
 SPRÁVA ZÁKLADNÍCH REGISTRŮ	 * S Z R A X 0 0 3 6 0 B D * SZRAX00360BD prvotní identifikátor	
	SZR- 1038-2/Ř-2021	
	POL046B-2019	
POLITIKA	počet stran	46
	přílohy	0

NCA – Certifikační politika vydávání certifikátů pro OCSP respondéry (kryptografie RSA)

Oblast působnosti:

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

Gestor: Ing. Libor KALENSKÝ	Nahrazuje: POL046A-2019
Zpracovatel: Ing. František KNOTEK	Klasifikace: VEŘEJNÝ
Odborný garant: RNDr. Miroslav ŠEDIVÝ	Schváleno dne: 15. 03. 2021
Schvalovatel: <i>podepsáno elektronicky</i> Ing. Michal PEŠEK	Účinnost od dne: 15. 03. 2021

HISTORIE DOKUMENTU:

ID	Verze	Datum	Autor	Popis
-	1.01	06. 12. 2018	První certifikační autorita, a.s.	Vytvoření první verze dokumentu.
	1.02	25. 01. 2019	První certifikační autorita, a.s.	Aktualizace mailových adres, uvedení www adres do souladu s profilem certifikátu. Upravena formulace krytí pojištěním.
	1.03	07. 05. 2019	První certifikační autorita, a.s. Eva Kaletová	Doplněna platnost dokumentu. Aktualizace dle grafického manuálu SZR.
A	1.04	21. 04. 2020	Eva Kaletová	Aktualizace fyzické bezpečnosti.
B	1.05	15.03.2021	První certifikační autorita, a.s.	Zohledněna existence více podřízených certifikačních autorit.

OBSAH:

1.	Úvod	5
1.1	Přehled.....	5
1.2	Název a jednoznačné určení dokumentu	6
1.3	Participující subjekty	6
1.4	Použití certifikátu.....	6
1.5	Správa politiky.....	7
1.6	Přehled použitých pojmů a zkratk.....	7
2.	Odovědnost za zveřejňování a za úložiště	11
2.1	Úložiště	11
2.2	Zveřejňování certifikačních informací	11
2.3	Čas nebo četnost zveřejňování	11
2.4	Řízení přístupu k jednotlivým typům úložišť	12
3.	Identifikace a autentizace	13
3.1	Pojmenování	13
3.2	Počáteční ověření identity	13
3.3	Identifikace a autentizace při požadavku na výměnu klíče.....	14
3.4	Identifikace a autentizace při požadavku na zneplatnění certifikátu	14
4.	Požadavky na životní cyklus certifikátu	16
4.1	Žádost o vydání certifikátu	16
4.2	Zpracování žádosti o certifikát	16
4.3	Vydání certifikátu	17
4.4	Převzetí vydaného certifikátu.....	17
4.5	Použití párových dat a certifikátu.....	17
4.6	Obnovení certifikátu	18
4.7	Výměna veřejného klíče v certifikátu	18
4.8	Změna údajů v certifikátu.....	19
4.9	Zneplatnění a pozastavení platnosti certifikátu	19
4.10	Služby ověřování stavu certifikátu	21
4.11	Konec smlouvy o vydávání certifikátů.....	21
4.12	Úschova a obnova klíčů.....	22
5.	Postupy správy, řízení a provozu	23
5.1	Fyzická bezpečnost	23
5.2	Procedurální postupy	24
5.3	Personální postupy	24
5.4	Postupy zpracování auditních záznamů	26
5.5	Uchovávání záznamů	27
5.6	Výměna klíče	28
5.7	Obnova po havárii nebo kompromitaci	28
5.8	Ukončení činnosti CA nebo RA	29

Veřejný řídicí dokument.

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

6.	Řízení technické bezpečnosti	30
6.1	Generování a instalace párových dat	30
6.2	Ochrana soukromého klíče a technologie kryptografických modulů	31
6.3	Další aspekty správy párových dat	33
6.4	Aktivační data	33
6.5	Řízení počítačové bezpečnosti	33
6.6	Technické řízení životního cyklu	35
6.7	Řízení bezpečnosti sítě.....	35
6.8	Označování časovými razítky	36
7.	Profily certifikátu, seznamu zneplatněných certifikátů a OCSP	37
7.1	Profil certifikátu	37
7.2	Profil seznamu zneplatněných certifikátů	39
7.3	Profil OCSP	40
8.	Hodnocení shody a jiná hodnocení	41
8.1	Periodicita nebo okolnosti hodnocení	41
8.2	Identita a kvalifikace hodnotitele	41
8.3	Vztah hodnotitele k hodnocenému subjektu	41
8.4	Hodnocené oblasti	41
8.5	Postup v případě zjištění nedostatků	41
8.6	Sdělování výsledků hodnocení	41
9.	Ostatní obchodní a právní záležitosti	42
9.1	Poplatky	42
9.2	Finanční odpovědnost.....	42
9.3	Důvěrnost obchodních informací	42
9.4	Ochrana osobních údajů.....	43
9.5	Práva duševního vlastnictví	43
9.6	Zastupování a záruky.....	43
9.7	Zřeknutí se záruk	44
9.8	Omezení odpovědnosti.....	44
9.9	Záruky a odškodnění	44
9.10	Doba platnosti, ukončení platnosti.....	44
9.11	Individuální upozorňování a komunikace se zúčastněnými subjekty	45
9.12	Novelizace	45
9.13	Ustanovení o řešení sporů.....	45
9.14	Rozhodné právo.....	45
9.15	Shoda s platnými právními předpisy.....	45
9.16	Různá ustanovení	45
9.17	Další ustanovení	46

1. Úvod

Tento dokument stanoví zásady, které organizační složka státu Správa základních registrů (dále též SZR), kvalifikovaný poskytovatel služeb vytvářejících důvěru, uplatňuje při vydávání certifikátů pro OCSP respondéry (dále též Služba, Certifikát) certifikačních autorit. Pro Službu poskytovanou podle této certifikační politiky (dále též CP) je využíván algoritmus RSA.

Zákonné požadavky na Službu jsou definovány:

- nařízením Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS),
- zákonem České republiky č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce ve znění zákona č. 183/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o odpovědnosti za přestupky a řízení o nich a zákona o některých přestupcích.

Pozn.: Pokud jsou 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 byla tato politika v rozporu se standardy nebo zákony, které nahradí dosud platné, bude vydána její nová verze.

Přehled

Dokument **Certifikační politika vydávání certifikátů pro OCSP respondéry (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.

Veřejný řídicí dokument.

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

OCSP respondéry, provozované SZR jsou autorizovanými respondéry v souladu se standardem RFC 2560, tzn. certifikát veřejného klíče OCSP respondéru je vydán tou certifikační autoritou, která vydala certifikát, na jehož stav tento OCSP respondér odpovídá.

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 CPS).

Název a jednoznačné určení dokumentu

Název tohoto dokumentu: Certifikační politika vydávání certifikátů pro OCSP respondéry (kryptografie RSA), verze 1.05

OID politiky: 1.2.203.72054506.10.1.80.1.0

Participující subjekty

Certifikační autority (dále „CA“)

Národní Kořenová certifikační autorita NCA vydala ve dvoustupňové struktuře certifikačních autorit, v souladu s platnou legislativou a s požadavky technických standardů a norem, certifikát podřízené certifikační autoritě, provozované SZR. Kořenová certifikační autorita i podřízená certifikační autorita (dále též Autorita) vydávají Certifikáty dle této CP a dále certifikáty dle příslušných certifikačních politik.

Registrační autority NCA (dále „RA“)

Na procesech životního cyklu certifikátů vydávaných dle této CP se podílí registrační autorita NCA ve vlastnictví SZR.

Držitelé certifikátů

Držitelem vydávaného Certifikátu je Správa základních registrů, která požádala o vydání Certifikátu pro jí provozovanou certifikační autoritu a je identifikovaná v Certifikátu jako držitel soukromého klíče spojeného s veřejným klíčem, uvedeným v tomto Certifikátu.

Spoléhající se strany

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

Jiné participující subjekty

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

Použití certifikátu

Přípustné použití certifikátu

Certifikáty vydávané podle této CP smějí být používány výhradně v procesu ověřování odpovědí s využitím protokolu OCSP na stav certifikátu vydaného SZR.

Zakázané použití certifikátu

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

Správa politiky

Organizace spravující dokument

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

Kontaktní osoba

Kontaktní osoba SZR v souvislosti s touto CP, resp. s odpovídající CPS je pověřený zaměstnanec bezpečnostního oddělení SZR uvedený na webu SZR.

Osoba rozhodující o souladu CPS s certifikační politikou

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů SZR uvedených v CPS s touto CP, je ředitel SZR.

Postupy při schvalování CPS

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

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	kvalifikované elektronické časové razítko dle platné legislativy pro služby vytvářející důvěru
dvoufaktorová autentizace	autentizace využívající dvou ze tří faktorů - něco vím (heslo), něco mám (např. čipová karta, hardwarový token) nebo něco jsem (otisky prstů, snímání oční sítnice či duhovky)
elektronická pečeť	elektronická pečeť, nebo zaručená elektronická pečeť, nebo uznávaná elektronická pečeť, nebo kvalifikovaná elektronická pečeť dle platné legislativy pro služby vytvářející důvěru
elektronický podpis	elektronický podpis, nebo zaručený elektronický podpis, nebo kvalifikovaný elektronický podpis, nebo uznávaný elektronický podpis dle platné legislativy 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
kvalifikovaná služba vytvářející důvěru	služba vytvářející důvěru, která splňuje požadavky stanovené v eIDAS
kvalifikovaný certifikát pro elektronický podpis	certifikát definovaný platnou legislativou pro služby vytvářející důvěru
kvalifikovaný prostředek pro vytváření elektronických podpisů	prostředek pro vytváření elektronických podpisů, který splňuje požadavky stanovené v příloze II eIDAS

legislativa pro služby vytvářející důvěru	legislativa České republiky vztahující se ke službám vytvářejícím důvěru pro elektronické transakce a nařízení eIDAS
OCSP respondér	server poskytující protokolem OCSP údaje o stavu certifikátu veřejného klíče
orgán dohledu	orgán dohlížející na kvalifikované poskytovatele služeb vytvářejících důvěru
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické nebo listinné podobě
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	poskytovatel vybraných služeb vytvářejících důvěru, který zajišťuje na základě písemné smlouvy pro SZR 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 České republiky 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
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci

Veřejný řídicí dokument.

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

	a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ESI	Electronic Signatures and Infrastructures
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
GDPR	Global Data Protection Regulation, NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
html	Hypertext Markup Language, značkovací jazyk pro vytváření hypertextových dokumentů
http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
https	Hypertext Transfer Protocol Secure, protokol pro zabezpečenou výměnu textových dokumentů ve formátu html
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
IPS	Intrusion Prevention System, systém prevence průniku
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
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, objektový identifikátor, číselná identifikace objektu
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování-Zavedení-Kontrola-Využití, Demingův cyklus, metoda neustálého zlepšování
PDS	PKI Disclosure Statement, zpráva pro uživatele

PKCS	Public Key Cryptography Standards, označení skupiny standardů pro kryptografii s veřejným klíčem
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
PUB	Publication, označení standardu FIPS
QSCD	Qualified Electronic Signature/Seal Creation Device, zařízení pro tvorbu kvalifikovaného elektronického podpisu nebo pečetě
RA	registrační autorita NCA
RFC	Request for Comments, označení řady standardů a dalších dokumentů popisujících internetové protokoly, systémy apod.
RSA	šifra s veřejným klíčem pro podepisování a šifrování (iniciály původních autorů Rivest, Shamir a Adleman)
SHA	typ hashovací funkce
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 časoměřiče“ atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
ZOOÚ	aktuální legislativa týkající se ochrany osobních údajů

1. Odpovědnost za zveřejňování a za úložiště

Úložiště

SZR zřizuje a provozuje úložiště veřejných i neveřejných informací.

Zveřejňování certifikačních informací

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

- adresa sídla SZR:
Správa základních registrů
Na Vápence 915/14
130 00 Praha 3
Česká republika
- internetová adresa <http://www.narodni-ca.cz>,
- sídla registračních autorit.

Elektronická adresa, která slouží pro kontakt se SZR, je podpora@szrcr.cz.

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. SZR 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 SZR tuto skutečnost na své internetové informační adrese a prostřednictvím celostátně distribuovaného deníku Hospodářské noviny nebo Mladá fronta Dnes.

Čas nebo četnost zveřejňování

SZR zveřejňuje informace s následující periodicitou:

- certifikační politika - po schválení a vydání nové verze,
- certifikační prováděcí směrnice - neprodleně,

Veřejný řídicí dokument.

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

- 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.

Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje SZR bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům SZR, nebo subjektům definovaným příslušnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

2. Identifikace a autentizace

Pojmenování

Typy jmen

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

Požadavek na významovost jmen

V procesu vydávání Certifikátu je vždy vyžadována významovost všech ověřitelných jmen, uvedených v položkách pole Subject. Podporované položky tohoto pole a rozšíření jsou uvedeny v kapitole 7.

Anonymita nebo používání pseudonymu držitele certifikátu

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

Pravidla pro interpretaci různých forem jmen

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

Jedinečnost jmen

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

Uznávání, ověřování a posláním obchodních značek

Certifikáty vydávané podle této CP mohou obsahovat pouze obchodní značky vlastněné SZR.

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.

Ověřování vlastnictví soukromého klíče

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

Ověřování identity organizace

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.

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

Ověřování identity fyzické osoby

Kapitola popisuje způsob ověřování identity fyzické osoby, tj. osoby zastupující SZR (dále též Osoba) žádající o vydání Certifikátu.

V procesu ověřování identity Osoby jsou vyžadovány dva doklady, primární a sekundární, obsahující údaje uvedené níže v této kapitole.

Veřejný řídicí dokument.

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

Primárním osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Primárním 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 primárním dokladu uvedeno,
- číslo předloženého primárního osobního dokladu,
- adresa trvalého bydliště (je-li v primárním dokladu uvedena).

Sekundární osobní doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s primárním osobním dokladem a musí obsahovat alespoň jeden z následujících údajů:

- datum narození (nebo rodné číslo, je-li uvedeno),
- adresu trvalého bydliště,
- fotografii obličeje.

Údaje v sekundárním osobním dokladu sloužící k jednoznačné identifikaci osoby zastupující Organizaci musí být shodné s těmito údaji v primárním osobním dokladu.

Pokud osoba zastupující SZR není osobou ze zákona oprávněnou k zastupování SZR, je dále požadována úředně ověřená plná moc k zastupování SZR podepsaná statutárním zástupcem SZR.

Neověřované informace vztahující se k držiteli certifikátu

Všechny informace žádosti jsou ověřovány.

Ověřování kompetencí

Není relevantní pro tento dokument.

Kritéria pro interoperabilitu

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

Identifikace a autentizace při požadavku na výměnu klíče

Identifikace a autentizace při běžném požadavku na výměnu klíče

Je nutné vydat nový Certifikát s novým veřejným klíčem. Platí stejné požadavky, jako v případě počátečního ověření identity.

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.

Identifikace a autentizace při požadavku na zneplatnění certifikátu

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

Žádost o zneplatnění Certifikátu musí být vždy písemná a:

- V případě žádosti podávané SZR musí být podepsaná ředitelem SZR, nebo jím pověřenou osobou. Identita žadatele musí být řádně ověřena primárním osobním

Veřejný řídicí dokument.

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

dokladem. Pokud pověřená osoba není osobou ze zákona oprávněnou k zastupování SZR, je dále požadována úředně ověřená plná moc k zastupování SZR podepsaná statutárním zástupcem.

- V případě žádosti podávané orgánem dohledu nebo dalším subjektem definovaným platnou legislativou pro služby vytvářející důvěru musí být žádost doručena do datové schránky SZR, autenticita musí operátorem RA ověřena a realizaci musí písemně potvrdit ředitel SZR, nebo jím pověřená osoba.

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

3. Požadavky na životní cyklus certifikátu

Žádost o vydání certifikátu

Kdo může požádat o vydání certifikátu

O vydání Certifikátu může požádat ředitel SZR, případně jím pověřený člen vedení SZR (vždy to musí být ředitel odboru, nikoliv zastupující vedoucí oddělení).

Registrační proces a odpovědnosti

Písemná žádost o vydání Certifikátu je předkládána vedení SZR ředitelem SZR, nebo jím pověřeným členem vedení SZR a musí obsahovat název a OID této certifikační politiky, včetně uvedení požadovaného jména CA (tzv. commonName). Žádost musí být ředitelem SZR, nebo jím pověřeným členem vedení SZR podepsána.

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

- seznámit se s touto CP a 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:

- v procesu vydávání Certifikátu na RA ověřit všechny ověřitelné údaje uvedené v žádosti podle předložených dokladů,
- 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 vydané Certifikáty,
- činnosti spojené se Službou poskytovat v souladu s platnou legislativou pro služby vytvářející důvěru, příslušnými technickými standardy a normami, touto CP, příslušnou CPS, Systémovou bezpečnostní politikou a provozní dokumentací.

Zpracování žádosti o certifikát

Provádění identifikace a autentizace

V procesu identifikace a autentizace je prováděna kontrola písemné žádosti o vydání Certifikátu (viz kapitola 4.1.2) a kontroly podle kapitol 3.2.1 – 3.2.4.

Schválení nebo zamítnutí žádosti o certifikát

Na základě písemné žádosti rozhodne vedení SZR o vydání Certifikátu s příslušným obsahem pole Subject, resp. Issuer, případně o zamítnutí žádosti. Výsledek je dokumentován.

Samotný proces vydání Certifikátu je popsán v kapitole 4.3.

Doba zpracování žádosti o certifikát

Doba zpracování písemné žádosti o vydání Certifikátu nepřekročí pět pracovních dnů ode dne předložení žádosti vedení SZR.

Po kladném rozhodnutí o vydání Certifikátu je SZR povinna Certifikát vydat. Doba vydání Certifikátu nepřekročí jednotky minut.

Veřejný řídicí dokument.

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

Vydání certifikátu

Úkony CA v průběhu vydávání certifikátu

V procesu vydávání Certifikátu provádějí pracovnice/pracovníci (dále jen pracovníci) RA:

- kontroly, uvedené v kapitole 4.2.1,
- vizuální kontrolu shody údajů obsažených v žádosti o Certifikát (struktura PKCS#10) a údajů doplněných pracovníkem RA,
- vizuální kontroly formální správnosti údajů.

Ověřování vlastnictví soukromého klíče, podporovaných hashovacích funkcí v žádosti o Certifikát (minimálně sha-256), kontrola kompetencí a kontroly formální správnosti údajů jsou prováděny jak programovým vybavením umístěným na pracovních stanicích operátorů RA, tak programovým vybavením jádra systému CA. Pokud některá z uvedených kontrol skončí negativně, proces vydání Certifikátu je ukončen.

Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

Držitel Certifikátu je o vydání informován prostřednictvím pracovníka RA.

Převzetí vydaného certifikátu

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.

Zveřejňování certifikátů certifikační autoritou

Certifikáty vydané podle této CP jsou zveřejněny způsobem podle bodu 2.2.

Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Platí ustanovení kapitoly 4.4.2 a požadavky platné legislativy pro služby vytvářející důvěru.

Použití párových dat a certifikátu

Použití soukromého klíče a certifikátu držitelem certifikátu

Povinností držitele Certifikátu je zejména:

- používat soukromý klíč a jemu odpovídající veřejný klíč obsažený ve vydaném Certifikátu v souladu s touto CP,
- nakládat se soukromým klíčem, odpovídajícím veřejnému klíči v Certifikátu vydaném podle této CP, tak, aby nemohlo dojít k jeho neoprávněnému použití.
- v případě kompromitace, nebo podezření na kompromitaci, soukromého klíče odpovídajícího veřejnému klíči v Certifikátu vydaném podle této CP, případně o této skutečnosti okamžitě informovat v souladu s platnou legislativou pro služby vytvářející důvěru a ukončit jeho používání.

Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje 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,

Veřejný řídicí dokument.

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

- dodržovat veškerá ustanovení této CP a platné legislativy pro služby vytvářející důvěru, vztahující se k povinnostem spoléhající se strany.

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 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.

Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

Kdo může žádat o obnovení

Viz kapitola 4.6.

Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.6.

Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

Zveřejňování obnovených certifikátů certifikační autoritou

Viz kapitola 4.6.

Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.6.

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 Certifikátu, jehož veřejný klíč je předmětem výměny.

Služba výměny veřejného klíče není poskytována. V případě této CP se 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.

Podmínky pro výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

Kdo může žádat o výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

Zpracování požadavku na výměnu veřejného klíče v certifikátu

Viz kapitola 4.7.

Veřejný řídicí dokument.

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

Oznámení o vydání nového certifikátu držiteli certifikátu

Viz kapitola 4.7.

Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Viz kapitola 4.7.

Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Viz kapitola 4.7.

Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.7.

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 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 výměny.

Služba změny údajů v 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.

Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

Kdo může požádat o změnu údajů v certifikátu

Viz kapitola 4.8.

Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Viz kapitola 4.8.

Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Viz kapitola 4.8.

Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Viz kapitola 4.8.

Zneplatnění a pozastavení platnosti certifikátu

Zneplatnění Certifikátu znamená, že do doby vydání Certifikátu nového je služba OCSP respondéru příslušné Autority pozastavena.

Službu pozastavení platnosti Certifikátu SZR neposkytuje.

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,
- technický obsah nebo formát Certifikátu představují neakceptovatelné riziko (např. daný kryptografický/podepisovací algoritmus nebo délka klíče),
- v případech, kdy nastanou skutečnosti uvedené v platné legislativě služby vytvářející důvěru nebo příslušných technických standardech a normám (např. neplatnost údajů v Certifikátu).

Kdo může požádat o zneplatnění

Žádost o zneplatnění Certifikátu mohou podat:

- držitel Certifikátu (oprávněným žadatelem o zneplatnění Certifikátu vydaného SZR je v ředitel SZR, nebo jím pověřený člen vedení SZR (vždy to musí být ředitel odboru, nikoliv zastupující vedoucí oddělení),
- případně orgán dohledu nebo další subjekty definované platnou legislativou pro služby vytvářející důvěru.

Postup při žádosti o zneplatnění

Zneplatnění Certifikátu probíhá za osobní účasti ředitele SZR nebo jím pověřeného pracovníka.

Písemná žádost o zneplatnění Certifikátu musí obsahovat sériové číslo Certifikátu buď v dekadickém nebo hexadecimálním tvaru (uvozeno řetězcem „0x“) a jméno Autority, která Certifikát vydala jméno a příjmení fyzické osoby oprávněné zastupující žadatele. V případě žádosti podávané držitelem Certifikátu musí být dále uvedeno heslo pro zneplatnění Certifikátu. Pokud fyzická osoba oprávněná žádat zneplatnění Certifikátu heslo pro zneplatnění nezná, musí tuto skutečnost do písemné žádosti explicitně uvést.

Postup identifikace je popsán v kapitole 3.4.

Prodleva při požadavku na zneplatnění certifikátu

Požadavek na zneplatnění Certifikátu musí být podán bezodkladně.

Doba zpracování žádosti o zneplatnění

Pokud žádost požadavky splňuje, odpovědný pracovník Certifikát v systému CA neprodleně zneplatní - datum a čas zneplatnění Certifikátu jsou dány zpracováním tohoto požadavku. CRL obsahující sériové číslo zneplatněného Certifikátu musí být vydán neprodleně po zneplatnění tohoto Certifikátu.

Povinnosti třetích stran při kontrole zneplatnění

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

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 v případě podřízené certifikační autority vydáván zpravidla v intervalu 8 hodin, nejvýše však 24 hodin od vydání předchozího CRL. V případě kořenové certifikační autority zpravidla v půlročním intervalu, nejvýše však jeden rok od vydání předchozího CRL.

Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL podřízené certifikační autority je vždy vydán nejvýše 24 hodin od vydání předchozího CRL. CRL kořenové certifikační autority je vždy vydán nejvýše jeden rok od vydání předchozího CRL.

Dostupnost ověřování stavu certifikátu on-line

Není relevantní pro tento dokument, stav Certifikátu není ověřován on-line.

Požadavky při ověřování stavu certifikátu on-line

Viz kapitola 4.9.9.

Jiné možné způsoby oznamování zneplatnění

Není relevantní pro tento dokument.

Zvláštní postupy při kompromitaci klíče

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

Podmínky pro pozastavení platnosti

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

Kdo může požádat o pozastavení platnosti

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

Postup při žádosti o pozastavení platnosti

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

Omezení doby pozastavení platnosti

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

Služby ověřování stavu certifikátu

Funkční charakteristiky

Seznamy veřejných certifikátů jsou poskytovány formou zveřejňování informací, seznamy zneplatněných certifikátů jsou poskytovány formou zveřejňování informací.

Skutečnost, že Autorita poskytuje informace o stavu certifikátu formou OCSP (služba OCSP), je uvedena v jí vydaných certifikátech.

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.

Další charakteristiky služeb stavu certifikátu

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

Konec smlouvy o vydávání certifikátů

Není relevantní pro tento dokument.

Veřejný řídicí dokument.

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

Úschova a obnova klíčů

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

Politika a postupy při úschově a obnově klíčů

Viz kapitola 4.12.

Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Viz kapitola 4.12.

4. 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, Systémová bezpečnostní politika NCA (CA a TSA), Certifikační prováděcí směrnice a Řízení kontinuity provozu NCA, tak v upřesňujících interních dokumentech. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

Fyzická bezpečnost

Umístění a konstrukce

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

Fyzický přístup

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

Elektrina a klimatizace

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

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.

Protipožární opatření a ochrana

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

Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezorech.

Papírová média, která je nutno dle platné legislativy pro služby vytvářející důvěru uchovávat, jsou obvykle skladována přímo v lokalitách, kde jsou umístěny registrační autority. Papírová média ukládaná na SZR jsou uchovávána v kovové, uzamykatelné skříni, dokumenty jsou skenovány a příslušná elektronická média jsou ukládána v geograficky odlišné lokalitě.

Nakládání s odpady

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

Zálohy mimo budovu

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

Procedurální postupy

Důvěryhodné role

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

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

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.

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.

Role vyžadující rozdělení povinností

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

Personální postupy

Požadavky na kvalifikaci, praxi a bezúhonnost

Zaměstnanci SZR 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

Veřejný řídicí dokument.

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

a komunikačních technologií, přičemž z toho nejméně jeden rok v oblasti poskytování služeb vytvářejících důvěru,

- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

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

- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.
- Pro vykonávání řídicí funkce musí mít vedoucí zaměstnanci zkušenosti získané praxí nebo odbornými školeními s ohledem na důvěryhodnost Služby, znalost bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích SZR 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.

Požadavky na školení

Zaměstnanci SZR 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.

Požadavky a periodicita doškolování

Dvakrát za 12 měsíců jsou zaměstnancům SZR 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.

Periodicita a posloupnost rotace pracovníků mezi různými rolemi

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

Postihy za neoprávněné činnosti

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

Požadavky na nezávislé dodavatele

SZR 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

Veřejný řídicí dokument.

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

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.

Dokumentace poskytovaná zaměstnancům

Zaměstnanci SZR 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.

Postupy zpracování auditních záznamů

Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované platnou legislativou pro služby vytvářející důvěru a 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 legislativou pro služby vytvářející důvěru a s relevantními technickými standardy a normami, přičemž platí, že:

- je prováděno podle připraveného scénáře ve fyzicky zabezpečeném prostředí,
- o provedení je vydána zpráva, že generování proběhlo podle připraveného scénáře a že byly zajištěny jeho důvěrnost a integrita,
- v případě Autority je osobně přítomen buď auditor kvalifikovaný v souladu s platnými technickými standardy, nebo notář, který zprávu podepíše jako svědek, že zpráva správně popisuje postup generování,
- v případě podřízených 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.

Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní dokumentaci, v případě bezpečnostního incidentu okamžitě.

Doba uchování auditních záznamů

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

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 ohnivzdorném trezoru SZR v místnosti s řízeným přístupem.

Auditní záznamy v papírové formě jsou ukládány v trezoru. Jsou skenovány a oskenovaná podoba je ukládána v geograficky odlišné lokalitě.

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci.

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.

Systém shromažďování auditních záznamů (interní nebo externí)

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

Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

Hodnocení zranitelnosti

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

Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je v SZR upraveno interní dokumentací.

Typy uchovávaných záznamů

SZR uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí s poskytovanými službami vytvářejícími důvěru, zejména:

- zprávy o průběhu generování párových dat certifikačních autorit,
- dokumenty související s životním cyklem vydaných Certifikátů, včetně těchto Certifikátů,
- záznamy o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, politiky, provozní a bezpečnostní dokumentaci.

Doba uchování záznamů

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

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

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.

Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

Požadavky na používání časových razítek při uchovávání záznamů

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

Veřejný řídicí dokument.

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

Systém shromažďování uchovávaných záznamů (interní nebo externí)

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

Postupy pro získání a ověření uchovávaných informací

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

- zaměstnancům SZR, pokud je to k jejich činnosti vyžadováno,
- oprávněným kontrolním subjektům, orgánům činným v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

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.

Obnova po havárii nebo kompromitaci

Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto událostí postupuje SZR v souladu s interním dokumentem pro řízení kontinuity provozu a případně s další relevantní interní dokumentací.

Poškození výpočetních prostředků, programového vybavení nebo dat

Viz kapitola 5.7.1.

Postup při kompromitaci soukromého klíče

V případě vzniku důvodné obavy z kompromitace soukromého klíče certifikačních autorit postupuje SZR 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,
- 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 služeb vytvářejících důvěru.

Schopnost obnovit činnost po havárii

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

Ukončení činnosti CA nebo RA

Ukončení činnosti Autority je popsáno v certifikační politice příslušné Autority (vydávající certifikáty koncovým uživatelům).

5. Řízení technické bezpečnosti

Generování a instalace párových dat

Generování párových dat

Generování párových dat kořenové certifikační autority, resp. podřízených certifikačních autorit, o jehož průběhu je vyhotovena písemná zpráva, je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 úroveň 3. Procesu jsou přítomni ředitel SZR, nebo jím pověřená osoba a dále alespoň dvě osoby v důvěryhodných rolích. Generování párových dat kořenové CA je dále přítomen buď auditor, nebo notář, a to jako svědek, že generování proběhlo tak, jak zpráva popisuje. Další podrobnosti viz kapitola 5.4.1.

Generování párových dat OCSP respondérů certifikačních autorit je rovněž prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 úroveň 3.

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

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.

Předávání soukromého klíče jeho držiteli

Není relevantní pro tento dokument, soukromé klíče Autority a OCSP respondérů jsou uloženy v kryptografickém modulu, který je pod výhradní kontrolou SZR.

Předávání veřejného klíče vydavateli certifikátu

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

Poskytování veřejného klíče CA spoléhajícím se stranám

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

- obdržení na RA (osobní návštěva),
- prostřednictvím internetových informačních adres SZR,
- prostřednictvím příslušného orgánu dohledu, resp. prostřednictvím věstníku příslušného orgánu dohledu.

Získání veřejného klíče OCSP respondéru obsaženého v jeho certifikátu je garantováno následujícími způsoby:

- obdržení na RA,
- jako součást OCSP odpovědi.

Délky klíčů tady

Pro Službu poskytovanou podle této CP je výhradně využíván asymetrický algoritmus RSA. Mohutnost klíče (resp. parametrů daného algoritmu) kořenové certifikační autority SZR je 3072 bitů, mohutnost klíčů (resp. parametrů daného algoritmu) v jí vydávaných certifikátech podřízeným certifikačním autoritám je rovněž 3072 bitů. Mohutnost klíčů v certifikátech vydávaných podle této CP je 2048 bitů.

Parametry veřejného klíče a kontrola jeho kvality

Parametry algoritmů použitých při generování veřejných klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky uvedené v platné legislativě pro služby vytvářející důvěru, resp. v ní odkazovaných technických standardech nebo normách.

Veřejný řídicí dokument.

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

Parametry algoritmů použitých při generování veřejných klíčů koncových uživatelů musí tyto požadavky rovněž splňovat.

SZR kontroluje povolenou délku klíčů a možný dvojitý výskyt veřejného klíče ve vydávaných certifikátech. V případě duplicitního výskytu je příslušný certifikát neprodleně zneplatněn, držitel takového certifikátu o tomto neprodleně a vhodným způsobem informován a vyzván ke generování nových párových dat.

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

Možnosti použití klíče jsou uvedeny v rozšíření certifikátu.

Ochrana soukromého klíče a technologie kryptografických modulů

Řízení a standardy kryptografických modulů

Generování párových dat a uložení soukromých klíčů certifikačních autorit a jejich OCSP respondérů probíhá v kryptografických modulech, které splňují požadavky platné legislativy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3.

Soukromý klíč pod kontrolou více osob (m z n)

Pokud je pro činnosti spojené se soukromým klíčem certifikační autority nebo OCSP serveru nezbytná přítomnost dvou osob v důvěryhodných rolích, pak v případě činností citlivých každá z těchto osob zná pouze část kódu k provedení těchto činností.

Úschova soukromého klíče

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

Zálohování soukromého klíče

Kryptografický modul použitý pro správu párových dat certifikačních autorit a jejich OCSP respondérů umožňuje zálohování soukromých klíčů. Soukromé klíče jsou zálohovány s využitím nativních prostředků kryptografického modulu v zašifrované podobě.

Uchovávání soukromého klíče

Po uplynutí doby platnosti soukromých klíčů certifikačních autorit a jejich OCSP respondérů jsou tyto včetně záloh zničeny. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, proto je zakázáno.

Transfer soukromého klíče do nebo z kryptografického modulu

Transfer soukromého klíče Autority z a do kryptografického modulu probíhá za přímé osobní účasti ředitele SZR, nebo jím určené osoby.

Transfer soukromých klíčů ostatních certifikačních autorit a všech OCSP respondérů z a do kryptografického modulu probíhá za přímé osobní účasti nejméně jednoho člena vedení SZR.

O provedeném transferu je vždy pořízen písemný záznam.

Uložení soukromého klíče v kryptografickém modulu

Soukromé klíče certifikačních autorit a jejich OCSP respondérů jsou uloženy v kryptografickém modulu, splňujícím požadavky platné legislativy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3.

Postup aktivace soukromého klíče

Aktivace soukromého klíče certifikačních autorit uložených v kryptografickém modulu je prováděna za přímé osobní účasti ředitele SZR, nebo jím určené osoby s využitím aktivační

Veřejný řídicí dokument.

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

čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené aktivaci je pořízen písemný záznam.

Aktivace soukromých klíčů všech OCSP respondérů uložených v kryptografickém modulu je prováděna za přímé osobní účasti nejméně jednoho člena vedení SZR s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené aktivaci je pořízen písemný záznam.

Soukromý klíč využívaný k vytváření kvalifikovaných elektronických pečeti je aktivován pouze v případě vložení jemu příslušné čipové karty do kryptografického modulu.

Aktivace soukromého klíče TSU systému TSA vygenerovaného v kryptografickém modulu je prováděna výběrem příslušného profilu. O provedené aktivaci je pořízen písemný záznam.

Postup deaktivace soukromého klíče

Deaktivace soukromého klíče certifikačních autorit uložených v kryptografickém modulu je prováděna za přímé osobní účasti ředitele SZR, nebo jím určené osoby s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené aktivaci je pořízen písemný záznam.

Deaktivace soukromých klíčů všech OCSP respondérů uložených v kryptografickém modulu je prováděna za přímé osobní účasti nejméně jednoho člena vedení SZR s využitím aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. O provedené aktivaci je pořízen písemný záznam.

Soukromý klíč využívaný k vytváření kvalifikovaných elektronických pečeti je deaktivován, a tedy není možné ho použít v případě vyjmutí jemu příslušné čipové karty z kryptografického modulu.

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

Postup ničení soukromého klíče

Ničení soukromých klíčů certifikačních autorit a všech OCSP responderů uložených v kryptografickém modulu je realizováno nativními prostředky tohoto kryptografického modulu a za přímé osobní účasti ředitele SZR nebo jím určené osoby podle přesně určeného postupu, který je upraven interní dokumentací. O provedeném ničení je pořízen písemný záznam.

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

Soukromé klíče TSU systému TSA jsou uloženy v kryptografickém modulu. Jejich ničení spočívá v bezpečném rušení bezpečně a certifikovaně šifrované adresářové struktury.

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

Hodnocení kryptografických modulů

Kryptografické moduly sloužící ke generování párových dat a uložení soukromých klíčů certifikačních autorit a jejich OCSP respondérů splňují požadavky legislativy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3. Bezpečnost modulů je sledována po celou dobu jejich využívání.

Další aspekty správy párových dat

Uchovávání veřejných klíčů

Veřejné klíče certifikačních autorit a jejich OCSP respondérů jsou uchovávány po celou dobu existence SZR.

Doba funkčnosti certifikátu a doba použitelnosti párových dat

Maximální doba platnosti každého vydaného certifikátu je uvedena v těle tohoto certifikátu.

Aktivační data

Generování a instalace aktivačních dat

Aktivační data certifikačních autorit a jejich OCSP respondérů jsou vytvářena v průběhu generování odpovídajících párových dat.

Ochrana aktivačních dat

Aktivační data certifikačních autorit a jejich OCSP respondérů jsou chráněna způsobem popsaným v interní dokumentaci.

Ostatní aspekty aktivačních dat

Aktivační data soukromých klíčů certifikačních autorit a jejich OCSP respondérů jsou určena výhradně pro poskytování služeb vytvářejících důvěru a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě. Veškeré aspekty jsou popsány v interní dokumentaci.

Řízení počítačové bezpečnosti

Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování Služby je definována platnou legislativou pro služby vytvářející důvěru, resp. v ní odkazovanými technickými standardy a normami.

Hodnocení počítačové bezpečnosti

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

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb - Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

- ČSN ETSI EN 319 411-1 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 1: Obecné požadavky.
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 2: Požadavky na poskytovatele důvěryhodných služeb vydávající kvalifikované certifikáty EU.
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
- 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 Authority 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 2560 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.
- 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.

Veřejný řídicí dokument.

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

- ČSN ETSI EN 319 412-3 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 3: Profil certifikátu pro certifikáty vydávané právníkům osobám.
- ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to legal persons.
- ČSN ETSI EN 319 412-5 Elektronické podpisy a infrastruktury (ESI) - Profily certifikátu - Část 5: Prohlášení „QC Statements“.
- ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

Technické řízení životního cyklu

Řízení vývoje systému

Při vývoji systému je postupováno v souladu s Rámcovou smlouvou ze dne 31. 8. 2018 a jednotlivými dílčími dohodami, které jsou pro vývoj a zajištění provozu NCA uzavřeny.

Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu s technickými standardy a normami, je prováděna v rámci periodických kontrol služeb vytvářejících důvěru a dále formou auditů systému řízení bezpečnosti informací (ISMS).

Bezpečnost informací se v SZR 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.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

Řízení bezpečnosti životního cyklu

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

- vybudování - stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou,
- 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 SZR k posouzení,
- údržba a zlepšování - provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

Řízení bezpečnosti sítě

Důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru nejsou přímo dostupné z veřejné sítě Internet. Tyto systémy jsou chráněny komerčním produktem typu firewall

POL046B-2019, NCA - Certifikační politika vydávání certifikátů pro OCSP respondéry (kryptografie RSA)

s integrovaným systémem IPS (Intrusion Prevention System) v redundantní konfiguraci. Veškerá komunikace mezi RA a provozním pracovištěm je vedena šifrovaně.

Označování časovými razítky

Řešení je uvedeno v kapitole 5.5.5.

6. Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

Profil certifikátu

Tabulka 3 - Základní pole certifikátu OCSP respondéru

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

Pole	Obsah
Version	v3 (0x2)
SerialNumber	jedinečné sériové číslo certifikátu
SignatureAlgorithm	sha256withRSAEncryption
Issuer	stejný jako Subject vydavatele Certifikátu
Validity	
notBefore	počátek platnosti Certifikátu (UTC)
notAfter	konec platnosti Certifikátu (UTC) = počátek platnosti Certifikátu plus: <ul style="list-style-type: none">kořenová CA - maximálně 365 dnůpodřízená CA - 110 dnů
Subject*	
commonName	OCSP responder - <Subject.CN vydávající CA>
organizationName	Správa základních registrů
organizationIdentifier	NTRCZ-72054506
organizationalUnitName	stejně jako u vydavatele Certifikátu
countryName	CZ
SubjectPublicKeyInfo	
Algorithm	rsaEncryption
subjectPublicKey	2048 bitů
Extensions	rozšíření Certifikátu (viz Tabulka 4)
Signature	zaručená elektronická pečeť Autority

* Maximální délka všech atributů pole Subject je 64 znaků.

Číslo verze

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

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

Rozšíření certifikátu

Tabulka 4 - Rozšíření² certifikátu OCSP respondéru

Rozšíření	Obsah	Poznámka
CertificatePolicies		nekritické, vytváří Autorita
.PolicyInformation (1) policyIdentifier	1.2.203.72054506.A.B.C.D.E*	Certifikát vydán dle této CP
BasicConstraints		nekritická, povinná
cA	False	
KeyUsage	digitalSignature	kritická, povinná
ExtendedKeyUsage	id-kp-OCSPSigning	kritická, povinná
id-pkix-ocsp-nocheck	NULL	nekritická, povinná
SubjectKeyIdentifier	hash veřejného klíče (subjectPublicKey) v tomto Certifikátu	nekritické
AuthorityKeyIdentifier KeyIdentifier	hash veřejného klíče Autority	nekritické
authorityInformationAccess		nekritická
id-ad-caIssuers**	http://cacerts.narodni-ca.cz/XXRR_rsa.cer	http URI certifikátu Autority

* A.B.C.D.E = posledních pět čísel z OID této CP - viz kapitola 1.2.

** RR = poslední dvě číslice roku vydání certifikátu Autority, XX = „subnCA“ pro podřízenou CA (kde n = pořadové číslo subCA), „rca“ pro kořenovou CA.

Objektové identifikátory algoritmů

V procesu poskytování služeb vytvářejících důvěru jsou využívány algoritmy v souladu s příslušnými technickými standardy a normami.

Tvary jmen

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

Omezení jmen

Není relevantní pro Certifikáty vydávané dle této CP.

Objektový identifikátor certifikační politiky

OID tohoto dokumentu/politiky je uveden v kapitole 1.2.

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

Veřejný řídicí dokument.

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

Použití rozšíření Policy Constraints

Není relevantní pro Certifikáty vydávané dle této CP.

Syntaxe a sémantika kvalifikátorů politiky

Viz rozšíření Certifikátu v kapitole 7.1.2 výše.

Zpracování sémantiky kritického rozšíření Certificate Policies

Není relevantní pro tento dokument - není označeno jako kritické.

Profil seznamu zneplatněných certifikátů

Tabulka 5 - 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 6
crlExtensions	rozšíření CRL - viz Tabulka 6
Signature	zaručená elektronická pečeť vydavatele CRL (Authority)

Číslo verze

Seznamy zneplatněných certifikátů jsou vydávány dle X509 verze 2.

Rozšíření CRL a záznamů v CRL

Tabulka 6 - Rozšíření CRL⁴

Rozšíření	Obsah	Poznámka
crlEntryExtensions		
CRLReason	důvod zneplatnění certifikátu; důvod certificateHold je nepřipustný, proto SZR nepoužívá	nekritické
crlExtensions		
AuthorityKeyIdentifier		

³ SZR si vyhrazuje právo upravit množinu a obsah polí CRL, vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami

⁴ SZR si vyhrazuje právo upravit množinu a obsah rozšíření CRL vyžadovanou aktualizacemi standardů ETSI, nebo třetími stranami

Veřejný řídicí dokument.

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

.KeyIdentifier	hash veřejného klíče vydavatele CRL (Authority)	nekritické
CRLNumber	jedinečné číslo vydávaného CRL	nekritické

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.

Číslo verze

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

Rozšíření OCSP

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

7. Hodnocení shody a jiná hodnocení

Periodicita nebo okolnosti hodnocení

Hodnocení shody je popsáno v certifikační politice konkrétní služby využívající OCSP respondér.

Identita a kvalifikace hodnotitele

Viz kapitola 8.

Vztah hodnotitele k hodnocenému subjektu

Viz kapitola 8.

Hodnocené oblasti

Viz kapitola 8.

Postup v případě zjištění nedostatků

Viz kapitola 8.

Sdělování výsledků hodnocení

Viz kapitola 8.

8. Ostatní obchodní a právní záležitosti

Poplatky

Poplatky za vydání nebo obnovení certifikátu

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

Služba obnovení certifikátů certifikačních autorit a OCSP respondérů není poskytována.

Poplatky za přístup k certifikátu

Přístup elektronickou cestou k certifikátům není zpoplatněn.

Zneplatnění nebo přístup k informaci o stavu certifikátu

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

Poplatky za další služby

Není relevantní pro tento dokument.

Postup při refundování

Není relevantní pro tento dokument.

Finanční odpovědnost

Krytí pojištěním

Kvalifikovaným poskytovatelem služeb vytvářejících důvěru je organizační složka státu. Tyto se nepojišťují, případné škody jsou kryty státním rozpočtem.

Další aktiva

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

Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument.

Důvěrnost obchodních informací

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,
- obchodní informace SZR,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

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.

Veřejný řídicí dokument.

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

Odpovědnost za ochranu důvěrných informací

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

Ochrana osobních údajů

Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v SZR řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

Informace považované za osobní údaje

Osobními informacemi jsou veškeré osobní údaje podléhající ochraně ve smyslu příslušných zákonných norem, tedy ZOOÚ.

Zaměstnanci SZR, případně subjekty definované platnou legislativou 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.

Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespádají do působnosti příslušných zákonných norem, tedy ZOOÚ.

Odpovědnost za ochranu osobních údajů

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

Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání osobních údajů a souhlasu s jejich zpracováním je v SZR řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní, účely je v SZR řešeno v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje SZR striktně podle požadavků příslušných zákonných norem, tedy ZOOÚ.

Práva duševního vlastnictví

Tato CP, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systémů poskytujících služby vytvářející důvěru, jsou chráněny autorskými právy SZR.

Zastupování a záruky

Zastupování a záruky CA

SZR zaručuje, že:

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

Veřejný řídicí dokument.

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

- použije soukromé klíče OCSP respondérů certifikačních autorit pouze v procesech poskytování odpovědí na stav certifikátu,
- vydávané certifikáty splňují náležitosti požadované platnou legislativou pro služby vytvářející důvěru a relevantními technickými standardy a normami,
- zneplatní vydané Certifikáty, pokud byla žádost o ukončení jejich platnosti podána způsobem definovaným v této CP.

Zastupování a záruky RA

Určená RA:

- přijímá závazek za správnost jí poskytovaných služeb,
- nevyřídí kladně žádost o Certifikát, pokud se nepodařilo ověřit některou z položek žádosti nebo žadatel není oprávněn k podání žádosti o Certifikát.

Zastupování a záruky držitele certifikátu

Držitel Certifikátu je povinen řídit se ustanoveními této CP.

Zastupování a záruky spoléhajících se stran

Záruky spoléhajících se stran jsou popsány v certifikační politice konkrétní služby využívající OCSP respondér.

Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

Zřeknutí se záruk

SZR poskytuje pro pouze záruky uvedené v kapitole 9.6.

Omezení odpovědnosti

SZR neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované touto CP. Dále neodpovídá za škody vzniklé v důsledku porušení závazků SZR z důvodu vyšší moci.

Záruky a odškodnění

Není relevantní pro tento dokument, je řešeno v certifikační politice konkrétní služby využívající OCSP respondér.

Doba platnosti, ukončení platnosti

Doba platnosti

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

Ukončení platnosti

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CP, je ředitel SZR.

Důsledky ukončení a přetrvání závazků

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

Veřejný řídicí dokument.

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

Individuální upozorňování a komunikace se zúčastněnými subjekty

Komunikace mezi subjekty, které jsou organizačními částmi SZR, se řídí interními pravidly SZR.

Způsob komunikace se spoléhajícími se stranami je vždy uveden v certifikační politice konkrétní služby využívající OCSP respondér.

Novelizace

Postup při novelizaci

Postup je realizován řízeným procesem popsaným v interním dokumentu.

Postup a periodičita oznamování

Vydání nové verze CP je vždy oznámeno formou zveřejňování informací.

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.

Ustanovení o řešení sporů

Řešení sporů mezi organizačními částmi SZR se řídí interními pravidly SZR.

Rozhodné právo

SZR se řídí právním řádem České republiky.

Shoda s platnými právními předpisy

Systém poskytování Služby je provozován ve shodě s legislativními požadavky České republiky a dále s relevantními mezinárodními standardy.

Různá ustanovení

Vždy popsáno v certifikační politice konkrétní certifikační služby využívající OCSP respondér.

Rámcová dohoda

Viz kapitola 9.16.

Postoupení práv

Viz kapitola 9.16.

Oddělitelnost ustanovení

Viz kapitola 9.16.

Zřeknutí se práv

Viz kapitola 9.16.

Vyšší moc

Viz kapitola 9.16.

Další ustanovení

Není relevantní pro tento dokument.