SPRÁVA ZÁKLADNÍCH REGISTRŮ		
POLITIKA	počet stran	34
	přílohy	0

NCA

Prováděcí směrnice vydávání kvalifikovaných elektronických časových razítek systémem TSA

(kryptografie RSA)

Oblast působnosti:
Zaměstnanci vybraných subjektů veřejné správy, mezi které patří bezpečností složky, zpravodajské služby a vybrané útvary resortu Ministerstva vnitra.

Gestor, podpis: Josef KNOTEK	**Nahrazuje:**
Zpracovatel, podpis: Ing. František KNOTEK	**Schvalovatel, podpis:** Ing. Michal PEŠEK
Odborný garant, podpis: RNDr. Miroslav ŠEDIVÝ	**Schváleno dne: 7. 5. 2019**
Klasifikace: VEŘEJNÝ	**Účinnost od dne: 8. 5. 2019**

HISTORIE DOKUMENTU:

Verze	Datum	Autor	Popis
1.00	06. 12. 2018	První certifikační autorita, a.s.	Vytvoření první verze dokumentu
1.01	25. 01. 2019	První certifikační autorita, a.s.	Aktualizace mailových adres, uvedení www adres do souladu s profilem certifikátu. Upravena formulace krytí pojištěním.
1.02	07. 05. 2019	První certifikační autorita, a.s. Eva Kaletová	Doplněna platnost dokumentu. Aktualizace dle grafického manuálu SZR.

OBSAH

1. Úvod

Tento dokument, Prováděcí směrnice vydávání kvalifikovaných elektronických časových razítek systémem TSA (algoritmus RSA), dále též Směrnice, rozpracovává a upřesňuje zásady uvedené v dokumentu Politika vydávání kvalifikovaných elektronických časových razítek systémem TSA (algoritmus RSA), dále též Politika. Směrnice byla vypracována na základě požadavků platné legislativy, zabývá se skutečnostmi vztahujícími se k procesům vydávání a využívání kvalifikovaných elektronických časových razítek (zkráceně jen časových razítek) a zahrnuje všechny požadavky politiky BTSP (Best practices Time-Stamp Policy) uvedené ve standardu EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Legislativní požadavky 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.

Poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

Pozn.: Pokud jsou v textu uváděny odkazy na standardy nebo zákony, jedná se vždy buď o uvedený standard nebo zákon, resp. o standard či zákon, který ho nahrazuje. Pokud by byla tato Politika v rozporu se standardy nebo zákony, které nahradí dosud platné, bude vydána nová verze Politiky.

1.1 Přehled

Dokument je rozdělen do šesti základních kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 uvádí do problematiky a identifikuje tento dokument názvem a verzí.
- Kapitola 2 uvádí seznamy použitých pojmů a zkratek.
- Kapitola 3 popisuje základní pojetí služby autority časových razítek, obecně popisuje subjekty, které se na službě podílejí.
- Kapitola 4 popisuje použitelnost vydávaných časových razítek a postupy hodnocení shody.
- Kapitola 5 popisuje závazky a odpovědnosti zúčastněných stran.
- Kapitola 6 popisuje postupy autority časových razítek, profilů žádostí o vydání časových razítek a vydávaných časových razítek, včetně problematiky obchodní a právní.

V procesu poskytování služby vytvářející důvěru v oblasti vydávání časových razítek (dále též Služba) provozuje organizační složkou státu Správa základních registrů, dále též SZR systém TSA skládající se z jednotlivých jednotek TSU. Podrobný popis procesů této autority časových razítek je uveden v dalších dokumentech, které jsou obecně neveřejné. Tyto dokumenty, včetně dalších zpráv, výsledků testů a interních kontrol, tvoří dokumentační sadu, dosažitelnou výhradně autorizovanému personálu a auditorům.

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu:	Prováděcí směrnice vydávání kvalifikovaných elektronických časových razítek systémem TSA (kryptografie RSA), verze 1.02
OID směrnice:	není přiřazeno

2. Přehled použitých pojmů a zkratek

Dále uvedený přehled pojmů a zkratek je platný pro tento dokument. Použité zkratky mají alternativní charakter, tzn. v textu může být použit jak plný text, tak i jeho zkratka, přičemž obojí má totožnou obsahovou hodnotu.

2.1 Použité pojmy

Tabulka 1 - Pojmy

Pojem	Vysvětlení
bit	z anglického *binary digit* - číslice dvojkové soustavy - základní a současně nejmenší jednotka informace v číslicové technice
časové razítko	elektronické časové razítko nebo 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
hashovací funkce	transformace, která jako vstup přijímá řetězec znaků o libovolné délce a výsledkem je řetězec znaků s pevnou délkou (hash)
klient	žadatel o časové razítko nebo spoléhající se strana
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
párová data	soukromý a jemu odpovídající veřejný klíč
písemná smlouva	text smlouvy v elektronické, nebo listinné podobě
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 elektronické pečetě
spoléhající se strana	subjekt spoléhající se při své činnosti na časové razítko vydané SZR
veřejný klíč	jedinečná data pro ověřování elektronické pečetě
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
žadatel o časové razítko	individuální koncový uživatel (fyzická osoba), právnická osoba nebo organizační složka státu (zahrnující několik koncových uživatelů), resp. systém, provozovaný výše zmíněnými subjekty

2.2 Zkratky

Tabulka 2 - Zkratky

Pojem	Vysvětlení
CA	certifikační autorita
CCTV	Closed Circuit Television, uzavřený televizní okruh
CEN	European Committee for Standardization, asociace sdružující národní standardizační orgány
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 č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
EKV	elektronická kontrola vstupu.
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ESI	Electronic Signatures and Infrastructures
ETSI	the European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EZS	elektronická zabezpečovací signalizace
FIPS	Federal Information Processing Standard, označení standardů v oblasti informačních technologií pro nevojenské státní organizace ve Spojených státech
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
IP	Internet Protocol, komunikační protokol síťové vrstvy
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
OCSP	Online Certificate Status Protocol, protokol pro zjišťování stavu certifikátu veřejného klíče
OID	Object Identifier, číselná identifikace objektu

PDCA	Plan-Do-Check-Act, Plánování-Zavedení-Kontrola-Využití, Demingův cyklus, metoda neustálého zlepšování
PDF	Portable Document Format, standard formátu souboru
PKI	Public Key Infrastructure, infrastruktura veřejných klíčů
RA	registrační autorita
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
TSA	Time Stamping Authority, autorita časových razítek, obsahující více jednotek opatřujících časová razítka zaručenou elektronickou pečetí, kdy každá z nich disponuje jedinečným soukromým klíčem a odpovídajícím certifikátem
TSU	Time Stamp Unit, jednotka opatřující vydávaná časová razítka zaručenou elektronickou pečetí
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
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

3. Základní pojetí

3.1 Služby autority časových razítek

Služby autority časových razítek provozované SZR, zahrnující oblasti vytváření a vydávání časových razítek a implementaci autentizace žadatelů o časová razítka, jsou poskytovány v souladu s relevantní legislativou a technickými standardy.

3.2 Autorita časových razítek

Systém TSA je z pohledu klientů důvěryhodná výpočetní a komunikační infrastruktura, vydávající časová razítka. Z titulu provozovatele nese celkovou odpovědnost za poskytování služeb vytvářejících důvěru v oblasti vydávání časových razítek SZR.

3.3 Žadatelé o časové razítko

Žadatelem o časové razítko mohou být na základě písemné smlouvy se SZR:

- bezpečnostní/zvláštní složky,
- orgány veřejné moci uvedené v rejstříku orgánů veřejné moci vedeném Ministerstvem vnitra,
- státního úřady, nebo organizační a jiné složky státu nevykonávající veřejnou moc.
- fyzické osoby určená ze strany orgánů veřejné moci.

3.4 Spoléhající se strana

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na časová razítka vydávaná podle této Směrnice, resp. odpovídající Politiky.

4. Politika autority časových razítek

4.1 Použití časových razítek

Tato Směrnice, resp. odpovídající Politika nedefinuje žádná omezení použitelnosti časového razítka, vydaného v souladu s jejím obsahem.

4.2 Hodnocení shody a jiná hodnocení

V SZR jsou prováděna hodnocení bezpečnosti v oblastech, uvedených v kapitole 4.2.4. Součástí těchto hodnocení je mimo jiné sledování, zda jsou plně dodržovány standardy, uvedené v kapitole 6.4.7.2. Oblasti hodnocení jsou upraveny interním dokumentem:

- „NCA - Kontrolní činnost, bezúhonnost a odbornost“.

SZR si vyhrazuje právo provádění i jiných forem kontrol.

4.2.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicita hodnocení, včetně okolností pro provádění hodnocení, je dána platnou legislativou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, dle kterých je hodnocení prováděno.

Periodicita jiných hodnocení je dána příslušnými technickými standardy a normami.

4.2.2 Identita a kvalifikace hodnotitele

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení podle platné legislativy pro služby vytvářející důvěru, je dána touto legislativou a jí odkazovanými technickými standardy a normami.

Kvalifikace hodnotitele provádějícího jiná hodnocení je dána příslušnými technickými standardy a normami.

4.2.3 Vztah hodnotitele k hodnocenému subjektu

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

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

4.2.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného platnou legislativou pro služby vytvářející důvěru jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány technickými standardy a normami, podle kterých je hodnocení prováděno.

4.2.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer SZR, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat konkrétní službu vytvářející důvěru, přeruší SZR tuto službu do doby, než budou tyto nedostatky odstraněny.

4.2.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům legislativy pro služby vytvářející důvěru a 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 SZR, které s obsahem závěrečné zprávy seznámí.

5. Závazky a odpovědnosti

5.1 Závazky autority časových razítek

5.1.1 Obecné závazky autority časových razítek

SZR zaručuje zejména:

- přístup ke Službě:
  - nepřetržitý, s výjimkou plánovaných (předem ohlášených) časových přerušení spojených s technickými zásahy,
  - za podmínek uvedených v písemné smlouvě,
- striktní dodržování platné legislativy vztahující se k celému procesu vydávání časových razítek, včetně neporušování autorských ani licenčních práv,
- poskytování Služby osobami s odbornými znalostmi a kvalifikací nezbytnou pro poskytování této Služby a obeznámenými s příslušnými bezpečnostními postupy,
- používání bezpečných systémů a bezpečných nástrojů, zajištění dostatečné bezpečnosti postupů, které tyto systémy a nástroje podporují včetně dostatečné kryptografické bezpečnosti těchto nástrojů,
- písemné informování žadatele o vydávání časových razítek o přesných podmínkách pro využívání této Služby před uzavřením smlouvy, včetně případných omezení pro její použití, a o podmínkách reklamací a řešení vzniklých sporů a o tom, zda je či není kvalifikovaným poskytovatelem Služby,
- mlčenlivost kmenových zaměstnanců, případně jiných fyzických osob, které přicházejí do styku s osobními údaji 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).

5.1.2 Závazky autority časových razítek ve vztahu k žadatelům o časové razítko a držitelům časových razítek

SZR zaručuje zejména, že:

- jí vydávaná časová razítka obsahují všechny náležitosti stanovené platnou legislativou pro služby vytvářející důvěru,
- použije soukromé klíče certifikátů certifikačních autority vydávajících certifikáty pro jednotlivá TSU pouze v procesech vydávání těchto certifikátů a dalších typů certifikátů a pro vydávání seznamů zneplatněných certifikátů,
- použije soukromé klíče OCSP respondérů pouze v procesech poskytování odpovědí na stav certifikátu,
- použije soukromé klíče příslušné certifikátům TSU pouze k opatřování vydávaných časových razítek zaručenou elektronickou pečetí,
- implementovala odpovídající opatření proti padělání časových razítek,
- vydá časové razítko neprodleně po obdržení platného požadavku,
- žádným způsobem neověřuje hash, kterému má být časové razítko přiřazeno (s výjimkou identifikace kryptografického algoritmu),
- využívá důvěryhodnou časovou synchronizaci,
- jí vydaná odpověď na žádost o časové razítko obsahuje minimálně:

- □ sériové číslo, které je pro konkrétní TSU systému TSA jedinečné,
- □ identifikátor politiky, podle níž bylo časové razítko vydáno,
- □ časový údaj odpovídající hodnotě koordinovaného světového času (UTC) v době vytváření časového razítka s přesností jedna sekunda,
- □ data v elektronické podobě obsažená v žádosti o časové razítko (hash dokumentu opatřovaného časovým razítkem),
- □ zaručenou elektronickou pečeť TSU.

5.2 Závazky žadatelů o časové razítko a držitelů časového razítka

Žadatel o časové razítko, resp. jeho držitel ručí za informace, které uvedl ve smlouvě o poskytování časových razítek a postupuje v souladu s platnou legislativou pro služby vytvářející důvěru, touto Politikou a zmíněnou smlouvou.

Žadatelé o časového razítka, resp. jeho držitelé jsou vždy po obdržení odpovědi na žádost o časové razítko povinni zjistit stav odpovědi. V případě chyby není časové razítko v odpovědi obsaženo a žadatel, resp. držitel je povinen překontrolovat odpovídající chybové hlášení. V opačném případě je žadatel, resp. držitel povinen zejména:

- ■ ověřit platnost zaručené elektronické pečetě časového razítka a následně všech certifikátů, vztahujících se k TSU, která tuto zaručenou elektronickou pečeť vytvořila,
- ■ ověřit, zda vrácený hash je totožný s tím odeslaným v žádosti,
- ■ v případě, že žádost obsahovala položky „nonce“ nebo „reqPolicy“ ověřit, že jejich hodnota v odpovědi je totožná.

5.3 Závazky spoléhajících se stran

Spoléhající se strany postupují v souladu s touto Politikou. Jejich závazkem je zejména:

- ■ ověření platnosti zaručené elektronické pečetě časového razítka včetně kontroly odvolání certifikátů v certifikační cestě,
- ■ vzít v úvahu případné omezení použitelnosti časových razítek uvedená v této Směrnici, resp. odpovídající Politice,
- ■ vzít v úvahu další opatření předepsaná smlouvou.

5.4 Odpovědnost

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platné legislativy týkající se vztahů mezi poskytovatelem a spotřebitelem a dále takové záruky, které byly sjednány mezi SZR a žadatelem o Službu. Smlouva nesmí být v rozporu s platnou legislativou pro služby vytvářející důvěru a musí být vždy v elektronické nebo listinné formě.

SZR:

- ■ se zavazuje, že splní veškeré povinnosti definované jak platnou legislativou, včetně legislativy pro služby vytvářející důvěru, tak příslušnými politikami,
- ■ splní výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služby,
- ■ další možné náhrady škody vycházejí z ustanovení příslušné legislativy a o jejich výši může rozhodnout soud,
- ■ jiné záruky, než výše uvedené, neposkytuje.

Další možné náhrady škody vycházejí z ustanovení příslušných zákonů a o jejich výši může rozhodnout soud.

SZR neodpovídá:

- za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služby držitelem časového razítka, zejména za využívání v rozporu s podmínkami uvedenými v této Politice,
- za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení.

Reklamaci je možné podat těmito způsoby:

- e-mailem na adresu podpora@szrcr.cz, předmět zprávy musí začínat textem NCA,
- prostřednictvím datové schránky SZR,
- doporučenou poštovní zásilkou na adresu sídla SZR,
- osobně v sídle SZR.

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

- co nejvýstižnější popis závady,
- sériové číslo reklamovaného produktu,
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne SZR 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 třiceti dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

5.5 Ukončení poskytování služeb vydávání časových razítek

Službu vydávání časových razítek pro konkrétního uživatele ukončuje buď tento uživatel, tj. žadatel o časové razítko, nebo SZR, nejsou-li ze strany žadatele dodrženy podmínky písemné smlouvy.

6. Požadavky na postupy autority časových razítek

6.1 Správa politiky

6.1.1 Organizace spravující politiku nebo prováděcí směrnici autority časových razítek

Tuto Směrnici, resp. odpovídající Politiku spravuje SZR.

6.1.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici autority časových razítek

Kontaktní osoba SZR v souvislosti s touto Politikou, resp. s odpovídající Směrnicí pověřený zaměstnanec bezpečnostního oddělení SZR uvedený na webu SZR.

6.1.3 Osoba rozhodující o souladu prováděcí směrnice s politikou autority časových razítek

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů SZR uvedených ve Směrnici s touto Politikou, je ředitel SZR.

6.1.4 Postupy při schvalování prováděcí směrnice autority časových razítek

Pokud je potřebné provést změny v příslušné Směrnici a vytvořit její novou verzi, určuje ředitel SZR osobu, která je oprávněna tyto změny provést. Detailní řešení je popsáno v interním dokumentu:

- „NCA - Změnové řízení“.

Nabytí platnosti nové verze Směrnice předchází její schválení ředitelem SZR.

6.2 Požadavky na životní cyklus párových dat autority časových razítek

6.2.1 Generování a instalace párových dat

6.2.1.1 Generování párových dat

Generování párových dat TSU systému TSA probíhá v zabezpečené oblasti a je prováděno v kryptografickém modulu, který byl hodnocen podle FIPS 140-2 úroveň 3. Konkrétní technický postup generování párových dat, sloužících k opatřování časových razítek zaručenou elektronickou pečetí je popsán v interních dokumentech:

- „NCA - Řízení fyzického přístupu do provozních prostor“,
- „NCA - Správa TSS“.

O generování je pořízen písemný záznam obsahující mj.:

- jmenný seznam přítomných pracovníků s uvedením jména, příjmení a titulu, včetně jejich podpisu,
- datum a čas zahájení a ukončení generování párových dat s přesností minimálně na minuty,
- místo, kde ke generování párových dat došlo,

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

6.2.1.2 Poskytování veřejných klíčů

Veřejné klíče, sloužící pro ověřování elektronických pečetí vydávaných časových razítek, jsou obsaženy v certifikátu relevantního TSU. Tento certifikát je možno získat nejméně dvěma nezávislými kanály:

- prostřednictvím internetových informačních adres SZR,
- prostřednictvím internetové adresy orgánu dohledu.

6.2.1.3 Délky párových dat

Systém TSA používá asymetrický šifrový algoritmus RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) použitých pro opatřování vydávaných časových razítek zaručenou elektronickou pečetí je 2048 bitů.

6.2.2 Ochrana soukromého klíče

6.2.2.1 Standardy a podmínky používání kryptografických modulů

Soukromé klíče, sloužící pro vytváření zaručených elektronických pečetí vydávaných časových razítek, jsou uloženy v kryptografickém modulu, který byl hodnocen podle standardu FIPS 140-2 úroveň 3 a splňuje tak požadavky platné legislativy pro služby vytvářející důvěru.

6.2.2.2 Zálohování soukromých klíčů

Soukromý klíč TSU systému TSA je zálohován jako součást bezpečně a certifikovaně šifrované adresářové struktury. Konkrétní postup je popsán v interním dokumentu:

- „NCA - Správa TSS“.

6.2.2.3 Uchovávání soukromých klíčů

Po uplynutí doby platnosti soukromých klíčů určených k opatřování vydávaných časových razítek zaručenou elektronickou pečetí jsou tyto klíče, včetně jejich záloh, zničeny. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, proto je zakázáno. Konkrétní postup je popsán v interním dokumentu:

- „NCA - Správa TSS“.

6.2.2.4 Transfer soukromých klíčů

Soukromé klíče sloužící k vytváření zaručených elektronických pečetí vydávaných časových razítek jsou generována přímo v kryptografickém modulu relevantního TSU.

Pro transfer soukromého klíče TSU systému TSA z kryptografického modulu není relevantní, jedná se o běžnou zálohu bezpečně a certifikovaně zašifrované adresářové struktury.

Transfer soukromého klíče TSU systému TSA do kryptografického modulu probíhá prostřednictvím administrátorských čipových karet kryptografického modulu.

O provedeném transferu je vždy pořízen písemný záznam.

6.2.2.5 Uložení soukromých klíčů v kryptografickém modulu

Soukromé klíče TSU systému TSA se v otevřeném tvaru nacházejí pouze v kryptografickém modulu splňujícím požadavky platné legislativy pro služby vytvářející důvěru, tedy standardu FIPS PUB 140-2 úroveň 3. Jinak jsou bezpečným a certifikovaným způsobem šifrovaně uloženy.

6.2.2.6 Aktivační data

Není relevantní pro tento dokument, aktivační data TSU systému TSA neexistují.

6.2.2.7 Postup při aktivaci soukromých klíčů

Aktivace soukromého klíče TSU systému TSA vygenerovaného v kryptografickém modulu prováděna není, klíč je aktivován okamžikem vygenerování.

6.2.2.8 Postup při deaktivaci soukromých klíčů

Deaktivace původního soukromého klíče TSU systému TSA prováděna není.

6.2.2.9 Postup při ničení soukromých klíčů

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

6.2.2.10 Uchovávání veřejných klíčů

Veřejné klíče sloužící k ověřování zaručených elektronických pečetí vydávaných časových razítek jsou obsaženy v certifikátech relevantních TSU. Tyto certifikáty jsou uchovávány za celou dobu existence SZR.

6.2.3 Profil certifikátu autority časových razítek

Podrobný popis profilu certifikátu TSU systému TSA je uveden v dokumentu Certifikační politika vydávání certifikátů pro systém TSA (algoritmus RSA) dostupném na internetové adrese SZR.

6.2.4 Výměna párových dat

Platnost párových dat (veřejný a soukromý klíč) pro tvorbu zaručené elektronické pečetě, resp. ověřování zaručené elektronické pečetě kvalifikovaných elektronických časových razítek, je omezena platností Certifikátu (obvykle na dobu šesti let).

V prvním roce po vygenerování párových dat a vydání Certifikátu veřejného klíče je klíč soukromý používán pro tvorbu zaručené elektronické pečetě kvalifikovaných elektronických časových razítek. Před koncem tohoto období jsou vygenerována nová párová data a vydán Certifikát příslušného veřejného klíče. K tvorbě zaručené elektronické pečetě kvalifikovaných elektronických časových razítek je dále využíván nejnovější soukromý klíč. Veřejné klíče, staré i nejnovější, jsou využívány k ověřování zaručených elektronických pečetí vytvořených odpovídajícím soukromým klíčem.

V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, které by mohly ohrozit bezpečnost procesu tvorby elektronických pečetí kvalifikovaných elektronických časových razítek a je nutná změna kryptografických algoritmů, délky klíčů atd.) je generování nových párových dat a vydání příslušného Certifikátu provedeno v adekvátním, co nejkratším časovém období.

6.2.5 Ukončení životního cyklu párových dat

Doba platnosti certifikátu TSU systému TSA je uvedena v těle tohoto certifikátu. Po této době lze data pro ověřování zaručených elektronických pečetí použít bez záruky.

6.2.5.1 Zneplatnění a pozastavení platnosti certifikátu TSU

Certifikát TSU může být zneplatněn pouze na základě následujících okolností:

- nastanou-li skutečnosti uvedené v platné legislativě pro služby vytvářející důvěru,
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci soukromého klíče certifikační autority vydávající certifikáty pro TSU systému TSA a svůj OCSP respondér,
- dojde ke kompromitaci nebo existuje důvodné podezření, že došlo ke kompromitaci soukromého klíče konkrétního TSU.

Služba pozastavení platnosti certifikátu není poskytována.

Profil seznamu zneplatněných certifikátů odpovídá relevantním technickým standardům a normám.

6.2.6 Správa kryptografického modulu používaného při vytváření časových razítek

Konkrétní postupy správy TSU jsou popsány v interním dokumentu:

- „NCA - Správa TSS“.

6.2.6.1 Hodnocení kryptografického modulu

Kryptografický modul, sloužící pro opatřování vydávaných časových razítek zaručenou elektronickou pečetí, splňuje požadavky na kryptografické moduly FIPS 140-2 úroveň 3.

6.3 Vydávání časových razítek

6.3.1 Uzavření smlouvy

Vydávání časových razítek je službou poskytovanou subjektům uvedeným v kapitole 3.3 na základě písemné smlouvy uzavírané způsobem běžným v obchodním styku. Zmíněný subjekt se uzavřením smlouvy zaváže jednat podle této Směrnice, resp. odpovídající Politiky.

6.3.2 Identifikace a autentizace

Identifikace a autentizace žadatele o časové razítko, je-li požadována, je prováděna jménem a heslem.

6.3.3 Přijetí nebo zamítnutí žádosti o časové razítko

Po vytvoření žádosti je tato předána systému TSA. V případě, že žádost nesplňuje požadavky této Politiky, je systémem TSA zamítnuta. Struktura žádosti o časové razítko je popsána v kapitole 6.3.3 odpovídající politiky.

6.3.4 Vydání časového razítka

Doba zpracování žádosti o časové razítko nepřesáhne řádově jednotky sekund.

6.3.5 Úkony autority časových razítek v průběhu vydávání časového razítka

Systém TSA provádí veškeré kontroly formální správnosti žádosti o časové razítko a na základě jejich výsledku vytvoří konkrétní TSU odpověď, obsahující stav odpovědi a v případě kladného výsledku kontrol i časové razítko (viz RFC 3161). Časové razítko je opatřeno zaručenou elektronickou pečetí konkrétního TSU.

Každá odpověď na žádost o časové razítko je umístěna úložišti systému TSA.

Odpověď na žádost o časové razítko obsahuje vždy stav odpovědi a v případě úspěšného vydání i časové razítko. Struktura odpovědi na žádost o časové razítko a časového razítka jsou popsány v kapitole 6.3.5 odpovídající Politiky.

6.3.6 Převzetí časového razítka

Po obdržení odpovědi na žádost o časové razítko je žadatel povinen zjistit její stav. Obsahuje-li odpověď časové razítko, je žadatel povinen postupovat v souladu s kapitolou 5.2.

6.3.7 Synchronizace s UTC

6.3.7.1 Synchronizace

TSS servery synchronizují průběžně svůj čas NTP serverem, který získává čas prostřednictvím systému GPS a Galileo. Postup je popsán v interní dokumentaci:

- „NCA - Správa TSS“.

6.3.7.2 Bezpečnost NTP a TSS serveru

Viz kapitola 6.4.6.

6.3.7.3 Detekce odchýlení času

Systémový čas TSS kontroluje v pravidelných intervalech spouštěná kontrolní aplikace proti druhému nezávislému zdroji času. Čas tohoto zdroje je opět synchronizován s UTC.

Výsledkem úspěšné kontroly je časově omezený auditní "token", který povolí TSU vydávání časových razítek do doby, která je v tokenu uvedena. Před uplynutím této doby musí proběhnout nová (úspěšná) kontrola, jinak TSU zastaví vydávání časových razítek.

V případě zjištění odchylky větší než je maximální přípustná odchylka pro vydávání časových razítek nastavená v konfiguraci vytvoří kontrolní aplikace neplatný token (na základě toho TSU okamžitě zastaví vydávání časových razítek) a současně vygeneruje alarm pro provozní obsluhu (o zastavení vydávání časových razítek).

Postup je popsán v interním dokumentaci:

- „Správa TSS“.

6.3.7.4 Přestupná sekunda

Přestupná sekunda je řešena manuálně, postup je popsán v interní dokumentaci:

- „Správa TSS“.

6.4 Správa a provozní bezpečnost autority časových razítek

6.4.1 Řízení bezpečnosti

Řízení bezpečnosti je popsáno v interní dokumentaci SZR:

- „Politika bezpečnosti informací SZR“,
- „NCA - Bezpečnostní incidenty“.

6.4.2 Hodnocení a řízení rizik

V SZR byly provedeny následující činnosti:

- identifikace aktiv (programové vybavení, technické vybavení, data) a jejich vazeb,
- hodnocení aktiv informačního systému,
- stanovení relevantních hrozeb a zranitelností,
- hodnocení hrozeb a zranitelností,
- určení míry rizika pro každou kombinaci aktiva (skupiny aktiv), hrozby a zranitelnosti.

Problematikou hodnocení a řízení rizik se zabývají interní dokumenty:

- „NCA - Systémová bezpečnostní politika (CA a TSA)“,
- „NCA - Kontrolní činnost, bezúhonnost a odbornost“,
- „NCA - Bezpečnostní incidenty“.

6.4.3 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.

6.4.4 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

6.4.5 Personální bezpečnost

6.4.5.1 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:

- „NCA - Systémová bezpečnostní politika (CA a TSA)“,
- „Politika bezpečnosti informací SZR“,
- „NCA - Příručka administrátora systémů CA, TSA“.

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

6.4.5.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro níže uvedené činnosti je nezbytná přítomnost více než jediné osoby:

- generování párových dat TSU systému TSA,
- ničení soukromého klíče TSU systému TSA,
- zálohování/obnova soukromého klíče TSU systému TSA.

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

6.4.5.3 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.

6.4.5.4 Role vyžadující rozdělení povinností

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

6.4.5.5 Požadavky na kvalifikaci, zkušenost a bezúhonnost

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

- občanská bezúhonnost - prokazováno výpisem z rejstříku trestů, nebo čestným prohlášením,
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně tři roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně pět let praxe v

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

- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

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

- vysokoškolské vzdělání v rámci akreditovaného bakalářského, resp. magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

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

Problematika je detailně popsána v interním dokumentaci:

- „NCA - Kontrolní činnost, bezúhonnost a odbornost".

6.4.5.6 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.

6.4.5.7 Požadavky na přípravu pro výkon role, vstupní 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.

Problematika je detailně popsána v interním dokumentu:

- „NCA - Kontrolní činnost, bezúhonnost a odbornost".

6.4.5.8 Požadavky a periodicita doškolování

Dvakrát za 12 měsíců jsou příslušným 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.

Problematika je detailně popsána v interním dokumentaci:

- „NCA - Kontrolní činnost, bezúhonnost a odbornost".

6.4.5.9 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.

6.4.5.10 Postihy za neoprávněné činnosti zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným pracovníkem postupováno způsobem, popsaným v interní dokumentaci a řídí se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

6.4.5.11 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 aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími politikami, relevantními částmi interní dokumentace SZR, 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.

6.4.5.12 Dokumentace poskytovaná zaměstnancům

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

6.4.6 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně popsána v interních dokumentech:

- „NCA - Řízení fyzického přístupu do provozních prostor“,
- „NCA - Požární bezpečnost“,
- „NCA - Bezpečnostní incidenty“,
- „NCA - Obnova systémů CA, TSA“,
- „NCA - Přemístění systémů CA, TSA“,
- „NCA - Projekt fyzické bezpečnosti prostor“.

6.4.6.1 Umístění a konstrukce

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

6.4.6.2 Fyzický přístup

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

6.4.6.3 Elektřina a klimatizace

V prostorách, kde jsou umístěny důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru, je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20°C ± 5°C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

6.4.6.4 Vliv vody

Důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru 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.

6.4.6.5 Protipožární opatření a ochrana

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

6.4.6.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v protipožárním trezoru.

Papírová média, která je nutno dle platné legislativy pro služby vytvářející důvěru uchovávat, jsou skladována na pracovištích registračních autorit bezpečnostních/zvláštních složek, orgánů veřejné moci uvedených v rejstříku orgánů veřejné moci vedeném Ministerstvem vnitra, státních úřadů, nebo organizačních a jiných složek státu nevykonávajících veřejnou moc. Papírová média ukládaná na SZR jsou uchovávána v trezoru, dokumenty jsou skenovány a příslušná elektronická média jsou ukládána v geograficky odlišné lokalitě.

6.4.6.7 Nakládání s odpady

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

6.4.6.8 Zálohy mimo budovu

Kopie záloh pro úplnou obnovu systému a hesla jsou uloženy ve schránce ČNB.

6.4.7 Provozní řízení

Úroveň bezpečnosti použitých komponent pro poskytování služeb vytvářejících důvěru je definována technickými standardy. Detailní řešení specifických technických požadavků počítačové bezpečnosti a jejich řešení je popsáno v interních dokumentech:

- „NCA - Systémová bezpečnostní politika (CA a TSA)“,
- „NCA - Řízení fyzického přístupu do provozních prostor“,
- „NCA - Uchování dat a informací“,
- „NCA - Záloha dat systémů“,
- „NCA - Příručka administrátora systémů CA, TSA“,
- „NCA - Obnova systémů CA, TSA“,
- „NCA - Přemístění systémů CA, TSA“,
- „NCA - Správa TSS“,
- „NCA - Řízení kontinuity provozu“.

6.4.7.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti použitých komponent pro poskytování služeb vytvářejících důvěru je definována technickými standardy.

6.4.7.2 Hodnocení počítačové bezpečnosti

Hodnocení bezpečnosti SZR je založeno na mezinárodních a národních standardech:

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 421 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající časová razítka.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ČSN ETSI EN 319 422 Elektronické podpisy a infrastruktury (ESI) - Protokol pro vyznačení času a profily časového razítka.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- 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.

6.4.8 Řízení přístupu do systému

Interní subsystémy systému TSA jsou dostupné pouze pověřeným pracovníkům SZR, smluvním partnerům nebo subjektům definovaným platnou legislativou pro služby vytvářející důvěru. Přístup k těmto informacím je řízen pravidly, uvedenými v interní dokumentaci:

- „NCA - Řízení fyzického přístupu do provozních prostor“,
- „NCA - Příručka administrátora systémů CA, TSA“,
- „NCA - Správa TSS“.

6.4.9 Vývoj a údržba důvěryhodných systémů

6.4.9.1 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.

6.4.9.2 Kontroly řízení 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, resp. originální verze ISO/IEC 27000 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky, resp. originální verze ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací, resp. originální verze ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security controls.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací, resp. originální verze ISO/IEC 27006 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.

6.4.9.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v SZR 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.

6.4.10 Obnova po havárii nebo kompromitaci

6.4.10.1 Postup v případě incidentu a kompromitace

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

- „NCA - Řízení kontinuity provozu“,
- „NCA - Bezpečnostní incidenty“,
- „NCA - Obnova systémů CA, TSA“,
- „NCA - Přemístění systémů CA, TSA“.

6.4.10.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz předchozí kapitola.

6.4.10.3 Postup při zjištění odchylky času

Pokud je zjištěná odchylka času od UTC mimo specifikovaný interval, definovaný při inicializaci TSU, je jeho činnost okamžitě ukončena a do provedení nové inicializace není služba vydávání časových razítek tímto TSU poskytována. Problematika je popsána v interní dokumentaci:

- „NCA - Správa TSS“.

6.4.10.4 Postup při kompromitaci soukromého klíče TSU

V případě kompromitace nebo vzniku důvodné obavy ze zneužití soukromého klíče TSU systému TSA SZR:

- okamžitě ukončí jeho používání a prokazatelně zneplatní certifikát tohoto TSU - o této skutečnosti, včetně důvodu, informuje na své internetové informační adrese, pro zpřístupnění této informace je využit i seznam zneplatněných certifikátů,
- pokud je to možné, informuje klienty služby vydávání časových razítek o zneplatnění certifikátu relevantního TSU, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly ve smlouvě - součástí této informace je důvod ukončení platnosti certifikátu relevantního TSU,
- oznámí příslušnému orgánu dohledu informaci o zneplatnění certifikátu TSU s uvedením důvodu zneplatnění,
- vydá nový certifikát relevantnímu TSU - postup je stejný jako při vydání prvotního certifikátu tohoto TSU.

6.4.10.5 Schopnosti obnovit činnost po havárii

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

- „NCA - Řízení kontinuity provozu“,
- „NCA . Bezpečnostní incidenty“,
- „NCA - Obnova systémů CA, TSA“,
- „NCA - Přemístění systémů CA, TSA“.

6.4.11 Ukončení činnosti autority časových razítek

Pro ukončování činnosti systému TSA platí následující pravidla:

- ukončení činnosti musí být písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou písemnou smlouvu vztahující se k poskytování Služby,

- ukončení činnosti musí být zveřejněno na internetové adrese,
- soukromé klíče TSU systému TSA musí být prokazatelně zničeny a o tomto zničení proveden záznam, který bude uchováván podle pravidel této Politiky.

Ukončování činnosti je řízený proces probíhající podle předem připraveného plánu.

Problematika plánovaného ukončení činnosti SZR jako kvalifikovaného poskytovatele služeb vytvářejících důvěru je detailně popsána v interní dokumentaci:

- „NCA - Ukončení činnosti CA, TSA“.

6.4.12 Shoda s platnými právními předpisy

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

6.4.13 Úložiště informací a dokumentace, které se týkají provozu autority časových razítek

6.4.13.1 Auditní záznamy (logy)

Zásady vytváření, zpracování a uchovávání auditních logů jsou popsány v interní dokumentaci:

- „NCA - Systémová bezpečnostní politika (CA a TSA)“,
- „NCA - Řízení fyzického přístupu provozních prostor“,
- „NCA - Uchovávání dat a informací“,
- „NCA - Záloha dat systémů“,
- „NCA - Příručka administrátora systémů CA, TSA“,
- „NCA - Správa TSS“.

6.4.13.1.1 Typy zaznamenávaných událostí

S ohledem na požadavky:

- CEN/TS 419261 Security requirements for trustworthy systems managing certificates and time-stamps,
- ČSN ETSI EN 319 421 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající časová razítka, resp.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps,

jsou v důvěryhodných systémech SZR do elektronického auditního logu zaznamenávány následující bezpečnostně relevantní provozní události:

- z hlediska systému významné události prostředí a klíčového hospodářství,
- spuštění a ukončení funkcí auditu,
- změny parametrů auditu,
- akce prováděné při chybách úložiště auditních záznamů,
- všechny pokusy o přístupu k systému,
- veškeré události, vztahující se k požadavkům na certifikát TSU,
- veškeré chyby (včetně časových odchylek mimo povolenou toleranci), spojené s důvěryhodným zdrojem času,
- veškeré události, vztahující se k životnímu cyklu párových dat TSU,

- veškeré události, vztahující se k životnímu cyklu certifikátů TSU,
- veškeré události, vztahující se k synchronizaci časového údaje měřidla času serveru vydávajícího časová razítka s UTC,
- veškeré události, vztahující se ke ztrátě synchronizace.

Všechny záznamy v auditním souboru obsahují následující údaje:

- datum (rok, měsíc, den) a čas (hodina, minuta, sekunda) události,
- typ události,
- identitu entity, která je za akci odpovědná,
- úspěšnost /neúspěšnost auditované události.

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

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditní 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.

6.4.13.1.2 Periodicita zpracování záznamů

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

- „Příručka administrátora systémů CA, TSA“,

v případě bezpečnostního incidentu okamžitě.

6.4.13.1.3 Doba uchovávání auditních záznamů

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

6.4.13.1.4 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 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, zejména:

- „NCA - Příručka administrátora systémů CA, TSA“,
- „NCA - Uchovávání dat a informací“,
- „NCA - Záloha dat systémů“.

6.4.13.1.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem, jako zálohovaní ostatních elektronických informací. Zálohování auditních záznamů v papírové formě prováděno není. Procesy jsou popsány v interních dokumentaci, zejména :

- „NCA - Příručka administrátora systémů CA, TSA“,
- „NCA - Záloha dat systémů“.

6.4.13.1.6 Systém shromažďování auditních záznamů (interní nebo externí)

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

6.4.13.2 Uchovávání záznamů

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

- „NCA - Řízení fyzického přístupu do provozních prostor“,
- „NCA - Uchovávání dat a informací“,
- „NCA - Záloha dat systémů“.
- „NCA - Příručka administrátora systémů CA, TSA“,
- „NCA - Spisový a skartační řád“,
- „NCA - Spisový a skartační plán“.

6.4.13.2.1 Typy uchovávaných záznamů

SZR uchovává následující typy záznamů, které souvisejí s poskytovanými službami vytvářejícími důvěru v oblasti časových razítek, zejména:

- smlouvy o poskytování Služby,
- dokumenty související s životním cyklem vydaných certifikátů TSU systému TSA, včetně těchto certifikátů a certifikátů s nimi souvisejících,
- vydaná časová razítka,
- záznamy o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

6.4.13.2.2 Doba uchovávání záznamů

Výše uvedené záznamy jsou uchovávány po celou dobu existence SZR. Ostatní záznamy jsou uchovávány v souladu s ustanoveními kapitoly 6.4.13.1.3.

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

6.4.13.2.3 Ochrana úložiště záznamů

Prostory, ve kterých se uchovávané záznamy nacházejí, 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.

6.4.13.2.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací - viz kapitola 6.4.13.2.

6.4.13.2.5 Požadavky na používání časových razítek při uchovávání záznamů

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

6.4.13.2.6 Systém shromažďování uchovávaných záznamů (interní, externí)

Systém shromažďování uchovávaných záznamů je z pohledu systémů poskytujících služby vytvářející důvěru interní.

6.4.13.2.7 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 činných v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

Postupy jsou popsány v interní dokumentaci - viz kapitola 6.4.13.2.

6.4.13.3 Odpovědnosti za zveřejňování, úložiště informací a dokumentace

6.4.13.3.1 Úložiště informací a dokumentace

SZR zřizuje a provozuje úložiště veřejných i neveřejných informací.

6.4.13.3.2 Zveřejňování informací a dokumentace

Základní adresy (dále též informační adresy), na nichž lze nalézt informace o SZR jsou:

- adresa sídla:

  Správa základních registrů

  Na Vápence 14

  130 00 Praha 3

  Česká republika
- internetová adresa http://www.narodni-ca.cz,
- sídla registračních autorit.

Elektronickou adresou sloužící pro kontakt se SZR je podpora@szrcr.cz.

6.4.13.3.3 Periodicita zveřejňování informací

SZR zveřejňuje informace týkající se oblasti časových razítek s následující periodicitou:

- Politika - před prvním vydáním časového razítka podle této Politiky,
- Směrnice - neprodleně (je-li určena ke zveřejnění),
- seznam vydaných certifikátů – aktualizace při každém vydání nového certifikátu,
- seznam zneplatněných certifikátů (CRL) - po každém zneplatnění certifikátu TSU systému TSA a dále v pravidelných intervalech, nejvýše 24 hodin od vydání předchozího CRL,
- zneplatnění certifikátu CA vydávající certifikáty pro jednotlivé TSU, nebo certifikátu TSU systému TSA s uvedením důvodu zneplatnění – bezodkladně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb vytvářejících důvěru.

6.4.13.3.4 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 platnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

6.5 Ostatní obchodní a právní záležitosti

6.5.1 Poplatky

6.5.1.1 Poplatky za vydávání časových razítek

Poplatky za vydávání časových razítek subjektům uvedeným v kapitole 3.3 nejsou účtovány.

6.5.1.2 Poplatky za přístup k certifikátům poskytovatele

Přístup k certifikátům CA a TSU systému TSA elektronickou cestou SZR nezpoplatňuje.

6.5.1.3 Poplatky za informace o stavu certifikátu a o zneplatnění

Přístup elektronickou cestou k informacím o zneplatněných certifikátech (CRL) a o stavech jí vydaných certifikátů SZR nezpoplatňuje.

6.5.1.4 Poplatky za další služby

Není relevantní pro tento dokument.

6.5.1.5 Postup při refundování

Není relevantní pro tento dokument.

6.5.2 Finanční odpovědnost

6.5.2.1 Krytí pojištěním

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

6.5.2.2 Další aktiva a záruky

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

6.5.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

6.5.3 Důvěrnost obchodních informací

6.5.3.1 Rozsah důvěrných informací

Důvěrnými informacemi SZR jsou veškeré informace, které nejsou označeny jako veřejné a nejsou zveřejňovány způsobem uvedeným v kapitole 6.4.13.2, zejména:

- veškeré soukromé klíče sloužící v procesu poskytování služeb vytvářejících důvěru,
- obchodní informace SZR,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

6.5.3.2 Informace mimo rámec důvěrných informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kapitole 6.4.13.3.2.

6.5.3.3 Odpovědnost za ochranu důvěrných informací

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

6.5.4 Ochrana osobních údajů

6.5.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v SZR řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ. Tyto požadavky jsou rozpracovány v interní dokumentaci:

- „Metodika nakládání s osobními údaji na SZR“,
- „Politika bezpečnosti informací SZR“.

6.5.4.2 Osobní údaje

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

Zaměstnanci SZR, případně jiné fyzické osoby, které přicházejí 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.

6.5.4.3 Údaje, které nejsou považovány za důvěrné

Za citlivé nejsou považovány údaje, které nespadají do působnosti příslušných zákonných norem, tedy ZOOÚ.

6.5.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel SZR.

6.5.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

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

6.5.4.6 Poskytování citlivých informací 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.

6.5.4.7 Jiné náležitosti zpřístupňování osobních údajů

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

6.5.5 Práva duševního vlastnictví

Tato Politika, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systémů poskytujících služby vytvářející důvěru, jsou chráněny autorskými právy SZR a představují její významné know-how.

6.5.6 Doba platnosti, ukončení platnosti

6.5.6.1 Doba platnosti

Tento dokument nabývá platnosti dnem účinnosti uvedeným na titulní straně dokumentu a platí do odvolání.

6.5.6.2 Ukončení platnosti

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

6.5.6.3 Důsledky ukončení a přetrvání závazků

Ukončení Služby neznamená neplatnost časového razítka vydaného v době platnosti této Politiky.

6.5.7 Komunikace mezi zúčastněnými subjekty

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

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

6.5.8 Změny

6.5.8.1 Postup při změnách

Postup je realizován řízeným procesem popsaným v interní dokumentaci.

6.5.8.2 Postup při oznamování změn

Vydání nové verze Politiky je vždy oznámeno formou zveřejňování informací.

6.5.8.3 Okolnosti, při kterých musí být změněno OID

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

6.5.9 Řešení sporů

V případě, že držitel časového razítka nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

- odpovědný pracovník SZR (nutné elektronické nebo listinné podání),
- ředitel SZR (nutné elektronické nebo listinné podání).

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

6.5.10 Rozhodné právo

SZR se řídí právním řádem České republiky.

6.5.11 Shoda s právními předpisy

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

6.5.12 Další ustanovení

6.5.12.1 Rámcová dohoda

Není relevantní pro tento dokument.

6.5.12.2 Postoupení práv

Není relevantní pro tento dokument.

6.5.12.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto Politikou, stanoví, že provádění některého povinného požadavku je nelegální, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a legální.

6.5.12.4 Zřeknutí se práv

Není relevantní pro tento dokument.

6.5.12.5 Vyšší moc

SZR neodpovídá za porušení svých povinností vyplývající 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.

6.5.12.6 Další opatření

Není relevantní pro tento dokument.