CERTIFIKAČNÍ POLITIKA TSA

verze: 1.1

Ministerstvo financí České republiky

Historie dokumentu

Verze	Datum	Provedená změna	Provedl	Platnost CP od
0.91	04.04.2008	Pre-verze předkládaná MF ČR k připomínkám	RNDr. Petr Tesař, Asseco CR	
0.95	26.05.2008	Připomínky osobních porad	RNDr. Petr Tesař, Asseco CR	
0.98	02.06.2008	Připomínky osobních porad	RNDr. Petr Tesař, Asseco CR	
1.0	05.06.2008	Finální výstup projektu PKI (akceptovaný) k doplnění odpovědné osoby ze strany MF ČR	RNDr. Petr Tesař, Asseco CR	
1.1	2.12.2008	Změna v kapitole 9.17, rozšíření této tabulky	RNDr. Miroslav Šedivý, TO2 CR	7.12.2008

OBSAH

1 Úvod

Tento dokument představuje Certifikační politiku (dále jen „CP“) platnou pro autoritu časového razítka (dále jen „TSA“) provozovanou resortní certifikační autoritou Ministerstva financí ČR (dále jen „CA MF ČR“).

Touto CP se TSA řídí při poskytování služeb spojených s vydáváním časových razítek.

CP je závazná v plném rozsahu pro všechny výkonné a administrativní složky TSA, v určeném rozsahu pak i pro spolupracující strany.

1.1 Obecný přehled

CP odpovídá požadavkům stanoveným v ETSI TS 102 023 v.1.2.1.(2003-01) Electronic Signatures and Infrastructures (ESI), Policy requirements for time-stamping authorities a RFC 3647, s přihlédnutím k doporučením orgánů EU a k legislativě ČR v daném oboru. CP představuje souhrn závazných postupů při vydávání, časových razítek TSA, včetně postupů při technické realizaci konkrétních opatření.

1.2 Identifikace dokumentu

Název:	**Certifikační politika resortní Certifikační autority Ministerstva financí ČR**
Organizace:	Certifikační autorita Ministerstva financí ČR
Schválil:	Ředitel odboru 33 MF ČR
Schváleno:	Dnem zveřejnění na webových stránkách CA resortu MF ČR

1.3 Účastné strany

1.3.1 Navazující autority (certifikační cesta)

Autorita časového razítka TSA je koncipována jako resortní časová autorita MF ČR. TSA je v rámci CA MF ČR začleněna do její hierarchické struktury pod mezilehlou certifikační autoritu (dále jen „CA_Intermediate“). CA_Intermedate vydávává pro TSA certifikáty, na základě k nim přidruženého privátního klíče provádí TSA vydávání vlastních časových razítek.

1.3.2 Registrační autority

TSA pro svojí činnost nevyžaduje spolupráci s registrační autoritou (dále jen „RA“).

1.3.3 Uživatelé

Uživatelem může být pouze osoba, která je oprávněná k právním úkonům dle příslušné legislativní normy a je v zaměstnaneckém poměru s organizační složkou MF ČR, která může využívat certifikačních služeb TSA.

1.3.4 Spoléhající strany

Jsou fyzické osoby a procesy, které se při své činnosti spoléhají na časové razítko opatřené platným digitálním podpisem ověřovaným veřejným klíčem obsaženým v certifikátu TSA.

1.3.5 Ostatní účastníci

Další subjekty, které se podílí na PKI orientovaných službách, jako dodavatelé specializovaného hardware, software, čipových karet, zabezpečovací techniky atp.

1.4 Použitelnost časového razítka

1.4.1 Povolená použití časových razítek

Časová razítka, které vydává TSA, mohou být používány v aplikacích pro následující účely:

- zajištění skutečnosti, že data existovala v čase před časem uvedeným v časovém razítku vystaveném pro tato data.

Použití časového razítka pro tyto účely se řídí příslušnými standardy.

1.4.2 Zakázaná použití časových razítek

Časová razítka nelze používat k jiným účelům, nežli je stanoveno v odstavci 1.4.1.

1.5 Administrace dokumentu

1.5.1 Řízení a specifikace CP

Použití časových razítek vydaných TSA se řídí CP TSA, kterou vydává CA MF ČR. Tuto CP TSA zveřejňuje CA MF ČR na webových stránkách MF ČR. Veškeré dotazy týkající se interpretace CP TSA je nutno směřovat na kontaktní adresu, která slouží pro kontakt uživatele s CA MF ČR (článek 1.5.2)

1.5.2 Kontaktní adresy

Kontaktní adresa: certifikacniautorita@mfcr.cz

1.5.3 Osoba určující shodu CP TSA s odpovídající certifikační prováděcí směrnicí

Vedoucího CA MF ČR , který určuje shodu certifikační prováděcí směrnice TSA (dále jen „CPS TSA“) s CP TSA, určuje ředitel odboru 33 MF ČR. Pouze vedoucí CA MF ČR je oprávněn provádět změny v CP TSA při změně či doplnění CPS TSA.

1.5.4 Schvalování CP TSA

CP TSA schvaluje ředitel odboru 33 MF ČR

1.6 Definice a pojmy

Pojem	Význam
Autentizace	Je proces ověření a tím i ustavení identity (uživatele, procesu nebo jiné entity) s požadovanou mírou záruky.
Autorizace	Je udělení určitých práv a určení povolených aktivit.
Certifikační autorita (v oblasti PKI)	Poskytovatel certifikačních služeb zaměřený zejména na vydávání certifikátů a jejich správu. V mnoha případech se certifikační autorita (dále též. CA) chápe jako synonymum pro termín poskytovatel certifikačních služeb.
Certifikát (v oblasti PKI)	Je datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje veřejný klíč (=data pro ověřování elektronických podpisů) s podepisující osobou a umožňuje ověřit její identitu.
CRL	Seznam zneplatněných certifikátů
Časové razítko (time stamp)	Je datová zpráva, kterou vydal poskytovatel certifikačních služeb a která důvěryhodným způsobem spojuje.data v elektronické podobě s časovým okamžikem, a zaručuje, že uvedená data v elektronické podobě existovala před daným časovým okamžikem

Systém PKI

Pojem	Význam
Digitální podpis	Jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují jednoznačné ověření identity podepsaného subjektu ve vztahu k datové zprávě
Důvěrnost	Znamená skutečnost, že informace není prozrazena neoprávněným stranám.
Elektronický podpis	Jsou údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které umožňují jednoznačné ověření identity podepsané osoby ve vztahu k datové zprávě
Expirovaný certifikát	Certifikát po skončení doby platnosti uvedené v tomto certifikátu.
Hashovací funkce	Je funkce, která přiřazuje libovolně dlouhé zprávě M, kratší než-li stanovená maximální délka, otisk (=hash) H pevné délky. Tato funkce musí dále splňovat: 1. Pro danou M je snadné spočítat H. 2. Pro dané H je velmi těžké spočítat příslušnou M. 3. Pro danou M a její H je velmi těžké zjistit jinou M´ takovou, že má stejnou hash H.
Identifikace	Proces prohlášení identity danou entitou (fyzickou osobou, serverem apod.).
Nadřízený certifikát	Certifikát, s nímž spojené párové klíče slouží k podepisování a ověřování certifikátů nebo časových razítek.
Následný certifikát	Certifikát, který byl v souladu s platnou certifikační politikou vydán držiteli v době platnosti již vydaného certifikátu a který má stejné údaje uvedené v tomto certifikátu, a liší se ve veřejném klíči a sériovém čísle certifikátu.
Nepopíratelnost (non-repudiation)	Představuje vlastnost získanou na základě kryptografických metod, kdy je jednotlivým stranám zabráněno popřít, že uskutečnily určitou akci týkající se dat (jako například mechanismy k - zabránění popření autorství, - k dokázání povinnosti, záměru nebo závazku nebo - dokázání vlastnictví)
Nonce	Párovací číslo – dlouhé (minimálně 64 bitů) náhodně generované číslo sloužící ke kontrole, že odpověď autority časového razítka je na danou žádost.
NTMS	Network Time Management System - systém správy času prostřednictvím telekomunikační sítě

Systém PKI

Pojem	Význam
NTP	Network Time Protocol časový síťový protokol
Otisk	Výstup hashovaní funkce.
Párové klíče	Vzájemně svázaná dvojice klíčů pro vytváření digitálních podpisů (privátní klíč) a pro ověřování digitálních podpisů (veřejný klíč). Veřejné klíče jsou vesměs publikovány v certifikátech spolu s dalšími údaji zejména o identitě podepisujícího subjektu.
Pozastavený certifikát	Certifikát ve stavu, kdy jej nelze používat pro ověřování digitálních podpisů a příslušný privátní klíč nelze používat pro vytváření digitálních podpisů, nicméně vydávající certifikační autorita jej může učinit znovu platným.
Služba (service)	Souhrn úloh, které tvoří z pohledu poskytovatele služby i žadatele služby jeden celek.
Podepisující osoba	Fyzická osoba, která je držitelem prostředku pro vytváření digitálních podpisů a jedná svým jménem nebo jménem jiné fyzické či právnické osoby.
Privátní klíč	Jiný výraz pro data pro vytváření digitálních podpisů.
Spoléhající se strana	Subjekt spoléhající se při své činnosti na vydaný certifikát.
Statut certifikátu	Stav ve kterém se certifikát nachází, tj. platný, zneplatněný, zablokovaný, pozastavený, expirovaný.
Subjekt	Fyzická osoba, právnická osoba nebo softwarový modul s neodmítnutelnou odpovědností konkrétní fyzické osoby.
Systém správy klíčů	Představuje systém pro generování, ukládání, distribuci, odvolání, zrušení, archivování, ničení, certifikaci nebo aplikaci kryptografických klíčů.
TSA	Certifikační autorita vydávající časová razítka. Pro účely této CP se tím rozumí resortní autorita časového razítka MF ČR, která je součástí certifikační autority MF ČR.
TMC	Trusted Master Clock - hodiny v kořenové úrovni služby distribuce důvěryhodného času
TSQ	Time Stamp Query - žádost o časové razítko
TSR	Time Stamp Response - odpověď na žádost o časové razítko
TSU	Time Stamp Unit - server vydávající časová razítka
TST	Time Stamp Token – část časového razítka obsahující jméno TSU, UTC čas, přesnost, sériové číslo, hash algoritmus, nonce
UTC	Universal Co-ordinated Time - standard přijatý 1.1.1972

Pojem	Význam
	pro světový koordinovaný čas (Coordinated Universal Time – UTC). Funkci "oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIPM).
Uživatel	Držitel, spoléhající se strana, žadatel, popř. subjekt, rozhodující se o využívání poskytované certifikační služby.
Veřejný klíč	Jiný výraz pro data pro ověřování digitálního podpisu.
Zablokovaný certifikát	Stav ve kterém se certifikát nachází od okamžiku, kdy jej poskytovatel certifikačních služeb, který jej vydal, zneplatnil do doby, kdy tento poskytovatel certifikačních služeb zveřejnil CRL, ve kterém je tento certifikát poprvé zařazen.
Zneplatněný certifikát	Certifikát, který byl poskytovatelem verifikačních služeb, který jej vydal, zneplatněn bez možnosti obnovení platnosti.

2 Uveřejňování a uchování informací

2.1 Sklady

TSA nezřizuje za účelem poskytování služeb sklady vydaných časových razítek. Informace o nadřízených certifikátech vydaných pro TSA jsou dosažitelné v příslušném skladu u CA_Intermediate.

2.2 Zveřejňování certifikačních informací

CA MF ČR poskytne informace o této CP TSA jakož i o příslušné CPS TSA všem oprávněným subjektům v potřebném rozsahu.

CA MF ČR zveřejňuje nadřízené certifikáty pro TSA tak, aby byly k dispozici všem uživatelům. CA MF ČR rovněž zveřejňuje statut nadřízených certifikátů vydaných pro TSA.

2.3 Frekvence zveřejňování

CA_Intermediate aktualizuje seznam nadřízených certifikátů vydaných pro TSA pouze v případě, že pro TSA byl vydán nový nadřízený certifikát. Doba od vydání nadřízeného certifikátu do jeho zveřejnění nesmí přesáhnout 8 hodin.

TSA nevydává CRL.

Nadřízené certifikáty TSA jsou zveřejňovány na stránkách MF ČR nejméně 24 hodin před nabytím jejich platnosti. Při změně statutu nadřízených certifikátů TSA se oznamuje tato skutečnost neprodleně prostřednictvím stránek MF ČR, nejpozději však do 2 hodin.

2.4 Způsoby přístupu k uloženým informacím

K uloženým informacím tj. vlastním nadřízeným certifikátům TSA, CRL, této CPS TSA a CP TSA lze přistupovat vzdáleným přístupem přes lokální síť a Internet.

3 Identifikace a autentizace

Služba vydání časového razítka je povolena pro žadatele, kteří byli určeni odpovědným nadřízeným funkcionářem.

3.1 Prvotní identifikace žadatele

TSA neprovádí identifikaci žadatele o časové razítko.

4 Operační požadavky životního cyklu časového razítka

4.1 Žádost o časové razítko

4.1.1 Žadatelé o časové razítko

Žadatelem o vydání časového razítka může být pouze fyzická osoba, která je v době žádosti v zaměstnaneckém poměru k organizační složce MF ČR, která je oprávněna využívat služeb TSA.

4.1.2 Vytvoření žádosti

Uživatelský specializovaný software převezme dokument nebo obecně jakákoliv data a vytvoří jejich otisk. Uživatelský specializovaný software následně vygeneruje žádost o časovou značku dle RFC 3161 a tuto žádost odešle při použití protokolu HTTP serveru TSU.

4.2 Zpracování žádosti o časové razítko

4.2.1 Identifikační a autentizační proces

TSA neprovádí identifikaci a autentizaci žadatele o vystavení časového razítka. Zda byl žadatel oprávněn k žádosti o vydání časového razítka je kontrolovatelné pouze organizačními opatřeními.

4.2.2 Schválení a odmítnutí žádosti o vydání časového razítka

TSU přijme žádost o časové razítko a zkontroluje její formální správnost. Pokud je přijatá žádost v pořádku, získá TSU aktuální přesný čas a vygeneruje odpověď s časovým razítkem. Jestliže je v žádosti objevena chyba, TSU vrátí pouze chybové hlášení bez časového razítka. Uživatelský specializovaný software zpracuje odpověď serveru, ověří její správnost včetně digitálního podpisu TSA a uloží časové razítko. Ověření časového razítka je uživatel schopen provádět opětovně a podávat tak důkaz o existenci určitých dat před časem uvedeným na časovém razítku.

4.2.3 Lhůty vyřízení žádosti o časové razítko

TSA nestanovuje pevný časový limit, ve kterém dojde ke zpracování žádosti o časové razítko, neboť se jedná časový sled následujících činností, z nichž některé záleží pouze na elektronickém přenosu žádosti k systému TSA. Ilustrativní časové údaje:

generování žádosti o vydání časového razítka – řádově sekundy,

vygenerování časového razítka – řádově ms.

4.3 Vydání časového razítka

4.3.1 Postup TSA při vydání časového razítka

TSA provede postupně následující operace:

- TSU provede veškeré kontroly formální správnosti žádosti. . V případě chyby v žádosti TSU vytvoří novou datovou strukturu v normovaném formátu dle RFC 3161, obsahující odpovídající chybový status
- v případě kladného výsledku kontrol žádosti je k otisku, obsaženém v žádosti, přidán časový údaj, který je získán z měřidla důvěryhodného času, a takto vytvořená data jsou do výše uvedené datové struktury uložena.
- datová struktura, vytvořená v předchozích bodech, je následně digitálně podepsána TSU - tím se tento TSU nezpochybnitelným způsobem zaručuje za správnost informací uvedených ve vygenerovaném časovém razítku.
- tato datová struktura – odpověď na žádost o časové razítko, je odeslána řídící aplikaci komunikačního serveru.

4.3.2 Zpráva o vydání časového razítka žádající osobě

TSA nezasílá žadateli zprávu o vydání časového razítka. Časové razítko (pokud bylo vydáno) je získáno uživatelským softwarem pomocí protokolu http.

4.4 Akceptování časového razítka

4.4.1 Postup žadatele při akceptaci časového razítka

Po obdržení odpovědi (TSR) na žádost (TSQ) o časové razítko je uživatel povinen zjistit status. V případě chyby není časové razítko v odpovědi obsaženo a uživatel by měl překontrolovat status a odpovídající chybovou hlášku. V opačném případě je uživatel povinen postupovat v souladu s kapitolou 9.6.2.

4.4.2 Zveřejňování vydaných časových razítek

Časová razítka vydaná TSA nejsou podle této CP zveřejňována.

4.4.3 Zpráva TSA o vydání časového razítka dalším stranám

TSA nezasílá jiným stranám informaci o vydání časového razítka.

4.5 Použití časového razítka

CP ve vztahu k vydávání časových razítek nedefinuje žádná omezení použitelnosti časového razítka vydaného v souladu s touto CP. Obecně platí, že časové razítko slouží jako důkaz, že datový objekt, ke kterému je časové razítko připojeno, existoval bezprostředně před časovým údajem uloženým v tomto časovém razítku. Časová razítka je možné použít např. v oblastech :

- elektronických podpisů nebo elektronických značek, kdy je třeba ověřit, že byly vytvořeny v době, kdy certifikát veřejného klíče podepisující nebo označující entity byl platný. Tato kontrola je nezbytná z následujících dvou důvodů :
  - během platnosti certifikátu elektronicky podepisující nebo elektronicky označující entity byl odpovídající privátní klíč kompromitován,
  - elektronický podpis nebo elektronická značka byl vytvořen po ukončení doby platnosti příslušného certifikátu.
- ochraně spustitelného kódu
- transakcí prováděných na síti
- libovolných dokumentů u kterých je třeba ověřit jejich existenci před určitým časovým okamžikem

4.5.1 Privátní klíč podepisujícího subjektu a užití certifikátu

Privátní klíč podepisující TSA lze používat výhradně k vytváření digitálních podpisů pro tvorbu časových razítek.

4.5.2 Veřejný klíč a spoléhající se strana

Spoléhající se strana použije veřejný klíč z nadřízeného certifikátu TSA k verifikování příslušného digitálního podpisu na vydaném časovém razítku. V případě platnosti digitálního podpisu a platnosti nadřízeného certifikátu může spoléhající strana předpokládat, že předmětný digitální podpis vytvořila TSA, která je uvedena v tomto nadřízeném certifikátu.

4.6 Prodloužení platnosti časového razítka

Časovým razítkům vydaným TSA nelze prodlužovat dobu platnosti.

4.7 Služby spojené se statutem certifikátu TSA

4.7.1 Operační charakteristiky

Nadřízený certifikát TSA určený pro ověřování vydaných časových razítek vydaných podle této CP může mít pouze následující statuty:

- Platný
- Zneplatněný
- Zablokovaný
- Expirovaný

Služba ověření, zda nadřízený certifikát TSA nebyl zneplatněn, je podporována pomocí kontroly na vydaném CRL nadřízenou autoritou CA_Intermediate.

4.7.2 Dostupnost služeb

Aktuální CRL vydané CA_Intermediate je dostupné na elektronické adrese uvedené v certifikátu v X509v3 extenzi CRL Dstribution Points.

4.7.3 Volitelné vlastnosti

Tato CP nepodporuje další volitelné možnosti služby ověřování statutu nadřízeného certifikátu TSA.

4.8 Ukončení využívání služeb TSA

Uživatel který ukončuje využívání služeb TSA, například z důvodu rozvázání pracovního poměru je povinen přestat využívat službu vydání časového razítka od TSA.

4.9 Úschova a obnovení privátního klíče

4.9.1 Politika úschovy

Tyto skutečnosti nejsou relevantní pro tuto CP.

4.9.2 Politika obnovení privátního klíče

Tyto skutečnosti nejsou relevantní pro tuto CP.

5 Fyzické, procedurální a personální bezpečnostní mechanismy

5.1 Fyzická bezpečnost

Fyzická bezpečnost je velmi důležitým faktorem zajišťujícím důvěryhodnost certifikačních služeb TSA. Ochrana je zaměřena na hlavní systémy, kterými jsou ty, které přímo provádějí podepisování časových značek.

5.1.1 Umístění a konstrukce

Zařízení určené k výkonu hlavních certifikačních služeb TSA je umístěno v budově, která patří MF ČR. Budova má kontrolovaný vstupní režim. Podrobné nároky na objektovou bezpečnost jsou uvedeny v CPS TSA.

5.1.2 Fyzický přístup

Přístup do vlastní budovy je kontrolovaný ostrahou. Přístup do místnosti s vlastní podepisující technikou je povolen pouze určeným pracovníkům TSA a v případě, kdy je TSU umístěn ve společné serverové místnosti organizační součásti MF ČR je přístup do místnosti povolen i zde pracujícím administrátorům. Ostatní osoby mohou být v místnosti pouze za přítomnosti některého z určených pracovníků CA MF ČR nebo zde pracujícího administrátora. Vstupní dveře do místnosti jsou z vnější strany opatřeny nepohyblivou klikou a jsou neustále zamčené.

5.1.3 Klimatizace a přívod elektrické energie

V místnosti je dostatečně dimenzovaná aktivní klimatizace. Přívod elektrické energie je jištěn pomocí UPS. Vlastní TSU je napájen přes filtr zamezující případnému úniku informace do elektrické rozvodné sítě.

5.1.4 Ohrožení vodními zdroji

Budova, ve které je umístěna TSA stoji na pozemku, který není na příslušných katastrálních mapách uveden v záplavové zóně.

5.1.5 Požární ochrana

Vstupní dveře do místnosti se serverem TSA jsou vybavena protipožární vložkou. V místnosti se nachází hasební přístroj a požární čidlo.

5.1.6 Uchování datových médií

Datová média obsahující archivní informace, které jsou nutné pro řádnou činnost autority TSA jsou skladována v jiné geografické lokalitě.

5.1.7 Kancelářský odpad

Veškerý papírový kancelářský odpad je před opuštěním pracoviště TSA znehodnocen sešrotováním.

5.1.8 Vnější uložení záloh

Pracovní zálohy jsou uloženy v prostorách TSA. Ostatní zálohy jsou uloženy na místě určeném vedením CA MF ČR. Ostatní zálohy nesmějí být uloženy ve stejném objektu jako pracovní zálohy.

5.2 Procedurální bezpečnost

5.2.1 Důvěryhodné role

Důvěryhodné role u CA MF ČR a z nich vyplývající hlavní kompetence vzhledem k TSA jsou:

- Ředitel odboru 33 MF ČR – schvaluje CPS TSA, CP TSA, jmenuje vedoucího CA MF ČR. Schvaluje žádosti o vydání nadřízeného certifikátu TSA.
- Vedoucí CA MF ČR – řídí činnost TSA. Zodpovídá za aktualizaci stavu dokumentace CPS TSA a CP TSA, podílí se na zálohování klíčů TSA, podává žádost o vydání nadřízeného certifikátu TSA. Zneplatňuje nadřízený certifikát TSA.
- Bezpečnostní správce CA MF ČR - provádí činnosti v oblasti bezpečnosti informačního systému CA MF ČR ve kterém je zahrnuta i TSA, podílí se na likvidaci mimořádných událostí.
- Administrátor TSA - spouští službu TSA, zastavuje službu TSA, zálohuje klíče TSA, obnovuje klíče TSA, instaluje nový nadřízený certifikát TSA.
- Koordinátor řízení kontinuity činnost CA MF ČR – řídí činnosti nutné v případě krizových situací, včetně zajištění obnovy činnost. Udržuje v aktuálním stavu dokumentaci pro zvládání krizových situací a plán obnovy a vypracovává konkrétní směrnice pro obnovu informačního systému TSA.
- Bezpečnostní auditor – provádí bezpečnostní audit informačního systému TSA.

Mezi důvěryhodné role jsou zařazeny i celorezortní role bezpečnostní architekt MF ČR a bezpečnostní inspektor MF ČR, jejichž činnost se promítá do bezpečnostní oblasti CA MF ČR.

Důvěryhodné role pro TSA jsou spojeny s důvěryhodnými rolemi pro CA_Intermediate.

5.2.2 Počty osob pro provádění úloh

Při provádění úloh, které souvisejí se zásadními činnostmi TSA, tedy pro

- zálohování privátního klíče TSA
- obnova ze zálohy privátního klíče TSA
- aktivace TSA

je nezbytná přítomnost nejméně dvou pověřených pracovníků TSA.

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

5.2.3 Identifikace a autentizace pro každou roli

Identifikace a autentizace jednotlivých pracovníků je realizována pomocí čipových karet obsahujících mimo jiné i osobní certifikáty a privátní klíče pro vytváření digitálních podpisů.

5.2.4 Neslučitelné role

Následující tabulka definuje, které role nemohou být současně vykonávány stejným pracovníkem. Tabulka zahrnuje všechny důvěryhodné role, které se v rámci CA MF ČR mohou vyskytnout. Použité zkratky

DI – ředitel odboru 33 MF ČR

VE - vedoucí CA MF ČR

SP – správce CA_Local

BA - bezpečnostní architekt MF ČR

BI - bezpečnostní inspektor MF ČR

BS - bezpečnostní správce CA MF ČR

SA - administrátor TSA

DA - databázový administrátor

KR – koordinátor řízení kontinuity činnosti CA MF ČR

AU – bezpečnostní auditor

OC – operátor CA

OR – operátor RA

Tabulka rolí vyžadujících rozdělení povinností:

	DI	**VE**	**SP**	**BA**	**BI**	**BS**	**SA**	**DA**	**KR**	**AU**	**OC**	**OR**
DI	X	S	S	N	N	N	N	N	N	N	N	N
VE	N	X	S	N	N	S	N	N	S	N	N	N

SP	N	N	X	N	N	S	N	N	S	N	N	N
BA	N	N	N	X	S	S	N	N	S	N	N	N
BI	N	N	N	S	X	S	N	N	S	S	N	N
BS	N	N	N	N	N	X	N	N	S	N	N	N
SA	N	N	N	N	N	N	X	S	N	N	S	S
DA	N	N	N	N	N	N	S	X	N	N	S	S
KR	N	S	S	N	N	S	N	N	X	N	N	N
AU	N	N	N	N	N	N	N	N	N	X	N	N
OC	N	N	N	N	N	N	N	N	N	N	X	S
OR	N	N	N	N	N	N	N	N	N	N	S	X

S - Ano, role v řádku může být sloučena s rolí ve sloupci

N - Ne, role v řádku nemůže být sloučena s rolí ve sloupci

X - Daná kombinace není slučováním různých důvěryhodných rolí

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a prověření

Všichni pracovníci TSA v důvěryhodných rolích jsou přijímáni na základě personálních kriterií popsaných v CPS TSA.

5.3.2 Ověřování znalostí

Ověřované znalostí v tomto odstavci jsou speciální znalosti pro práci v CA MF ČR. Tímto odstavcem není dotčena povinnost podrobení se případnému ověřování dalších znalostí a předpisů požadovaných příslušnými orgány MF ČR. Podrobnější popis je v CPS TSA.

.

5.3.3 Požadavky na zaškolení

Pracovníci CA MF ČR musí být odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samopřípravy a metodickým vedením již zaškoleným pracovníkem.

5.3.4 Pravidelnost školení a příslušné požadavky

Všichni pracovníci jsou pravidelně minimálně jednou ročně zařazováni do zdokonalovacích školení.

5.3.5 Požadavky na změny rolí

Z důvodů možné zastupitelnosti v mimořádných případech jsou pracovníci CA MF ČR motivováni na získávání znalostí potřebných na zastávání jiné důvěryhodné funkce v rámci CA MF ČR. Změna role je možná pouze v mimořádných případech (epidemické onemocnění atp.) jako dočasné opatření. Pro vykonávání jiné důvěryhodné funkce je potřeba souhlas vedoucím zaměstnancem příslušné organizační složky. V případě, že je nutné sloučit některé důvěryhodné role do jednoho pracovníka, je nutné se řídit tabulkou neslučitelnosti důvěryhodných rolí uvedenou v odstavci 5.2.4 .

5.3.6 Sankce při neautorizovaných činnostech

Neoprávněné provedení neautorizované činnosti je považováno za hrubé porušení pracovní kázně. Postih pracovníka podle zákoníku práce nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti.

5.3.7 Požadavky na pracovníky třetích stran

MF ČR smluvně nezajišťuje, kromě servisní a technické podpory, žádné činnosti související s certifikačními službami.

5.3.8 Dokumentace poskytovaná personálu

Personál má k dispozici CP TSA a příslušné příručky pro výkon dané služby.

5.4 Procedury auditu logování událostí

Logování událostí provádí server, na němž služba TSA běží.

V rámci této CP TSA je TSA jako služba pracující na serveru, který zajišťuje CA_Intermediate.

V rámci této CP TSA není prováděno logování žádných dalších událostí.

5.5 Archivace záznamů

Podle této CP není prováděna žádná archivace záznamů.

5.6 Výměna klíče

V případě změny vlastního nadřízeného certifikátu TSA se zveřejní nový nadřízený certifikát na stránkách MF ČR a na stránkách CA_Intermediate.

5.7 Odhalení kompromitací a nehod

5.7.1 Zneplatnění certifikátu TSA

V případě zneplatnění veřejného klíče TSA používaného k ověřování podepsaných časových razítek informuje o této skutečnosti CA MF ČR na webových stránkách MF ČR a na stránkách CA_Intermediate. Touto situací se rozumí jiné důvody, než-li kompromitace příslušného privátního klíče. Jde zejména o následující důvody:

- změna jména subjektu (**affiliationChanged)** indikuje, že se změnilo jméno autority TSA nebo jiné informace byly v certifikátu modifikovány, ale není žádné podezření z kompromitace příslušného privátního klíče,
- náhrada (**superseded)** indikuje případ nahrazení certifikátu jiným bez podezření z kompromitace příslušného privátního klíče,
- ukončení činnosti **(cessation**) indikuje případ, že certifikát není dále potřebný pro činnost pro kterou byl vydán (např. činnost nebude dále provozována), bez podezření z kompromitace příslušného privátního klíče.

5.7.2 Poškození výpočetních zdrojů, softwaru, dat

V případě poškození výpočetních zdrojů, softwaru a dat postupuje TSA v souladu s havarijním plánem obnovy.

V případě, kdy došlo k poškození serveru pro vytváření podpisů vydávaných časových razítek, je toto zařízení nahrazeno záložním počítačem. Pevný disk záložního počítače se před použitím naformátuje. Do záložního počítače je poté nainstalován serverový operační systém, specializovaný software realizující TSA a zaveden privátní klíč TSA z bezpečné zálohy. Po zavedení privátního klíče se prověří funkčnost zařízení a v případě správné funkčnosti se zařízení zapojí.

Obdobně se postupuje při poškození souvisejících výpočetních zdrojů.

V případě poškození softwaru se poškozený software nahradí funkčním softwarem z bezpečné zálohy.

Použitá protiopatření musí být zaznamenána do protokolu.

5.7.3 Postup při kompromitaci privátního klíče

V případě kompromitace vlastního privátního klíče TSA sloužícího pro podepisování vydávaných časových razítek je TSA povinna neprodleně zneplatnit příslušný vlastní nadřízený certifikát. O této skutečnosti informuje bezodkladně

na stránkách MF ČR a informuje vedoucího CA MF ČR. Vlastníky časových razítek, jejichž důvěryhodnost byla uvedenou kompromitací dotčena TSA vyzve k vystavení nového časového razítka.

5.7.4 Obnovení činnosti po mimořádných událostech

Postupy pro případy obnovení činnosti po mimořádných situacích jsou popsány v Plánu pro zvládání krizových situací a obnovy a příslušných návazných směrnicích.

5.8 Ukončení činnosti TSA

V případě ukončení činnosti z jiných důvodů než-li jsou mimořádné události jakými jsou stávky, občanské nepokoje, válečný stav, přírodní katastrofy nebo jiné výsledky působení vyšší moci, zajistí TSA:

- zpřístupnění informace o ukončení své činnosti všem osobám spoléhajícím na její certifikát, držitelům a jiným osobám, se kterými má smluvní nebo jiné obdobné vztahy týkající se poskytování certifikačních služeb,
- ukončí vydávání časových známek,
- prokazatelně zničí svůj privátní klíč určený pro podepisování vydaných časových razítek.

6 Technická bezpečnost

6.1 Generování párových klíčů a instalace

Párové klíče tj. vzájemně svázaná dvojice privátního klíče (tj. dat pro vytváření digitálních podpisů) a s nimi souvisejícího veřejného klíče (tj. dat pro ověřování digitálních podpisů) jsou fakticky nejdůležitější data, která zásadním způsobem ovlivňují kryptologickou kvalitu digitálního podpisu a s ním spojených PKI aplikací. Kompromitace privátního klíče je jednoznačně nejhorším incidentem, který se může držiteli příslušného certifikátu přihodit.

6.1.1 Generování párových klíčů

Párové klíče se zásadně generují přímo na TSU.

6.1.2 Doručení veřejného klíče TSA uživatelům

Certifikát veřejného klíč TSA je přístupný na webové stránce MF ČR a stránce CA_Intermediate.

6.1.3 Velikost klíčů

TSA používá nejprověřenější klasický asymetrický šifrový algoritmus – RSA. Mohutnost (=velikost) směnných prvků (klíčů) použitých pro podepisování časových razítek je stanovena na 2048 bitů.

6.1.4 Tvorba parametrů pro PKI klíče

Algoritmy použité pro generování celočíselných hodnot nutných pro fungování digitálního podpisu (např. testy prvočíselnosti atp.) musí mít parametry uvedené v příslušných normách. Příkladem mezinárodně používané normy je FIPS PUB 186-2 Digital Signature Standard.

6.2 Ochrana privátních klíčů TSA

Otázky ochrany privátních klíčů příslušných k nadřízeným certifikátům TSA, normy pro kryptografické moduly, metody sdílení tajemství, zálohování těchto privátních klíčů, aktivace, deaktivace, import, export privátního klíče, uložení a ničení privátního klíče jsou podrobně popsány v CPS TSA a Bezpečnostní politice CA.

6.3 Další požadavky na správu párových klíčů

6.3.1 Archivace veřejných klíčů

Veřejné klíče TSA jsou nezbytná pro důvěryhodnost a ověřování platnosti časových razítek vydaných TSA. Tato data jsou obsažena v nadřízených certifikátech TSA. Na rozdíl od jím příslušných privátních klíčů je důležité tato data archivovat pro případ následné kontroly pravosti vydaných časových razítek. Nadřízené certifikáty TSA jsou archivovány vypálením do CD-ROM a uložením ve dvou geograficky oddělených místech. TSA tato data archivuje, respektive zajistí jejich archivaci, ještě 10 let po případném ukončení své činnosti.

6.3.2 Období životností párových klíčů

Platnost dat určených k podepisování vydaných časových razítek je 5 let. Platnost dat určených k ověřování podepsaných vydaných časových razítek je dána platností vydaných nadřízených certifikátů TSA, která se řídí výše uvedeným schématem životnosti dat určených k podepisování časových razítek.

Platnost časových razítek vydaných TSA je 4 roky.

6.4 Aktivační data

Problematika aktivačních dat je popsána v CPS TSA.

6.5 Bezpečnost počítačového vybavení

6.5.1 Specifické požadavky na počítačovou bezpečnost

Otázky bezpečnosti počítačového vybavení TSA jsou popsány v CPS TSA a Bezpečnostní politice CA.

6.6 Technické podmínky v době životnosti

Technické podmínky v době životnosti jsou popsány v CPS TSA.

6.7 Podmínky bezpečnosti počítačové sítě

Podmínky bezpečnosti počítačové sítě jsou popsány v CPS TSA a Bezpečnostní politice CA.

6.8 Časová razítka

Časová razítka nejsou pro potřeby samotné TSA používána.

7 Profil časového razítka a profily CRL

7.1 Profil časového razítka

Profily časových razítek jsou podle RFC 3161.

7.1.1 Čísla verzí

Všechny časová razítka vydávaná TSA jsou verze 1 podle RFC 3161.

7.1.2 Položky žádosti o časové razítko

Položky žádosti o vydání časového razítka TSA :

- version – číslo verze = 1
- messageImprint – OID hash algoritmu a vlastní hash hodnota
- reqPolicy – OID vydávací politiky
- nonce – párové číslo (nepovinná položka)
- certReq – vyžádání certifikátu TSA do odpovědi (když je nastavena na TRUE). Nepovinná položka, implicitně FALSE.

7.1.3 Položky odpovědí na žádost o časové razítko

Odpověď na žádost o časové razítko obsahuje následující položky:

- status – dává informaci, zda odpověď obsahuje časové razítko a pokud neobsahuje, tak z jakého důvodu. RFC 3161 uvádí osm možných důvodů.
- timeStampToken - v této části (pokud odpověď obsahuje časové razítko) jsou podepsané údaje které obsahují
  - version - verze = 1,
  - policy - OID vydávací politiky TSA,
  - messageImprint – musí obsahovat stejné hodnoty jako tato položka v žádosti,
  - serialNumber – číslo přidělené TSA unikátně pro každý timeStampToken. Velikost je povolena až 160 bitů,
  - genTime - UTC časový údaj ve formátu YYYYMMDDhhmmssZ, kde YYYY je rok, MM měsíc, DD den, hh hodina, mm minuta, ss vteřina, Z je povinné zakončení,
  - accuracy – přesnost uvedeno času (nepovinná položka),
  - ordering – implicitně nastaven na FALSE. Pokud tato položka chybí nebo je FALSE, lze vydané timeStampToken řadit podle položky genTime jenom pokud jsou v čase od

sebe vzdáleny nad rozlišovací přesnost určování času (položka accuracy). Pokud je tato položka TRUE, lze vždy řadit timeStampToken podle položky genTime,

- nonce – párové číslo, musí být stejné jako v žádosti o časové razítko (pokud bylo použito v TSQ),
- tsa – jméno autority časového razítka (nepovinná položka),
- extensions – nepovinné další položky.

Jako kryptografických algoritmů se používá SHA-1 a RSA.

7.2 CRL

TSA nevydává CRL.

7.3 Synchronizace měřidla času s UTC

7.3.1 Měřidlo času

Jako měřidlo času používá TSA systémový čas serveru TSU.

7.3.2 Synchronizace času

Synchronizace měřidla času s důvěryhodným synchronizačním zdrojem UTC je prováděna jednou denně. Pro synchronizaci a audit časového údaje, vkládaného do generovaných časových razítek je využívána pravidelná časová synchronizace oproti NTP stratum 2 serverům MF (172.18.7.1 a 172.18.7.2)

7.3.3 Bezpečnost měřidla času

Bezpečnost měřidla času je popsána v CPS TSA a Bezpečnostní politice CA.

8 Audit

Audit má za úkol vyhodnotit shodu činnosti TSA s CP TSA, CPS TSA a dalšími dokumenty, které upravují činnost TSA. Výstupem auditu je hodnotící zpráva a seznam doporučení, která vedou k nápravě případných nedostatků.

Další postupy

- způsob provádění auditu
- kvalifikace auditora
- auditorův vztah k auditované straně
- témata zahrnující audit
- opatření v případě zjištění nedostatků
- předání výsledků a odvolání proti výsledkům auditu

jsou popsány v CPS TSA.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.2 Finanční odpovědnost

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.3 Důvěrnost obchodních informací

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.4 Důvěrnost osobních informací

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.5 Duševní vlastnictví

Tato CP TSA plně respektuje zákon č. 121/2000 Sb. autorský zákon, a zákon č. 137/1995 Sb. o ochranných známkách.

9.6 Zajištění a záruky

9.6.1 Zajištění a záruky TSA

TSA zajišťuje a zaručuje, že :

- jí vydávaná časová razítka obsahují všechny náležitosti stanovené touto CP TSA
- použije privátní klíče příslušné svým nadřízeným certifikátům pouze k vydávání časových razítek
- data v elektronické podobě, která jsou předmětem žádosti o vydání časového razítka, jednoznačně odpovídají datům v elektronické podobě obsaženým ve vydaném časovém razítku,
- implementovala odpovídající opatření proti padělání časových razítek,
- vydá časové razítko neprodleně po obdržení platného požadavku,
- žádným způsobem neověřuje otisk, kterému má být časové razítko přiřazeno (s výjimkou jeho délky),
- využívá důvěryhodnou časovou synchronizaci,

- jí vydané časové razítko obsahuje minimálně:
  - verzi struktury TSTInfo,
  - OID CP TSA, podle které bylo časové razítko vydáno,
  - data v elektronické podobě - otisk, pro která bylo časové razítko vydáno,
  - sériové číslo časového razítka,
  - čas (GeneralizedTime),
  - digitální podpis TSU, který časové razítko vydal.

Nonce je zahrnuto pouze tehdy, jestliže je obsaženo v žádosti o vydání časového razítka.

9.6.2 Závazky žadatelů a držitelů časového razítka

Žadatelé jsou vždy po obdržení odpovědi (TSR) na žádost (TSQ) o časové razítko povinni zjistit chybový status. V případě chyby není časové razítko v odpovědi obsaženo a žadatel je povinen překontrolovat odpovídající chybovou hlášku. V opačném případě je předplatitel povinen :

- ověřit digitální podpis TST a zkontrolovat, zda nadřízený certifikát serveru TSU nebyl odvolán – CRL je přístupné na adrese uvedené v nadřízeném certifikátu TSA.
- ověřit, zda vrácený otisk je totožný s odeslaným,
- ověřit, že hodnota nonce (pokud byla použita) v odpovědi je totožná s hodnotou v žádosti.

9.6.3 Závazky spoléhající strany

Obecným závazkem spoléhajících se stran je ověření elektronické značky TST. Spoléhající se strana je povinna:

- ověřit platnost nadřízeného certifikátu serveru TSU vydávajícího časová razítka,
- překontrolovat, zda CP TSA, pod kterou bylo časové razítko vydáno, je akceptovatelná jejím potřebám, popř. potřebám jí provozované aplikace.

V případě ověřování časového razítka po ukončení platnosti nadřízeného certifikátu serveru TSA vydávajícího časová razítka jsou spoléhající se strany povinny :

- ověřit, zda nadřízený certifikát serveru TSU vydávajícího časová razítka nebyl v době vydání časového razítka zneplatněn - CRL je přístupné na elektronické informační adrese (kapitola 1.5.2)
- ověřit, zda kryptografická funkce pro tvorbu otisku v časovém razítku je stále bezpečná – uvedeno na elektronické informační adrese (kapitola 1.5.2)
- ujistit se, zda délka kryptografického klíče a algoritmus jsou stále považovány za bezpečné - uvedeno na elektronické informační adrese (kapitola 1.5.2).

9.7 Zmocněnecké vztahy

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.8 Limity záruk

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.9 Kompenzace ze strany vlastníků certifikátů a uživatelů

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.10 Lhůty a zánik platnosti CP

9.10.1 Lhůty platnosti

Platnost této CP TSA je 5 let ode dne kdy tato CP TSA nabývá platnost.

9.10.2 Zánik platnosti

Po vypršení lhůty platnosti zaniká platnost této CP TSA. Vedoucí CA MF ČR nebo ředitel odboru 33 MF ČR je oprávněn lhůtu platnosti CP TSA prodloužit.

9.10.3 Důsledky zániku platnosti

V případě jakýchkoliv změn, které mají za následek neplatnost některého z článků této CP TSA, ostatní články zůstávají v platnosti do vydání nové CP TSA. Do té doby se bude rovněž vymáhat odpovědnost za dodržování této CP TSA v platných článcích. Výklad platnosti v přechodném období je právem CA MF ČR.

9.11 Zásady komunikace s účastníky

Komunikace mezi stranami uvedenými v této CP TSA za účelem poskytování certifikačních služeb je popsána v příslušných odstavcích. Obecná zásada je, že jde buď o komunikaci přímou nebo komunikaci dálkovou. Při žádostech o vystavení časového razítka se používá výhradně dálková komunikaci.

9.12 Změny v CP

9.12.1 Postup provádění změn

V době platnosti CP TSA navrhuje změny v CP TSA pracovník uvedený v odstavci 1.5.3 na základě dokumentovatelné potřeby TSA. Změnu posoudí příslušní

pracovníci CA MF ČR a vedoucí CA MF ČR a ředitel odboru 33 MF ČR rozhodne. Rozhodnutí ředitele odboru 33 MF ČR je konečné.

9.12.2 Postup zveřejnění změn

Schválená změna je integrována do CP TSA, a takto upravená CP TSA je publikována stejným způsobem jako předchozí verze CP TSA.

9.12.3 Okolnosti za kterých se mění OID

Změny v CP TSA, které se týkají zásadních skutečností významně ovlivňujících základní bezpečnostní funkce časových razítek jako změna délky platnosti nadřízených certifikátů, změna kryptografických aspektů (použité algoritmy, velkosti klíčů, hashovací funkce) apod. jsou okolnostmi na základě kterých je nutné nové verzi CP TSA přidělit nové OID. V případě ostatních změn v CP TSA je možné ponechat stávající OID.

9.13 Řešení případných neshod

Konečné právo výkladu této CP TSA náleží CA MF ČR. V případě, že některá ze stran nesouhlasí s předloženým výkladem, může se obrátit na vyšší instanci. Jednotlivé stupně obecně tvoří:

1. Vedoucí CA MF ČR
2. Ředitel odboru 33 MF ČR

Rozhodnutí ředitele odboru 33 MF ČR je v oblastech popsaných touto CP TSA konečné.

9.14 Právní výkon

Právní výkon v souvislosti s touto CP TSA se řídí příslušnými legislativními ustanoveními ČR.

9.15 Soulad s platnými zákony

Jakékoliv změny v této CP TSA nesmějí být v protikladu se zákony ČR.

9.16 Různá smluvní ustanovení

Tyto skutečnosti nejsou relevantní pro tuto CP TSA.

9.17 Závěrečné ustanovení

Tato CP TSA vydaná pro resortní autoritu časového razítka Ministerstva financí České republiky, nabývá účinnosti dnem stanoveným v tabulce Historie dokumentu v úvodu této CP.