

SPRÁVA STÁTNÍCH SLUŽEB VYTVÁŘEJÍCÍCH DŮVĚRU		
	SSVDX000FZUN prvotní identifikátor	
	SSSVD- 203-1/KŘ-2025	
	PD001C-2023	
PROVOZNÍ DOKUMENT	počet stran	59
	přílohy	0

NCA – Certifikační politika vydávání komerčních certifikátů fyzickým osobám (kryptografie RSA)

Oblast působnosti: Všichni zaměstnanci SSSVD, vybrané subjekty veřejné správy, mezi které patří bezpečnostní složky, zpravodajské služby a vybrané útvary resortu Ministerstva vnitra	
Gestor: Ing. Josef SCHOVAJSA	Nahrazuje: PD001B-2023 / v 1.02
Zpracovatel: František MARTINKA	Klasifikace: VEŘEJNÝ
Odborný garant: Jan STRNAD	Schváleno dne: <i>Datum uvedeno v doložce elektronického podpisu</i>
Schvalovatel: <i>podepsáno elektronicky</i> Ing. Michal PEŠEK, MBA	Účinnost od dne: 01. 08. 2025

HISTORIE DOKUMENTU:

ID	Verze	Datum	Autor	Popis změn
-	1.00	15. 09. 2023	První certifikační autorita, a.s.	Vytvoření první verze dokumentu
A	1.01	27. 09. 2023	První certifikační autorita, a.s.	Změna zkratky, změna doménové adresy
B	1.02	16. 11. 2023	První certifikační autorita, a.s.	Zpracovány připomínky auditora a orgánu dohledu
C	1.03	25. 07. 2025	František Martinka	Změna algoritmu podpisu

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	8
1.6	Přehled použitých pojmů a zkratk	9
2.	Odpovědnost za zveřejňování a za úložiště	13
2.1	Úložiště	13
2.2	Zveřejňování certifikačních informací	13
2.3	Čas nebo četnost zveřejňování	14
2.4	Řízení přístupu k jednotlivým typům úložišť	14
3.	Identifikace a autentizace	15
3.1	Pojmenování	15
3.2	Počáteční ověření identity	15
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	20
4.3	Vydání certifikátu	20
4.4	Převzetí vydaného certifikátu	21
4.5	Použití párových dat a certifikátu	21
4.6	Obnovení certifikátu	21
4.7	Výměna veřejného klíče v certifikátu	22
4.8	Změna údajů v certifikátu	23
4.9	Zneplatnění a pozastavení platnosti certifikátu	24
4.10	Služby ověřování stavu certifikátu	27
4.11	Konec smlouvy o vydávání certifikátů	28
4.12	Úschova a obnova klíčů	28
5.	Postupy správy, řízení a provozu	29
5.1	Fyzická bezpečnost	29
5.2	Procedurální postupy	30
5.3	Personální postupy	31
5.4	Postupy zpracování auditních záznamů	32
5.5	Uchovávání záznamů	34

Veřejný řídicí dokument

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

5.6	Výměna klíče	35
5.7	Obnova po havárii nebo kompromitaci	35
5.8	Ukončení činnosti CA nebo RA	36
6.	Řízení technické bezpečnosti	37
6.1	Generování a instalace párových dat	37
6.2	Ochrana soukromého klíče a technologie kryptografických modulů	38
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	43
6.8	Označování časovými razítky	43
7.	Profily certifikátu, seznamu zneplatněných certifikátů a OCSP	44
7.1	Profil certifikátu	44
7.2	Profil seznamu zneplatněných certifikátů	50
7.3	Profil OCSP	51
8.	Hodnocení shody a jiná hodnocení	52
8.1	Periodicita nebo okolnosti hodnocení	52
8.2	Identita a kvalifikace hodnotitele	52
8.3	Vztah hodnotitele k hodnocenému subjektu	52
8.4	Hodnocené oblasti	52
8.5	Postup v případě zjištění nedostatků	52
8.6	Sdělování výsledků hodnocení	52
9.	Ostatní obchodní a právní záležitosti	53
9.1	Poplatky	53
9.2	Finanční odpovědnost	53
9.3	Důvěrnost obchodních informací	53
9.4	Ochrana osobních údajů	54
9.5	Práva duševního vlastnictví	55
9.6	Zastupování a záruky	55
9.7	Zřeknutí se záruk	56
9.8	Omezení odpovědnosti	56
9.9	Záruky a odškodnění	56
9.10	Doba platnosti, ukončení platnosti	57
9.11	Individuální upozorňování a komunikace se zúčastněnými subjekty	58
9.12	Novelizace	58
9.13	Ustanovení o řešení sporů	58

9.14	Rozhodné právo	58
9.15	Shoda s platnými právními předpisy	58
9.16	Různá ustanovení.....	59
9.17	Další ustanovení.....	59

1. Úvod

Tento dokument stanoví zásady, 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 vydávání komerčních certifikátů (dále též „Služba, Certifikát“) fyzickým osobám. Pro Službu poskytovanou podle této certifikační politiky (dále též „CP“) je využíván algoritmus RSA.

Certifikáty vydávané podle této CP jsou určené pro ověřování elektronických podpisů, autentizaci klienta a šifrování.

Služba je poskytována všem koncovým uživatelům na základě uzavřeného smluvního vztahu. Správa nijak neomezuje potenciální koncové uživatele, poskytování Služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

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) v platném znění,
- 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 se standardy, normami nebo zákony, které nahradí dosud platné, bude vydána jeho nová verze.

1.1 Přehled

Dokument **NCA – Certifikační politika vydávání komerčních certifikátů fyzickým osobám (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.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání 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.

Bližší podrobnosti o naplnění polí a rozšíření Certifikátů vydávaných podle této CP a o jejich správě mohou být uvedeny v odpovídající certifikační prováděcí směrnici (dále jen „CPS“).

1.2 Název a jednoznačné určení dokumentu

Název tohoto dokumentu: NCA – Certifikační politika vydávání komerčních certifikátů fyzickým osobám (kryptografie RSA), verze 1.03

OID politiky: 1.2.203.19122063.10.1.71.1.0

1.3 Participující subjekty

1.3.1 Certifikační autority (dále “CA”)

Kořenová certifikační autorita Správy vydala ve dvoustupňové struktuře certifikačních autorit, v souladu s platnou právní úpravou a s požadavky technických standardů a norem, certifikát podřízené certifikační autoritě (dále též „Autorita“), provozované Správou. Tato Autorita vydává certifikáty dle této CP, certifikáty koncovým uživatelům podle jiných CP a certifikáty pro vlastní OCSP respondér.

1.3.2 Registrační autority (dále “RA”)

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

- 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.

Veřejný řídicí dokument

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

- 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

Držitelem vydávaného Certifikátu může být fyzická osoba, a to:

- zaměstnanec bezpečnostní/zvláštní složky,
- zaměstnanec Správy,
- zaměstnanec orgánu veřejné moci uvedeného v rejstříku orgánů veřejné moci vedeném Digitální a informační agenturou,
- zaměstnanec státního úřadu, nebo organizačních a jiných složek státu nevykonávající veřejnou moc,
- fyzická osoba určená ze strany orgánů veřejné moci.

Tato fyzická osoba je identifikovaná v Certifikátu jako držitel soukromého klíče spojeného s veřejným klíčem uvedeným v tomto Certifikátu.

Bezpečnostní/zvláštní složky, Správa, orgány veřejné moci uvedené v rejstříku orgánů veřejné moci vedeném Digitální a informační agenturou a státní úřady, nebo organizační a jiné složky státu nevykonávající veřejnou moc jsou dále též označovány jako Organizace.

1.3.4 Spoléhající se strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na Certifikáty vydávané podle této CP.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení a další, kterým to podle platné právní úpravy přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydávané podle této CP lze využívat v procesech ověřování elektronického podpisu, šifrování nebo pro autentizaci klienta.

1.4.2 Zakázané použití certifikátu

Certifikáty vydávané podle této CP nesmějí být používány v rozporu s přípustným použitím popsaným v kapitole 1.4.1 a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující dokument

Tuto CP, resp. jí odpovídající CPS, spravuje Správa.

1.5.2 Kontaktní osoba

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

Veřejný řídicí dokument

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

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů Správy uvedených v CPS s touto 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
bit	z anglického <i>binary digit</i> – číslice dvojkové soustavy – základní a současně nejmenší jednotka informace v číslicové technice
časové razítko	elektronické časové razítko, nebo 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	zaručená elektronická pečeť dle právní úpravy pro služby vytvářející důvěru
elektronický podpis	nebo zaručený 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
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
orgán dohledu	subjekt, dohlížejí na dodržování právní úpravy pro služby vytvářející důvěru
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické nebo listinné podobě
právní úprava pro služby vytvářející důvěru	nařízení eIDAS

prostředek pro vytváření elektronických podpisů	konfigurované programové vybavení nebo technické zařízení, které se používá k vytváření elektronických podpisů
služba vytvářející důvěru / kvalifikovaná služba vytvářející důvěru	elektronická služba / kvalifikovaná služba vytvářející důvěru, definovaná eIDAS
smluvní partner	subjekt zajišťující na základě písemné smlouvy pro Správu služby vytvářející důvěru nebo jejich části – nejčastěji se jedná o smluvní RA
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
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
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

Veřejný řídicí dokument

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

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
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

Veřejný řídicí dokument

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

PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
PSS	Probabilistic Signature Scheme, schéma elektronického podpisu vyvinuté M. Bellare a P. Rogawayem a standardizované jako část PKCS#1 v2.1
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu
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
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
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 časoměříče“ 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 kořenové certifikační autority nebo certifikátu podřízené vydávající autority 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

Správa zveřejňuje informace s následující periodicitou:

- certifikační politika - po schválení a vydání nové verze,
- certifikační prováděcí směrnice - neprodleně,
- seznam vydaných Certifikátů - aktualizace při každém vydání nového Certifikátu určeného ke zveřejnění,
- seznam zneplatněných certifikátů (CRL) - viz kapitola 4.9.7,
- ostatní veřejné informace - není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb.

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.

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 kapitole 7.

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Certifikáty vydávané podle této CP nepodporují anonymitu, podporují používání pseudonymu.

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

Autorita zaručuje jedinečnost obsahu pole Subject v Certifikátu příslušného držitele tohoto Certifikátu.

3.1.6 Uznávání, ověřování a posílání obchodních značek

Certifikáty vydávané podle této CP mohou obsahovat pouze obchodní značky, jejichž vlastnictví nebo pronájem byly doloženy. Veškeré důsledky plynoucí z neoprávněného užívání ochranné známky nese držitel Certifikátu.

3.2 Počáteční ověření identity

Subjekty oprávněné podat žádost o vydání Certifikátu jsou vyjmenovány v kapitole 4.1.1. V následujících kapitolách jsou uvedena pravidla pro počáteční ověření jejich identity.

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 elektronicky podepsána a držitel soukromého klíče tak prokazuje, že v době tvorby elektronického podpisu tento soukromý klíč vlastnil.

3.2.2 Ověřování identity organizace

Pro ověření právnické osoby nebo organizační složky státu musí být předložen:

- originál nebo úředně ověřená kopie výpisu z obchodního nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy, nebo

- vytištěný výtah z veřejně dostupných registrů, který předloží žadatel nebo jej vyhotoví operátor RA.

Tento dokument musí obsahovat úplné obchodní jméno, identifikační číslo (je-li přiřazeno), adresu sídla, jméno/jména osoby/osob oprávněné/oprávněných k zastupování (statutárních zástupců).

3.2.3 Ověřování identity fyzické osoby

Kapitola popisuje způsob ověřování identity fyzické osoby, tj.:

- fyzické osoby, držitele Certifikátu,
- fyzické osoby zastupující Organizaci žádající o vydání Certifikátu pro držitele Certifikátu (zaměstnance).

V případě, že se jedná o žádost o Certifikát bez pseudonymu, osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Osobním dokladem pro cizince je platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu.

Z tohoto dokladu jsou ověřovány následující údaje:

- celé občanské jméno,
- datum a místo narození, nebo rodné číslo, je-li v dokladu uvedeno,
- číslo předloženého osobního dokladu,
- adresa trvalého bydliště (je-li v dokladu uvedena).

Pokud v předloženém osobním dokladu není adresa trvalého bydliště uvedena, nemůže být uvedena v žádosti o Certifikát a následně ve vydaném Certifikátu.

V případě zaměstnance Organizace je dále vyžadováno potvrzení o zaměstnaneckém poměru k Organizaci. Toto potvrzení předloží držitel Certifikátu na RA, může však být prokázáno způsobem definovaným v uzavřené smlouvě mezi Správou a Organizací.

V případě, že se jedná o žádost o Certifikát s pseudonymem, osobním dokladem může být kromě platného občanského průkazu nebo cestovního pasu také platný služební průkaz obsahující minimálně fotografii žadatele a jemu přidělené služební číslo. Pokud osobním dokladem je služební průkaz, musí být dále dodáno potvrzení vystavené příslušným personálním oddělením o tom, že žadatel je oprávněn žádat o Certifikát s pseudonymem. V potvrzení musí být uvedeno přidělené služební číslo shodné se služebním číslem uvedeným na služebním průkazu. Toto potvrzení se považuje rovněž za potvrzení o zaměstnaneckém poměru.

Podmínkou použití služebního průkazu jako osobního dokladu je, aby organizace, která služební průkaz vydala, uchovala po dobu 25 let údaje, na jejichž základě je možné jednoznačně identifikovat osobu, které byl služební průkaz vydán.

Osoba oprávněná jednat za Organizaci se musí prokázat osobním dokladem – viz výše. V případě, že tato osoba není ze zákona osobou oprávněnou k zastupování Organizace, je dále požadována úředně ověřená plná moc k zastupování Organizace podepsaná statutárním zástupcem Organizace.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Neověřovanými informacemi jsou:

- generationQualifier (generační kvalifikátor).

3.2.5 Ověřování kompetencí

Příznak, že klíčový pár byl generován a uložen na bezpečném kryptografickém zařízení, lze do Certifikátu vložit pouze tehdy, byla-li tato skutečnost v procesu vydání Certifikátu pro tuto žádost ověřena.

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

Identifikace a autentizace při běžném požadavku na výměnu klíče se prokazuje tak, že žádost o vydání následného Certifikátu ve struktuře PKCS#10 musí být navíc opatřena elektronickým podpisem s využitím soukromého klíče odpovídajícího veřejnému klíči obsaženému v platném Certifikátu, který je předmětem výměny.

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 (prvotní) Certifikát s novým veřejným klíčem. Platí stejné požadavky jako v případě počátečního ověření identity.

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Subjekty oprávněné podat žádost o zneplatnění Certifikátu jsou vyjmenovány v kapitole 4.9.2.

Pro žádost podanou držitelem certifikátu platí:

- V případě **osobního předání žádosti o zneplatnění Certifikátu na RA** musí být žádost o zneplatnění Certifikátu písemná a podepsaná osobou, jejíž identita musí být řádně ověřena osobním dokladem (viz kapitola 3.2.3).
- V případě **předání žádosti o zneplatnění Certifikátu elektronickou cestou** jsou přípustné tyto způsoby identifikace a autentizace:
 - prostřednictvím formuláře na webových stránkách Správy (s využitím hesla pro zneplatnění Certifikátu),
 - prostřednictvím nepodepsané elektronické zprávy obsahující heslo pro zneplatnění Certifikátu odeslané na adresu uvedenou v kapitole 2.2, předmět zprávy musí začínat textem NCA ZNEPLATNĚNÍ,

- prostřednictvím podepsané elektronické zprávy (elektronický podpis musí být realizován soukromým klíčem příslušným k Certifikátu, který má být zneplatněn), odeslané na adresu uvedenou v kapitole 2.2, předmět zprávy musí začínat textem NCA ZNEPLATNĚNÍ,
 - prostřednictvím datové schránky Správy (s využitím hesla pro zneplatnění Certifikátu),
 - prostřednictvím definované osoby pověřené za Organizaci vystupovat ve smluvním vztahu se Správou.
- V případě použití listovní zásilky pro předání žádosti o zneplatnění Certifikátu s využitím hesla pro zneplatnění Certifikátu musí být tato zaslána doporučeně na adresu sídla Správy.

Pro žádost podanou subjektem, který k tomu byl explicitně určen ve smlouvě o poskytování Služby podle této CP, nebo osobou pověřenou jednáním za právního nástupce původního subjektu (Organizace), jemuž byl pro jeho zaměstnance Certifikát vydán, platí:

- Žádost musí být písemná a podepsaná osobou explicitně určenou ve smlouvě. Její identita musí být řádně ověřena osobním dokladem.
- V případě jednání za právního nástupce musí být dále předložen originál, nebo ověřená kopie rozhodnutí o nástupnictví.

Pro žádost podanou poskytovatelem Služby platí:

- Žádost musí být podepsaná ředitelem Správy, nebo jím pověřenou osobou. Jejich identita musí být řádně ověřena osobním dokladem. Pokud pověřená osoba není osobou ze zákona oprávněnou k zastupování Správy, je dále požadována úředně ověřená plná moc k zastupování Správy podepsaná statutárním zástupcem.

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

Správa si vyhrazuje právo akceptování i jiných forem postupů při identifikaci a autentizaci požadavků na zneplatnění Certifikátu, které však nesmí být v rozporu s platnou právní úpravou nebo s požadavky technických standardů a norem.

4. Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

O vydání Certifikátu mohou požádat Organizace pro svého zaměstnance, nebo fyzická osoba pro sebe samu – viz kapitola 1.3.3.

4.1.2 Registrační proces a odpovědnosti

Registrační proces prováděný pouze v případě vydávání prvotního Certifikátu zahajuje držitel soukromého klíče dostavením se s potřebnými dokumenty a případně s žádostí o Certifikát na pracoviště RA, kde případně probíhá zanesení údajů obsažených v předkládaných dokladech do informačního systému Autority a zpracování žádosti o Certifikát.

Držitel soukromého klíče, resp. držitel Certifikátu je povinen zejména:

- seznámit se s touto CP a smluvně se zavázat jednat podle ní,
- poskytovat pravdivé a úplné informace pro vydání Certifikátu,
- překontrolovat, zda údaje uvedené v žádosti o Certifikát a ve vydaném Certifikátu jsou správné a odpovídají požadovaným údajům,
- zvolit vhodné heslo pro zneplatnění Certifikátu (minimální/maximální délka hesla 4/32 znaků, povolené znaky 0..9, A..Z, a..z).

Poskytovatel Služby je povinen zejména:

- před uzavřením smlouvy o vydání Certifikátu informovat držitele Certifikátu, popř. Organizaci o smluvních podmínkách,
- uzavírat s držitelem Certifikátu, popř. s Organizací smlouvu o vydání Certifikátu, obsahující náležitosti požadované technickými standardy a normami,
- v procesu vydávání Certifikátu na RA ověřit všechny ověřitelné údaje uvedené v žádosti podle předložených dokladů,
- v případě, že soukromý klíč byl generován a uložen na bezpečném kryptografickém zařízení, vyžadovat prokázání této skutečnosti,
- vydat Certifikát obsahující věcně správné údaje na základě informací, které jsou poskytovateli Služby k dispozici v době vydávání tohoto Certifikátu,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- zveřejnit certifikáty Autority a kořenové CA,
- činnosti spojené se Službou poskytovat v souladu s uzavřenou smlouvou, touto CP, příslušnou CPS, Systémovou bezpečnostní politikou a provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Provádění identifikace a autentizace

Při vydávání **prvotního Certifikátu** jsou identifikace a autentizace prováděny podle kapitoly 3.2.3, případně kapitoly 3.2.2, v případě vydávání **následného Certifikátu** pak podle kapitoly 3.3.1.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

V procesu rozhodování o přijetí nebo zamítnutí žádosti o vydání **prvotního Certifikátu** provádějí pracovnice/pracovníci (dále jen pracovníci) RA:

- vizuální kontrolu shody údajů obsažených v žádosti o Certifikát (struktura PKCS#10) s údaji obsaženými v předkládaných dokladech,
- vizuální kontrolu formální správnosti údajů.

Ověřování vlastnictví soukromého klíče, kontrola kompetencí a kontroly formální správnosti údajů jsou prováděny i programovým vybavením systému RA.

Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen, v opačném případě je postupováno v souladu s ustanoveními kapitoly 4.3.

Postup vydání **následného Certifikátu** je popsán v kapitole 4.3.

4.2.3 Doba zpracování žádosti o certifikát

Po kladném rozhodnutí o vydání Certifikátu je Správa povinna neprodleně Certifikát vydat. Přibližné časové údaje pro vydání Certifikátu v pracovní dny a hodiny, není-li smluvně ošetřeno jinak, jsou uvedeny v následujícím seznamu:

- prvotní Certifikát - doba vydání je do 15 minut a jen ve výjimečných případech může být tato doba delší,
- následný Certifikát - jednotky minut.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

V procesu vydávání Certifikátu je programovým vybavením jádra systému CA prováděno další ověřování vlastnictví soukromého klíče, podporovaných hashovacích funkcí v žádosti o Certifikát (minimálně sha-256), kontrola kompetencí a kontroly formální správnosti údajů. Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen, v opačném případě je Certifikát vydán.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

V procesu vydávání **prvotního Certifikátu** je držitel Certifikátu, resp. držitel soukromého klíče informován prostřednictvím pracovníka RA a Certifikát je zaslán na e-mailovou adresu, pokud byla v žádosti o Certifikát uvedena.

V případě vydání **následného Certifikátu** je tento Certifikát získán s využitím programového vybavení na zařízení koncového uživatele, případně zaslán na e-mailovou adresu, pokud byla v žádosti o prvotní Certifikát uvedena.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání Certifikátu, je povinností držitele Certifikátu tento Certifikát přijmout. Jediným způsobem, jak odmítnout převzetí Certifikátu, je zažádat v souladu s touto CP o jeho zneplatnění.

4.4.2 Zveřejňování certifikátů certifikační autoritou

Správa zajistí zveřejnění jí vydaných Certifikátů.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitelů Certifikátů je zejména:

- dodržovat veškerá relevantní ustanovení smlouvy o poskytování této Služby,
- používat soukromý klíč a odpovídající Certifikát vydaný podle této CP pouze pro účely stanovené v této CP,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči obsaženému v Certifikátu vydaném podle této CP, takovým způsobem, aby nemohlo dojít k jeho neoprávněnému použití,
- neprodleně uvědomit poskytovatele Služby o skutečnostech, které vedou ke zneplatnění Certifikátu, zejména o podezření, že soukromý klíč byl zneužit, resp. o neplatnosti údajů v Certifikátu, v takovém případě 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:

- získat z bezpečného zdroje (www.narodni-ca.gov.cz, pracoviště RA) certifikáty certifikačních autorit související s Certifikátem vydaným podle této CP, ověřit hodnoty jejich otisků a jejich platnost,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že Certifikát je platný,
- dodržovat veškerá ustanovení této CP.

4.6 Obnovení certifikátu

Službou obnovení Certifikátu je podle této CP 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 (prvotního) 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.

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Kdo může žádat o obnovení

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 4.6.

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.6.

4.7 Výměna veřejného klíče v certifikátu

Službou výměny veřejného klíče v Certifikátu je podle této CP míněno vydání nového Certifikátu s jiným veřejným klíčem, ale s totožným obsahem položek uvedených v poli Subject nebo rozšíření SubjectAlternativeName Certifikátu, jehož veřejný klíč je předmětem výměny.

V případě, že proces vydání nového Certifikátu probíhá výhradně elektronickou cestou, kdy není vyžadována přítomnost fyzické osoby na pracovišti RA, jedná se o vydání následného Certifikátu. Požadavky na ověření elektronické žádosti o vydání následného Certifikátu jsou uvedeny v kapitole 4.7.1, pokud splněny nejsou, jedná se o vydání prvotního Certifikátu počínající registračním procesem.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Žádost o vydání následného Certifikátu (struktura pkcs#10] s vyměněným veřejným klíčem musí splňovat níže uvedené podmínky:

- položky pole Subject nebo rozšíření SubjectAlternativeName musí být totožné jako v Certifikátu, který je předmětem výměny,
- veřejný klíč musí být jiný než v Certifikátu, který je předmětem výměny,
- proces ověření elektronické žádosti o vydání následného Certifikátu je proveden v souladu s kapitolou 3.3.1.

4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu

Výměnu veřejného klíče v příslušném Certifikátu je oprávněn požadovat držitel tohoto Certifikátu.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Pokud jsou splněny podmínky pro výměnu veřejného klíče, je postupováno v souladu s kapitolami 4.2 a 4.3.1, v opačném případě je řízení k vydání Certifikátu ukončeno.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Uvedeno v kapitole 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Uvedeno v kapitole 4.4.1.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Uvedeno v kapitole 4.4.2.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Uvedeno v kapitole 4.4.3.

4.8 Změna údajů v certifikátu

Službou změny údajů v Certifikátu je podle této CP míněno vydání nového Certifikátu s minimálně jednou změnou v obsahu položek uvedených v poli Subject nebo rozšíření SubjectAlternativeName vztahujících se k držiteli Certifikátu, nebo s odebraným, nebo přidaným dalším polem, jehož obsah musí být ověřen. Veřejný klíč musí být jiný než v Certifikátu, který je předmětem změny.

Služba změny údajů v Certifikátu není poskytována. Vždy jedná o vydání nového (prvotního) 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.

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádost o zneplatnění Certifikátu přijímá Správa nepřetržitě pouze prostřednictvím předání žádosti elektronickou cestou a listovní zásilkou. Osobní předání na RA je možné pouze v pracovní době příslušné RA.

Službu pozastavení platnosti Certifikátu Správa neposkytuje.

4.9.1 Podmínky pro zneplatnění

Certifikát musí být zneplatněn mj. 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 této CP ze strany držitele Certifikátu, popř. Organizace,
- v případech, kdy nastanou skutečnosti uvedené v 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.

Správa si vyhrazuje právo akceptování i jiných podmínek na zneplatnění Certifikátu, které však nesmí být v rozporu s platnou právní úpravou.

4.9.2 Kdo může požádat o zneplatnění

Žádost o zneplatnění Certifikátu mohou podat:

- držitel Certifikátu,
- subjekt, který k tomu byl explicitně určen ve smlouvě o poskytování Služby podle této CP,
- osoba oprávněná z pozůstalostního řízení držitele Certifikátu, pokud nebyl zaměstnancem Organizace,
- osoba pověřená jednáním za právního nástupce Organizace,,
- poskytovatel této 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,

Veřejný řídicí dokument

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

- dozví-li se prokazatelně, že Certifikát byl použit v rozporu s omezením definovaným v kapitole 1.4.2,
- 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.

4.9.3 Postup při žádosti o zneplatnění

V případě osobního předání žádosti o zneplatnění Certifikátu na RA musí žádost obsahovat sériové číslo Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“), jméno, popř. jména a příjmení fyzické osoby oprávněné žádat zneplatnění Certifikátu a heslo pro zneplatnění Certifikátu. Pokud fyzická osoba oprávněná žádat zneplatnění Certifikátu heslo pro zneplatnění nezná, musí tuto skutečnost do písemné žádosti explicitně uvést, včetně čísla osobního dokladu předloženého při žádosti o vydání Certifikátu, nebo čísla nového osobního dokladu, pokud byl původní nahrazen novým. Tímto osobním dokladem se musí pracovníkovi RA prokázat. V případě, že je žádost oprávněná, pracovník RA Certifikát zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku. V případě, že žádost o zneplatnění Certifikátu nelze akceptovat (nesprávné heslo pro zneplatnění, neprokazatelná identita fyzické osoby oprávněné žádat zneplatnění Certifikátu), pokusí se pracovník RA tyto skutečnosti napravit a pokud to z libovolného důvodu nebude možné, žádost o zneplatnění Certifikátu bude zamítnuta. Žadatel o zneplatnění Certifikátu je vždy o výsledku informován prostřednictvím pracovníka RA.

V případě předání žádosti o zneplatnění Certifikátu elektronickou cestou jsou přípustné následující možnosti:

- Prostřednictvím formuláře na internetové informační adrese. Datum a čas zneplatnění Certifikátu jsou dány zpracováním platné žádosti o zneplatnění Certifikátu informačním systémem CA. O kladném vyřízení je žadatel informován.
- Elektronicky podepsaná zpráva – tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

Zadam o zneplatneni certifikatu cislo = xxxxxxxx,

kde „xxxxxxx“ je sériové číslo Certifikátu a musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

Zpráva musí být elektronicky podepsána soukromým klíčem odpovídajícím veřejnému klíči ve zneplatňovaném Certifikátu.

- Elektronicky nepodepsaná elektronická zpráva - tělo zprávy musí obsahovat text (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

Zadam o zneplatneni certifikatu cislo = xxxxxxxx

Heslo pro zneplatneni = yyyyyyy,

kde „xxxxxxx“ je sériové číslo Certifikátu a „yyyyyy“ je heslo pro zneplatnění. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

- Elektronicky podepsaná či ve zvláštních případech nepodepsaná zpráva odeslaná definovanou osobou pověřenou za Organizaci vystupovat ve smluvním vztahu se Správa:

Zadam o zneplatneni certifikatu cislo = xxxxxxxx

kde „xxxxxxx“ je sériové číslo Certifikátu. Sériové číslo musí být buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“).

Pozn.: Pokud žádost splňuje požadavky tří výše uvedených možností, odpovědný pracovník Certifikát v systému CA neprodleně zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku informačním systémem CA. O kladném vyřízení je žadatel informován.

V případě použití doporučené listovní zásilky pro podání žádosti o zneplatnění Certifikátu musí být žádost v následujícím tvaru (v českém nebo slovenském jazyce, s diakritikou nebo bez diakritiky, případně v jazyce anglickém):

Zadam o zneplatneni certifikatu cislo = xxxxxxxx

Heslo pro zneplatneni = yyyyyy,

kde „xxxxxxx“ je sériové číslo Certifikátu a „yyyyyy“ je heslo pro zneplatnění. Sériové číslo je buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“). V případě, že žádost uvedené požadavky splňuje, odpovědný pracovník Správy Certifikát v informačním systému CA zneplatní – datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku v informačním systémem CA. V případě, že žádost nelze akceptovat (nesprávné heslo pro zneplatnění) bude žádost o zneplatnění Certifikátu zamítnuta. O vyřízení žádosti je žadatel informován doporučeným dopisem na poštovní adresu uvedenou jako adresa odesílatele.

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 spoléhajících se stran při kontrole zneplatnění

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

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je vydáván neprodleně po kladném zpracování žádosti o zneplatnění Certifikátu. Nedojde-li ke zneplatnění Certifikátu, je nový CRL vydáván zpravidla dvakrát denně, nejvýše však 24 hodin od vydání předchozího CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL je vždy vydán nejvýše 24 hodin od vydání předchozího CRL.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Služba ověřování stavu Certifikátu 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.

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 v Autoritou vydaných Certifikátech.

Skutečnost, že Autorita poskytuje informace o stavu Certifikátu formou OCSP, je uvedena v jí vydaných Certifikátech.

4.10.2 Dostupnost služeb

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

4.10.3 Další charakteristiky služeb stavu certifikátu

Není relevantní pro tento dokument, další charakteristiky služeb stavu certifikátu nejsou poskytovány.

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.

4.12.1 Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

4.12.2 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

5.1.1 Umístění a konstrukce

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

5.1.2 Fyzický přístup

Ochrana prostor, kde jsou umístěny důvěryhodné systémy určené k podpoře Služby, je řešena elektronickým zabezpečovacím systémem (EVS), 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 $20\text{ }^{\circ}\text{C} \pm 5\text{ }^{\circ}\text{C}$. 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 stoletou 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 Služby, je instalována elektronická požární signalizace (EPS). Vstupní dveře těchto prostor jsou opatřeny protipožární vložkou. V místnosti pro administraci se nachází hasicí přístroj.

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 (3. 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.

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

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.

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.

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 Služby,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní zaměstnanci Správy podílející se na zajištění Služby 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.

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.

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.

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.

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.

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 popsaným v interních dokumentech a řídícím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

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.

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

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované příslušnými technickými standardy a normami, mj. o životním cyklu Certifikátů.

Speciálním případem zaznamenávání událostí je událost generování párových dat certifikačních autorit. Celý proces probíhá v souladu 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 kořenové certifikační 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 vydávajících certifikačních autorit zprávu jako svědek, že zpráva správně popisuje postup generování, podepisuje osoba v důvěryhodné roli.

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.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní dokumentaci, 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.

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 s důvěryhodnými systémy určenými k podpoře Služby je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

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

5.5.1 Typy uchovávaných záznamů

Správa uchovává níže uvedené záznamy (v elektronické nebo papírové podobě), které souvisejí s poskytovanou Službou, zejména:

- zprávy o průběhu generování párových dat certifikačních autorit,
- dokumenty související s životním cyklem vydaných Certifikátů, včetně těchto Certifikátů a certifikátů s nimi souvisejících,
- 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.

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.

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:

Veřejný řídicí dokument

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

- 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.

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 interním dokumentem pro řízení kontinuity provozu a případně s další relevantní interní dokumentací.

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,
- případně oznámí 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 bezprostředně ohrožena bezpečnost Služby.

5.7.4 Schopnost obnovit činnost po havárii

V případě havárie postupuje Správa v souladu s interním dokumentem pro řízení kontinuity provozu s další relevantní interní dokumentací.

5.8 Ukončení činnosti CA nebo RA

Pro ukončování činnosti Autority platí následující pravidla:

- ukončení činnosti Autority musí být písemně oznámeno všem držitelům platných Certifikátů a subjektům, které mají se Správou uzavřenou smlouvu přímo se vztahující k poskytování Služby,
- ukončení činnosti Autority musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- pokud je součástí ukončení činnosti Autority 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 i jen jediného Certifikátu vydaného Autoritou musí Autorita či její nástupce v případě zániku zajistit alespoň služby zneplatňování Certifikátů a vydávání CRL,
- následně Autorita prokazatelně zničí svůj soukromý klíč a o tomto zničení provede záznam, který bude uchováván podle pravidel této CP.

V případě ukončení poskytování Služby bude postupováno v souladu s uzavřenými smlouvami, případně s příslušnými technickými standardy nebo normami.

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

Problematika plánovaného ukončení činnosti Správy jako kvalifikovaného poskytovatele služeb vytvářejících důvěru je detailně uvedena v interní dokumentaci.

6. Řízení technické bezpečnosti

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat certifikačních autorit a jejich OCSP respondérů, které probíhá v zabezpečených vyhrazených prostorách provozních pracovišť v souladu s požadavky kapitol 5.2 a 5.4.1, je prováděno v kryptografických modulech, které splňují požadavky právní úpravy pro služby vytvářející důvěru, tedy standardů ETSI a CEN.

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.

Veškeré požadavky na proces generování výše uvedených párových dat jsou popsány v interní dokumentaci.

Generování párových dat vztahujících se k Certifikátům je prováděno na zařízeních, která jsou pod výhradní kontrolou příslušných držitelů soukromých klíčů. Úložištěm těchto párových dat může být jak hardware, tak software.

6.1.2 Předávání soukromého klíče jeho držiteli

Pro soukromé klíče certifikačních autorit a jejich OCSP respondérů není relevantní – soukromé klíče jsou uloženy v kryptografických modulech.

Služba generování párových dat držitelům Certifikátů a pracovníkům podílejícím se na vydávání certifikátů není poskytována.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

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

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Získání veřejného klíče certifikační autority obsaženého v jejím certifikátu je garantováno následujícími způsoby:

- obdržení na RA (osobní návštěva),
- prostřednictvím internetových informačních adres Správy, příslušného orgánu dohledu, resp. prostřednictvím věstníku tohoto orgánu dohledu,
- každý žadatel o certifikát obdrží příslušné certifikáty certifikačních autorit při získání svého prvotního certifikátu.

6.1.5 Délky klíčů

Pro Službu poskytovanou podle této CP je výhradně využíván asymetrický algoritmus RSA. Mohutnost klíče kořenové certifikační autority Správy je 3072 bitů, mohutnost klíčů v jí vydávaných certifikátech podřízených certifikačních autorit je rovněž 3072 bitů, mohutnost klíčů vydávaných certifikátů OCSP respondérů je 2048 bitů. Mohutnost klíčů v certifikátech vydávaných podle této CP je 2048 bitů.

Veřejný řídicí dokument

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

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit a jejich OCSP respondérů 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

6.2.1 Řízení a standardy kryptografických modulů

Generování párových dat certifikačních autorit a jejich OCSP respondérů a uložení odpovídajících soukromých klíčů je prováděno 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 koncovými uživateli je plně v jejich kompetenci.

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

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 a jejich OCSP respondérů 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 koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.5 Uchovávání soukromého klíče

Soukromé klíče certifikačních autorit a jejich OCSP respondérů 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 koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů 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.

Transfer soukromých klíčů koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů 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 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 a jejich OCSP respondérů 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 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 a jejich OCSP respondérů v kryptografických modulech je provedena vyjmutím čipové karty nebo ukončením příslušné aplikace.

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

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

6.2.10 Postup ničení soukromého klíče

Po uplynutí doby platnosti soukromého klíče příslušné certifikační autority a na základě následného potvrzení ředitelem Správy je tento soukromý klíč včetně jeho záloh zničen určeným postupem. O provedeném zničení je pořízen písemný záznam.

V případě soukromých klíčů OCSP respondérů je jejich ničení prováděno na příkaz osoby zastupující Správu při vydání certifikátu OCSP respondéru. O provedeném zničení je pořízen písemný záznam.

Ničení soukromých klíčů pracovníků podílejících se na vydávání certifikátů je plně v kompetenci těchto pracovníků, není předepsáno. Nutné je pouze v případě zaplnění paměti čipové karty.

Ničení soukromých klíčů koncových uživatelů je plně v kompetenci těchto koncových uživatelů.

6.2.11 Hodnocení kryptografických modulů

Kryptografické moduly použité pro generování párových dat a uložení příslušných soukromých klíčů certifikačních autorit a jejich OCSP respondérů 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.

Případné použití kryptografických modulů 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

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 párových dat.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit a jejich OCSP respondérů (čipová karta nebo softcard) jsou vytvářena před generováním nebo v průběhu generování příslušných párových dat.

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

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

6.4.2 Ochrana aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit a jejich OCSP respondérů (čipová karta nebo softcard) jsou chráněna nastaveným heslem.

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

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

6.4.3 Ostatní aspekty aktivačních dat

Není relevantní pro tento dokument.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti komponent použitých pro poskytování Služby je, včetně rozsahu potřebných kontrol, tj. i kontrol konfigurace důvěryhodných systémů a jejich periodicity, definována platnými technickými standardy a normami.

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.
- 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.

Veřejný řídicí dokument

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

- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.

Činnost Autority se dále řídí požadavky technických standardů a norem:

- FIPS PUB 140-2 Requirements for Cryptographic Modules.
- 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.
- 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.
- EN 301 549 Accessibility requirements for ICT products and services.
- 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.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Při vývoji systému je postupováno v souladu s Rámcovou dohodou NCA ze dne 20. 10. 2020 a s jednotlivými dílčími dohodami, které jsou pro vývoj a zajištění provozu NCA, resp. NCA uzavřeny.

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.

6.6.3 Řízení životního cyklu bezpečnosti

Řízení životního cyklu bezpečnosti 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,
- implementace a provoz - účelné a systematické prosazení vybraných bezpečnostních opatření,
- monitorování a přehodnocování - zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení Správy k posouzení,
- údržba a zlepšování - provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

6.7 Řízení bezpečnosti sítě

Důvěryhodné systémy určené k podpoře Služby 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.

6.8 Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

7. Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

7.1 Profil certifikátu

Tabulka 3 - Základní pole Certifikátu

Pole	Obsah
Version	v3 (0x2)
SerialNumber	jedinečné sériové číslo Certifikátu
SignatureAlgorithm	signatureAlgorithm podle typu žádosti (a v závislosti na algoritmu podpisu certifikátu) jedna z možností: ▪ minimálně sha256withRSAEncryption (s parametry= NULL, pkcs#1 1v5), ▪ rsassaPss (pkcs#1 2v1) s parametry: – hashAlgorithm: minimálně sha256, – maskGenAlgorithm: mgf1 s hash funkcí stejnou jako v hashAlgorithm, – saltLength: v závislosti na použité hash funkci, – trailerField: 0xBC (default)
Issuer	vydavatel Certifikátu
Validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	konec platnosti Certifikátu (UTC) = počátek platnosti Certifikátu + 1095 dní
Subject	informace o držiteli Certifikátu (viz Tabulka 4)
SubjectPublicKeyInfo	
Algorithm	rsaEncryption
subjectPublicKey	2048 bitů
SubjectPublicKeyInfo	
Extensions	rozšíření Certifikátu (viz Tabulka 5)
Signature	zaručená elektronická pečeť Authority

Tabulka 4 - Pole Subject Certifikátu

Všechny položky¹ pole Subject jsou převzaty ze žádosti o Certifikát s výjimkou položek vytvářených Autoritou. Povinné položky musí být v žádosti obsaženy.

Položka	Poznámka
countryName*	povinná, kód státu ISO 3166, jediný výskyt
givenName	povinná v případě neuvedení položky pseudonym, jediný výskyt
surName	povinná v případě neuvedení položky pseudonym, jediný výskyt
pseudonym	povinná v případě neuvedení položek givenName a surName, jediný výskyt, obsah položky pseudonym je naplněn řetězcem „NCA“
serialNumber	povinná pro unikátnost subjektu (jednoznačná identifikace držitele Certifikátu): - při uvedení položek givenName a surName: - pokud v žádosti o prvotní Certifikát není položka serialNumber obsažena, unikátní číslo subjektu ve formátu "NCA - zzzzzzz" (přiřazuje Autorita), - pokud je v žádosti položka serialNumber obsažena, potom jedna ze dvou možností: – IDCss-nnnnnnnn, – PASss-nnnnnnnn, kde ss je kód státu (ISO 3166) vydávající doklad, nnnnnnnn je číslo dokladu, - při uvedení položky pseudonym: unikátní číslo subjektu ve formátu "NCA - zzzzzzz" (přiřazuje příslušná CA)
commonName	povinná, jediný výskyt - v případě uvedení položek givenName a surName musí být tyto obsahem položky commonName (případně včetně titulů) - v případě uvedení položky pseudonym je obsah naplněn řetězcem „PSEUDONYM NCA“
initials	volitelná, pouze v případě neuvedení položky pseudonym, jediný výskyt
generationQualifier	volitelná, pouze v případě neuvedení položky pseudonym, jediný výskyt

¹ Správa si vyhrazuje právo upravit množinu a obsah položek pole Subject, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami.

organizationName	volitelná, pro obsah platí: - pouze v případě neuvedení položky pseudonym, - jediný výskyt – pro spojení zaměstnance s organizací, - pokud je uvedena, musí obsahovat přesný název Organizace z předem definovaného seznamu
organizationIdentifier	volitelná, pouze v případě neuvedení položky pseudonym a zároveň uvedení položky organizationName, jediný výskyt – jedna ze tří možností: - NTRss-id, (National Trade Register, tzn. IČ), - VATss-id, (Value Added Tax, tzn. DIČ), - XX:ss-id, kde: - ss je kód státu (ISO 3166) registrace zaměstnavatele nebo OSVČ (nemusí být shodná s countryName), - id je identifikační číslo Organizace v příslušném registru, - XX jsou dva znaky definované autoritou příslušného státu, následované znakem „:“ (dvojtečka) - jiný typ národního registru než VAT a NTR
organizationalUnitName	volitelná, pouze v případě neuvedení položky pseudonym, možný vícenásobný výskyt
title	volitelná, pouze v případě neuvedení položky pseudonym, možný vícenásobný výskyt
stateOrProvinceName*	volitelná pouze v případě neuvedení položky pseudonym, jediný výskyt
localityName*	volitelná, pouze v případě neuvedení položky pseudonym, jediný výskyt pokud bude uvedena, musí být také uvedeny položky streetAddress a postalCode
streetAddress*	volitelná, pouze v případě neuvedení položky pseudonym, jediný výskyt pokud bude uvedena, musí být také uvedeny položky localityName a postalCode
postalCode*	volitelná, pouze v případě neuvedení položky pseudonym, jediný výskyt pokud bude uvedena, musí být také uvedeny položky localityName a streetAddress

- * Položky countryName, stateOrProvinceName, localityName, streetAddress a postalCode se vztahují k údajům uvedeným v primárním dokladu.

7.1.1 Číslo verze

Vydávané certifikáty jsou v souladu se standardem X.509 ve verzi 3.

7.1.2 Rozšíření certifikátu

Tabulka 5 - Rozšíření² Certifikátu

Rozšíření	Obsah	Poznámka
CertificatePolicies		nekritické, povinné
PolicyInformation (1)		
policyIdentifier	viz kapitola 1.2	
policyQualifiers		
cPSuri	https://www.narodni-ca.gov.cz	
PolicyInformation (2)		
policyIdentifier	jedna ze dvou možností: • OID (NCP): 0.4.0.2042.1.1 (soukromý klíč není generován a uložen na bezpečném kryptografickém zařízení), • OID (NCP+): 0.4.0.2042.1.2 (soukromý klíč je generován a uložen na bezpečném kryptografickém zařízení)	
CRLDistributionPoints	http://crl1c.narodni-ca.gov.cz/XXRR_rsa.crl * http://crl2c.narodni-ca.gov.cz/XXRR_rsa.crl * http://crl3c.narodni-ca.gov.cz/XXRR_rsa.crl *	nekritické, povinné
AuthorityInformationAccess		nekritické, povinné
id-ad-calssuers	http://cacertsc.narodni-ca.gov.cz/XXRR_rsa.cer *	
id-ad-ocsp	http://ocspc.narodni-ca.gov.cz/XXRR_rsa *	
BasicConstraints		nekritické, povinné

² Správa si vyhrazuje právo upravit množinu a obsah rozšíření Certifikátu, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami.

cA	False	
KeyUsage	na základě obsahu žádosti o Certifikát kombinace možností (bitů v bitové masce): - digitalSignature, - keyEncipherment, - nonRepudiation, s výjimkou nepovolených kombinací: - nulová kombinace – všechny výše uvedené bity nulové, - keyEncipherment+nonRepudiation	kritické, povinné v případě, že žádost bude obsahovat nepodporované použití, bude odebráno v případě absence tohoto rozšíření v žádosti bude doplněna kombinace digitalSignature + nonRepudiation + keyEncipherment
ExtendedKeyUsage	na základě obsahu žádosti o Certifikát jakákoli kombinace z možností: - id-kp-clientAuth, - id-kp-emailProtection, - Microsoft SmartCard Logon, - maximálně tři jiná specifická OID	nekritické, povinné v případě absence tohoto rozšíření v žádosti bude doplněno: id-kp-clientAuth, id-kp-emailProtection
SubjectKeyIdentifier	hash veřejného klíče v Certifikátu	nekritické, povinné
AuthorityKeyIdentifier		nekritické, povinné
keyIdentifier	hash veřejného klíče Authority	
SubjectAlternativeName		nekritické, volitelné

rfc822Name	e-mail adresa	pouze v případě neuvedení položky pseudonym, možný vícenásobný výskyt
otherName	Microsoft_OID: UPN	volitelné, při uvedení v žádosti o Certifikát
nsComment	identifikační číslo bezpečného kryptografického zařízení	nekritické a povinné pouze pro čipovou kartu Starcos v případě neuvedení položky pseudonym
I.CA_CERT_INTERCON NECTION: 1.3.6.1.4.1.23624.4.7	v případě vydávání více typů certifikátů jednomu subjektu (vazba subjektu k vydávaným certifikátům)	nekritické, volitelné

* *RR* = poslední dvě číslice roku vydání certifikátu Autority. *XX* = "sub2CA" pro druhou podřízenou CA.

7.1.3 Objektové identifikátory algoritmů

V procesu poskytování Služby jsou využívány algoritmy v souladu s příslušnými technickými standardy a normami.

7.1.4 Tvary jmen

Autorita vydává certifikáty s tvary jmen, vyhovujícími standardu RFC 5280. Dále platí ustanovení kapitoly 3.1.

7.1.5 Omezení jmen

Není relevantní pro Certifikáty vydávané dle této CP.

7.1.6 Objektový identifikátor certifikační politiky

Správa vkládá do vydávaných Certifikátů níže uvedené objektové identifikátory certifikačních politik:

- OID certifikační politiky Správy, dle které je Certifikát vydán,

- OID příslušné certifikační politiky určené normou ETSI EN 319 411-1, resp. ČSN ETSI EN 319 411-1 s ohledem na generování a uložení soukromého klíče.

7.1.7 Použití rozšíření Policy Constraints

Není relevantní pro Certifikáty vydávané dle této CP.

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Viz rozšíření Certifikátu v kapitole 7.1.2 výše.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Není relevantní pro tento dokument – rozšíření není označeno jako kritické.

7.2 Profil seznamu zneplatněných certifikátů

Tabulka 6 - Profil CRL³

Pole	Obsah
Version	v2(0x1)
SignatureAlgorithm	sha256withRSAEncryption
Issuer	vydavatel CRL (Autorita)
thisUpdate	datum a čas vydání CRL (UTC)
nextUpdate	datum a předpokládaný čas vydání následujícího CRL (UTC)
revokedCertificates	seznam zneplatněných certifikátů
userCertificate	sériové číslo zneplatněného certifikátu
revocationDate	datum a čas zneplatnění certifikátu
crlEntryExtensions	rozšíření položky seznamu – viz Tabulka 7
crlExtensions	rozšíření CRL – viz Tabulka 7
Signature	zaručená elektronická pečeť vydavatele CRL

7.2.1 Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X509 verze 2.

³ Správa si vyhrazuje právo upravit množinu a obsah polí CRL, vyžadovanou aktualizacími standardů ETSI, nebo třetími stranami.

7.2.2 Rozšíření CRL a záznamů v CRL

Tabulka 7 - Rozšíření CRL⁴

Rozšíření	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění certifikátu důvod certificateHold je nepřipustný, proto Správa nepoužívá	nekritické, volitelné
crlExtensions		
AuthorityKeyIdentifier		
keyIdentifier	hash veřejného klíče vydavatele CRL (Authority)	nekritické
CRLNumber	jedinečné číslo vydávaného CRL	nekritické

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.

Bližší podrobnosti jsou uvedeny v odpovídající certifikační prováděcí směrnici.

7.3.1 Číslo verze

V žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP je uvedena verze 1.

7.3.2 Rozšíření OCSP

Konkrétní rozšíření uváděná v žádosti a odpovědi na stav certifikátu s využitím protokolu OCSP jsou uvedena v odpovídající certifikační prováděcí směrnici.

⁴ Správa si vyhrazuje právo upravit množinu a obsah rozšíření CRL, vyžadovanou aktualizacími standardů ETSI, nebo třetími stranami.

8. Hodnocení shody a jiná hodnocení

8.1 Periodicita nebo okolnosti hodnocení

Periodicita hodnocení, včetně okolností pro provádění hodnocení, je dána technickými standardy a normami, dle kterých je hodnocení prováděno.

8.2 Identita a kvalifikace hodnotitele

Kvalifikace hodnotitele je dána příslušnými technickými standardy a normami.

8.3 Vztah hodnotitele k hodnocenému subjektu

V případě interního hodnotitele platí, že tento není ve vztahu podřízenosti vůči organizační jednotce, která zajišťuje provoz Služby.

V případě externího hodnotitele platí, že se jedná o subjekt, který není se Správou majetkově ani personálně svázán.

8.4 Hodnocené oblasti

Hodnocené oblasti jsou konkretizovány technickými standardy a normami, podle kterých je hodnocení prováděno.

8.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat Službu, přeruší ji Správa do doby, než budou tyto nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům příslušných technických standardů a norem.

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána bezpečnostnímu manažerovi.

V nejbližším možném termínu svolá bezpečnostní manažer schůzi bezpečnostního výboru, na které musí být přítomni členové vedení Správy, které s obsahem závěrečné zprávy seznámí.

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 Certifikátu nejsou účtovány.

Služba obnovení certifikátů certifikačních autorit, OCSP respondérů a Certifikátu 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) vydaných dle této CP 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

Poskytovatelem Služby 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 Služby 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,
- 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

9.4.1 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.

9.4.2 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.

9.4.3 Informace nepovažované za osobní údaje

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

9.4.4 Odpovědnost za ochranu osobních údajů

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

9.4.5 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.

9.4.6 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.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

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

9.5 Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek a procedury zajišťující provoz důvěryhodných systémů určených k podpoře Služby jsou chráněny autorskými právy Správy.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

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,
- vydané Certifikáty splňují náležitosti požadované příslušnými technickými standardy a normami,
- zneplatní vydané Certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

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

- držitel Certifikátu neporušil povinnosti plynoucí mu ze smlouvy o poskytování Služby a této CP,
- spoléhající se strana neporušila povinnosti této CP.

Držitel Certifikátu vydaného podle této 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 své CP a CPS.

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 certifikátů,
- že Certifikát může být zneplatněn z důvodů uvedených v této 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 Autority,
- odpovídá za vyřizování připomínek a stížností.

9.6.3 Zastupování a záruky držitele certifikátu

Ve smlouvě mezi Správou a držitelem Certifikátu je uvedeno, že je povinen řídit se ustanoveními této CP.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují podle této CP.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

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 omezení odpovědnosti mohou být uvedena v jednotlivých zápisech se zvláštní složkou.

9.9 Záruky a odškodnění

Pro poskytování Služby 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 Službu. Smlouva musí být vždy v elektronické nebo listinné formě.

Správa:

- se zavazuje, že splní veškeré povinnosti definované zavřenou smlouvou i příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služby,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele.

Veřejný řídicí dokument

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

Správa neodpovídá:

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služby držitelem Certifikátu, zejména za využívání v rozporu s podmínkami uvedenými v této 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.

Reklamace, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do 30 dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

Nový Certifikát bude příslušnému držiteli Certifikátu poskytnut v následujících případech:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority,
- v případě, že Autorita při příjmu žádosti o vydání Certifikátu zjistí, že existuje jiný certifikát s duplicitním veřejným klíčem.

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

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CP nabývá platnosti dnem účinnosti uvedeným na titulní straně dokumentu a platí minimálně po dobu platnosti posledního podle ní vydaného Certifikátu.

9.10.2 Ukončení platnosti

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CP, 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

Po ukončení platnosti této CP přetrvávají z ní vyplývající závazky Správy, a to po dobu platnosti posledního podle ní vydaného Certifikátu.

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

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 rovněž způsoby uvedenými na internetové informační adrese.

9.12 Novelizace

9.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsáním v interním dokumentu.

9.12.2 Postup a periodičita oznamování

Vydání nové verze CP je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněn OID

OID politiky musí být změněn v případě významných změn ve způsobu poskytování této Služby.

V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

9.13 Ustanovení o řešení sporů

V případě, že 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 Služby je provozován ve shodě s právními předpisy České republiky a dále s relevantními mezinárodními standardy.

9.16 Různá ustanovení

9.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

9.16.2 Postoupení práv

Není relevantní pro tento dokument.

9.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto CP, stanoví, že provádění některého povinného požadavku je protiprávní, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a v souladu s platnou právní úpravou.

9.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

9.16.5 Vyšší moc

Správa neodpovídá za porušení svých povinností vyplývajících ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu, popř. výpadku komunikačního spojení.

9.17 Další ustanovení

Není relevantní pro tento dokument.