


SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU		
	SZRAX0041X9K prvotní identifikátor	
	SZR-423-2/Ř-2023	
	PD023B-2023	
PROVOZNÍ DOKUMENT	počet stran	60
	přílohy	0

NCA – Certifikační prováděcí směrnice

(kryptografie RSA)

Oblast působnosti:

Zaměstnanci Správy státních služeb vytvářejících důvěru, vybraných subjektů veřejné správy, mezi které patří bezpečnostní složky, zpravodajské služby a vybrané útvary resortu Ministerstva vnitra.

Gestor: Ing. Josef SCHOVAJSA	Nahrazuje: PD023A-2023 / v 1.01
Zpracovatel: První certifikační autorita, a.s.	Klasifikace: VEŘEJNÝ
Odborný garant: RNDr. Miroslav ŠEDIVÝ	Schváleno dne: 23. 11. 2023
Schvalovatel: <i>podepsáno elektronicky</i> Ing. Michal PEŠEK	Účinnost od dne: 23. 11. 2023

HISTORIE DOKUMENTU:

ID	Verze	Datum	Autor	Popis
-	1.00	15. 9. 2023	První certifikační autorita, a.s.	Vytvoření první verze dokumentu.
A	1.01	27. 9. 2023	První certifikační autorita, a.s.	Změna zkratky
B	1.02	23. 11. 2023	První certifikační autorita, a.s.	Zpracovány připomínky auditora a orgánu dohledu.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

OBSAH

1.	Úvod	6
1.1	Přehled	6
1.2	Název a jednoznačné určení dokumentu	7
1.3	Participující subjekty	7
1.4	Použití certifikátu	8
1.5	Správa politiky	9
1.6	Přehled použitých pojmů a zkratk	9
2.	Odpovědnost za zveřejňování a za úložiště	14
2.1	Úložiště.....	14
2.2	Zveřejňování certifikačních informací.....	14
2.3	Čas nebo četnost zveřejňování	14
2.4	Řízení přístupu k jednotlivým typům úložišť	15
3.	Identifikace a autentizace	16
3.1	Pojmenování.....	16
3.2	Počáteční ověření identity.....	16
3.3	Identifikace a autentizace při požadavku na výměnu klíče	17
3.4	Identifikace a autentizace při požadavku na zneplatnění certifikátu	17
4.	Požadavky na životní cyklus certifikátu	19
4.1	Žádost o vydání certifikátu	19
4.2	Zpracování žádosti o certifikát	19
4.3	Vydání certifikátu	19
4.4	Převzetí vydaného certifikátu	20
4.5	Použití párových dat a certifikátu	20
4.6	Obnovení certifikátu	21
4.7	Výměna veřejného klíče v certifikátu.....	21
4.8	Změna údajů v certifikátu.....	22
4.9	Zneplatnění a pozastavení platnosti certifikátu	23
4.10	Služby ověřování stavu certifikátu.....	25
4.11	Konec smlouvy o vydávání certifikátů	26
4.12	Úschova a obnova klíčů.....	26
5.	Postupy správy, řízení a provozu	27
5.1	Fyzická bezpečnost	27
5.2	Procedurální postupy	28
5.3	Personální postupy	29
5.4	Postupy zpracování auditních záznamů.....	31
5.5	Uchovávání záznamů	32

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

5.6	Výměna klíče	33
5.7	Obnova po havárii nebo kompromitaci.....	34
5.8	Ukončení činnosti CA nebo RA.....	34
6.	Řízení technické bezpečnosti.....	36
6.1	Generování a instalace párových dat.....	36
6.2	Ochrana soukromého klíče a technologie kryptografických modulů	37
6.3	Další aspekty správy párových dat.....	40
6.4	Aktivační data	40
6.5	Řízení počítačové bezpečnosti	41
6.6	Technické řízení životního cyklu	43
6.7	Řízení bezpečnosti sítě.....	44
7.	Profily certifikátu, seznamu zneplatněných certifikátů a OCSP.....	46
7.1	Profil certifikátu	47
7.2	Profil seznamu zneplatněných certifikátů	48
7.3	Profil OCSP	48
8.	Hodnocení shody a jiná hodnocení	53
8.1	Periodicita nebo okolnosti hodnocení.....	53
8.2	Identita a kvalifikace hodnotitele	53
8.3	Vztah hodnotitele k hodnocenému subjektu.....	53
8.4	Hodnocené oblasti	53
8.5	Postup v případě zjištění nedostatků	53
8.6	Sdělování výsledků hodnocení	53
9.	Ostatní obchodní a právní záležitosti	54
9.1	Poplatky.....	54
9.2	Finanční odpovědnost.....	54
9.3	Důvěrnost obchodních informací	54
9.4	Ochrana osobních údajů.....	55
9.5	Práva duševního vlastnictví	56
9.6	Zastupování a záruky.....	56
9.7	Zřeknutí se záruk	57
9.8	Omezení odpovědnosti	57
9.9	Záruky a odškodnění	57
9.10	Doba platnosti, ukončení platnosti	58
9.11	Individuální upozorňování a komunikace se zúčastněnými subjekty	59
9.12	Novelizace	59
9.13	Ustanovení o řešení sporů.....	59
9.14	Rozhodné právo	59

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

9.15	Shoda s platnými právními předpisy	59
9.16	Různá ustanovení	60
9.17	Další ustanovení	60

1. Úvod

Tento dokument rozpracovává a upřesňuje zásady z konkrétních certifikačních politik (dále též CP), které státní příspěvková organizace Správa státních služeb vytvářejících důvěru (dále též Správa), na kterou podle § 14 zákona č. 297/2016 Sb. přešly práva a povinnosti týkající se služeb vytvářejících důvěru od organizační složky státu Správa základních registrů, jako provozovatel Národní certifikační autority (dále též NCA), kvalifikovaný poskytovatel služeb vytvářejících důvěru, uplatňuje při poskytování kvalifikovaných služeb vytvářejících důvěru, služeb vytvářejících důvěru a při vydávání dalších typů certifikátů (dále též Služby). Pro Služby poskytované podle této certifikační prováděcí směrnice (dále též CPS), resp. příslušných certifikačních politik je využíván algoritmus RSA.

Služby, pokud je to relevantní, jsou poskytovány nediskriminačně, včetně jejich zpřístupnění pro osoby se zdravotním postižením. Podrobnosti jsou popsány v interní dokumentaci:

„NCA – Směrnice pro pracovníky RA“.

Právní požadavky na Službu jsou definovány:

nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS),

zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů

zákonem České republiky č. 471/2022 Sb., kterým se mění zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů, a další související zákony, ze dne 23. prosince 2022 (dále též „transformační zákon“).

Pozn.: Jsou-li v dalším textu uváděny odkazy na technické standardy, normy nebo zákony, jedná se vždy buď o uvedený technický standard, normu nebo zákon, resp. o technický standard, normu či zákon, který je nahrazuje. Pokud by byl tento dokument v rozporu s aktuálně platnými standardy, normami nebo zákony, bude vydána jeho nová verze.

1.1 Přehled

Dokument **NCA – Certifikační prováděcí směrnice (kryptografie RSA)** se zabývá skutečnostmi vztahujícími se k procesům životního cyklu Certifikátů a striktně dodržuje strukturu, jejíž předlohou je osnova platného standardu RFC 3647, s přihlédnutím k platným technickým standardům a normám Evropské unie a k právu České republiky v dané oblasti (jednotlivé kapitoly jsou proto v tomto dokumentu zachovány i v případě, že jsou ve vztahu k ní irelevantní). Dokument je rozdělen do devíti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

Kapitola 1 identifikuje tento dokument přiřazeným jedinečným identifikátorem, obecně popisuje subjekty participující na poskytování Služby a definuje přípustné využívání vydávaných Certifikátů.

Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.

Kapitola 3 popisuje procesy identifikace a autentizace žadatele o vydání Certifikátu, resp. zneplatnění Certifikátu, včetně definování typů a obsahů používaných jmen ve vydávaných Certifikátech.

Kapitola 4 definuje procesy životního cyklu jí vydávaných Certifikátů, tzn. žádost o vydání a vlastní vydání Certifikátu, žádost o zneplatnění a vlastní zneplatnění Certifikátu, služby související s ověřováním stavu Certifikátu, ukončení poskytování Služby atd.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchování těchto záznamů a reakce po haváriích nebo kompromitaci.

Kapitola 6 je zaměřena na technickou bezpečnost typu generování veřejných a soukromých klíčů, ochrany soukromých klíčů, včetně počítačové a síťové ochrany.

Kapitola 7 definuje profil vydávaných Certifikátů a seznamů zneplatněných certifikátů.

Kapitola 8 je zaměřena na problematiku hodnocení poskytované Služby.

Kapitola 9 zahrnuje problematiku obchodní a právní.

1.2 Název a jednoznačné určení dokumentu

Název tohoto dokumentu: NCA – Certifikační prováděcí směrnice (kryptografie RSA), verze 1.02

OID politiky: není přiřazen

Tato CPS se vztahuje k následujícím CP*:

OID	CP
1.2.203.19122063.10.1.10.x.y	Certifikační politika kořenové certifikační autority (algoritmus RSA)
1.2.203.19122063.10.1.30.x.y	Certifikační politika vydávání kvalifikovaných certifikátů pro ověřování elektronických podpisů (kryptografie RSA)
1.2.203.19122063.10.1.31.x.y	Certifikační politika vydávání kvalifikovaných certifikátů pro ověřování elektronických pečeti (kryptografie RSA)
1.2.203.19122063.10.1.32.x.y	Certifikační politika vydávání certifikátů pro systém TSA (kryptografie RSA)
1.2.203.19122063.10.1.71.x.y	Certifikační politika vydávání komerčních certifikátů fyzickým osobám (kryptografie RSA)
1.2.203.19122063.10.1.72.x.y	Certifikační politika vydávání komerčních technologických certifikátů (kryptografie RSA)
1.2.203.19122063.10.1.80.x.y	Certifikační politika vydávání certifikátů pro OCSP respondéry (kryptografie RSA)

* Vždy se jedná o aktuální verzi politiky ve tvaru x.yz, která je vystavena na webu Správy (viz kapitola 2.2), přičemž x a y jsou součástí OID politiky.

Služba vydávání kvalifikovaných certifikátů je v souladu s nařízením eIDAS zařazena na důvěryhodném seznamu udržovaném orgánem dohledu.

1.3 Participující subjekty

1.3.1 Certifikační autority (dále "CA")

1.3.1.1 Kořenová certifikační autorita

Kořenová certifikační autorita NCA vydala ve dvoustupňové struktuře certifikačních autorit, v souladu s platnou právní úpravou a s požadavky technických standardů a norem, certifikát podřízené certifikační autoritě provozované Správou a svému OCSP respondéru. Tato autorita vydává certifikáty koncovým uživatelům a pro vlastní OCSP respondéry.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Kořenová certifikační autorita je ve stavu off-line a v žádném okamžiku tedy nemá propojení s externí sítí. Ve stavu on-line je pouze její OCSP respondér. Fyzicky je její informační systém realizován vyhrazenými počítači.

1.3.1.2 Vydávající certifikační autorita

Certifikační autorita provozovaná Správou poskytující Služby koncovým uživatelům a systému TSA.

1.3.2 Registrační autority (dále "RA")

Poskytování služeb vytvářejících důvěru Správou se realizuje prostřednictvím registračních autorit, které jsou vlastní, nebo smluvní (poskytují služby svým zaměstnancům). Tyto RA:

Přijímají žádosti o služby uvedené v této CP, zejména přijímají žádosti o vydání Certifikátu, zprostředkovávají předání Certifikátů a seznamů zneplatněných certifikátů, poskytují potřebné informace, přijímají reklamace atd.

Jsou oprávněny z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti.

Jsou zmocněny jménem Správy uzavírat smlouvy o poskytování Služby.

V případě smluvní RA plní tato jménem Správy obdobné funkce jako vlastní RA, a to na základě písemné smlouvy mezi Správou a provozovatelem smluvní RA.

1.3.3 Držitelé certifikátů

1.3.3.1 Certifikáty poskytovatele

Certifikáty jsou vydávány výhradně pro certifikační autority, jejich OCSP respondéry a pro časové servery autorit časových razítek, vše provozované Správou. Oprávněným žadatelem a následně držitelem certifikátů je Správa. Dále jsou fyzickým osobám, zaměstnancům Správy a zaměstnancům smluvních partnerů vydávány infrastrukturní certifikáty.

1.3.3.2 Certifikáty koncových uživatelů

Certifikáty jsou vydávány koncovým uživatelům, využívajícím certifikační služby Správy.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na certifikáty vydávané v rámci poskytování Služeb.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dohledu a další, kterým to podle právní úpravy pro služby vytvářející důvěru přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty kořenové CA smějí být používány výhradně pro ověřování jí vydaných certifikátů, seznamů jí zneplatněných certifikátů (CRL, resp. ARL) a OCSP odpovědí vydaných jejím OCSP respondérem.

Certifikáty vydávajících certifikačních autorit smějí být používány výhradně pro ověřování certifikátů a seznamů zneplatněných certifikátů (CRL) vydaných těmito vydávajícími

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

certifikačními autoritami a OCSP odpovědi vydaných OCSP respondéry (jsou-li implementovány) těchto vydávajících certifikačních autorit.

Certifikáty časových serverů autorit časových razítek smějí být používány výhradně pro ověřování časových razítek vydaných těmito časovými servery.

Certifikáty koncových uživatelů smějí být používány obecně v procesech PKI, tedy ověřování elektronických podpisů a elektronických pečeti, pro identifikaci, autentizaci a šifrování.

1.4.2 Zakázané použití certifikátu

Certifikáty vydávané v souladu s konkrétní CP nesmějí být používány v rozporu s použitím popsáním v této CP a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující dokument

Tuto CPS a jí odpovídající certifikační politiky spravuje Správa.

1.5.2 Kontaktní osoba

Kontaktní osobou Správy v souvislosti s touto CPS, resp. s odpovídající CP je ředitel Správy uvedený na webu Správy.

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů Správy uvedených v této CPS a v konkrétní CP, je ředitel Správy.

1.5.4 Postupy při schvalování CPS

Pokud je potřebné provést změny v příslušné CPS a vytvořit její novou verzi, určuje ředitel Správy osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze CPS předchází její schválení ředitelem Správy.

1.6 Přehled použitých pojmů a zkratk

Tabulka 1 - Pojmy

Pojem	Vysvětlení
bezpečné kryptografické zařízení	zařízení, na kterém je uložen soukromý klíč
bit	z anglického <i>binary digit</i> – číslice dvojkové soustavy – základní a současně nejmenší jednotka informace v číslicové technice
časové razítko	kvalifikované elektronické časové razítko dle právní úpravy pro služby vytvářející důvěru
dvoufaktorová autentizace	autentizace využívající dvou ze tří faktorů – něco vím (heslo), něco mám (např. čipová karta, hardwarový token) nebo něco jsem (otisky prstů, snímání oční sítnice či duhovky)
elektronická pečeť	elektronická pečeť, nebo zaručená elektronická pečeť, nebo uznávaná elektronická pečeť, nebo kvalifikovaná elektronická pečeť dle právní úpravy pro služby vytvářející důvěru

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

elektronický podpis	elektronický podpis, nebo zaručený elektronický podpis, nebo kvalifikovaný elektronický podpis, nebo uznávaný elektronický podpis dle právní úpravy pro služby vytvářející důvěru
hashovací funkce	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou (hash)
kořenová CA	certifikační autorita vydávající certifikáty podřízeným certifikačním autoritám
kvalifikovaný certifikát pro elektronický podpis	certifikát definovaný platnou právní úpravou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II eIDAS
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
orgán dohledu	orgán dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické nebo listinné podobě
právní úprava pro služby vytvářející důvěru	platné právní předpisy České republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru	elektronická služba / kvalifikovaná služba vytvářející důvěru, definovaná eIDAS
smluvní partner	poskyvatel vybraných služeb vytvářejících důvěru, který zajišťuje na základě písemné smlouvy pro Správu služby vytvářející důvěru nebo jejich části – nejčastěji se jedná o smluvní RA
softcard	programová emulace čipové karty pro přístup k soukromému klíči uloženému v HSM
soukromý klíč	jedinečná data pro vytváření elektronického podpisu/pečetě
spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát
veřejný klíč	jedinečná data pro ověřování elektronického podpisu/pečetě
vydávající, podřízená CA	pro účely tohoto dokumentu CA vydávající certifikáty koncovým uživatelům
zákoník práce	zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

Tabulka 2 - Zkratky

Zkratka	Vysvětlení
BIH	Bureau International de l'Heure, (anglicky The International Time Bureau), Mezinárodní časová služba

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

CA	certifikační autorita
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
CP	certifikační politika
CPS	certifikační prováděcí směrnice
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
ČR	Česká republika
ČSN	označení českých technických norem
DER, PEM	způsoby zakódování (formáty) certifikátu
DIA	Digitální a informační agentura
EAL	Evaluation Assurance Level, úroveň hodnocení záruky
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
GDPR	Global Data Protection Regulation, 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 (obecné nařízení o ochraně osobních údajů)
html	Hypertext Markup Language, značkovací jazyk pro vytváření hypertextových dokumentů
http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
https	Hypertext Transfer Protocol Secure, protokol pro zabezpečenou výměnu textových dokumentů ve formátu html
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IPS	Intrusion Prevention System, systém prevence průniku

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

ISMS	Information Security Management System, systém řízení bezpečnosti informací
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector of ITU
NCA	Národní certifikační autorita, provozovaná Správou státních služeb vytvářejících důvěru
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování - Zavedení - Kontrola - Využití, Demingův cyklus, metoda neustálého zlepšování
PDS	PKI Disclosure Statement, zpráva pro uživatele
PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu nebo pečetě
RA	registrační autorita NCA
RFC	Request for Comments, označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.
RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
SHA	typ hashovací funkce
SSSVD	Správa státních služeb vytvářejících důvěru
TS	Technical Specification, typ ETSI standardu
TSA	Time Stamping Authority, autorita časových razítek, obsahující více serverů, vydávajících časová razítka, kdy každý z nich disponuje jedinečným soukromým klíčem a tedy i kvalifikovaným systémovým certifikátem
TSP	Trust Service Provider, poskytovatel služeb vytvářejících důvěru
TSS	Time-Stamp Server, server časových razítek
TSU	Time-Stamp Unit, jednotka vydávající časová razítka
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

URI	Uniform Resource Identifier, textový řetězec s definovanou strukturou sloužící k přesné specifikaci zdroje informací
UTC	Coordinated Universal Time, standard přijatý 1.1.1972 pro světový koordinovaný čas - funkci „oficiálního časoměřiče“ atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
ZOOÚ	aktuální právní úprava týkající se ochrany osobních údajů

2. Odpovědnost za zveřejňování a za úložiště

2.1 Úložiště

Správa zřizuje a provozuje úložiště veřejných i neveřejných informací.

2.2 Zveřejňování certifikačních informací

Základní adresy (dále též informační adresy), na nichž lze získat informace o Správě, případně odkazy pro zjištění dalších informací, jsou:

adresa sídla:

Správa státních služeb vytvářejících důvěru

Na Vápence 915/14

130 00 Praha 3

Česká republika

internetová adresa <http://www.narodni-ca.gov.cz>,

sídla registračních autorit.

Elektronická adresa, která slouží pro kontakt se Správou, je podpora@sssud.gov.cz, ID datové schránky Správy je pp634ge.

Na výše uvedené internetové adrese lze získat informace o:

veřejných certifikátech - přímo se zveřejňují následující informace (ostatní informace lze získat z certifikátu):

- číslo certifikátu,
- obsah položky Obecné jméno (commonName),
- údaj o počátku platnosti (s uvedením hodiny, minuty a sekundy),
- odkazy na místo, kde lze certifikát získat v určených formátech (DER, PEM, TXT),

seznamech zneplatněných certifikátů (CRL) - přímo se zveřejňují následující informace (ostatní informace lze získat ze samotného CRL):

- datum vydání CRL,
- číslo CRL,
- odkazy na místo, kde lze CRL získat v určených formátech (DER, PEM, TXT),

certifikačních a jiných politikách, prováděcích směrnicích a další veřejné informace.

Povolenými protokoly pro přístup k veřejným informacím jsou http a https. Správa může bez udání důvodu přístup k některým informacím zrušit nebo pozastavit.

V případě zneplatnění Certifikátu z důvodu podezření na kompromitaci, případně samotné kompromitace příslušného soukromého klíče oznámí Správa tuto skutečnost na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku.

2.3 Čas nebo četnost zveřejňování

Viz kapitola 2.3 konkrétní CP.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje Správa bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům Správy, nebo subjektům definovaným příslušnou právní úpravou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci, zejména:

- „NCA – Směrnice pro pracovníky RA“,
- „Politika řízení bezpečnosti informací“,
- „NCA – Příručka administrátora systémů CA, TSA“,
- „Metodika řízení kybernetických bezpečnostních incidentů“,
- „NCA – HSM nShield, Směrnice pro správu“,
- „NCA – Správa TSS“.

3. Identifikace a autentizace

3.1 Pojmenování

3.1.1 Typy jmen

Veškerá jména jsou konstruována v souladu s platnými technickými standardy a normami.

3.1.2 Požadavek na významovost jmen

V procesu vydávání certifikátu je vždy vyžadována významovost všech ověřitelných jmen uvedených v položkách pole Subject, resp. rozšíření SubjectAlternativeName. Podporované položky tohoto pole a rozšíření jsou uvedeny v konkrétní CP.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Viz kapitola 3.1.3 konkrétní CP.

3.1.4 Pravidla pro interpretaci různých forem jmen

Údaje uváděné v žádosti o Certifikát (formát PKCS#10) se do pole Subject, resp. rozšíření SubjectAlternativeName ve vydávaných Certifikátech přenášejí ve tvaru, ve kterém jsou uvedeny v předkládané žádosti.

3.1.5 Jedinečnost jmen

Uvedeno v kapitole 3.1.5 konkrétní certifikační politiky.

3.1.6 Uznávání, ověřování a posláním obchodních značek

Certifikáty, vydávané podle této CPS, resp. příslušných CP mohou obsahovat pouze obchodní značky, jejichž vlastnictví nebo pronájem byly doloženy. Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nesou držitelé certifikátů.

3.2 Počáteční ověření identity

Postup ověřování identity je uveden v kapitole 3.2 konkrétní CP a dále upřesněn v interním dokumentu:

„NCA – Směrnice pro pracovníky RA“.

3.2.1 Ověřování vlastnictví soukromého klíče

Vlastnictví soukromého klíče odpovídajícího veřejnému klíči v žádosti o Certifikát se prokazuje předložením žádosti ve formátu PKCS#10. Ta je zmíněným soukromým klíčem opatřena elektronickou pečetí a držitel soukromého klíče tak prokazuje, že v době tvorby elektronické pečeti tento soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Postup popsán v kapitole 3.2.2 konkrétní CP a dále v interním dokumentu:

„NCA – Směrnice pro pracovníky RA“.

3.2.3 Ověřování identity fyzické osoby

Postup je popsán v kapitole 3.2.3 konkrétní CP a dále v interním dokumentu:

„NCA – Směrnice pro pracovníky RA“.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při výtiskání.“

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Neověřované informace jsou vždy uvedeny v kapitole 3.2.4 konkrétní CP.

3.2.5 Ověřování kompetencí

Adresu elektronické pošty je možno umístit v rozšíření certifikátu, konkrétně v poli rfc822Name položky SubjectAlternativeName, pouze tehdy, byla-li tato skutečnost v procesu vydání certifikátu pro tuto žádost ověřena.

Příznak, že klíčový pár byl generován na zařízení typu QSCD lze do certifikátu vložit pouze tehdy, byla-li tato skutečnost v procesu vydání certifikátu pro tuto žádost ověřena.

Postup ověřování dalších specifických práv je popsán v kapitole 3.2.5 konkrétní CP.

3.2.6 Kritéria pro interoperabilitu

Případná spolupráce Správy s jinými poskytovateli služeb vytvářejících důvěru je vždy založena na písemné smlouvě s těmito poskytovateli.

3.3 Identifikace a autentizace při požadavku na výměnu klíče

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Vždy je nutné vydat nový certifikát s novým veřejným klíčem. Požadavky jsou uvedeny v kapitole 3.3.1 konkrétní CP.

3.3.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu

Není relevantní pro tento dokument, služba výměny veřejného klíče po zneplatnění certifikátu není podporována. Je nutné vydat nový certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Způsoby identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu jsou uvedeny v kapitole 3.4 konkrétní CP.

3.4.1 Certifikáty poskytovatele

Oprávněnou osobou žádat o zneplatnění certifikátu:

kořenové certifikační autority i jí vydaného certifikátu OCSP respondéru,
vydávající certifikační autority i jí vydaného certifikátu OCSP respondéru,
časového serveru autority časových razítek,
je ředitel Správy, nebo jím pověřená osoba.

Žadatelem o zneplatnění certifikátu kořenové certifikační autority, popř. certifikátu, souvisejícího s kvalifikovanými certifikačními službami, může být taktéž představitel úřadu, který Správě udělil statut kvalifikovaného poskytovatele služeb vytvářejících důvěru. Žádost od úřadu musí být písemná, nebo být doručena do datové schránky Správy. Samotnému procesu zneplatnění takového certifikátu musí být ředitel Správy vždy osobně přítomen.

3.4.2 Certifikáty koncových uživatelů

Možné způsoby identifikace a autentizace jsou následující:

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

osobně na RA,

prostřednictvím formuláře na webových stránkách Správy (s využitím hesla pro zneplatnění certifikátu),

prostřednictvím nepodepsané elektronické zprávy (obsahující heslo pro zneplatnění certifikátu),

prostřednictvím datové schránky (s využitím hesla pro zneplatnění certifikátu).

Údaje, které musí žádost o zneplatnění certifikátu obsahovat, jsou uvedeny v kapitole 4.9.3.

Správa si vyhrazuje právo akceptování i jiných forem postupů pro identifikaci a autentizaci zpracování požadavku na zneplatnění certifikátu.

4. Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

Subjekty oprávněné podat žádost o vydání certifikátu jsou uvedeny v kapitole 4.1.1 konkrétní CP.

4.1.2 Registrační proces a odpovědnosti

Procesy prováděné v průběhu registračního procesu jsou uvedeny v konkrétní CP.

Žadatel je povinen zejména:

poskytovat pravdivé a úplné informace při registraci žádosti o vydání certifikátu, seznámit se s CP, podle které mu bude vydán certifikát.

Poskytovatel Služeb je zejména povinen Služby poskytovat v souladu s platnou právní úpravou, konkrétní CP a touto CPS, Systémovou bezpečnostní politikou a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

Proces zpracování žádosti o certifikát je popsán v interní dokumentaci:

„NCA – Směrnice pro pracovníky RA“.

4.2.1 Provádění identifikace a autentizace

Žadatel o certifikát se identifikuje a autentizuje způsobem, popsáným v kapitolách 3.2.2 a 3.2.3 konkrétní CP.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

V případě vydávání certifikátů poskytovatele Služeb rozhodne vedení Správy na základě písemné žádosti o vydání certifikátu, případně o zamítnutí žádosti. Výsledek je dokumentován.

Pokud některá z ověření, prováděna pracovníkem RA skončí negativně, proces vydání certifikátu je ukončen. V opačném případě pracovník RA vydání certifikátu schválí.

Postupy pro přijetí nebo odmítnutí žádosti o certifikát jsou uvedeny v kapitole 4.2.2 konkrétní CP a v interní dokumentaci:

„NCA – Směrnice pro pracovníky RA“.

4.2.3 Doba zpracování žádosti o certifikát

Pro certifikáty koncových uživatelů platí, že po kladném rozhodnutí o vydání certifikátu je Správa povinna neprodleně certifikát vydat. Platí, že doba vydání je do 15 minut a jen ve výjimečných případech může být tato doba delší.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání certifikátu provádějí pracovnice / pracovníci (dále jen „pracovníci“) RA kontroly na shodnost údajů, obsažených v žádosti o certifikát (struktura PKCS#10). Kontroly na formální správnost údajů jsou taktéž prováděny programovým vybavením informačního systému CA.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Postupy jsou uvedeny v kapitole 4.3.1 konkrétní CP a upřesněny v interní dokumentaci:

„NCA – Směrnice pro pracovníky RA“,

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

V případě, že žadatel o certifikát je osobně přítomen vydání certifikátu, získá oznámení o jeho vydání od pracovníka RA. Vydaný certifikát je zaslán na e-mailovou adresu žadatele, pokud byla v žádosti uvedena.

Uvedené postupy jsou detailně popsány v interní dokumentaci:

„NCA – Směrnice pro pracovníky RA“.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Úkony spojené s převzetím certifikátu jsou vždy popsány v kapitole 4.4.1 konkrétní CP.

Detailně je proces je popsán v interní dokumentaci:

„NCA – Směrnice pro pracovníky RA“.

4.4.2 Zveřejňování certifikátů certifikační autoritou

Certifikáty poskytovatele jsou zveřejňovány na webových stránkách Správy, certifikáty související s kvalifikovanými službami vytvářejícími důvěru jsou navíc předány orgánu dohledu.

Pro certifikáty koncových uživatelů Správa zajistí zveřejnění.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2 a požadavky právní úpravy pro služby vytvářející důvěru – certifikát kořenové certifikační autority a certifikáty podřízených certifikačních autorit související se službami vytvářejícími důvěru jsou předávány orgánu dohledu.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitele certifikátu mj. je:

dodržovat veškerá relevantní ustanovení smlouvy o poskytování Služeb,

užívat soukromý klíč a odpovídající certifikát vydaný podle konkrétní CP pouze pro účely stanovené v této CP a případně právní úpravou pro služby vytvářející důvěru,

nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v certifikátu vydaném podle konkrétní CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,

neprodleně uvědomit poskytovatele Služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

získat z bezpečného zdroje certifikáty certifikačních autorit související s certifikátem koncového uživatele vydaným podle konkrétní CP, ověřit hodnoty jejich otisků a jejich platnost,

provádět veškeré úkony potřebné k tomu, aby si ověřily, že certifikát je platný, tj.:

- ověřit platnost certifikátu podle RFC5280, kapitola 6 (včetně celé certifikační cesty a odvolání platnosti certifikát),
- ověřit kvalifikovanost vydavatele kvalifikovaného certifikátu (jeho uvedení na seznamu důvěryhodných služeb s příslušnými atributy),

dodržovat veškerá ustanovení odpovídající CP a případně právní úpravy pro služby vytvářející důvěru, vztahující se k povinnostem spoléhající se strany.

4.6 Obnovení certifikátu

Službou obnovení certifikátu je míněno vydání následného certifikátu k ještě platnému certifikátu, aniž by byl změněn veřejný klíč, nebo jiné informace v certifikátu, nebo k zneplatněnému certifikátu, nebo k expirovanému certifikátu.

Služba obnovení certifikátu není poskytována. Vždy se jedná o vydání nového Certifikátu s novým veřejným klíčem, kdy všechny informace musí být řádným způsobem ověřeny. Platí stejné požadavky jako v případě počátečního ověření identity – viz kapitola 3.2.

Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

Kdo může žádat o obnovení

Viz kapitola 4.6.

Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.6.

Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 4.6.

Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.6.

4.7 Výměna veřejného klíče v certifikátu

Popsáno v kapitole 4.7 konkrétní certifikační politiky.

Podmínky pro výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Kdo může žádat o výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

Zpracování požadavku na výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.7.

Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz kapitola 4.7.

Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Viz kapitola 4.7.

Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

Popsáno v kapitole 4.8 konkrétní certifikační politiky.

Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Podmínky pro zneplatnění

Kromě podmínek uvedených v následujících podkapitolách si Správa vyhrazuje právo akceptování i jiných okolností podmínek na zneplatnění certifikátu.

4.9.1.1 Certifikáty poskytovatele

Certifikát musí být zneplatněn na základě následujících okolností:

dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče odpovídajícího veřejnému klíči tohoto certifikátu,

žádost ředitele Správy,

nastanou-li skutečnosti uvedené v právní úpravě pro služby vytvářející důvěru, resp. v technických standardech a normách.

4.9.1.2 Certifikáty koncových uživatelů

Certifikát musí být zneplatněn na základě následujících okolností:

dojde ke kompromitaci, resp. existuje důvodné podezření, že došlo ke kompromitaci, soukromého klíče odpovídajícího veřejnému klíči tohoto certifikátu,

je porušeno ustanovení smlouvy o poskytování Služby podle konkrétní CP ze strany držitele certifikátu,

v případech, kdy nastanou skutečnosti uvedené v právní úpravě pro služby vytvářející důvěru nebo příslušných technických standardech a normách (např. neplatnost údajů v certifikátu),

pokud je veřejný klíč v žádosti o vydání Certifikátu duplicitní s veřejným klíčem v již vydaném Certifikátu.

4.9.2 Kdo může požádat o zneplatnění

4.9.2.1 Certifikáty poskytovatele

Žádost o zneplatnění mohou podat:

ředitel Správy,

případně další subjekty definované právní úpravou pro služby vytvářející důvěru.

4.9.2.2 Certifikáty koncových uživatelů

Žádost o zneplatnění mohou podat:

držitel certifikátu,

subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování příslušné Služby,

poskytovatel Služby (oprávněným žadatelem o zneplatnění Certifikátu vydaného Správou je v tomto případě ředitel Správy):

- v případě, že certifikát byl vydán na základě nepravdivých údajů,
- pokud prokazatelně zjistí, že soukromý klíč, patřící k veřejnému klíči uvedenému v certifikátu, byl kompromitován,
- dozví-li se prokazatelně, že certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

- dozví-li se prokazatelně, že držitel Certifikátu zemřel, nebo soud držiteli Certifikátu omezil svéprávnost, nebo pokud údaje, na jejichž základě byl Certifikát vydán, pozbyly pravdivosti,
- pokud je veřejný klíč v žádosti o vydání certifikátu duplicitní s veřejným klíčem v již vydaném certifikátu,
- pokud zjistí, že při vydání certifikátu nebyly splněny požadavky právní úpravy pro služby vytvářející důvěru,

případně orgán dohledu, resp. subjekty definované právní úpravou pro služby vytvářející důvěru.

4.9.3 Postup při žádosti o zneplatnění

Způsob podání žádosti o zneplatnění certifikátu koncového uživatele je vždy popsán v kapitole 4.9.3 konkrétní CP.

Požadavky na identifikaci a autentizaci jsou uvedeny v kapitole 3.4 tamtéž.

4.9.4 Prodleva při požadavku na zneplatnění certifikátu

Požadavek na zneplatnění Certifikátu musí být podán bezodkladně.

4.9.5 Doba zpracování žádosti o zneplatnění

Maximální doba mezi přijetím žádosti o zneplatnění certifikátu a jeho zneplatněním je 24 hodin.

4.9.6 Povinnosti třetích stran při kontrole zneplatnění

Spoléhající se strany jsou povinny provádět veškeré úkony uvedené v kapitole 4.5.2 příslušné CP.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Periodicita vydávání seznamu zneplatněných certifikátů je uvedena v kapitole 4.9.7 konkrétní CP.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL kořenové CA je vždy vydán nejvýše jeden rok od vydání předchozího CRL. CRL vydávající CA je vždy vydán nejvýše 24 hodin od vydání předchozího CRL.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba uvěřování stavu certifikátu certifikační autority s využitím protokolu OCSP je veřejně dostupná. Každý certifikát vydaný podle této CP, obsahuje odkaz na příslušný OCSP respondér.

OCSP odpovědi vyhovují normám RFC 6960 a RFC 5019. Certifikát OCSP respondéru obsahuje rozšíření typu id-pkix-ocsp-nocheck, jak je definováno v RFC 6960.

4.9.10 Požadavky při ověřování stavu certifikátu on-line

Viz kapitola 4.9.9.

4.9.11 Jiné možné způsoby oznamování zneplatnění

Není relevantní pro tento dokument.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

4.9.12 Zvláštní postupy při kompromitaci klíče

Postup pro zneplatnění certifikátu v případě kompromitace soukromého klíče není odlišný od výše popsaného postupu pro zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.14 Kdo může požádat o pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.15 Postup při žádosti o pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.9.16 Omezení doby pozastavení platnosti

Není relevantní pro tento dokument, služba pozastavení platnosti certifikátu není poskytována.

4.10 Služby ověřování stavu certifikátu

4.10.1 Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány jak formou zveřejňování informací, tak uvedením distribučních míst CRL ve vydaných certifikátech.

Skutečnost, že certifikační autorita poskytuje informace o stavu certifikátu formou OCSP (služba OCSP), je uvedena ve vydaných certifikátech.

4.10.2 Dostupnost služeb

Správa garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu, 24 hodin denně) a integrity seznamu jí vydaných certifikátů a seznamů zneplatněných certifikátů (platné CRL), a dále dostupnost služby OCSP.

Postup je uveden v interních dokumentech, zejména:

„NCA – Příručka administrátora systémů CA, TSA“,

„NCA – Obnova systémů CA, TSA“,

„NCA – Přemístění systémů CA, TSA“.

4.10.3 Další charakteristiky služeb stavu certifikátu

Správa na seznamu zneplatněných certifikátů udržuje i expirované certifikáty, a to po dobu tří dnů po jejich expiraci. Důvodem omezení doby, po kterou jsou expirované certifikáty na CRL uváděny, je snaha udržet rozsah CRL v rozumných mezích.

V případě rozhodnutí o ukončení služby poskytování stavu certifikátů (CRL), Správa vydá a zveřejní poslední CRL s hodnotou položky "nextupdate" rovnou "99991231235959Z".

Správa ve službě stavu certifikátu (OCSP) poskytuje v odpovědi i informaci o stavu expirovaných certifikátů, pokud od jejich expirace neuplynula doba delší než tři dny (v souladu s CRL a s ohledem na konzistentnost informací v CRL a OCSP).

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

V případě, že se pro certifikát vydávající CA blíží doba jeho expirace, uvede Správa v poslední OCSP odpovědi pro každý vydaný certifikát hodnotu položky "nextupdate" rovnou "99991231235959Z".

4.11 Konec smlouvy o vydávání certifikátů

Po ukončení platnosti smlouvy o vydávání certifikátů přetrvávají z ní vyplývající závazky Správy, a to po dobu platnosti posledního podle ní vydaného certifikátu.

4.12 Úschova a obnova klíčů

Není relevantní pro tento dokument, služba úschovy soukromého klíče není poskytována.

Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

5. Postupy správy, řízení a provozu

Postupy správy, řízení a provozu jsou zaměřeny především na:

důvěryhodné systémy určené k podpoře Služby,
veškeré procesy podporující poskytování Služby.

Postupy správy, řízení a provozu jsou řešeny jak v základních dokumentech NCA – Systémová bezpečnostní politika (CA a TSA), Certifikační prováděcí směrnice a NCA – Řízení kontinuity provozu, tak v upřesňujících interních dokumentech. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně popsána v interní dokumentaci, zejména:

„Řízení fyzického přístupu do provozních prostor Národní certifikační autority“,

„NCA – Kontrolní činnost, bezúhonnost a odbornost“,

„Metodika řízení kybernetických bezpečnostních incidentů“,

„NCA – Obnova systémů CA, TSA“,

„NCA – Přemístění systému CA, TSA“.

5.1.1 Umístění a konstrukce

Důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru jsou umístěny ve vyhrazených prostorách objektu navrženého s odolností proti výbuchu. Objekt je vybaven celoplošnou ochranou pomocí infrazávor (dle ČSN) a elektronickým zabezpečovacím zařízením (EZS) Je střežen ozbrojenou ochrankou v režimu 24/365.

5.1.2 Fyzický přístup

Ochrana prostor, kde jsou umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru, je řešena elektronickým zabezpečovacím systémem (EZS), systémem pro snímání, přenos a zobrazování pohybu osob (CCTV) a dopravních prostředků a elektronickým systémem kontroly vstupu (EKV). Podrobně jsou požadavky na řízení fyzického přístupu uvedeny v interní dokumentaci.

5.1.3 Elektřina a klimatizace

V prostorách, kde jsou umístěny důvěryhodné systémy určené k podpoře Služby, je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí $20\text{ °C} \pm 5\text{ °C}$. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 Vlivy vody

Důvěryhodné systémy určené k podpoře Služby jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stouletou vodou. Provozní pracoviště je vybaveno čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

Ve vyhrazených prostorách, kde jsou umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru, je instalována elektronická požární signalizace (EPS). Vstupní dveře těchto prostor jsou opatřeny protipožární vložkou. V místnosti pro administraci se nachází hasicí přístroj.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

5.1.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, karty a přístupová hesla jsou ukládána v trezoru.

Papírová média, která je nutno dle právní úpravy pro služby vytvářející důvěru uchovávat, jsou obvykle skladována přímo v lokalitách, kde jsou umístěny registrační autority. Papírová média ukládaná na Správě jsou uchovávána v kovové, uzamykatelné skříni v místnosti s řízeným přístupem č. 342 (třetí podlaží budovy Správy). Dokumenty jsou skenovány a oskenovaná podoba je ukládána na úložišti k tomu určeném (server NCA záloha, určený pro výhradní potřebu Správy).

5.1.7 Nakládání s odpady

Veškerý papírový kancelářský odpad je před opuštěním provozních pracovišť znehodnocen skartováním.

5.1.8 Zálohy mimo budovu

Kopie záloh pro úplnou obnovu systému a hesla jsou uloženy v geograficky odlišné lokalitě.

5.2 Procedurální postupy

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou ve Správě definovány důvěryhodné role. Postup jmenování zaměstnanců do důvěryhodných rolí, specifikace těchto rolí včetně odpovídajících činností a odpovědností jsou uvedeny v interní dokumentaci, zejména v dokumentech:

„NCA – Systémová bezpečnostní politika (CA a TSA)“,

„Politika řízení bezpečnosti informací“,

„NCA – Příručka administrátora systémů CA, TSA“.

Zaměstnanci Správy v důvěryhodných rolích nesmí být ve střetu zájmů, který by mohl ohrozit nestrannost operací systému NCA.

5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností

Pro procesy související s párovými daty certifikačních autorit a OCSP respondérů jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

inicializaci kryptografického modulu,

generování párových dat v kryptografického modulu,

ničení soukromých klíčů v kryptografického modulu,

zálohování a obnova soukromých klíčů z nebo do kryptografického modulu,

aktivaci a deaktivaci soukromých klíčů.

Pro provádění ostatních úloh není počet přítomných osob určen, musí však jít výhradně o pověřené pracovníky.

Podrobné informace jsou vždy uvedeny v kapitole 5.2.2 konkrétní CP a v interní dokumentaci:

„NCA – Příručka administrátora systémů CA, TSA“,

„NCA – HSM nShield, Postupy generování klíčů a certifikátů CA a OCSP“,

„NCA – HSM nShield, Směrnice pro správu“.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vtištění.“

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci (jméno, certifikát) a autentizaci (heslo, soukromý klíč) k těm komponentám, které jsou pro jejich činnost nezbytné. Problematika je upravena v interní dokumentaci, zejména:

„NCA – Směrnice pro pracovníky RA“,

„NCA – Příručka administrátora systémů CA, TSA“.

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

5.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány v interní dokumentaci:

„NCA – Systémová bezpečnostní politika (CA a TSA)“.

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

Zaměstnanci Správy v důvěryhodných rolích jsou přednostně vybíráni a přijímáni na základě dále popsaných personálních kritérií:

občanská bezúhonnost - prokazováno výpisem z rejstříku trestů, nebo čestným prohlášením,

vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně tři roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně pět let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně jeden rok v oblasti poskytování služeb vytvářejících důvěru,

znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní zaměstnanci Správy podílející se na zajištění služeb vytvářejících důvěru jsou přijímáni na základě následujících kritérií:

vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu, nebo středoškolské vzdělání,

základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Pro vykonávání řídicí funkce musí mít vedoucí zaměstnanci zkušenosti získané praxí nebo odbornými školeními s ohledem na důvěryhodnost Služby, znalost bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

Problematika je detailně popsána v interním dokumentu:

„NCA – Kontrolní činnost, bezúhonnost a odbornost“.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích Správy podílejících se na činnosti NCA jsou:

sami tito zaměstnanci,

osoby, které tyto zaměstnance znají,

veřejné zdroje informací.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Zaměstnanci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, ty jsou aktualizovány při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru. Součástí prvotních informací je dále doložení beztrestnosti výpisem z rejstříku trestů.

Problematika je detailně popsána v interním dokumentu:

„NCA – Kontrolní činnost, bezúhonnost a odbornost“.

5.3.3 Požadavky na školení

Zaměstnanci Správy jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samostudia a metodickým vedením již zaškoleným pracovníkem. Školení zahrnuje oblasti informační bezpečnosti, ochrany osobních údajů a další relevantní témata.

Problematika je detailně popsána v interním dokumentu:

„NCA – Kontrolní činnost, bezúhonnost a odbornost“.

5.3.4 Požadavky a periodicita doškolování

Dvakrát za 12 měsíců jsou příslušným zaměstnancům Správy poskytovány aktuální informace o vývoji v předmětných oblastech.

Pro pracovníky RA je minimálně jednou za tři roky pořádáno školení zaměřené na procesy spojené s činností RA.

Problematika je detailně popsána v interním dokumentu:

„NCA – Kontrolní činnost, bezúhonnost a odbornost“.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou vybraní zaměstnanci Správy motivováni k získávání znalostí potřebných pro zastávání jiné role ve Správě.

5.3.6 Postihy za neoprávněné činnosti

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsáným v interních dokumentech a řídicím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

Problematika je detailně popsána v interním dokumentu:

„Provozní řád SSSVD“.

5.3.7 Požadavky na nezávislé dodavatele

Správa může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. Tyto obchodně právní vztahy jsou upraveny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími certifikačními politikami, relevantními částmi interní dokumentace, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci Správy mají k dispozici kromě certifikační politiky, certifikační prováděcí směrnice, bezpečnostní a provozní dokumentace veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

5.4 Postupy zpracování auditních záznamů

Zaznamenávají jsou veškeré události požadované v případě kvalifikovaných certifikátů právní úpravou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, v ostatních případech relevantními technickými standardy a normami, mj. o životním cyklu vydávaných certifikátů, nakládání se soukromými klíči poskytovatele a o dalších událostech, jako je např. ukončení činnosti certifikační autority.

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

Problematika spojená s vytvářením, zpracováním a uchováváním auditních logů je detailně řešena v interní dokumentaci, zejména:

„NCA – Příručka administrátora systémů CA, TSA“,

„NCA – Uchovávání dat a informací“,

„NCA – Záloha dat systémů“,

„Spisový a skartační řád SSSVD“,

5.4.1 Typy zaznamenávaných událostí

Speciálním případem zaznamenávání událostí je událost generování párových dat certifikačních autorit. Celý proces probíhá v souladu s právní úpravou pro služby vytvářející důvěru a s relevantními technickými standardy a normami, přičemž platí, že:

je prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí,

o provedení je vydána zpráva, že generování proběhlo podle připraveného scénáře a že byly zajištěny jeho důvěrnost a integrita,

v případě Autority je osobně přítomen buď auditor kvalifikovaný v souladu s platnými technickými standardy, nebo notář, který zprávu podepíše jako svědek, že zpráva správně popisuje postup generování,

v případě podřízených certifikačních autorit je osobně přítomen ředitel Správy, nebo jím pověřená osoba, který zprávu podepíše jako svědek, že zpráva správně popisuje postup generování.

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje integritu auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní dokumentaci:

„NCA – Příručka administrátora systémů CA, TSA“,

v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

Nestanoví-li relevantní právní úprava jinak, jsou auditní záznamy uchovávány po dobu nejméně 10 let od jejich vzniku.

5.4.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem zajišťujícím ochranu před jejich změnami, krádeží a zničením (ať již úmyslným, nebo neúmyslným).

Elektronické auditní záznamy jsou ukládány v plechové skříni Správy v místnosti s řízeným přístupem.

Auditní záznamy v papírové formě jsou ukládány v plechové skříni Správy v místnosti s řízeným přístupem. Jsou skenovány a oskenovaná podoba je ukládána na úložišti k tomu určeném.

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci – viz kapitola 5.4.

5.4.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem, jako zálohování ostatních elektronických informací. Zálohování auditních záznamů v papírové formě prováděno není.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů CA interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve Správě prováděno v periodických intervalech jako součást analýzy rizik. Sledování zranitelnosti zařízení a programového vybavení souvisejících se službami vytvářejícími důvěru je popsáno v interní dokumentaci:

„NCA – Příručka administrátora systémů CA, TSA“.

5.5 Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je ve Správě upraveno interní dokumentací:

„Řízení fyzického přístupu do provozních prostor Národní certifikační autority“,

„NCA – Uchovávání dat a informací“,

„NCA – Záloha dat systémů“,

„NCA – Příručka administrátora systémů CA, TSA“,

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

„Spisový a skartační řád SSSVD“.

5.5.1 Typy uchovávaných záznamů

Správa uchovává níže uvedené typy záznamů (v elektronické nebo papírové podobě), které souvisejí s poskytovanými službami vytvářejícími důvěru, zejména:

zprávy o průběhu generování párových dat certifikačních autorit,

dokumenty související s životním cyklem vydaných Certifikátů a certifikátů OCSP, včetně těchto certifikátů,

záznamy o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),

politiky, provozní a bezpečnostní dokumentaci.

5.5.2 Doba uchování záznamů

Výše uvedené záznamy jsou uchovávány po celou dobu existence Správy. Ostatní záznamy jsou uchovávány v souladu s ustanoveními kapitoly 5.4.3.

Postupy při uchovávání záznamů jsou upraveny interní dokumentací – viz kapitola 5.5.

5.5.3 Ochrana úložiště záznamů

Prostory, ve kterých jsou záznamy uchovávány, se nacházejí v budově střežené v režimu 24x365. Přístup do nich je řízen, jsou vybaveny detektory kouře a průniku vody. Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací – viz kapitola 5.5.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

V případě, že jsou využívána časová razítka, jedná se o kvalifikovaná elektronická časová razítka vydávaná Správou.

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

Systém shromažďování uchovávaných záznamů je z pohledu informačních systémů CA interní.

5.5.7 Postupy pro získání a ověření uchovávaných informací

Uchovávané informace a záznamy jsou umístěny v lokalitách k tomu určených a jsou přístupné:

zaměstnancům Správy, pokud je to k jejich činnosti vyžadováno,

oprávněným kontrolním subjektům, orgánům činným v trestním řízení a soudům, pokud je to právními předpisy vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Výměna klíče

Výměna párových dat certifikačních autorit v případě standardních situací (uplynutí platnosti certifikátů certifikačních autorit) je prováděna s dostatečným časovým předstihem (minimálně jeden rok před uplynutím doby platnosti tohoto certifikátu) formou vydání nového certifikátu.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu vydávání certifikátů, tzn. změny kryptografických algoritmů, délky klíčů atd.) je tato činnost prováděna v adekvátním, co nejkratším časovém období.

Jak v případě standardních, tak nestandardních situací je výměna veřejného klíče v certifikátech certifikačních autorit veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto událostí postupuje Správa v souladu s interní dokumentací:

„NCA – Řízení kontinuity provozu“,

„NCA – Obnova systémů CA, TSA“,

„NCA – Přemístění systémů CA, TSA“,

„Metodika řízení kybernetických bezpečnostních incidentů“.

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

5.7.3 Postup při kompromitaci soukromého klíče

V případě vzniku důvodné obavy z kompromitace soukromého klíče certifikačních autorit postupuje Správa tak, že:

ukončí jeho používání,

okamžitě a trvale zneplatní příslušný certifikát a zničí jemu odpovídající soukromý klíč, zneplatní všechny platné certifikáty vydané příslušnou certifikační autoritou,

bezodkladně o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese, uveřejní oznámení v tisku - viz kapitola 2.2, pro zpřístupnění této informace je využít i seznam zneplatněných certifikátů,

oznámi orgánu dohledu informaci o zneplatnění příslušného certifikátu s uvedením důvodu.

Obdobný postup bude uplatněn i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), že by mohla být prostředně ohrožena bezpečnost Služby.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje Správa v souladu s interní dokumentací:

„NCA – Řízení kontinuity provozu“,

„NCA – Obnova systémů CA, TSA“,

„NCA – Přemístění systémů CA, TSA“.

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti CA platí následující pravidla:

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

ukončení činnosti CA musí být písemně oznámeno všem držitelům platných certifikátů, subjektům, které mají se Správou uzavřenou smlouvu přímo se vztahující k poskytování certifikačních Služeb a v případě kvalifikovaných certifikátů orgánu dohledu,

ukončení činnosti CA musí být zveřejněno na internetové adrese podle kapitoly 2.2,

pokud je součástí ukončení činnosti CA ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně uvedení důvodu ukončení platnosti,

ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchovávání a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity Služeb,

po dobu platnosti jediného certifikátu vydaného certifikační autoritou musí tato zajistit alespoň funkce zneplatňování certifikátu a vydávání CRL,

následně CA prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván v souladu s pravidly této CPS, resp. konkrétní CP.

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru:

informace musí být písemně nebo elektronicky oznámena všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování služeb vytvářejících důvěru,

informace musí být zveřejněna v souladu s kapitolou 2.2 a na všech pracovištích registračních autorit; součástí informace bude i sdělení, že kvalifikované systémové certifikáty nelze nadále používat v souladu s účelem jejich vydání,

o dalším postupu rozhodne ředitel Správy na základě rozhodnutí orgánu dohledu.

V případě ukončení činnosti konkrétního pracoviště RA je tato skutečnost oznámena na internetové adrese Správy (viz kapitola 2.2).

Problematika plánovaného ukončení činnosti Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru je detailně uvedena v interním dokumentu:

„NCA – Ukončení činnosti CA, TSA“.

6. Řízení technické bezpečnosti

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit, jim odpovídajících OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti, které probíhá v zabezpečených vyhrazených prostorách provozních pracovišť, podle předem připraveného scénáře, v souladu s požadavky kapitol 5.2 a 5.4.1 a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN.

Veškeré požadavky na proces generování párových dat CA jsou popsány v interní dokumentaci:

„Řízení fyzického přístupu do provozních prostor Národní certifikační autority

„NCA – HSM nShield, Směrnice pro správu“,

„NCA – HSM nShield, Postupy generování klíčů a certifikátů CA a OCSP“,

„NCA – Správa TSS“.

Protokol o průběhu generování párových dat obsahuje minimálně:

jmenný seznam přítomných zaměstnanců,

datum a čas zahájení a ukončení generace párových dat s přesností minimálně na minuty, místo, kde bylo generování prováděno,

popis zařízení, na kterém bylo generování prováděno, umožňující jednoznačnou identifikaci tohoto zařízení,

datum vyhotovení protokolu,

vlastnoruční podpisy všech pracovníků, kteří generování párových dat prováděli.

Generování párových dat pracovníků podílejících se na vydávání certifikátů je prováděno na čipových kartách, splňujících požadavky na QSCD. Soukromé klíče těchto párových dat jsou na čipové kartě uloženy v neexportovatelném tvaru a k jejich použití je nutné zadat PIN.

Generování párových dat vztahujících se k certifikátům vydávaným koncovým uživatelům je prováděno na zařízeních, která jsou pod výhradní kontrolou příslušných držitelů soukromých klíčů. Úložištěm těchto párových dat může být jak hardware, tak software. V případě kvalifikovaných certifikátů, jejichž soukromý klíč odpovídající veřejnému klíči v Certifikátu je uložen na zařízení typu QSCD, je průběžně prováděna kontrola přítomnosti zařízení na důvěryhodném seznamu EU.

6.1.2 Předávání soukromého klíče jeho držiteli

Pro soukromé klíče certifikačních autorit, jim odpovídajících OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti není relevantní – soukromé klíče jsou uloženy v kryptografických modulech.

Služba generování párových dat koncovým uživatelům a pracovníkům podílejícím se na vydávání certifikátů není poskytována.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejný klíč je certifikační autoritě doručen v žádosti o vydání certifikátu (formát PKCS#10).

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Veřejné klíče certifikačních autorit jsou obsaženy v certifikátech těchto certifikačních autorit, jejich získání je garantováno následujícími způsoby:

obdržením na RA,

prostřednictvím internetových informačních adres Správy, příslušného orgánu dohledu, resp. prostřednictvím věstníku příslušného orgánu dohledu,

každý žadatel o certifikát obdrží příslušné certifikáty certifikačních autorit při získání svého prvotního certifikátu.

6.1.5 Délky klíčů

Mohutnost klíčů kořenové certifikační autority Správy i vydávajících certifikačních autorit využívajících algoritmus RSA je 3072 bitů. Mohutnost klíčů ostatních vydávaných certifikátů je vždy uvedena v konkrétní CP.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti splňují požadavky uvedené v právní úpravě pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech nebo normách. Tyto klíče jsou generovány a kontrolovány příslušným technickým a programovým vybavením.

Parametry algoritmů použitých při generování veřejných klíčů ostatních držitelů certifikátů musí tyto požadavky rovněž splňovat a jsou stejným způsobem kontrolovány.

6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3)

Možnosti použití klíče jsou uvedeny v rozšíření certifikátu.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

Konkrétní postupy ochrany soukromého klíče uloženého v kryptografickém modulu pod kontrolu Správy jsou popsány v interní dokumentaci:

„Řízení fyzického přístupu provozních prostor Národní certifikační autority“,

„NCA – HSM nShield, Směrnice pro správu“,

„NCA – HSM nShield, Postupy generování klíčů a certifikátů CA a OCSP“,

„NCA – Správa TSS“.

6.2.1 Řízení a standardy kryptografických modulů

Generování párových dat a uložení soukromých klíčů certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti probíhá v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s jejich certifikací.

Pracovníci podílející se na vydávání certifikátů využívají čipové karty splňující požadavky na QSCD.

Používání kryptografických modulů dat ostatními koncovými uživateli je plně v jejich kompetenci.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

6.2.2 Soukromý klíč pod kontrolou více osob (m z n)

Pokud je pro činnosti spojené s kryptografickým modulem nezbytná přítomnost více osob, potom každá z nich zná pouze část kódu k provedení těchto činností.

6.2.3 Úschova soukromého klíče

Není relevantní pro tento dokument, služba úschovy soukromého klíče není poskytována.

6.2.4 Zálohování soukromého klíče

Soukromé klíče certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti chráněné kryptografickými moduly jsou zálohovány v zašifrované podobě, která zajišťuje stejnou úroveň ochrany jako kryptografické zařízení.

Pro soukromé klíče pracovníků podílejících se na vydávání certifikátů není relevantní, jsou vygenerovány na čipových kartách v neexportovatelném tvaru.

Zálohování soukromých klíčů ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.5 Uchovávání soukromého klíče

Soukromé klíče certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti nejsou nikde uchovávány, po uplynutí doby platnosti jsou včetně jejich záloh zničeny.

Doba uchování soukromých klíčů pracovníků podílejících se na vydávání certifikátů je dána kapacitou paměti čipové karty.

Uchovávání soukromých klíčů ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Soukromé klíče certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti jsou generovány v kryptografických modulech (jako neexportovatelné) a nelze je z kryptografického modulu (provozovaného v certifikovaném režimu) exportovat v žádném tvaru. Import soukromého klíče CA do kryptografického modulu není prováděn.

Pro transfer soukromých klíčů pracovníků podílejících se na vydávání certifikátů není relevantní, jsou vygenerovány v neexportovatelném tvaru.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti jsou uloženy v kryptografických modulech splňujících požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN.

Soukromé klíče pracovníků podílejících se na vydávání certifikátů jsou uloženy na čipových kartách splňujících požadavky na QSCD.

Případné uložení soukromých klíčů ostatních koncových uživatelů v kryptografických modulech je plně v kompetenci těchto koncových uživatelů.

6.2.8 Postup aktivace soukromého klíče

Aktivace soukromých klíčů (umožnění jejich použití) certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti v kryptografických modulech je prováděna:

v případě aktivace čipovou kartou – vložením čipové karty a zadáním hesla,

v případě aktivace pomocí softcard – předložením softcard a hesla.

Soukromé klíče pracovníků podílejících se na vydávání certifikátů jsou aktivovány vložením čipové karty do snímače a zadáním PIN.

Aktivace soukromých klíčů ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů a závisí na způsobu uložení těchto soukromých klíčů.

6.2.9 Postup deaktivace soukromého klíče

Deaktivace soukromých klíčů certifikačních autorit, jejich OCSP respondérů a soukromých klíčů pro vytváření kvalifikovaných elektronických pečeti v kryptografických modulech je provedena vyjmutím čipové karty nebo ukončením příslušné aplikace.

Deaktivace původního soukromého klíče TSU systému je provedena výběrem nového profilu.

Soukromé klíče pracovníků podílejících se na vydávání certifikátů jsou deaktivovány vyjmutím čipové karty ze snímače.

Deaktivace soukromých klíčů ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů a závisí na způsobu uložení těchto soukromých klíčů.

6.2.10 Postup ničení soukromého klíče

Ničení soukromých klíčů certifikačních autorit, jejich OCSP respondérů a TSU uložených v kryptografickém modulu je realizováno nativními prostředky tohoto kryptografického modulu a za přímé osobní účasti ředitele Správy nebo jím určené osoby podle přesně určeného postupu, který je upraven interní dokumentací:

„NCA – HSM nShield, Směrnice pro správu“.

O provedeném ničení je pořízen písemný záznam.

Nevratné znepřístupnění soukromého klíče využívaného k tvorbě kvalifikovaných elektronických pečeti je zajištěno vymazáním jemu příslušných čipových karet kryptografického modulu.

Externí média, na kterých jsou uloženy zálohy výše uvedených soukromých klíčů, jsou rovněž zničena. Ničení, spočívající ve fyzické destrukci těchto nosičů, probíhá za přímé osobní účasti ředitele Správy nebo jím určené osoby podle přesně určeného postupu, který je upraven interní dokumentací. O provedeném ničení je pořízen písemný záznam.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly, sloužící ke generování párových dat a využívané soukromými klíči certifikačních autorit, jejich OCSP respondérů, TSU a systému pro vytváření kvalifikovaných elektronických pečeti splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN, a jsou používány v souladu s příslušnou certifikací.

Čipové karty použité pro generování párových dat a uložení příslušných soukromých klíčů pracovníků podílejících se na vydávání certifikátů splňují požadavky na QSCD.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Případné použití kryptografických modulů ostatními koncovými uživateli včetně jejich hodnocení je plně v kompetenci těchto koncových uživatelů.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veškeré veřejné klíče jsou uchovávány ve formě certifikátů po celou dobu existence Správy.

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

Maximální doba platnosti každého vydaného certifikátu je uvedena v těle tohoto certifikátu a je stejná jako doba použitelnosti příslušných párových dat.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit, jejich OCSP respondérů, TSU i systému pro vytváření kvalifikovaných elektronických pečetí (čipová karta nebo softcard) jsou vytvářena před generováním nebo v průběhu generování příslušných párových dat.

Konkrétní postupy jsou popsány v interní dokumentaci:

„NCA – HSM nShield, Směrnice pro správu“,

„NCA – Správa TSS“.

Aktivačními daty soukromých klíčů pracovníků podílejících se na vydávání certifikátů je PIN, který je plně po kontrolou těchto pracovníků.

Případné použití aktivační dat ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.4.2 Ochrana aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit, jejich OCSP respondérů, TSU i systému pro vytváření kvalifikovaných elektronických pečetí (čipová karta nebo softcard) jsou chráněna nastaveným heslem.

Konkrétní postupy jsou popsány v interní dokumentaci:

„NCA – HSM nShield, Směrnice pro správu“,

„NCA – Správa TSS“.

Ochrana aktivačních dat soukromých klíčů pracovníků podílejících se na vydávání certifikátů je plně po kontrolou těchto pracovníků.

Případná ochrana aktivačních dat ostatních koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.4.3 Ostatní aspekty aktivačních dat

Není relevantní pro tento dokument.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování Služby je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů a jejich periodicity, definována právní úpravou pro služby vytvářející důvěru, resp. v ní odkazovanými technickými standardy a normami. Detailně je řešení popsáno v interní dokumentaci, zejména:

- „NCA – Systémová bezpečnostní politika (CA a TSA)“,
- „NCA – Řízení kontinuity provozu“,
- „NCA – Obnova systémů CA, TSA“,
- „NCA – Přemístění systémů CA, TSA“,
- „NCA – Záloha dat systémů“,
- „NCA – Uchovávání dat a informací“,
- „NCA – Příručka administrátora systémů CA, TSA“,
- „Řízení fyzického přístupu do provozních prostor Národní certifikační autority“,
- „NCA – HSM nShield, Směrnice pro správu“,
- „NCA – Správa TSS“.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti Správy je založeno na požadavcích uvedených v technických standardech a normách, zejména:

CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.

ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.

ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

ČSN ETSI EN 319 403 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb – Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb.

ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

ČSN ETSI EN 319 411-1 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 1: Obecné požadavky.

ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty – Část 2: Požadavky na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vtištění.“

ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

ČSN ETSI EN 319 412-1 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 1: Přehled a společné datové struktury.

ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.

ČSN ETSI EN 319 412-2 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 2: Profil certifikátu pro certifikáty vydávané fyzickým osobám.

ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.

ČSN ETSI EN 319 412-3 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 3: Profil certifikátu pro certifikáty vydávané právnickým osobám.

ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.

ČSN ETSI EN 319 412-4 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 4: Profil certifikátu pro certifikáty webových stránek.

ETSI EN 319 412-4 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.

ČSN ETSI EN 319 412-5 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu – Část 5: Prohlášení „QC Statements“.

ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

ČSN EN 419 221-5 Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby.

EN 419 221-5 Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services.

ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.

ČSN EN ISO/IEC 15408-2 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční komponenty.

ISO/IEC 15408-2:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components.

ČSN EN ISO/IEC 15408-3 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Komponenty bezpečnostních záruk.

ISO/IEC 15408-3:2008 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components.

FIPS PUB 140-2 Requirements for Cryptographic Modules.

ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

ČSN ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.

ISO 3166-1 Codes for the representation of names of countries and their subdivisions - Part 1: Country codes.

ITU-T - X.501 Information technology – Open Systems Interconnection – The Directory: Models.

ITU-T - X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

ITU-T - X.520 Information technology – Open Systems Interconnection – The Directory: Selected attribute types.

RSA Laboratories - PKCS#10: Certification Request Syntax Standard.

RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments.

RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

EN 301 549 Accessibility requirements for ICT products and services.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s Dohodou o narovnání uzavřenou mezi organizační složkou státu Správa základních registrů, organizační složkou státu Digitální a informační agentura a První certifikační autoritou, a.s., navazující na Rámcovou dohodu NCA ze dne 20. 10. 2020 a s jednotlivými dílčími dohodami, které jsou pro vývoj a zajištění provozu NCA uzavřeny a v souladu s interní dokumentací:

„Change management“.

6.6.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu s technickými standardy a normami, je prováděna v rámci periodických kontrol služeb vytvářejících důvěru.

Bezpečnost informací se ve Správě řídí těmito normami:

ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.

ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.

ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.

Detailně je problematika popsána v interním dokumentu:

„NCA – Kontrolní činnost, bezúhonnost a odbornost“.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při výtiskění.“

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je prováděno procesním přístupem typu „Plánování – Zavedení – Kontrola – Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

vybudování - stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou, což je popsáno v interní dokumentaci, mj.:

- „Politika řízení bezpečnosti informací“,
- „Zpráva o hodnocení aktiv a rizik systému NCA“
- „Bezpečnostní politika informačního systému NCA“,

implementace a provoz - účelné a systematické prosazení vybraných bezpečnostních opatření, což je popsáno v interní dokumentaci:

- „Řízení fyzického přístupu do provozních prostor Národní certifikační autority“,
- „NCA – HSM nShield, Směrnice pro správu“,
- „NCA – Záloha dat systémů“,
- „NCA – Příručka administrátora systémů CA, TSA“,
- „NCA – Kontrolní činnost, bezúhonnost a odbornost“,
- „Change management“,
- „Metodika řízení kybernetických bezpečnostních incidentů“,
- „NCA – Obnova systémů CA, TSA“,
- „NCA – Přemístění systémů CA, TSA“,

monitorování a přehodnocování - zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení Správy k posouzení, což je popsáno v dokumentech:

- zprávy z interních kontrol,
- zprávy z externích kontrol a auditů,

údržba a zlepšování - provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

6.7 Řízení bezpečnosti sítě

Důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru nejsou přímo dostupné z veřejné sítě Internet. Tyto systémy jsou chráněny komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System) v redundantní konfiguraci. Veškerá komunikace mezi RA a provozním pracovištěm je vedena šifrovaně.

Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

- „NCA – Systémová bezpečnostní politika (CA a TSA)“,
- „NCA – Příručka administrátora systémů CA, TSA“,
- „NCA – Řízení kontinuity provozu“,
- „NCA – Obnova systémů CA, TSA“,
- „NCA – Přemístění systémů CA, TSA“.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7. Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

Profily certifikátu, seznamu zneplatněných certifikátů a OCSP jsou vždy uvedeny v konkrétní CP. V následujících kapitolách mohou být případně popsány pouze změny, jejichž provedení si Správa v konkrétní certifikační politice vyhradila.

Přípustné typy a délka položek ve znacích pro pole Subject a SubjectAlternativeName, pokud jsou tyto v certifikátu obsaženy:

v kvalifikovaných certifikátech pro elektronický podpis a elektronickou pečeť jsou uvedeny v tabulce ve druhém sloupci tabulky 3

v nekvalifikovaných certifikátech jsou uvedeny ve třetím sloupci tabulky 3

Tabulka 3 - Typy a délka položek pole Subject a rozšíření SubjectAlternativeName

Pole/položka	Kvalifikované certifikáty pro elektronický podpis a elektronickou pečeť	Nekvalifikované certifikáty
Subject		
countryName	PrintableString (2)	PrintableString (2)
givenName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
surName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
pseudonym	UTF8String (1..128)	PrintableString, UTF8String (1..128)
serialNumber	PrintableString (1..64)	PrintableString (1..64)
commonName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
initials	UTF8String (1..64)	PrintableString, UTF8String (1..64)
emailAddress	IA5String (1..64)	IA5String (1..64)
name	UTF8String (1..128)	PrintableString, UTF8String (1..128)
generationQualifier	UTF8String (1..64)	PrintableString, UTF8String (1..64)
organizationName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
organizationalUnitName	UTF8String (1..64)	PrintableString, UTF8String (1..64)
title	UTF8String (1..64)	PrintableString,

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

		UTF8String (1..64)
stateOrProvinceName	UTF8String (1..128)	PrintableString, UTF8String (1..128)
localityName	UTF8String (1..128)	PrintableString, UTF8String (1..128)
streetAddress	UTF8String (1..128)	PrintableString, UTF8String (1..128)
postalCode	UTF8String (1..40)	PrintableString, UTF8String (1..40)
organizationIdentifier	UTF8String (1..128)	PrintableString, UTF8String (1..128)
businessCategory	UnboundDirectoryString (1..64)	
jurisdictionCountryName	PrintableString (2)	
jurisdictionStateOrProvince Name	UTF8String (1..128)	
jurisdictionLocalityName	UTF8String (1..128)	
SubjectAlternativeName		
rfc822Name	IA5String (1..320) kontrola: správný formát email adresy	IA5String (1..320) kontrola: správný formát email adresy

7.1 Profil certifikátu

Viz kapitola 7.

Číslo verze

Viz kapitola 7.

Rozšíření certifikátu

Viz kapitola 7.

Objektové identifikátory algoritmů

Viz kapitola 7.

Tvary jmen

Viz kapitola 7.

Omezení jmen

Viz kapitola 7.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

Objektový identifikátor certifikační politiky

Viz kapitola 7.

Použití rozšíření Policy Constraints

Viz kapitola 7.

Syntaxe a sémantika kvalifikátorů politiky

Viz kapitola 7.

Zpracování sémantiky kritického rozšíření Certificate Policies

Viz kapitola 7.

7.2 Profil seznamu zneplatněných certifikátů

Viz kapitola 7.

Číslo verze

Viz kapitola 7.

Rozšíření CRL a záznamů v CRL

Pro kvalifikované certifikáty obsahuje CRL rozšíření (ExpiredCertsOnCRL) udávající, že v něm jsou po definované dobu (viz 4.10.3) obsaženy i expirované certifikáty.

7.3 Profil OCSP

Profily OCSP žádosti i odpovědi jsou v souladu s RFC 6960 a RFC 5019.

OCSP odpovědi jsou typu BasicOCSPResponse a obsahují všechna povinná pole. V případě odvolaného certifikátu je uvedeno volitelné pole revocationReason. Pro certifikáty nevydané příslušnou CA je vrácena odpověď unAuthorized. Jako přenosový protokol je používáno pouze http.

Tabulka 4 - Profil OCSP žádosti

Položky žádosti	Poznámky
OCSPRequest ::= SEQUENCE {	
tbsRequest TBSRequest	
TBSRequest ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	
requestorName [1] EXPLICIT GeneralName OPTIONAL	
requestList SEQUENCE OF Request,	OCSP respondér odpoví pouze na první požadavek ze seznamu v OCSP žádosti, ostatní ignoruje (RFC 5019)
Request ::= SEQUENCE {	
<u>reqCert</u> CertID,	povinná položka, (pokud není obsažena, odpověď bude malformedRequest)
CertID ::= SEQUENCE {	

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

hashAlgorithm AlgorithmIdentifier,	OID hashovacího algoritmu pro následující dvě položky – identifikace vydavatele dotazovaného certifikátu specifikuje klient, OCSP respondér neomezuje (zpracuje žádosti se všemi hashAlgoritmy, které umí openssl).
issuerNameHash OCTET STRING,	hash pole vydavatele (Issuer) certifikátu, který je předmětem žádosti
issuerKeyHash OCTET STRING,	hash veřejného klíče vydavatele certifikátu, který je předmětem žádosti
serialNumber CertificateSerialNumber }	sériové číslo certifikátu, který je předmětem žádosti
<u>singleRequestExtensions</u> [0]EXPLICIT Extensions OPTIONAL	podle RFC 5019 nesmí být použito, pokud je přítomno v žádosti, je ignorováno
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	
Extension ::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	(podle RFC 6960 se zde se může vyskytovat: -ServiceLocator)
}	
requestExtensions [2] EXPLICIT Extensions OPTIONAL	ignorováno
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension	ignorována všechna Extensions
Extension ::= SEQUENCE {	
extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	(podle RFC 6960 se může vyskytovat: - Nonce – je ignorováno podle RFC 5019, - AcceptableResponses, - PreferredSignatureAlgorithms)
}	
optionalSignature [0] EXPLICIT Signature OPTIONAL	ignorováno (RFC 5019)
Signature ::= SEQUENCE {	
signatureAlgorithm AlgorithmIdentifier,	
signature BIT STRING	
certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL }	
}	

Tabulka 5 - Profil OCSP odpovědi

Položky odpovědi	Poznámky
OCSPResponse ::= SEQUENCE {	
responseStatus OCSPResponseStatus	
OCSPResponseStatus ::= ENUMERATED	(0) <i>successful</i> – úspěšná odpověď na OCSPRequest

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vtištění.“

	<p>(1) <i>malformedRequest</i> – vraceno v případě chyby syntaxe OCSPRequest; (2) <i>internalError</i> – interní chyba OCSP respondéru (3) <i>tryLater</i> – nepoužíváno (5) <i>sigRequired</i> – nikdy nevraceno, podpis žádosti není požadován (6) <i>unauthorized</i> – v případě, že OCSP respondér nepozná vydavatele = cizí certifikát (klient není oprávněn k provedení dotazu na tento server – RFC 6960, nebo server není schopen odpovědět autoritativně, např. nemá k dispozici autoritativní informaci o odvolání certifikátu – RFC5019)</p>
responseBytes [0] EXPLICIT ResponseBytes OPTIONAL }	pouze v případě OCSPResponseStatus= <i>successful</i>
ResponseBytes ::= SEQUENCE {	
responseType OBJECT IDENTIFIER	vždy <i>Basic OCSP Response</i>
response OCTET STRING	
BasicOCSPResponse ::= SEQUENCE {	
tbsResponseData ResponseData,	
ResponseData ::= SEQUENCE {	
version [0] EXPLICIT Version DEFAULT v1,	v1
responderID ResponderID,	
ResponderID ::= CHOICE { byName [1] Name, byKey [2] KeyHash }	vraceno byName=DN vydavatele
producedAt GeneralizedTime,	čas, kdy respondér podepsal odpověď
responses SEQUENCE OF SingleResponse,	vracena pouze jediná odpověď na první certifikát v seznamu v žádosti
SingleResponse ::= SEQUENCE {	
certID CertID,	
CertID ::= SEQUENCE { hashAlgorithm AlgorithmIdentifier, issuerNameHash OCTET STRING, issuerKeyHash OCTET STRING, serialNumber CertificateSerialNumber }	totožný obsah s atributem <i>CertID</i> uvedeným v žádosti
certStatus CertStatus,	stav odvolání platnosti certifikátu, jedna z vyjmenovaných možností níže
CertStatus ::= CHOICE {	
good [0] IMPLICIT NULL,	certifikát nebyl odvolán (v intervalu platnosti) nebo čas vytvoření OCSP

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

	odpovědi byl mimo interval platnosti certifikátu
revoked [1] IMPLICIT RevokedInfo,	certifikát byl odvolán (v intervalu platnosti)
RevokedInfo ::= SEQUENCE {	
revocationTime GeneralizedTime	čas zneplatnění certifikátu
revocationReason [0] EXPLICIT CRLReason OPTIONAL }	v odpovědi uváděn důvod
CRLReason ::= ENUMERATED	může obsahovat: <i>unspecified</i> (0), <i>keyCompromise</i> (1), <i>cACompromise</i> (2), <i>affiliationChanged</i> (3), <i>superseded</i> (4), <i>cessationOfOperation</i> (5), <i>removeFromCRL</i> (8), <i>privilegeWithdrawn</i> (9), <i>aACompromise</i> (10) Správa nepřipouští důvod odvolání <i>certificateHold</i> (6) = dočasné pozastavení, hodnota (7) není použita
unknown [2] IMPLICIT UnknownInfo UnknownInfo ::= NULL	Správa toto nepoužívá (používáno OCSPResponseStatus= unauthorized podle RFC 5019) (poskytovatel není schopen odpovědět, o stavu certifikátu „nic neví“, obvykle proto, že se jedná o cizí certifikát)
}	
thisUpdate GeneralizedTime,	čas, ke kterému je znám stav certifikátu
nextUpdate [1] EXPLICIT GeneralizedTime OPTIONAL,	vždy uvedeno (povinné dle RFC5019); čas, kdy končí platnost této odpovědi a do kdy bude dostupná nová odpověď
singleExtensions [1] EXPLICIT Extensions	
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension Extension ::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING }	odpověď může obsahovat rozšíření: - id-commonpki-at-certHash – vloženo nejméně u certifikátů SK (tzv. pozitivní prohlášení); pro hash z dotazovaného certifikátu se použije algoritmus podle podpisu certifikátu respondéru (sha256) - id-pkix-ocsp-archive-cutoff – pro kvalifikované certifikáty udává, po jakou dobu po expiraci certifikátu lze spoléhat na stav certifikátu uvedený v OCSP odpovědi
}	
responseExtensions [1] EXPLICIT Extensions OPTIONAL }	odpověď neobsahuje pole responseExtensions

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

<pre>Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension Extension ::= SEQUENCE { extnID OBJECT IDENTIFIER, critical BOOLEAN DEFAULT FALSE, extnValue OCTET STRING } } signatureAlgorithm AlgorithmIdentifier, signature BIT STRING, certs [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL } } } }</pre>	<p>(podle RFC 6960 zde může být: - id-pkix-ocsp-nonce, - id-pkix-ocsp-extended-revoke)</p> <p>sha256WithRSAEncryption</p> <p>uváděn: - certifikát vydávající CA - certifikát OCSP respondéru</p>
---	--

Číslo verze

Viz kapitola 7.3.

Rozšíření OCSP

Viz tabulky v kapitole 7.3.

OCSP odpověď vracející stav certifikátu "good" může obsahovat pozitivní prohlášení ve formě položky CertHash rozšíření singleExtensions.

8. Hodnocení shody a jiná hodnocení

Informace o hodnocení jsou uvedeny v konkrétních certifikačních politikách.

8.1 Periodicita nebo okolnosti hodnocení

Viz kapitola 8.

8.2 Identita a kvalifikace hodnotitele

Viz kapitola 8.

8.3 Vztah hodnotitele k hodnocenému subjektu

Viz kapitola 8.

8.4 Hodnocené oblasti

Viz kapitola 8.

8.5 Postup v případě zjištění nedostatků

Viz kapitola 8.

8.6 Sdělování výsledků hodnocení

Viz kapitola 8.

9. Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Provozovatelem všech certifikačních autorit a OCSP respondérů je Správa. Poplatky za vydávání certifikátů certifikačních autorit a OCSP respondérů nejsou účtovány.

Poplatky za vydání certifikátů koncových uživatelů nejsou účtovány.

Služba obnovení certifikátů certifikačních autorit a OCSP respondérů není poskytována.

9.1.2 Poplatky za přístup k certifikátu

Přístup elektronickou cestou k certifikátům není zpoplatněn.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) nebo stavech certifikátů (OCSP) není zpoplatněn.

9.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

9.1.5 Postup při refundování

Není relevantní pro tento dokument.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

Kvalifikovaným poskytovatelem služeb vytvářejících důvěru je státní příspěvková organizace. Za závazky příspěvkových organizací vzniklé v souvislosti s provozováním hlavní činnosti ručí stát dle § 74 zákona č. 218/2000 Sb. Tímto není dotčeno případné uzavření pojištění odpovědnosti Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru.

9.2.2 Další aktiva

Správa prohlašuje, že má k dispozici dostatečné finanční zdroje a jiná finanční zajištění na poskytování služeb vytvářejících důvěru s ohledem na riziko vzniku odpovědnosti za škodu.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument.

9.3 Důvěrnost obchodních informací

9.3.1 Rozsah důvěrných informací

Důvěrnými informacemi jsou veškeré informace, které nejsou označeny jako veřejné a nejsou zveřejňovány způsobem uvedeným v kapitole 2.2, zejména:

veškeré soukromé klíče, sloužící v procesu poskytování služeb systému NCA, případně obchodní informace Správy,

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

veškeré interní informace a dokumentace,
veškeré osobní údaje.

9.3.2 Informace mimo rámec důvěrných informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kapitole 2.2.

9.3.3 Odpovědnost za ochranu důvěrných informací

Žádný zaměstnanec Správy, který přijde do styku s důvěrnými informacemi, je nesmí bez souhlasu ředitele Správy poskytnout třetí straně.

9.4 Ochrana osobních údajů

Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je ve Správě řešena v souladu s požadavky příslušných právních předpisů, tedy zejména ZOOÚ a GDPR. Tyto požadavky jsou rozpracovány v interní dokumentaci:

„Interní směrnice SSSVD o ochraně osobních údajů v souladu s GDPR“,

„Politika řízení bezpečnosti informací“.

9.4.1 Informace považované za osobní údaje

Osobními informacemi jsou veškeré osobní údaje podléhající ochraně ve smyslu příslušných právních předpisů.

Zaměstnanci Správy, případně subjekty definované platnou právní úpravou přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

9.4.2 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespadají do působnosti příslušných právních předpisů.

9.4.3 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel Správy, je jmenován pověřenec pro GDPR.

9.4.4 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání osobních údajů a souhlasu s jejich zpracováním je ve Správě řešena v souladu s požadavky příslušných právních předpisů.

9.4.5 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní, účely je ve Správě řešeno v souladu s požadavky příslušných právních předpisů.

9.4.6 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje Správa striktně podle požadavků příslušných právních předpisů.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při výtiskání.“

9.5 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systémů poskytujících Službu, jsou chráněny autorskými právy Správy.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

Správa zaručuje, že:

použije soukromé klíče příslušné certifikátům Autority pouze k elektronickému označování vydávaných Certifikátů a seznamů zneplatněných certifikátů,

použije soukromé klíče OCSP respondéru Autority pouze v procesu poskytování odpovědí na stav Certifikátu,

vydávané certifikáty splňují náležitosti požadované právní úpravou pro služby vytvářející důvěru a relevantními technickými standardy a normami,

zneplatní Certifikáty vydané Autoritou, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

Správa zaručuje, že:

použije soukromé klíče certifikačních autorit pouze pro vydávání certifikátů koncovým uživatelům (vyjma kořenové certifikační autority Správy), vydávání seznamů zneplatněných certifikátů a k vydávání certifikátů OCSP respondérů,

použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,

certifikáty vydávané koncovým uživatelům splňují v případě certifikátů kvalifikovaných náležitosti požadované právní úpravou pro služby vytvářející důvěru a příslušnými technickými standardy a normami, v případě ostatních certifikátů náležitosti požadované příslušnými technickými standardy a normami,

zneplatní vydané certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CPS, resp. v konkrétní CP.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud:

držitel certifikátu neporušil povinnosti plynoucí mu ze smlouvy o poskytování Služeb, této CPS, resp. konkrétní CP,

spoléhající se strana neporušila povinnosti této CPS, resp. konkrétní CP.

Držitel certifikátu vydaného podle této CPS, resp. konkrétní CP uplatňuje záruku vždy u RA, která zpracovala jeho žádost o vydání tohoto certifikátu.

Správa vyjadřuje a poskytuje držitelům certifikátů a veškerým spoléhajícím se stranám záruky, že při vydávání těchto certifikátů a v průběhu doby jejich platnosti bude při jejich správě vyhovovat této CPS, resp. konkrétní CP.

Záruky zahrnují:

kontrolu práva žádat o certifikát,

ověření informací uváděných v žádosti o vydání certifikátu, včetně kontroly naplnění položek, obsažených v žádosti o certifikát (formát PKCS#10) a identity,

že smlouva o vydání certifikátu odpovídá platným právním předpisům,

že v režimu 24x7 je udržováno úložiště informací o stavu certifikátu,

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

že certifikát může být zneplatněn z důvodů uvedených v právní úpravě pro služby vytvářející důvěru a této CPS, resp. konkrétní CP.

9.6.2 Zastupování a záruky RA

Určená RA:

přejímá závazek za správnost jí poskytovaných služeb,

nevyřídí kladně žádost, pokud se nepodařilo ověřit některou z položek žádosti s výjimkou položek neověřovaných, nebo držitel certifikátu odmítá potřebné údaje sdělit, nebo není oprávněn k podání žádosti o certifikát,

v případě osobního podání žádosti o zneplatnění certifikátu odpovídá za včasné předání této žádosti k vyřízení na pracoviště CA,

odpovídá za vyřizování připomínek a stížností.

9.6.3 Zastupování a záruky držitele certifikátu

Ve smlouvě mezi Správou a držitelem certifikátu je vždy uvedeno, že je povinen řídit se ustanoveními CP, podle které byl certifikát vydán.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle CP, podle které byl certifikát vydán.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

9.7 Zřeknutí se záruk

Správa poskytuje pro pouze záruky uvedené v kapitole 9.6.

9.8 Omezení odpovědnosti

Správa neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované touto CP. Dále neodpovídá za škody vzniklé v důsledku porušení závazků Správy z důvodu vyšší moci. Další případná omezení odpovědnosti mohou být uvedena ve smlouvě (zápise) se zvláštní složkou.

9.9 Záruky a odškodnění

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platné právní úpravy týkající se vztahů mezi poskytovatelem a spotřebitelem a dále takové záruky, které byly sjednány mezi Správou a žadatelem o Služby. Smlouva nesmí být v rozporu s platnou právní úpravou a musí být vždy v elektronické nebo listinné formě.

Správa:

se zavazuje, že splní veškeré povinnosti definované jak platnou právní úpravou, včetně právní úpravy pro služby vytvářející důvěru v případě certifikátů kvalifikovaných, tak příslušnými politikami,

poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služeb,

další možné náhrady škody vycházejí z ustanovení příslušné právní úpravy a o jejich výši může rozhodnout soud.

Správa neodpovídá:

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služeb držitelem certifikátu, zejména za využívání v rozporu s podmínkami uvedenými v této CPS, resp. konkrétní CP, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení,

za škodu vyplývající z použití certifikátu v období po podání žádosti o jeho zneplatnění, pokud Správa dodrží definovanou lhůtu pro zveřejnění zneplatněného certifikátu na seznamu zneplatněných certifikátů (CRL nebo OCSP).

Reklamací je možné podat těmito způsoby:

e-mailem na adresu uvedenou v kapitole 2.2, předmět zprávy musí začínat textem NCA, prostřednictvím datové schránky Správy,

doporučenou poštovní zásilkou na adresu sídla Správy,

osobně v sídle Správy.

Reklamující osoba (držitel certifikátu nebo spoléhající se strana) je povinna uvést:

co nejvýstižnější popis závady,

sériové číslo reklamovaného produktu,

požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne Správa nejpozději do tří pracovních dnů od doručení reklamace. Vyrozumí o tom reklamujícího formou elektronické pošty, zprávy do datové schránky nebo doporučenou zásilkou, pokud se strany nedohodnou na jiném způsobu.

Reklamacie, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do třiceti dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

Nový certifikát bude příslušnému držiteli certifikátu poskytnut zdarma v následujících případech:

existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority,

v případě, že CA při příjmu žádosti o vydání certifikátu zjistí, že existuje jiný certifikát s duplicitním veřejným klíčem.

9.10 Doba platnosti, ukončení platnosti

Doba platnosti a podmínky ukončení platnosti certifikačních politik jsou vždy uvedeny v konkrétní CP.

9.10.1 Doba platnosti

Certifikační politiky – viz kapitole 9.10.

Tato CPS nabývá platnosti dnem účinnosti uvedeným na titulní straně dokumentu a platí do doby jejího nahrazení novou verzí, nebo minimálně po dobu platnosti posledního certifikátu vydané podle některé z certifikačních politik – viz kapitola 1.2.

9.10.2 Ukončení platnosti

Certifikační politiky – viz kapitola 9.10.

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CPS, je ředitel Správy.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

9.10.3 Důsledky ukončení a přetrvání závazků

Certifikační politiky – viz kapitola 9.10.

Tato CPS platí minimálně po dobu platnosti posledního certifikátu vydaného podle některé z certifikačních politik – viz kapitola 1.2.

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

Pokud jsou zúčastněné subjekty organizačnímu částmi Správy, řídí se komunikace mezi nimi interními pravidly Správy.

Pro individuální oznámení a komunikaci se zúčastněnými subjekty může Správa využít jimi dodané e-mailové adresy, poštovní adresy, telefonní čísla, osobní jednání atd.

Komunikovat se Správou lze taktéž způsoby uvedenými na internetové informační adrese.

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup v případě certifikačních politik je vždy popsán v konkrétní certifikační politice.

9.12.2 Postup a periodičita oznamování

Certifikační politiky – viz kapitola 9.12.

V případě této CPS – postup je realizován řízeným procesem popsáným v interním dokumentu.

9.12.3 Okolnosti, při kterých musí být změněn OID

Certifikační politiky – viz kapitola 9.12.

V případě této CPS – OID není přiřazován. V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

9.13 Ustanovení o řešení sporů

Pokud jsou všechny strany sporu organizačnímu částmi Správy, řídí se řešení sporů interními pravidly Správy.

V ostatních případech platí, že pokud držitel certifikátu nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

odpovědný pracovník RA,

odpovědný pracovník Správy (nutné elektronické nebo listinné podání),

ředitel Správy (nutné elektronické nebo listinné podání).

Uvedený postup dává nesouhlasící straně možnost prosazovat svůj názor rychlejším způsobem než soudní cestou.

9.14 Rozhodné právo

Správa se řídí právním řádem České republiky.

9.15 Shoda s platnými právními předpisy

Systém poskytování služeb vytvářejících důvěru je provozován ve shodě s právními předpisy České republiky a dále s relevantními mezinárodními standardy.

Veřejný řídicí dokument.

„Tento dokument pozbývá platnosti při jeho přemístění mimo referenční úložiště nebo při vytištění.“

9.16 Různá ustanovení

Další ustanovení jsou vždy popsána v konkrétní certifikační politice.

Rámcová dohoda

Viz kapitola 9.16.

Postoupení práv

Viz kapitola 9.16.

Oddělitelnost ustanovení

Viz kapitola 9.16.

Zřeknutí se práv

Viz kapitola 9.16.

Vyšší moc

Viz kapitola 9.16.

9.17 Další ustanovení

Není relevantní pro tento dokument.