnění certifikátu osobně nebo telefonicky, RA DIA odmítne žádost přijmout.

Pokud jsou údaje úplné a správné, RA DIA zablokuje přístup AIS k ISZR s použitím dotyčného certifikátu (ale zatím ho nezneplatní) a provede jednu z následujících akcí:

- pokud DIA obdržela žádost o zneplatnění prostřednictvím aplikace, kterou určila DIA, předá certifikát CA DIA k zneplatnění;
- pokud DIA obdržela žádost o zneplatnění certifikátu osobně nebo telefonicky, čeká na zneplatnění do doby, než dostane žádost o zneplatnění certifikátu prostřednictvím aplikace, kterou určila DIA.

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

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

4.9.3.2 Zneplatnění certifikátu z jiných důvodů

Pokud DIA potřebuje zneplatnit certifikát z jiných důvodů, než je žádost držitele certifikátu, postupuje takto:

a) pokud je nutné okamžitě zakázat používat certifikát pro přístup k ISZR, zablokuje RA DIA použití certifikátu pro přístup do základních registrů;
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 DIA zablokuje použití certifikátu pro přístup k ZR (pokud již není zablokován), CA DIA certifikát zneplatní a RA DIA 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 CA DIA a Root CA DIA. 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 DIA 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 nebo ISSS, je CRL vydán bezprostředně po zneplatnění certifikátu ISZR, respektive ISSS.

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 DIA tuto službu neposkytuje.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

PKI DIA tuto službu neposkytuje.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

PKI DIA 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 DIA tuto službu neposkytuje.

4.9.14 Subjekty oprávněné žádat o pozastavení platnosti certifikátu

PKI DIA tuto službu neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

PKI DIA tuto službu neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

PKI DIA tuto službu neposkytuje.

4.10 Služby ověření stavu certifikátu

4.10.1 Funkční charakteristiky

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

4.10.2 Dostupnost služeb

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

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

4.12 Úschova a obnovení soukromého klíče

PKI DIA 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 DIA se žádným způsobem nepodílí na ukládání ani zálohování soukromých klíčů k vydávaným certifikátům.

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

Prostory PKI DIA 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 DIA 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 DIA.

5.1.4 Vliv vody

Objekty, ve kterých jsou zařízení PKI DIA umístěna, jsou chráněny proti nežádoucím vlivům vody na provoz PKI DIA, 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 DIA 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 DIA.

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 DIA 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 DIA.

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 DIA zastávající důvěryhodné role musí splňovat:

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

5.3.2 Posouzení spolehlivosti osob

Řídí se interními předpisy DIA.

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

DIA nevyžaduje ani nepořádá pravidelná školení pracovníků PKI DIA.

DIA zajišťuje seznámení pracovníků PKI DIA s novými relevantními předpisy.

DIA pořádá školení pracovníků PKI DIA 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 DIA.

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 DIA 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 DIA, a na systémech, na kterých je provozována RA DIA;
g) provedení zálohy a obnovy CA DIA;
h) start a zastavení CA DIA;
i) konfigurační změny CA DIA.

5.4.2 Periodicita zpracování záznamů

Četnost kontroly a vyhodnocování záznamů jsou definovány interními předpisy DIA. 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 DIA interní, tj. události se zaznamenávají v rámci prostředí PKI DIA.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

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

5.4.8 Hodnocení zranitelnosti

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

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 DIA:

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

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

c) generování dalších klíčových párů pro CA DIA a Root CA DIA;
d) zničení klíčových párů pro CA DIA nebo Root CADIA;
e) aktualizované dokumenty PKI DIA, 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 CADIA. Při ukončení činnosti CA DIA 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 DIA interní, tj. informace a dokumentace se zaznamenávají v rámci prostředí PKI DIA.

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 DIA. Jiné osoby pouze na základě písemného povolení ředitele DIA.

5.6 Výměna veřejného klíče

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

Po ukončení platnosti je soukromý klíč CA 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 DIA 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 DIA kontinuitu činnosti podle plánů kontinuity.

Dále provede DIA obnovu stavu prostředků PKI DIA do původního stavu podle havarijních plánů.

5.7.3 Postup při kompromitaci soukromého klíče

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

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

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

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

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

Za kompromitaci podepisovacího klíče CA DIA 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 DIA motivováno organizačními hledisky nebo jinými důvody, které nesouvisí s bezpečností CA DIA, pak lze certifikáty vydané CA DIA nadále používat (dle uvážení držitelů certifikátů). Držitelé certifikátů musí zejména vzít v úvahu, že CA nebude aktualizovat seznam odvolaných certifikátů (CRL).

DIA provede při ukončení činnosti CA DIA následující akce:

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

5.8.2 Ukončení činnosti RA

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

5.8.3 Ukončení činnosti VA

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

V případě ukončení činnosti VA provede DIA 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 DIA pro podepisování vydaných certifikátů a popis použitých technických prostředků je uveden v technické dokumentaci PKI DIA.

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 DIA předáván žadatelem o certifikát elektronicky doručením souboru ve formátu PKCS#10 a kódování PEM prostřednictvím aplikace, kterou určila DIA.

6.1.4 Poskytování veřejných klíčů certifikační autoritou spoléhajícím se stranám

CA DIA neposkytuje veřejné klíče držitelů certifikátů spoléhajícím se stranám.

6.1.5 Délky klíčů

CA DIA používá algoritmus RSA a délky klíčů 3072 bitů a delší.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

CA DIA kontroluje veřejné klíče v žádostech o vydání certifikátu:

a) pokud obdrží klíč, který je již použitý v jiném certifikátu vydaném CA DIA, 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 DIA 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 DIA 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 DIA je uchováván tak, aby bylo možné jeho použití, a je současně chráněn proti neoprávněnému přístupu.

6.2.4 Zálohování soukromého klíče

PKI DIA vytváří záložní kopie soukromých klíčů všech certifikačních autorit DIA. 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 DIA 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 DIA archivuje vydané certifikáty po celou dobu činnosti PKI DIA.

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 DIA 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.

Servery CA DIA jsou určené pouze pro provoz CA. Nejsou na nich provozovány žádné jiné aplikace.

6.5.2 Hodnocení počítačové bezpečnosti

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

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

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

6.6.2 Kontroly řízení bezpečnosti

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

6.6.3 Řízení bezpečnosti životního cyklu

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

6.7 Síťová bezpečnost

Servery CA DIA jsou umístěny v zabezpečeném segmentu počítačové sítě a přístup k nim je řízen a kontrolován na síťové úrovni. Na serverech CA DIA 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 DIA 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.
CA vydává certifikáty podle normy X.509 verze 3.

7.1.1.2 Serial number

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

7.1.1.3 Signature algorithm

„sha384RSA“
Hodnotu definuje CA.

7.1.1.4 Issuer

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

7.1.1.5 Validity

Doba platnosti certifikátu.

Not before - CA dosadí čas vydání certifikátu.

Not after - CA dosadí čas vydání certifikátu plus 3 roky. CA 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 dosadí hodnotu z žádosti o certifikát.
V případě, že certifikát bude používaný pro publikaci dat AIS na ISSS, musí být v CN nebo SAN uvedené FQDN z domény cms2.cz.
V ostatních případech je položka nepovinná.

Maximální povolená délka je 64 znaků.

O = Označení (identifikace) žadatele o certifikát.
CA dosadí hodnotu z žádosti o certifikát.
Položka je povinná. Musí být uvedeno IČO správce AIS nebo identifikátor správce AIS v RPP, pokud správce AIS nemá IČO.
Maximální povolená délka je 64 znaků.

OU = Označení (identifikace) AIS.
CA dosadí hodnotu z žádosti o certifikát.
Položka je povinná. Musí být uvedeno číslo AIS z RPP doplněné o informaci, že jde o certifikát pro přístup do produkčního prostředí základních registrů.
Příklad: 567/PROD
Pokud se jedná o certifikát určený pro publikaci na ISSS, je doplněné o příznak "P", např. 567-P/PROD
Maximální povolená délka je 64 znaků.

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

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

C = Stát.
CA dosadí hodnotu z žádosti o certifikát.
Položka je nepovinná. Pokud je uvedená, musí obsahovat platný kód státu Evropské unie.

7.1.1.7 Subject Public key info

Informace o veřejném klíči.

Algorithm – CA dosadí hodnotu rsaEncryption.

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

7.1.1.8 Signature

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

7.1.2 Rozšiřující položky certifikátu

7.1.2.1 Authority key identifier

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

7.1.2.2 Subject key identifier

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

7.1.2.3 CRL Distribution Points

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

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.

7.1.2.5 Enhanced key usage

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

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.

7.1.2.7 Certificate template name

Označení šablony, podle které byl certifikát vydaný.
Hodnotu definuje CA.

7.1.2.8 Application policies

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

7.1.2.9 Subject Alternative Name

Alternativní označení předmětu certifikátu.
V případě, že certifikát bude používaný pro publikaci dat AIS na ISSS, musí být v CN nebo SAN uvedené FQDN z domény cms2.cz.
V ostatních případech je položka nepovinná.
Maximální povolená délka je 64 znaků.
CA dosadí hodnotu z žádosti o certifikát.

7.1.3 Objektové identifikátory algoritmů

Pro vydávání certifikátů se používá schéma sha384WithRSAEncryption (OID 1.2.840.113549.1.1.12).

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 uvedený v kapitole 1.1.

V certifikátech vydávaných CA se nepoužívá.

7.1.7 Rozšíření „Policy Constraints“

V certifikátech vydávaných CA se nepoužívá.

7.1.8 Syntaxe a schémata rozšíření „Policy Qualifiers“

V certifikátech vydávaných CA se nepoužívá.

7.1.9 Zpracování kritického rozšíření „Certificate Policies“

V certifikátech vydávaných CA se nepoužívá.

7.2 Profil CRL

7.2.1 Položky CRL

7.2.1.1 Version

„2“
Hodnotu definuje CA.

7.2.1.2 Signature algorithm

„sha384RSA“
Hodnotu definuje CA.

7.2.1.3 Issuer

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

7.2.1.4 This update

CA dosadí čas vydání CRL.

7.2.1.5 Next update

CA dosadí předpokládaný čas vydání příštího CRL.

7.2.1.6 Revoked certificates

CA 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.

7.2.2.2 CRL number

Pořadové číslo seznamu zneplatněných certifikátů.
Hodnotu definuje CA.

7.2.2.3 Delta CRL indicator

Rozšíření informuje o tom, že jde o rozdílový seznam zneplatněných certifikátů.
Hodnotu dosadí CA 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 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 DIA rozhoduje ředitel DIA. Provádí se v případě vážného bezpečnostního incidentu, v případě významných změn v oblasti kryptografie, v případě významných změn uvnitř DIA 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 DIA.

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

8.4 Hodnocené oblasti

Hodnocenými oblastmi jsou zejména:

a) certifikační politika;
b) ostatní navazující dokumentace;
c) uplatňování ustanovení certifikační politiky a ostatní bezpečnostní dokumentace;
d) technické aspekty provozu PKI DIA;
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 DIA.

8.5 Postup v případě zjištění nedostatků

Pokud hodnotitel zjistí během auditu zvlášť závažné nedostatky, které podle jeho názoru bezprostředně ohrožují bezpečnost PKI DIA, je jeho povinností to sdělit řediteli DIA a povinností ředitele DIA 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 řediteli DIA bez zbytečného prodlení po ukončení hodnocení. Procesní lhůty upravuje kontrolní řád.

Ředitel DIA zajistí projednání zprávy uvnitř DIA 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 DIA neúčtuje žádné poplatky.

9.1.2 Poplatky za přístup k certifikátu

DIA 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 DIA neúčtuje žádné poplatky.

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

9.1.4 Poplatky za další služby

DIA neúčtuje za PKI služby žádné poplatky.

9.1.5 Jiná ustanovení týkající se poplatků

Žádná opatření.

9.2 Finanční odpovědnost

DIA není finančně nijak odpovědná uživatelům certifikátů vydaných CA DIA.

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 DIA považuje zejména:

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

9.3.2 Informace mimo rámec citlivých informací

DIA 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 DIA podílí na provozu PKI DIA.

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 DIA.

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 DIA podílí na provozu PKI DIA.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

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

9.4.6 Poskytování osobních údajů pro soudní nebo správní účely

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

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva na ochranu duševního vlastnictví

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

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

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA DIA

CA DIA zastupuje ředitel DIA a osoby jím určené.

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

9.6.2 Zastupování a záruky RA DIA

RA DIA zastupuje ředitel DIA a osoby jím určené.

DIA zaručuje, že RA DIA 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 DIA je vymezena platnými a účinnými právními předpisy a touto CP.

9.9 Odpovědnost za škodu, náhrada škody

Odpovědnost DIA 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 DIA 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 ředitele DIA;

b) ukončením činnosti PKI DIA.

9.10.3 Důsledky ukončení a přetrvávání závazků

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

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

9.11 Komunikace mezi zúčastněnými subjekty

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

9.12 Změny CP

9.12.1 Postup při změnách

Změna CP je řízený proces definovaný v interní dokumentaci DIA.

9.12.2 Postup při oznamování změn

Nová verze CP bude oznámena a publikována na webových stránkách DIA .

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 DIA.

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 DIA 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 DIA 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

DIA neodpovídá za porušení svých povinností vyplývajících z této CP způsobených událostmi, které není v moci DIA 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 DIA certifikáty podle této politiky. Tento dokument je veřejný a je v platné verzi uložen také na webových stránkách DIA.