CERTIFIKAČNÍ POLITIKA (CA)

verze: 1.4

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	
0.92	07.04.2008	První připomínky	Ing. Jiří Samec, MF ČR	
0,93	10.04.2008	Zapracování připomínek z verze 0.92	RNDr. Petr Tesař, Asseco CR	
0.94	14.04.2008	Připomínky z osobní porady	RNDr. Petr Tesař, Asseco CR	
0.95	14.04.2008	Připomínky z druhé osobní porady	RNDr. Petr Tesař, Asseco CR	
1.0	09.06.2008	Zapracování připomínek z verze 0.95	RNDr. Miroslav Šedivý, TO2 CR	
1.1	17.06.2008	Úprava problematiky testovací RA	RNDr. Miroslav Šedivý, TO2	
1.2	2.12.2008	Změna v kapitolách 7.1.4 a 9.17, rozšíření této tabulky	RNDr. Miroslav Šedivý, TO2	7.12.2008
1.3	10.12.2009	Rozšíření o použití certifikátů pro mobilní zařízení	RNDr. Miroslav Šedivý, TO2	1.1.2010
1.4	27.01.2011	Doplnění CA GFŘ, úprava postupu zneplatnění	RNDr. Miroslav Šedivý, TO2	15. 4. 2011

OBSAH

1 Úvod

Tento dokument představuje Certifikační politiku (dále jen „CP") platnou pro resortní certifikační autoritou Ministerstva financí ČR (dále jen „CA MF ČR").

Touto CP se CA MF ČR řídí při poskytování služeb spojených s vydáváním certifikátů a seznamů zneplatněných certifikátů (dále jen „CRL").

CP je závazná v plném rozsahu pro všechny výkonné a administrativní složky CA MF ČR, v určeném rozsahu pak i pro uživatele a spolupracující strany.

Pro snazší orientaci uživatelů osobních certifikátů jsou části politiky týkající se především nadřízených certifikačních autorit vymezeny vodorovnými čarami, případně čarou a koncem kapitoly. Tyto části jsou pro uživatele osobních certifikátů informativní.

1.1 Obecný přehled

CP odpovídá požadavkům stanoveným v RFC 3647, s přihlédnutím k doporučením orgánů EU a k legislativě ČR v daném oboru. CP představuje souhrn závazných postupů při vydávání, následné správě a zneplatňování certifikátů CA MF ČR 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)

V rámci resortu MF ČR je zavedena hierarchická struktura certifikačních autorit. Pod pojmem CA MF ČR se rozumí celá tato hierarchická struktura certifikačních autorit. Na vrcholu hierarchie stojí kořenová certifikační autorita (dále jen „CA_Root"), která slouží jako vrchol stromu důvěry. Tato autorita vydává pouze svůj kořenový nadřízený certifikát a nadřízený certifikát pro mezilehlou certifikační autoritu (dále jen „CA_Intermediate") a příslušné CRL. CA_Intermediate slouží pro vydávání nadřízených certifikátů podřízeným vydávacím certifikačním autoritám (dále jen „CA_Local"). CA_Intermediate vydává dále nadřízené certifikáty pro resortní autoritu časového razítka MF ČR

(dále jen „TSA“). Pokud je použit termín certifikační autorita (nebo pouze CA) má se za to, že jde o libovolnou z CA_Root, CA_Intermediate, CA_Local.

Do struktury certifikačních autorit MF ČR je rovněž zařazena testovací certifikační autorita (CA Test). Tato certifikační autorita je na stejné úrovni jako CA_Local, proto veškerá ustanovení této certifikační politiky platná pro CA_Local platí i pro CA Test, pokud není výslovně stanoveno jinak.

1.3.2 Registrační autority

U každé CA_Local se zřizuje jedna nebo více registračních autorit (dále jen „RA“). RA nese odpovědnost za správné vyřízení žádostí o poskytování certifikačních služeb. RA nesmí kladně vyřídit žádost, pokud uživatel hodnověrným způsobem neprokázal svoji totožnost nebo odmítá potřebné údaje sdělit.

RA dále zodpovídá za včasné vyřízení oprávněných žádostí o zneplatnění certifikátů.

RA je základním místem styku žadatelů a uživatelů certifikačních služeb s poskytovatelem těchto služeb a odpovídá za vyřizování připomínek a stížností uživatelů.

V působnosti vedoucího CA MF ČR je pro potřeby vývoje a ověření provozní funkčnosti ICT u CA Test zřízena samostatná RA pro přijímání a vyřizování žádostí o poskytování testovacích certifikátů.

CA_Root a CA_Intermediate vydávají pouze nadřízené certifikáty. Vzhledem k tomu se obejdou bez služeb RA. Žádosti o vystavení nadřízeného certifikátu podávají přímo správci CA_Local nebo ředitelé organizačních složky. Nadřízené certifikáty pro CA_Root a CA_Intermediate jsou přímo v režii vedoucího CA MF ČR.

1.3.3 Uživatelé

Uživatelem osobního certifikátu může být pouze fyzická osoba, která je oprávněná k právním úkonům dle příslušné legislativní normy a je v pracovně právním vztahu s organizační složkou MF ČR, která provozuje danou CA_Local nebo za přesně stanovených podmínek, pracovníci třetích stran, kteří s touto složkou spolupracují nebo jí poskytují služby.

Uživatelem u CA_Root a CA_Intermediate jsou fakticky pouze podřízené certifikační autority. CA_Intermediate vydává a zneplatňuje ještě nadřízené certifikáty pro TSA. Žadatelem o vydání nadřízeného certifikátu nebo jeho zneplatnění, může být pouze fyzická osoba.

1.3.4 Spoléhající strany

Jsou fyzické osoby, technická zařízení. procesy a podřízené certifikační autority, které se při své činnosti spoléhají na platnost příslušného digitálního podpisu ověřovanou veřejným klíčem obsaženým v certifikátu vydaném CA MF ČR

1.3.5 Ostatní účastníci

Další subjekty, které se podílí na službách orientovaných do infrastruktury veřejných klíčů (dále jen „PKI"), jako dodavatelé specializovaného hardware, software, čipových karet, zabezpečovací techniky atp.

1.4 Typy a použitelnost certifikátu

1.4.1 Povolená použití certifikátů

Certifikáty, které vydávají jednotlivé CA mohou být používány v aplikacích pro následující účely:

- zajištění integrity dat
- zajištění neodmítnutelnosti odpovědnosti
- zajištění důvěrnosti dat
- ustanovení sdíleného tajemství (klíče) v rámci protokolu pro bezpečnou výměnu dat
- přímé šifrování a dešifrování dat
- podepisování a ověření certifikátů
- podepisování a ověřování CRL
- podepisování a ověřování časových razítek

V případech použití certifikátu (resp. privátního klíče s ním spojeného) pro tyto účely se vlastní použití řídí příslušnými standardy.

Pro certifikáty vydané testovací certifikační autoritou CA Test (dále také jen „testovací certifikáty") platí následující omezení:

- certifikáty nesmějí být v žádném případě použity pro
  - podepisování a ověření certifikátů
  - podepisování a ověřování CRL
  - podepisování a ověřování časových razítek
- certifikáty mohou být použity výhradně v testovacím prostředí

1.4.2 Zakázaná použití certifikátů

Certifikáty vydané podle této CP a s nimi spojené privátní klíče nelze používat pro jiné účely než-li uvedené v odstavci 1.4.1.

1.4.3 Typy vydávaných certifikátů

CA MF ČR vydává následující typy certifikátů.

1. Nadřízené certifikáty

- nadřízené certifikáty pro vydávání a ověřování certifikátů a CRL
- nadřízené certifikáty pro vydávání a ověřování časových razítek

Nadřízené certifikáty a k nim příslušné párové klíče slouží výhradně k podepisování a ověřování certifikátů, CRL a časových razítek.

2. Osobní certifikáty

- certifikáty pro autentizaci a podepisování
- certifikáty pro šifrování
- certifikáty pro ověřování softwarového kódu

Certifikáty pro autentizaci a podepisování a k nim příslušné párové klíče slouží při autentizaci fyzických osob například vůči vstupním kontrolním systémům, při přihlašování k osobním účtům v počítači, při přihlašování do aplikací (jako např. ADIS) atp. Tyto certifikáty a k nim příslušné párové klíče se rovněž použijí při vytváření a ověřování elektronických podpisů.

Certifikáty pro šifrování a k nim příslušné párové klíče slouží pro zajištění důvěrnosti dat, například při šifrování/dešifrování e-mailových zpráv, při zabezpečení uložených dat na pevném disku počítače v souborovém systému EFS firmy Microsoft atp.

Certifikáty pro ověřování softwarového kódu a k nim příslušné párové klíče jsou vydávány určeným pracovníkům, kteří pomocí příslušného privátního klíče zajišťují autenticitu určeného software.

3. Certifikáty pro aplikace

- certifikáty pro doménové řadiče
- certifikáty pro servery
- certifikáty pro konkrétní určenou aplikaci

Certifikáty pro aplikace a k nim příslušné párové klíče jsou používány automatickými procesy pro účely uvedené v odstavci 1.4.1 vyjma podepisování a ověření certifikátů, podepisování a ověřování CRL a podepisování a ověřování časových razítek.

4. Testovací certifikáty

- testovací certifikáty osobní
- testovací certifikáty pro aplikace

Testovací certifikáty vydává certifikační autorita CA Test, která je na úrovni CA_Local. Testovací certifikáty mohou být všech typů, které vydává CA_Local, vyjma certifikátu pro doménový řadič. Nadřízené certifikáty proto nemohou být vydávány v testovací verzi. Všechny procesy související s životním cyklem testovacího certifikátu jako identifikace žadatele, žádost o vydání, vydání, expirace, následný certifikát, zneplatnění atd., jsou (až na výjimky uvedené dále v příslušných ustanoveních) stejné jako u jeho řádného ekvivalentu.

Testovací certifikáty lze používat pouze pro testovací, technologické účely. Jejich použití v ostrém provozu je zakázáno.

1.5 Administrace dokumentu

1.5.1 Řízení a specifikace CP

Použití certifikátů vydaných CA MF ČR se řídí touto CP, kterou vydává MF ČR. Tuto CP zveřejňuje CA MF ČR na webových stránkách MF ČR. Veškeré dotazy týkající se interpretace CP 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 s odpovídající CPS

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

1.5.4 Schvalování CP

CP CA MF ČR 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.

Systém PKI

Pojem	Význam
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
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.).
Kořenový nadřízený certifikát	Nadřízený certifikát, který je podepsán privátním klíčem příslušným veřejnému klíči uvedenému v tomto certifikátu (angl. self-signed). Je na vrcholu hierarchie důvěry. V rámci CA MF ČR je pouze u CA_Root.
Mobilní zařízení	PDA, Smartphone, i-Phone, mobilní telefony s OS umožňujícím vzdálený přístup do sítě MF ČR

Systém PKI

Pojem	Význam
MSCA	Služba serverového operačního systému firmy Microsoft zajišťující funkce certifikační autority v rámci PKI.
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)
Otisk	Výstup hashovací 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.
Podepisující osoba	Fyzická osoba, která je držitelem prostředku pro vytváření digitálních podpisů a jedná svým jménem nebo jménem jiné fyzické či právnické osoby.
PKI	Infrastruktura veřejných klíčů – soubor technologií založených na asymetrických šifrách.
Privátní klíč	Jiný výraz pro data pro vytváření digitálních podpisů.
Služba (service)	Souhrn úloh, které tvoří z pohledu poskytovatele služby i žadatele služby jeden celek.
Služební identifikační číslo	Jednoznačný bezvýznamový identifikátor, kterým je osobní číslo zaměstnance, identifikační číslo externího pracovníka apod., které je zpravidla automaticky přidělováno personálním informačním systémem nebo jinou ověřenou databází

Systém PKI

Pojem	Význam
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.
Systém správy čipových karet (CMS)	Představuje systém pro generování obsahu, potisk, ukládání, distribuci, zrušení, mazaní obsahu a ničení čipových karet.
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 certifikačních služeb, který jej vydal, zneplatněn bez možnosti obnovení platnosti.

2 Uveřejňování a uchování informací

2.1 Sklady

CA MF ČR zřizuje za účelem poskytování certifikačních služeb sklady certifikátů. Sklady jsou zřízeny u CA_Intermediate a CA_Local. CA MF ČR zveřejňuje následující informace o certifikátech:

- informace o vydaných certifikátech včetně odkazů, na nichž lze požadovaný certifikát získat.
- informace o zneplatněných certifikátech včetně odkazů, na nichž je možné získat aktuální nebo archivní CRL.

2.2 Zveřejňování certifikačních informací

CA MF ČR poskytne informace o této CP všem oprávněným subjektům v potřebném rozsahu.

CA MF ČR zveřejňuje své vlastní nadřízené certifikáty, tak aby byly k dispozici všem uživatelům. CA MF ČR rovněž zveřejňuje statut svých vlastních nadřízených certifikátů.

2.3 Frekvence zveřejňování

CA_Local periodicky aktualizuje seznam vydaných certifikátů, doba od vydání certifikátu do jeho zveřejnění nesmí přesáhnout 8 hodin.

CA_Local periodicky aktualizuje CRL. Za tímto účelem CA_Local vydává aktuální CRL jednou za 48 hodin (2 dny), takto vydané CRL platí 96 hodin (4 dny).

CA_Root a CA_Intermediate aktualizují seznam jimi vydaných nadřízených certifikátů pouze v případě, že vydaly nový nadřízený certifikát. Doba od vydání nadřízeného certifikátu do jeho zveřejnění nesmí přesáhnout 8 hodin.

CA_Intermediate rovněž periodicky aktualizuje CRL, Za tímto účelem CA_Intermediate vydává aktuální CRL jednou za 30 kalendářních dní. V případě, že došlo k zneplatnění nadřízeného certifikátu, který CA_Intermediate vydala, je CRL vydáno bezprostředně.

CA_Root aktualizují CRL pouze v případě, že zneplatní nějaký nadřízený certifikát, který vydala. V takovém případě vydává CRL bez zbytečných průtahů nejpozději však do 2 hodin po zneplatnění takového nadřízeného certifikátu.

Vlastní nadřízené certifikáty zveřejňují všechny certifikační autority na webových stránkách MF ČR nejméně 24 hodin před nabytím jejich platnosti. Jsou rovněž povinné bezpečnou cestou předat tyto certifikáty RA nejméně 24 hodin předem před nabytím jejich platnosti.

Při změně statutu svých nadřízených certifikátů oznamují tuto skutečnost neprodleně prostřednictvím webových stránek MF ČR, nejpozději však do 2 hodin.

2.4 Způsoby přístupu k uloženým informacím

K uloženým informacím tj. seznamu vydaných certifikátů, CRL, této CP, CPS a vlastním nadřízeným certifikátům lze přistupovat vzdáleným přístupem přes lokální síť a Internet. Přístupové adresy jsou uvedeny i ve vydaných certifikátech.

3 Identifikace a autentizace

3.1 Jmenné konvence

3.1.1 Typy jmen

CA_Local přijímá žádosti o vydání certifikátů ve formátu X.509.

V souladu s požadavky norem řady X.500. povinnými položkami jsou:

V případě certifikátů pro aplikace:

- Obecné Jméno (CN) – musí být shodné se jménem aplikace
- země (C)

V případě osobních certifikátů umístěných na čipové kartě:

- Obecné Jméno (CN)
- Organizace (O): MFCR
- Organizační jednotka (OU): dle zařazení
- Title (T) – je použito (osobní) služební identifikační číslo
- Alternativní jméno předmětu
    - UPN uživatele pro přihlášení do sítě MF ČR (UPN)
    - e-mailová adresa (E)
- země (C)

V případě osobních certifikátů pro autentizaci a elektronické podepisování umístěných v mobilním zařízení:

- Obecné Jméno (CN)Organizace (O): MFCR
- Organizační jednotka (OU): dle zařazení
- Title (T) – je použito (osobní) služební identifikační číslo
- Alternativní jméno předmětu
    - UPN uživatele pro přihlášení do sítě MF ČR (UPN)
    - e-mailová adresa (E)
- země (C)

V případě osobních certifikátů pro autentizaci do VPN umístěných v mobilním zařízení:

- Obecné Jméno (CN) - je použito (osobní) služební identifikační číslo
- Organizace (O): MFCR
- Organizační jednotka (OU): dle zařazení
- Alternativní jméno předmětu
    - UPN uživatele pro přihlášení do sítě MF ČR (UPN)
    - e-mailová adresa (E)

- země (C)

Pro testovací certifikáty osobní platí stejné zásady jako pro osobní certifikáty, pouze položka CN musí být doplněna (zakončena) řetězcem „(TEST!)".

CA_Intermediate přijímá žádosti o vydání certifikátů ve formátu X.509.

V souladu s požadavky norem řady X.500. povinnými položkami jsou:

V případě nadřízených certifikátů pro CA_Local:

- Obecné Jméno (CN): Ministerstvo financi - CA /*název lokality*/
- země (C) : CZ
- organizace (O): MFCR

V případě nadřízených certifikátů pro TSA:

- Obecné Jméno (CN): Ministerstvo financi - TSA
- země (C) : CZ
- organizace (O): MFCR

CA_Root přijímá žádosti o vydání certifikátů ve formátu X.509.
V souladu s požadavky norem řady X.500. povinnými položkami jsou:

V případě kořenových nadřízených certifikátů pro CA_Root:

- Obecné Jméno (CN): Ministerstvo financi - CA Root
- země (C) : CZ
- organizace (O): MFCR

V případě nadřízených certifikátů pro CA_Intermediate:

- Obecné Jméno (CN): Ministerstvo financi - CA IM
- země (C) : CZ
- organizace (O): MFCR

3.1.2 Věcná správnost jmen

V případě osobních certifikátů se rovněž kontroluje přítomnost nepovolených znaků. V případě, že se nepovolené znaky vyskytnou, žádost se nepřijme.

Dále se kontroluje přítomnost všech povinných položek. Pokud některá z povinných položek není vyplněna, žádost se nepřijme.

Dále se kontroluje věcná správnost jmen.

Obecné Jméno (CN) - musí odpovídat některému z oficiálních jmen osoby nebo organizace. Přípustné hodnoty jsou pro fyzické osoby jméno a příjmení, v případě certifikátů pro autentizaci do VPN umístěných v mobilním zařízení osobní číslo uživatele. V případě certifikátů vydávaných testovací certifikační autoritou CA Test se na konec doplní řetězec „(TEST!)",

Elektronická adresa (E) – žadatel je povinen uvést odpovídající služební elektronickou adresu. Pokud je možné ověřit, že žadatel je vlastníkem nebo uživatelem předmětné elektronické adresy, musí tak být učiněno. Pokud toto není možné, musí být tato skutečnost zahrnuta do žádosti a je nutno požadovat po žadateli písemné potvrzení správnosti.

Název země (státu) (C) – může obsahovat pouze kód CZ – Česká republika.

Organizace (O) – může obsahovat pouze řetězec MFCR.

Organizační jednotka (OU) – může obsahovat pouze kód příslušné organizační jednotky.

Položka Title (T) – musí obsahovat osobní (služební) identifikační číslo.

Hlavní jméno uživatele (UPN) – musí obsahovat jméno uživatele pro přihlášení do sítě MF ČR

V případě certifikátů pro aplikaci se rovněž kontroluje přítomnost nepovolených znaků. V případě, že se nepovolené znaky vyskytnou, žádost se nepřijme. Dále se kontroluje přítomnost všech povinných položek. Pokud některá z povinných položek není vyplněna, žádost se nepřijme.

Dále se kontroluje věcná správnost jmen.

Název (CN) – zpravidla by měl obsahovat název aplikace. Pokud tak tomu není, musí být skutečnosti v názvu uváděné ověřeny, pokud se jedná o skutečnosti, které ověření vyžadují. V případě certifikátů vydávaných testovací certifikační autoritou CA Test se na konec doplní řetězec „(TEST!)"

Název země (státu) (C) – může obsahovat pouze kód CZ – Česká republika.

Pro nadřízené certifikáty se rovněž kontroluje věcná správnost jmen, kde jediná přípustná jména jsou uvedena v položkách v odstavci 3.1.1.

3.1.3 Použití pseudonymů

CA MF ČR nepodporuje používání pseudonymů ve vydávaných certifikátech.

3.1.4 Pravidla interpretace různých forem jmen

Pokud je použito alternativní jméno, je nutno rovněž ověřit skutečnosti v něm uváděné, pokud se jedná o skutečnosti vyžadující ověření.

Jako součást alternativního jména se připouští:

- elektronická adresa
- identifikátor zdroje v Internetu (URI)
- jméno doménového serveru
- IP adresa
- EDI jméno
- registrovaný identifikátor (OID)

3.1.5 Jednoznačnost jmen

V případě osobního certifikátu musí jednoznačnost jména zajišťovat položky **CN** (Obecné Jméno), **E** (elektronická adresa), **T** (osobní/služební identifikační číslo) a **C** (země / stát).

RA je povinna zjistit, zda žadatelem uvedené jméno nebylo v rámci vydaných certifikátů již použito. V případě, že žadatelovo jméno je již obsaženo ve vydaném certifikátu, RA vyzve příslušné personální oddělení ke změně, případně doplnění jména. Úpravu kolidujícího jména je povinno zajistit personální oddělení. Žádost s kolidujícím jménem musí RA odmítnout.

Pokud přes veškerá opatření dojde ke kolizi jmen, je v součinnosti s příslušným personálním oddělením provedena změna jména uživatel, který o vydání certifikátu s kolidujícím jménem požádal jako poslední. Uživatelův certifikát je zneplatněn. Po vyřešení kolize a sjednání nápravy je pro tohoto uživatele vyžádán a vydán nový certifikát.

V případě certifikátu pro aplikaci musí jednoznačnost jména zajišťovat položky **CN** (Obecné Jméno) a **C** (země / stát).

RA je povinna zjistit, zda žadatelem uvedené jméno nebylo v rámci vydaných certifikátů již použito.

V případě, že žadatelovo jméno je již obsaženo ve vydaném certifikátu, RA vyzve žadatele ke změně jména. Žadatel je povinen podat novou žádost s upraveným nekolidujícím jménem. Žádost s kolidujícím jménem musí RA odmítnout.

U vydávaných nadřízených certifikátů pokud je dodržen odstavec 3.1.2 je zároveň zajištěna jednoznačnost jmen.

3.1.6 Uznávání, autentizace a role ochranných známek

Tyto skutečnosti nejsou relevantní pro tuto CP.

3.2 Prvotní identifikace žadatele

3.2.1 Metody dokazování vlastnictví privátního klíče

Žadatel je povinen prokázat vlastnictví privátního klíče, pokud požaduje vystavení certifikátu, jehož součástí je odpovídající veřejný klíč.

Pokud je privátní klíč generován a uložen na čipové kartě, která bude předána žadateli, má se vlastnictví privátního klíče za prokázané. V ostatních případech je tento privátní klíč použit k podpisu digitální žádosti o vydání certifikátu, která obsahuje i jemu příslušný veřejný klíč. Pokud je podpis žádosti o certifikát úspěšně ověřen, má se vlastnictví privátního klíče za prokázané.

V případě žádosti o certifikát aplikace (např. serveru) jsou párové klíče generovány správci těchto aplikací pomocí administrátorských nástrojů dané aplikace. Privátní klíč certifikátu aplikace zůstává uložen na serveru, kde byly párové klíče generovány. Veřejný klíč se stává součástí digitální žádosti o certifikát, která je generována spolu s párovými klíčí a která je privátním klíčem

digitálně podepsána. Ověřením platnosti tohoto digitálního podpisu si RA nebo CA (u certifikátů pro doménové řadiče) ověřuje vlastnictví privátního klíče.

V případě vystavení nadřízeného certifikátu pro podřízené autority se vlastnictví privátního klíče dokladuje digitálním podpisem žádosti o vystavení certifikátu pro takovou autoritu.

3.2.2 Ověření organizační identity

Příslušnost žadatele k organizační jednotce v rámci které žádá o vydání certifikátu si ověřuje pracovník RA na základě údajů z personálního IS. Tyto skutečnosti jsou relevantní pouze pro CA_Local.

3.2.3 Ověření identity fyzické osoby

Individuální žadatel je povinen pracovníkovi RA prokázat svou identitu při registraci žádosti o vydání certifikátu na první nebo nové čipové kartě nebo při registraci žádosti o vydání certifikátu aplikace. Svoji identitu je žadatel rovněž povinen prokázat při osobním převzetí první nebo nové čipové karty nebo při převzetí certifikátu aplikace.

3.2.4 Neprověřované údaje žadatele

RA nezodpovídá za správnost ostatních atributů certifikátu vyjma CN, C, T, E a případně AN.

3.2.5 Ověření oprávnění

Pokud žadatel žádá o vydání certifikátu, který zajišťuje speciální oprávnění, např. oprávnění pro operátora CA, musí předložit písemný dokument/dokumenty vlastnoručně podepsané odpovědným řídícím pracovníkem, na základě kterých bude moci pracovník RA tyto skutečnosti věrohodně ověřit.

Pokud žadatel žádá o vydání certifikátu u CA Test, musí rovněž předložit písemný dokument/dokumenty vlastnoručně podepsané odpovědným řídícím pracovníkem, na základě kterých bude moci pracovník RA oprávněnost žádosti věrohodně ověřit.

Žadatelé o vydání nadřízených certifikátů, pokud nejsou přímo vedoucím CA MF ČR musí hodnověrným způsobem prokázat, že jsou oprávněni žádat o vydání nadřízených certifikátů.

3.2.6 Identifikace při PKI součinnosti

CA_Local nespolupracují s jinými certifikačními autoritami a nejsou oprávněné vydávat křížové certifikáty.

CA_Intermediate nespolupracuje s jinými certifikačními autoritami a není oprávněna vydávat křížové certifikáty.

CA_Root nespolupracuje s jinými certifikačními autoritami a není oprávněna vydávat křížové certifikáty.

3.3 Identifikace a autentizace při vydávání následného certifikátu

3.3.1 Identifikace a autentizace při standardním vydání následného certifikátu

Při standardním postupu žádosti o vydání následného certifikátu se identifikace a autentizace žadatele zajišťuje pomocí digitálního podpisu vytvořeného žadatelovým ještě platným privátním klíčem.

3.3.2 Identifikace a autentizace po zneplatnění certifikátu

Pokud byl certifikát zneplatněn, provede se identifikaci a autentizaci žadatele o následný certifikát jako v případě, kdy žadatel žádá o vydání nového certifikátu.

V případě že byl zneplatněn nadřízený certifikát provede CA, která jej vydala, identifikaci a autentizaci žadatele o následný nadřízený certifikát jako v případě, kdy se žádá o vydání nového nadřízeného certifikátu.

3.4 Identifikace a autentizace při žádosti o zneplatnění certifikátu

Osoba žádající o zneplatnění certifikátu může žádost podat buď fyzicky na RA, pomocí vzdáleného přístupu nebo přes službu Helpdesk.

V případě přímé žádosti na RA je žadatel povinen prokázat svoji totožnost. Pokud nejde přímo o držitele certifikátu, musí být tato osoba na seznamu oprávněných osob oprávněných zneplatňovat předmětný certifikát, který má pracovník RA k dispozici.

V případě žádosti podávané pomocí vzdáleného přístupu se žadatel o zneplatnění identifikuje a autentizuje použitím elektronického podpisu vytvořeného jeho privátním klíčem.

V případě žádosti podané přes Helpdesk se nejdříve identifikuje operátorovi Helpdesku pomocí stanoveného postupu, a poté podá žádost o zneplatnění certifikátu.

Vydaný certifikát je možné rovněž zneplatnit automaticky bez žádosti na základě zjištění, že osoba, která je držitelem certifikátu, již není v pracovním poměru nebo jsou zjištěny jiné závažné nedostatky (duplicity certifikátů apod.) a přitom nebyla podána žádost standardním způsobem, ačkoliv být podána měla.

O zneplatnění nadřízeného certifikátu vydaného CA_Root může žádost podat pouze ředitel odboru 33 MF ČR nebo vedoucí CA MF ČR.

O zneplatnění certifikátu vydaného CA_Intermediate může žádost podat pouze ředitel příslušné organizační složky nebo správce příslušné podřízené CA. V případě, že použije vzdálený přístup identifikuje a autentizuje se použitím elektronického podpisu vytvořeného svým osobním privátním klíčem na žádosti o zneplatnění a současně musí být žádost o zneplatnění certifikátu ověřena telefonickým hovorem mezi žadatelem a vedoucím CA MF ČR.

Žádost o zneplatnění certifikátu vydaného CA_Intermediate nelze podávat pomocí Helpdesku.

4 Operační požadavky životního cyklu certifikátu

Osobní certifikát pro autentizaci a podepisování je vydáván na čipovou kartu která slouží i jako vstupní průkaz a proto má potřebné vizuální identifikační data. Používání čipové karty pro přihlašování je povinnost. Žadateli může být na základě jeho žádosti vydán také certifikát pro použití v mobilním zařízení.

4.1 Žádost o certifikát

4.1.1 Žadatelé o certifikát

Žadatelem o vydání certifikátu může být pouze fyzická osoba, která v době žádosti splňuje podmínky odst. 1.3.3. Potvrzení podepisuje vedoucí organizační součásti pro kterou je daný typ certifikátu validní nebo jím ustanovený zástupce.

Žadatelem o vydání nadřízeného certifikátu může být pouze fyzická osoba, která je v době žádosti prokazatelně ředitelem příslušné organizační složky nebo je ve funkci správce CA respektive vedoucího CA MF ČR.

Žadatelem o vydání certifikátu pro doménový řadič je sám doménový řadič, který v okamžiku, kdy se doinstaluje, vyhledá MSCA, která je v jeho doméně a u ní si nechá (podle příslušné šablony) vystavit prvotní certifikát.

4.1.2 Registrační proces

Registrační proces se skládá z vypracování návrhu žádosti o vystavení certifikátu, schválení tohoto návrhu příslušným pracovníkem a vyřizováním této žádosti příslušnou registrační autoritou.

V případě nadřízených certifikátů se registrační proces skládá z vypracování návrhu žádosti o vystavení certifikátu a schválení tohoto návrhu ředitelem odboru 33 MF ČR.

V případě certifikátu doménového řadiče probíhá registrační proces automaticky mezi MSCA a doménovým řadičem na základě protokolů serverového operačního systému firmy Microsoft.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikační a autentizační proces

Identifikační a autentizační proces, vyjma případ doménového řadiče, provádí příslušná RA podle postupů podrobněji popsaných v odstavci 3.2.3.

Identifikační a autentizační proces v případě doménového řadiče probíhá automaticky na základě protokolů serverového operačního systému firmy Microsoft.

4.2.2 Schválení a odmítnutí žádosti o vydání certifikátu

Pracovník RA odmítne žádost o vydání certifikátu pokud

- žadatel není zaveden v personálním informačním systému nebo jiné ověřené databázi, popřípadě nepředloží platný občanský průkaz
- žadatel nepředloží podepsaný dokument podle 3.2.5 a vyžaduje vydání certifikátu, jehož vydání je na takový dokument vázáno
- žadatel žádá o vydání certifikátu, který není CA_Local podporován
- žádost neobsahuje povinné položky a žadatel odmítne nebo není schopen tyto doplnit

V ostatních případech pracovník RA žádost schválí.

Schválení nebo odmítnutí žádosti o vydáni nadřízeného certifikátu je plně v pravomoci ředitele odboru 33 MF ČR.

Tento postup není relevantní pro certifikát doménového řadiče.

4.2.3 Lhůty vyřízení žádosti o certifikát

Lhůta k vyřízení žádosti o certifikát je jeden pracovní den. V případě žádosti u CA_Intermediate jsou to 3 pracovní dny.

4.3 Vydání certifikátu

4.3.1 Postup CA při vydání certifikátu

Při prvotním výdeji osobního certifikátu, generuje certifikát CA_Local na základě požadavků přijatých od RA. Postup závisí na zařízení, které bude pro uchovávání a práci s certifikáty používáno.

Čipová karta

Párové klíče uživatele určené pro autentizaci a podepisování jsou vždy generovány v čipové kartě, pro ostatní použití jsou buď generovány v čipové kartě nebo jsou do ní nahrány. Privátní klíč pro autentizaci a podepisování nikdy neopustí čipovou kartu, všechny operace s ním se budou provádět v čipové kartě po zadání přístupového hesla - PIN (Personal Identification Number). K příslušnému veřejnému klíči a údajům z žádosti vystaví CA_Local certifikát, který je rovněž nahrán na čipovou kartu.

Mobilní zařízení

Párové klíče jsou generovány buď v samotném zařízení nebo na lokální stanici umístěné v lokální síti uživatele. V případě generace mimo zařízení musí být zajištěno, aby bylo možné certifikát i s privátním klíčem do zařízení importovat. CA_Local vystaví k příslušnému veřejnému klíči a údajům z žádosti certifikát, který je možné do zařízení importovat.

Při prvotním výdeji certifikátu pro aplikaci, vyjma doménového řadiče, digitálně podepisuje CA_Local tento certifikát na základě požadavku přijatého od RA. Certifikát aplikace spolu s platnými nadřízenými certifikáty je žadateli osobně předán na RA na externím médiu.

Při vydání kořenového nadřízeného certifikátu CA_Root je tento certifikát digitálně podepsán privátním klíčem příslušným k veřejnému klíči uvedenému v certifikátu CA_Root.

Nadřízený certifikát pro CA_Intermediate je rovněž podepsán privátním klíčem CA_Root.

Nadřízený certifikát pro CA_Local a TSA je při vydání digitálně podepsán privátním klíčem CA_Intermediate.

Žádost doménového řadiče je příslušnou MSCA zpracována a vyřízena v rámci procesů serverového operačního sytému firmy Microsoft.

4.3.2 Zpráva o vydání certifikátu žádající osobě

Zpráva o vydání certifikátu je společně s vydaným certifikátem zaslána na e-mailovou adresu žadatele.

4.4 Akceptování certifikátu

4.4.1 Postup žadatele při akceptaci certifikátu

Při vydání certifikátu na nové čipové kartě vyjádří žadatel akceptaci certifikátu vlastnoručním podpisem dokumentu o předání čipové karty na RA. Pokud odmítne certifikát akceptovat, vyznačí pracovník tuto skutečnost na dokumentu o předání čipové karty a požádá CA_Local o zneplatnění tohoto certifikátu.

V případě vydání certifikátu pro mobilní zařízení se akceptace provádí prostřednictvím elektronického potvrzení přijetí certifikátu s použitím čipové karty uživatele.

Řádně vydané nadřízené certifikáty musí být akceptovány.

4.4.2 Zveřejňování vydaných certifikátů CA

Certifikáty, které vydala CA MF ČR jsou přístupné na webových stránkách MF ČR a na webové stránce CA_Intermediate.

4.4.3 Zpráva CA o vydání certifikátů dalším stranám

CA MF ČR nezasílá jiným stranám informaci o vydání certifikátů, není-li ve zvláštních dohodách nebo smlouvách uvedeno jinak.

4.5 Párové klíče a použitelnost certifikátu

4.5.1 Privátní klíč podepisujícího subjektu a užití certifikátu

Privátní klíč podepisujícího subjektu lze používat výhradně k vytváření digitálních podpisů. Tyto digitální podpisy jsou použitelné pro účely, které odpovídají povolenému použití příslušného privátního klíče, tak jak je uvedené v atributu Key Usage a Extended Key Usage.

4.5.2 Veřejný klíč a spoléhající se strana

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

Spoléhající strana je povinna rovněž zkontrolovat obsah položky CN, zda neobsahuje řetězec „(TEST!)" – tyto certifikáty jsou určeny výhradně pro testování a podle toho je nutné s nimi nakládat.

4.6 Prodloužení platnosti certifikátu

Certifikátům vydaným podle této CP nelze prodlužovat dobu platnosti.

4.7 Následný certifikát

Následným certifikátem se rozumí certifikát, který byl v souladu s platnou CP vydán držiteli v době platnosti již vydaného certifikátu a který má stejné kontrolované údaje uvedené v tomto certifikátu, a liší se ve veřejném klíči a sériovém čísle certifikátu. V případě osobních certifikátů je za následný certifikát považován i takový, který může mít změny v některých kontrolovaných údajích, které jsou do certifikátu automaticky doplňovány z důvěryhodné databáze personálního oddělení. Tato výjimka se netýká údaje CN.

4.7.1 Okolnosti pro vydání následného certifikátu

Držitel certifikátu vydaného CA, jehož expirační doba vyprší a který i po této době bude mít právo držet certifikát stejného typu, bude vyzván k podání žádosti o vystavení následného certifikátu.

4.7.2 Žádost o vydání následného certifikátu

Při tvorbě následného osobního certifikátu, který je uložen na čipové kartě, si uživatel generuje nové párové klíče v čipové kartě. V ostatních případech probíhá generace nových párových klíčů s využitím programu Microsoft Internet Explorer, na k tomuto účelu připravené webové stránce veřejného rozhraní CA_Local. Přístup probíhá protokolem https, uživatel se autentizuje čipovou kartou s pomocí stávajících klíčů a certifikátů.

Žádost o následný certifikát digitálně podepisuje jak stávajícím, tak i novým privátním klíčem, čímž umožňuje dokázat vlastnictví privátních klíčů.

Při tvorbě následného nadřízeného certifikátu se vygenerují nové párové klíče na stejných zařízeních jako v případě prvního certifikátu tj. na přenosném počítači na kterém je realizována CA_Root, na speciálním kryptografickém modulu HSM, který je určen k podepisování nadřízených certifikátů a CRL vydávaných CA_Intermediate nebo na počítači na kterém je realizována CA_Local respektive TSA. Žádost o vydání následného certifikátu v elektronické podobě je v případě vydávání následného certifikátu pro CA_Intermediate, CA_Local a TSA.

4.7.3 Proces vydání následného certifikátu

Žádost o vystavení následného certifikátu je ověřována pomocí starého i nového veřejného klíče. Pokud jsou oba digitální podpisy platné je pro nový veřejný klíč vydán nový certifikát. V opačném případě je žádost zamítnuta. Pokud je žádost o vydání následného certifikátu zamítnuta je tato skutečnost žadateli sdělena na jeho e-mailovou adresu.

Žádost o vystavení následného nadřízeného certifikátu je ověřována pomocí starého i nového veřejného klíče. Pokud jsou oba digitální podpisy platné je pro nový veřejný klíč vydán nový nadřízený certifikát. Pokud tomu tak není je žádost o vydání následného nadřízeného certifikátu zamítnuta a tato skutečnost je žadateli sdělena na příslušnou e-mailovou adresu správce CA_Local nebo vedoucího CA MF ČR v případě CA_Root, CA_Intermediate a TSA.

4.7.4 Zpráva o vydání následného certifikátu žadateli

Zpráva o vydání následného certifikátu je společně s vydaným certifikátem zaslána na e-mailovou adresu žadatele.

4.7.5 Postup žadatele při akceptaci následného certifikátu

Všechny následné certifikáty vydané podle této CP musí být akceptovány.

4.7.6 Zveřejňování vydaných následných certifikátů CA

Následné certifikáty vydané CA jsou přístupné na webových stránkách MF ČR a na webové stránce CA_Intermediate.

4.7.7 Zpráva CA o vydání následných certifikátů dalším stranám

CA MF ČR nezasílá jiným stranám informaci o vydání následných certifikátů není-li ve zvláštních dohodách nebo smlouvách uvedeno jinak.

4.8 Modifikace certifikátu

CA MF ČR nepodporuje žádné vystavení dalšího nového certifikátu na párové klíče, které příslušely již jednou vystavenému certifikátu.

4.9 Zrušení a zneplatnění certifikátu

4.9.1 Okolnosti pro zneplatnění

Certifikát může být zneplatněn pouze na základě následujících okolností:

- držitel certifikátu nebo jím oprávněná osoba požádá o jeho zneplatnění
- na základě uživatelova sdělení se věcný obsah certifikátu stane neplatným
- na základě zjištění CA_Local nebo spolupracujících subjektů se věcný obsah certifikátu stane neplatným
- držitel certifikátu byl usvědčen ze závažného porušení pracovních povinností nebo povinností vyplývajících z CP
- je důvodné podezření, že došlo ke kompromitaci privátního klíče držitele certifikátu
- dojde ke kompromitaci privátního klíče CA_Local, který certifikát vydal
- držitel certifikátu ukončil pracovně právní vztah, nebo v případě pracovníků třetích stran došlo ke změně dohodnutých podmínek

Testovací certifikát musí být zneplatněn bezprostředně poté, co pominula nutnost jeho používání v procesu testování, o zneplatnění žádá vlastník certifikátu nebo správce aplikace pro niž byl testovací certifikát vydán.

Nadřízený certifikát může být zneplatněn pouze na základě následujících okolností:

- správce příslušné podřízené CA nebo ředitel organizační složky ve které je příslušná CA_Local zařazena požádá o jeho zneplatnění
- ředitel odboru 33 MF ČR nebo vedoucí CA MF ČR požádá o jeho zneplatnění
- na základě zjištění CA MF ČR se věcný obsah nadřízeného certifikátu stane neplatným
- je důvodné podezření, že došlo ke kompromitaci privátního klíče příslušného k tomuto nadřízenému certifikátu
- dojde ke kompromitaci privátního klíče CA_Root nebo CA_Intermediate.

4.9.2 Kdo může žádat o zneplatnění

O zneplatnění certifikátu může požádat:

- držitel certifikátu
- vedoucí zaměstnanec, který je oprávněn vydání certifikátu povolit
- RA, jejímž prostřednictvím bylo požádáno o jeho vydání
- CA_Local, která certifikát vydala

O zneplatnění nadřízeného certifikátu může požádat:

- ředitel odboru 33 MF ČR nebo vedoucí CA MF ČR
- správce podřízené CA nebo ředitel organizační složky u které je příslušná CA_Local zařazena

4.9.3 Procedura žádosti o zneplatnění

Vlastník certifikátu nebo oprávněný vedoucí zaměstnanec musí zaslat nebo osobně předat žádost o zneplatnění certifikátu způsobem uvedeným v článku 3.4.

V případě, že zneplatnění se uskutečňuje z iniciativy RA nebo CA_Local, je příslušný pracovník RA nebo CA_Local povinen zaznamenat tuto skutečnost do protokolu včetně důvodů tohoto rozhodnutí.

Výše uvedené neplatí, pokud se jedná o automatické zneplatnění osobního certifikátu na základě skutečnosti, že s dotyčnou osobou byl ukončen pracovní poměr a vydané certifikáty jí dosud nebyly zneplatněny. Požadovaný záznam je nahrazen v tomto případě záznamem příslušné aplikace.

Žádost o zneplatnění nadřízeného certifikátu se protokolárně předloží vedoucímu CA MF ČR, který o ní rozhodne s definitivní platností.

4.9.4 Lhůta pro podání žádosti o zneplatnění

Lhůta pro podání žádosti o zneplatnění není striktně stanovena. Každý kdo zjistí skutečnosti, které ve svých důsledcích ho povedou k podání žádosti o zneplatnění certifikátu, by měl tuto žádost podat bez zbytečného otálení. V případě nadřízených certifikátů by měl tyto skutečnosti předat osobě, která je oprávněna podat žádost o zneplatnění nadřízeného certifikátu.

Žádost o zneplatnění testovacího certifikátu v případě, že pominula nutnost jeho použití, musí příslušný vlastník (držitel), nebo správce aplikace podat bezodkladně.

4.9.5 Lhůta pro provedení zneplatnění CA

Lhůta pro provedení zneplatnění je stanovena na 48 hodin.

V časovém období, mezi okamžikem, kdy byl certifikát zneplatněn a okamžikem, kdy bylo zveřejněno CRL, na kterém byl tento zneplatněný certifikát poprvé zařazen je certifikát v zablokovaném stavu. Případné škody vzniklé použitím privátního klíče příslušného k zablokovanému certifikátu, jdou na vrub držitele tohoto certifikátu.

4.9.6 Požadavky na ověřování CRL

Spoléhající strana má v případech, ve kterých je to vyžadováno zvláštními předpisy, za povinnost při ověřování digitálního podpisu ověřit navíc i to, zda certifikát použitý při ověřování platnosti digitálního podpisu je v tomto okamžiku platný a rovněž platnost všech nadřízených certifikátů v cestě k tomuto certifikátu. Ověření této platnosti se provede pomocí platného CRL.

4.9.7 Četnost vydávání CRL

CA_Root vydává CRL pouze v případě, že zneplatní nějaký nadřízený certifikát, který vydala.

CA_Local vydává CRL jednou za 48 hodin (2 dny) s platností 96 hodin (4 dny).

CA_Intermediate vydává CRL jednou za 30 kalendářních dní s platností 60 kalendářních dní. V případě požadavku na zneplatnění některého z nadřízených certifikátů vystaví CA Intermediate CRL neprodleně.

4.9.8 Maximální zpoždění CRL mezi vydáním a zveřejněním

CA MF ČR garantuje maximální prodlevu mezi vydáním CRL a okamžikem, kdy bude toto nově vydané CRL přístupné spoléhajícím stranám na 5 hodin.

4.9.9 Přístupnost on-line ověřování statutu certifikátu

CA MF ČR nepodporuje on-line ověřování statutu certifikátu.

4.9.10 Požadavky na on-line ověřování statutu certifikátu

CA MF ČR nepodporuje on-line ověřování statutu certifikátu.

4.9.11 Další možnosti zneplatnění certifikátů

CA MF ČR nepodporuje další možnosti zneplatnění vydaných certifikátů.

4.9.12 Speciální požadavky při zneplatnění certifikátu jako důsledku kompromitaci privátního klíče

V případě certifikátů vydávaných dle této CP nejsou ze strany CA MF ČR žádné speciální požadavky na držitele při kompromitaci jeho privátního klíče příslušného tomuto certifikátu.

4.9.13 Okolnosti vedoucí k pozastavení platnosti

Certifikátům vydaným CA MF ČR nelze pozastavit platnost.

4.10 Služby spojené se statutem certifikátu

4.10.1 Operační charakteristiky

CA MF ČR podporuje pro certifikáty vydané podle této CP pouze následující statuty certifikátu:

- Platný
- Zneplatněný
- Zablokovaný
- Expirovaný
- Neaktivní

Certifikát je neaktivní v době před okamžikem zahájení platnosti (položka „Not before"). Tato situace nastane pokud je certifikát vydán dříve než-li začne platit.

Nadřízený certifikát nemůže být neaktivní.

Služba ověření, zda certifikát nebyl zneplatněn, je podporována pomocí kontroly ve vydaném CRL.

4.10.2 Dostupnost služeb

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

4.10.3 Volitelné vlastnosti

Tato CP nepodporuje další volitelné možnosti služby ověřování statutu certifikátu.

4.11 Ukončení využívání služeb CA

Držitel certifikátu, který ukončuje využívání služeb CA_Local, například z důvodu rozvázání pracovně právního poměru je povinen před ukončením požádat o zneplatnění certifikátů, kterých je držitel a na RA odevzdat příslušnou čipovou kartu. Pokud tak držitel neučiní zajistí zneplatnění příslušná RA.

Při ukončení využívání služeb poskytovaných CA_Root nebo CA_Intermediate je nutné provést zneplatnění certifikátů, které byly danou CA podepsány.

4.12 Úschova a obnovení privátního klíče

4.12.1 Politika úschovy

CA_Local provádí pouze úschovu privátních klíčů určených k souborovému šifrování pomocí EFS v operačních systémech firmy Microsoft, které EFS podporují a privátních klíčů určených k šifrování e-mailových zpráv v rámci MS Outlook.

CA_Root a CA_Intermediate neprovádí úschovu privátních klíčů.

4.12.2 Politika obnovení privátního klíče

Obnova privátních klíčů použitých pro šifrování dat ve specializovaných aplikacích (např. AreaGuard od firmy SODATSW spol. s r.o.) se řídí dokumenty a politikou platnou pro tyto aplikace (např. Dokumentace pro správu AreaGuard 3.1 od firmy SODATSW spol. s r.o.).

Obnovení privátních klíčů je dále podporováno pro aplikaci šifrování e-mail korespondence. CA_Local skladuje ke každému certifikátu, který slouží výhradně k šifrování e-mail korespondence (položka rozšířené použití klíče: E-mail Protection) i příslušný privátní klíč. V případě, že uživatel ztratí tento privátní klíč lze mu jej poskytnout dálkovým přenosem. Vlastní privátní klíč se přešifruje symetrickou šifrou a odešle se otevřeným e-mailem. Symetrický klíč použitý pro zašifrování tohoto privátního klíče se zašle jiným kanálem (například SMS zprávou na mobilní telefon).

V případech, kdy je privátní klíč používán k jinému účelu než-li šifrování dat, zejména v případech neodmítnutelnosti odpovědnosti, kdy je uložen na čipové

kartě bez možnosti exportu, nelze obnovu privátního klíče provést. V těchto případech se obecně generují nové párové klíče a vystavuje se nový certifikát.

Obnova privátních klíčů příslušných k nadřízeným certifikátům se řídí touto CP podle odstavce 6.2.

5 Fyzické, procedurální a personální bezpečnostní mechanismy

5.1 Fyzická bezpečnost

Fyzická bezpečnost je velmi důležitým faktorem zajišťujícím důvěryhodnost certifikačních služeb CA. Ochrana je zaměřena na hlavní systémy, kterými jsou ty, které přímo provádějí podepisování certifikátů a podepisování CRL.

5.1.1 Umístění a konstrukce

Zařízení určená k výkonu hlavních certifikačních služeb jsou umístěna v budovách, které spravuje Ministerstvo financí nebo jeho organizační složky. Budovy mají kontrolovaný vstupní režim. Podrobné nároky na objektovou bezpečnost jsou uvedeny v příslušné CPS.

5.1.2 Fyzický přístup

Přístup do vlastní budovy je kontrolovaný ostrahou. Přístup do místnosti s vlastní podepisující technikou je povolen pouze určeným pracovníkům CA a v případě, kdy jsou servery CA umístěny 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 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.

5.1.4 Ohrožení vodními zdroji

Budovy, ve kterých jsou umístěny CA stoji na pozemcích, které nejsou na příslušných katastrálních mapách uvedeny v záplavové zóně.

5.1.5 Požární ochrana

Vstupní dveře do místnosti se serverem CA jsou vybaveny protipožární vložkou. V místnostech se nachází hasební přístroj a požární alarm čidlo.

5.1.6 Uchování datových médií

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

5.1.7 Kancelářský odpad

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

5.1.8 Vnější uložení záloh

Pracovní zálohy jsou uloženy v prostorách CA. Ostatní zálohy jsou uloženy na místě určeném správcem CA. 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 jsou:

- Ředitel odboru 33 MF ČR – schvaluje CPS, CP, jmenuje vedoucího CA MF ČR. Schvaluje žádosti o vydání nadřízených certifikátů CA MF ČR.
- Vedoucí CA MF ČR – řídí činnost CA MF ČR. Zodpovídá za aktualizaci stavu dokumentace CPS a CP. Přímo řídí CA_Root, CA_Intermediate, TSA, CA_Local MF a dočasně i certifikační autoritu DS. Podílí se na zálohování klíčů jím přímo řízených CA a TSA. Podává žádosti o vydání nadřízených certifikátů pro jím přímo řízené CA a TSA. Zneplatňuje nadřízené certifikáty CA MF ČR.
- Správce CA_Local – řídí činnost CA_Local. Podává žádost o vydání nadřízeného certifikátu pro CA_Local.
- Bezpečnostní správce CA MF ČR - provádí činnosti v oblasti bezpečnosti informačního systému CA MF ČR, podílí se na likvidaci mimořádných událostí.
- Systémový administrátor - spouští službu MSCA, zastavuje službu MSCA, zálohuje klíče CA, obnovuje klíče CA, instaluje nový nadřízený certifikát CA.
- Databázový administrátor – zabezpečuje případné adresářové služby.
- 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 CA.
- Bezpečnostní auditor – provádí bezpečnostní audit informačního systému CA MF ČR.
- Operátor CA – zajišťuje běžný chod CA (případně i TSA).
- Operátor RA – zajišťuje běžný chod RA.

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 řízení CA_Root jsou spojeny s důvěryhodnými rolemi pro CA_Intermediate a pro TSA. Pracovníci ve funkcích u CA_Root zajišťují rovněž provoz CA Úřad a případný provoz původní certifikační autority DS.

5.2.2 Počty osob pro provádění úloh

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

- podepisování certifikátů a CRL
- zálohování privátního klíče CA
- obnova ze zálohy privátního klíče CA
- aktivace MSCA
- podepisování auditních záznamů
- podepisování archivních záznamů

je nezbytná přítomnost dvou pověřených pracovníků CA.

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. 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 – systémový administrátor

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 CA v důvěryhodných rolích a dále pracovníci RA přímo se podílející na styku s uživatelem jsou přijímáni na základě personálních kriterií popsaných v příslušné CPS.

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 příslušných CPS.

5.3.3 Požadavky na zaškolení

Pracovníci CA 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 následující 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. Problematika třetích stran je řešena v příslušných CPS.

5.3.8 Dokumentace poskytovaná personálu

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

5.4 Procedury auditu logování událostí

5.4.1 Typy zaznamenávaných událostí

Typy událostí, jež jsou zaznamenávány do auditního logu, jsou následující:

- záznam o registraci žadatele
- záznam o pokusu neoprávněné registrace žadatele
- záznam o zrušení registrace žadatele (údaje o žadateli se uchovávají)
- záznam o požadavku RA na vystavení certifikátu včetně výsledku
- záznam o požadavku na následný certifikát včetně výsledku
- záznam o neoprávněném požadavku na vystavení certifikátu včetně výsledku
- záznam o neoprávněném požadavku na následný certifikát včetně výsledku
- záznam o požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku
- záznam o neoprávněném požadavku na zneplatnění certifikátu včetně údajů o žádající osobě a výsledku
- záznam o pokusu neoprávněného přístupu do systému
- záznam o zveřejnění certifikátu včetně výsledku
- záznam o zanesení zneplatněného certifikátu do CRL
- záznam o zveřejnění CRL

5.4.2 Četnost zpracování auditních záznamů

Auditní záznamy u CA_Local jsou zpracovávány jednou denně. U CA_Root a CA_Intermediate jsou zpracovávány nepravidelně, vždy jen po výskytu zaznamenávané události. Po přezkoumání jsou záznamy uloženy do archívu.

5.4.3 Uschovací období pro auditní záznamy

Doba, po kterou se uchovávají auditní záznamy, je stanovena na 10 let.

5.4.4 Zabezpečení auditních záznamů

Auditní záznamy jsou přístupné pouze pověřenému pracovníku CA. Jednotlivé auditní záznamy jsou opatřeny pořadovým číslem a jsou digitálně podepsány. Privátní klíč určený k podpisu auditních záznamů není pracovníkům, majícím oprávnění prohlížet auditní záznamy, přístupný.

Po zpracování (článek 5.4.2) je znovu celý auditní log opět podepsán.

5.4.5 Audit log – archivace

Auditní záznamy jsou archivovány nejméně na dvou nezávislých médiích. Obě média musí být uložena nezávisle ve dvou místnostech. Jedenkrát měsíčně se provádí zálohování na další médium, které musí být uloženo mimo provozní prostory CA.

5.4.6 Systém shromažďování auditních záznamů

Systém shromažďování auditních záznamů je ve vztahu k CA interní.

5.4.7 Hlášení vzhledem k subjektu událostí

V případě neoprávněných pokusů není subjekt informován o zapsání auditního záznamu, v ostatních případech je informován.

5.4.8 Hodnocení zranitelnosti

Osoby odpovědné za vyhodnocování záznamů jsou povinny informovat určené pracovníky o zjištěných skutečnostech. Správce CA stanoví způsob a rozsah hlášení o incidentech. Odpovědní pracovníci CA pověření bezpečnostní údržbou, jsou povinni případné hrozby analyzovat a realizovat odpovídající protiopatření.

5.5 Archivace záznamů

Informace související s dále uvedenými situacemi a daty se u CA MF ČR uchovávají pro kontrolu činnosti CA a dále na základě požadavků relevantních právních norem. Toto uchování je na delší dobu než-li 1 rok, a proto mluvíme o archivaci záznamů. V zásadě nejsou určeny pro požadavky uživatelů, nicméně mohou sloužit pro interní potřebu, kde je to právními normami vyžadováno.

5.5.1 Typy zaznamenávaných událostí

Zaznamenávány jsou všechny informace a události vztahující se k registraci a životnímu cyklu vydávaných certifikátů, zejména pak:

- identifikační údaje osoby, která provedla ověření totožnosti žadatele,
- všechny požadavky na zneplatnění certifikátů a záznamy o jejich zneplatnění,
- všechny požadavky na vydání certifikátů.

Dále jsou zaznamenávány :

- všechny události vztahující se k životnímu cyklu párových klíčů CA

- všechny události vztahující se k životnímu cyklu nadřízených certifikátů CA

5.5.2 Uschovací období pro archivaci

CA zajistí zaznamenávání informací a událostí vztahujících se k vydání a další správě všech vydaných certifikátu a jejich uchování po dobu 10 let od ukončení jeho platnosti, a to v rozsahu uvedeném v odst. 5.5.1.

5.5.3 Ochrana archivu

Protože archivované informace obsahují i osobní data uživatelů, je vzhledem k zákonu 101/2000 Sb. dbáno zvýšené ochrany těchto informací. Data v písemné formě jsou ukládána do kovových uzamykatelných skříní. Data v elektronické formě jsou vypalována na CD (DVD) média a ukládána do kovových uzamykatelných skříní. Klíče od těchto skříní jsou ukládány do ochranných schránek a manipulaci s nimi mohou provádět pouze pověření pracovníci CA.

5.5.4 Archivační procedury

Jednotlivé elektronické archivní záznamy jsou před uložením na médium doplněna o časový údaj, kdy je archivace započata, a následně elektronicky podepsány. Přístup k privátnímu klíči mohou mít pouze pověření pracovníci. Smí být použit pouze privátní klíč, jemuž odpovídající veřejný klíč je součástí certifikátu vydaného CA_Local.

Po digitálním podepsání záznamů, jsou tyto ještě opatřeny časovým razítkem. Poté jsou tyto skutečnosti zaprotokolovány a data jsou uložena na medium.

5.5.5 Požadavky vzhledem k časovým razítkům

Součástí archivační procedury je i vydání časového razítka na digitálně podepsaná data. Časové razítko vydává TSA.

5.5.6 Systém sběru archivace (interní či externí)

Systém sběru archivace je ve vztahu k CA interní. Archivní záznamy se ukládají na místě, které určí CA, případně vedoucí CA MF ČR.

5.5.7 Procedury k ověřování archivované informace

Integrita archivovaných záznamů se ověřuje prostřednictvím veřejného klíče příslušného k privátnímu klíči, který byl použit pro podepsání záznamů. CA je odpovědná za uschování odpovídajícího certifikátu.

Přístup do archívu mají pouze oprávněné osoby jmenované vedením CA MF ČR.

5.6 Výměna klíče

.

V případě změny vlastního nadřízeného certifikátu CA zveřejní nový certifikát na webových stránkách MF ČR a na stránkách CA_Intermediate. Registrovaným uživatelům CA_Local zašle upozornění o platnosti nového certifikátu.

5.7 Odhalení kompromitací a nehod

5.7.1 Zneplatnění certifikátu CA

V případě zneplatnění veřejného klíče CA používaného k ověřování podepsaných certifikátů a CRL informuje o této skutečnosti CA 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 CA 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 CA v souladu s havarijním plánem obnovy.

V případě, kdy došlo k poškození serveru pro vytváření podpisů vydávaných certifikátů a CRL, je toto zařízení nahrazeno záložním počítačem. Pevný disk záložního počítače se před použitím naformátuje. Do záložního počítače je poté nainstalován serverový operační systém a zaveden privátní klíč CA 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 CA sloužícího pro podepisování vydávaných certifikátů a CRL je CA povinna neprodleně zneplatnit příslušný vlastní nadřízený certifikát. O této skutečnosti informuje bezodkladně na stránkách MF ČR a informuje vedoucího CA MF ČR. Vlastníky certifikátů, jejichž důvěryhodnost byla uvedenou kompromitací dotčena CA vyzve neprodleně k podání žádosti o vystavení nového certifikátu.

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 CA

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 CA:

- zpřístupnění informace o ukončení své činnosti všem stranám spoléhajícím na certifikát, držitelům a jiným stranám, se kterými má smluvní nebo jiné obdobné vztahy týkající se poskytování certifikačních služeb,
- ukončí vydávání certifikátů,
- uchování údajů získaných při registraci a záznamů událostí po dobu, nejméně 10 let pro osobní a serverové certifikáty, předáním nadřízené CA (pokud taková existuje), v opačném případě v takové situaci určenému orgánu MF ČR.
- prokazatelně zničí svůj privátní klíč určený pro podepisování vydaných certifikátů a CRL,
- podle pokynů vedení CA MF ČR převede platné certifikáty pod následnickou organizaci, nebo je na pokyn vedení CA MF ČR zneplatní.

6 Technická bezpečnost

6.1 Generování párových klíčů a instalace

Párové klíče tj. vzájemně svázaná dvojice privátního klíče (tj. dat pro vytváření digitálního podpisu) 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 určené k autentizaci a podepisování prostřednictvím čipové karty se zásadně generují přímo na čipové kartě, ze které nelze privátní klíč exportovat. Tím je zaručena podmínka, že výhradní kontrolu nad použitím privátního klíče bude mít pouze vlastník příslušné čipové karty. Použité čipové karty mají FIPS 140 – 2 level 3 certifikát. V případě, že vystavený certifikát slouží k šifrování je vyexportován i příslušný privátní klíč, který je uložen v zašifrovaném stavu ve skladech CA_Local a CA_Intermediate. Párové klíče pro aplikace a souborové šifrování EFS jsou generovány na příslušných PC a privátní klíče jsou uloženy na pevných discích.

V případě, že se jedná o certifikát určený k podepisování a autentizaci (případně certifikát určený k autentizaci do VPN) prostřednictvím mobilního zařízení, nemusí být splněna podmínka neexportovatelnosti privátních klíčů a samotná generace klíčů nemusí proběhnout v tomto zařízení, je možné klíče vygenerovat mimo zařízení a posléze i s certifikátem do zařízení importovat.

Generování párových klíčů pro nadřízené certifikáty je popsáno v příslušných CPS.

6.1.2 Doručení privátního klíče jeho vlastníku

Privátní klíč uložený v nově vydané čipové kartě je osobně předán držiteli certifikátu na registrační autoritě. V případě privátních klíčů souvisejících s následnými certifikáty jsou tyto generovány na čipové kartě nebo počítači, takže je má je má žadatel k dispozici.

V případě certifikátů pro mobilní zařízení je privátní klíč spolu s certifikátem předán uživateli v šifrovaném souboru formátu P12 (PFX) a příslušné jednorázové heslo k dešifraci je zasláno prostřednictvím SMS.

6.1.3 Doručení veřejného klíče k CA

Veřejný klíč žadatele o první nový certifikát určený k autentizaci nebo podepisování je v případě vydávání nové čipové karty doručen na CA_Local pomocí zprávy digitálně podepsané pracovníkem RA. V dalších případech je doručen v žádosti žadatele o certifikát, která je zabezpečena pomocí stávajícího privátního klíče žadatele.

Doručování veřejného klíče k vydávající CA v případě nadřízených certifikátů je popsáno v příslušných CPS.

6.1.4 Doručení veřejného klíče CA uživatelům

Nadřízený certifikát veřejného klíč CA_Local je každému žadateli o vydání čipové karty fyzicky vydán při jeho osobním přebírání čipové karty na RA. Obdobně jsou na čipovou kartu uloženy i nadřízené certifikáty z celé certifikační cesty.

V případě mobilních zařízení jsou uživateli certifikáty příslušných CA předány elektronickou cestou.

Dalším spoléhajícím stranám jsou tyto nadřízené certifikáty doručeny elektronickou cestou.

6.1.5 Velikost klíčů

CA MF ČR používá nejprověřenější klasický asymetrický šifrový algoritmus – RSA. Mohutnost (=velikost) směnných prvků (klíčů) použitých pro podepisování certifikátů je stanovena na 2048 bitů. Mohutnost klíčů na straně uživatelů je stanovena na 1024 bitů nebo větší.

6.1.6 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.

6.1.7 Možná použití veřejného klíče

Veřejný klíč obsažený v certifikátu vydaném CA_Local lze používat ve shodě s ISO/IEC 9594-8 k následujícím činnostem:

1. Pro ověřování digitálních podpisů mimo případy popsané v 2.
2. Pro účely neodmítnutelnosti odpovědnosti podepisujícího subjektu s výjimkou odpovědnosti za podepsání certifikátu a podepsání CRL.
3. Pro zašifrování klíčů nebo jiných směnných prvků, např. pro jejich přenos
4. Pro šifrování uživatelských dat mimo případů popsaných v 3.
5. Jako klíč do algoritmu ustanovení sdíleného tajemství, např. pro generování klíče pro spojení pomocí symetrické šifry (protokol: dohoda pomocí asymetrické šifry)

6. Pouze pro šifrování jako klíč v protokolu dohody pomocí asymetrické šifry. Je to v případech, kdy jsou data pro ověřování elektronických podpisů určena pro protokol dohody podle asymetrické šifry – dle 5.
7. Pouze pro dešifrování jako klíč v protokolu dohody pomocí asymetrické šifry. Je to v případech, kdy jsou data pro ověřování elektronických podpisů určena pro protokol dohody podle asymetrické šifry – dle 5.

Veřejný klíč obsažený v nadřízených certifikátech vydaných CA MF ČR lze používat ve shodě s ISO/IEC 9594-8 k následujícím činnostem:

- pro účely neodmítnutelnosti odpovědnosti za podepsání certifikátu a podepsání CRL.
- pro účely neodmítnutelnosti odpovědnosti za vystavení časového razítka.

6.2 Ochrana privátních klíčů CA

Otázky ochrany privátních klíčů příslušných k nadřízeným certifikátům jednotlivých úrovňových CA, 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 příslušných CPS a Bezpečnostní politice CA.

6.3 Další požadavky na správu párových klíčů

6.3.1 Archivace veřejných klíčů

Veřejné klíče CA jsou nezbytné pro důvěryhodnost a ověřování platnosti certifikátů a CRL vydaných CA. Tato data jsou obsažena v nadřízených certifikátech CA. Na rozdíl od jím příslušných privátních klíčů je důležité tato data archivovat pro případ následné kontroly pravosti vydaných certifikátů. Nadřízené certifikáty CA jsou archivovány vypálením na CD-ROM a po ověření čitelnosti uloženy ve dvou geograficky oddělených místech. CA 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 certifikátů a CRL vydávaných CA_Root je 15 let. Platnost dat určených k ověřování podepsaných certifikátů a seznamů CRL je dána platností vydaných kořenových nadřízených certifikátů CA_Root, která se řídí výše uvedeným schématem životnosti dat určených k podepisování certifikátů a seznamů CRL.

Platnost certifikátů vydaných pro CA_Intermediate je 10 let. Tím je rovněž definována platnost příslušných párových klíčů.

Platnost certifikátů vydaných pro CA_Local a TSA je 5 let. Tím je rovněž definována platnost příslušných párových klíčů.

Platnost certifikátů vydaných CA_Local je 2 roky. Tím je rovněž definována platnost příslušných párových klíčů.

Platnost certifikátů vydaných CA_Test je 3 měsíce. Tím je rovněž definována platnost příslušných párových klíčů.

6.4 Aktivační data

Problematika aktivačních dat je popsána v jednotlivých CPS.

6.5 Bezpečnost počítačového vybavení

Otázky bezpečnosti počítačového vybavení CA MF ČR jsou popsány v příslušných CPS a Bezpečnostní politice CA.

6.6 Technické podmínky v době životnosti

Technické podmínky v době životnosti jsou popsány v příslušných CPS.

6.7 Podmínky bezpečnosti počítačové sítě

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

6.8 Časová razítka

Použití časových razítek v rámci CA MF ČR je popsáno v příslušných CPS.

7 Certifikační profily a profily CRL

7.1 Profil certifikátu

Profily certifikátu jsou podle RFC 3280.

7.1.1 Čísla verzí

Všechny certifikáty vydávané CA MF ČR jsou X.509 verze 3.

7.1.2 Položky certifikátů

Položky kořenových nadřízených certifikátů vydávaných CA_Root :

- délka klíče: 2048 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN : Ministerstvo financi - CA Root
- položka O : MFCR
- položka C : CZ
- položka BasicConstraints : critical CA:TRUE
- platnost klíče: 15 let
- položka použití klíče: digital Signature, CertificateSign, CRLSign

Položky nadřízeného certifikátu vydaného CA_Root pro CA_Intermediate:

- délka klíče: 2048 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN : Ministerstvo financi - CA IM
- položka O : MFCR
- položka C : CZ
- položka BasicConstraints : critical CA:TRUE
- platnost klíče: 10 let
- položka použití klíče: digital Signature, CertificateSign, CRLSign

Položky nadřízených certifikátů vydávaných CA_Intermediate pro CA_Local:

- délka klíče: 2048 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,

- položka CN : Ministerstvo financi - CA /*název lokality*/
- položka O : MFCR
- položka C : CZ
- položka BasicConstraints : critical CA:TRUE
- platnost klíče: 5 let
- položka použití klíče: digital Signature, CertificateSign, CRLSign

Položky nadřízených certifikátů vydávaných CA_Intermediate pro CA Test:

- délka klíče: 2048 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN : Ministerstvo financi – CA Test
- položka O : MFCR
- položka C : CZ
- položka BasicConstraints : critical CA:TRUE
- platnost klíče: 5 let
- položka použití klíče: digital Signature, CertificateSign, CRLSign

Položky nadřízeného certifikátu vydávaného CA_Intermediate pro pro TSA:

- délka klíče: 2048 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN : Ministerstvo financi - TSA
- položka O : MFCR
- položka C : CZ
- platnost klíče: 5 let
- položka použití klíče: critical digital Signature, NonRepudation, Key Encipherment, Data Encipherment
- položka rozšířeného použití klíče: TimeStamping

Položky osobních certifikátů pro autentizaci a podepisování vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN
    - testovací CA : Titul Jméno Příjmení (TEST!)

    - ostatní CA_Local : Titul Jméno Příjmení
- položka O : MFCR
- položka C : CZ
- položka OU: dle organizační jednotky
- položka T: služební identifikační číslo
- alternativní jméno předmětu
    - položka E: e-mailová adresa žadatele
    - položka UPN: jméno uživatele pro přihlašování
- platnost klíče vydaného:
    - CA_Local je 2 roky
    - testovací CA je 3 měsíce
- položka použití klíče: digital Signature
- položka rozšířené použití klíče: E-mail Protection, TLS Web Client Authentication, Microsoft Smartcardlogin

Pokud osobní certifikát určený pro autentizaci a podepisování obsahuje v položce rozšířené použití klíče OID 1.2.203.6947.2.3.1.1.1 je tento certifikát použit aplikací ADIS jako přihlašovací do této aplikace.

Položky osobních certifikátů pro autentizaci a podepisování v mobilních zařízeních vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN
    - testovací CA : Titul Jméno Příjmení (TEST!)
    - ostatní CA_Local : Titul Jméno Příjmení
- položka O : MFCR
- položka C : CZ
- položka OU: dle organizační jednotky
- položka T: služební identifikační číslo
- alternativní jméno předmětu
    - položka E: e-mailová adresa žadatele
    - položka UPN: jméno uživatele pro přihlašování
- platnost klíče vydaného:
    - CA_Local je 2 roky
    - testovací CA je 3 měsíce

- položka použití klíče: digital Signature
- položka rozšířené použití klíče: E-mail Protection, Client Authentication

Položky osobních certifikátů pro autentizaci mobilních zařízeních do VPN vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN
  - testovací CA : Osobní číslo uživatele (TEST!)
  - ostatní CA_Local : Osobní číslo uživatele
- položka O : MFCR
- položka C : CZ
- položka OU: dle organizační jednotky
- alternativní jméno předmětu
  - položka E: e-mailová adresa žadatele
  - položka UPN: jméno uživatele pro přihlašování
- platnost klíče vydaného:
  - CA_Local je 2 roky
  - testovací CA je 3 měsíce
- položka použití klíče: digital Signature
- položka rozšířené použití klíče: Client Authentication

Položky osobních certifikátů pro šifrování vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN
  - testovací CA : Titul Jméno Příjmení (TEST!)
  - ostatní CA_Local : Titul Jméno Příjmení
- položka O : MFCR
- položka C : CZ
- položka OU: dle organizační jednotky
- položka T: služební identifikační číslo
- alternativní jméno předmětu
  - položka E: e-mailová adresa žadatele

    - položka UPN: jméno uživatele pro přihlašování
- platnost klíče vydaného:
    - CA_Local je 2 roky
    - testovací CA je 3 měsíce
- položka použití klíče: Key Encipherment
- položka rozšířené použití klíče: E-mail Protection, Microsoft Encrypted File System

Položky osobních certifikátů pro ověřování softwarového kódu vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN
    - testovací CA : Titul Jméno Příjmení (TEST!)
    - ostatní CA_Local : Titul Jméno Příjmení
- položka O : MFCR
- položka C : CZ
- položka OU: dle organizační jednotky
- položka T: služební identifikační číslo
- alternativní jméno předmětu
    - položka E: e-mailová adresa žadatele
    - položka UPN: jméno uživatele pro přihlašování
- platnost klíče vydaného:
    - CA_Local je 2 roky
    - testovací CA je 3 měsíce
- položka použití klíče: digital Signature
- položka rozšířené použití klíče: E-mail Protection, TLS Web Client Authentication, Microsoft Smartcardlogin, id-kp-codeSigning (OID 1.3.6.1.5.5.7.3.3)

Položky certifikátů aplikace doménového řadiče vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN : dle doménového řadiče
- položka O : MFCR

- položka C : CZ
- položka BasicConstrains : CA:FALSE
- platnost klíče: 1 rok
- položka použití klíče: digital Signature, Key Encipherment
- položka rozšířené použití klíče: TLS Web Client Authentication, TLS Web Server Authentication, Microsoft Smartcardlogin
- položka alternativní jméno: critical

Položky certifikátů aplikace serveru vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN
  - testovací CA : Dle serveru, musí končit řetězcem (TEST!)
  - ostatní CA_Local : Dle serveru
- položka O : MFCR
- položka C : CZ
- položka BasicConstrains : CA:FALSE
- platnost klíče vydaného:
  - CA_Local je 2 roky
  - testovací CA je 3 měsíce
- položka použití klíče: digital Signature, Key Encipherment
- položka rozšířené použití klíče: TLS Web Server Authentication

Položky certifikátů obecné aplikace vydávaných CA_Local:

- délka klíče: minimálně 1024 bitů,
- položka PublicKeyAlgorithm : rsaEncryption,
- položka SignatureAlgorithm: sha1withRSA,
- položka CN
  - testovací CA : dle potřeby, musí končit řetězcem (TEST!)
  - ostatní CA_Local : dle potřeby
- položka CN : dle potřeby
- položka O : MFCR
- položka C : CZ
- položka BasicConstrains : CA:FALSE

- platnost klíče vydaného:
  - CA_Local je 2 roky
  - testovací CA je 3 měsíce
- položka použití klíče: dle potřeby
- položka rozšířené použití klíče: dle potřeby

7.1.3 Identifikátory algoritmů

Certifikáty vydávané CA MF ČR podle této CP používají standardně užívaná OID. Podle této CP je používáno:

Signature Algorithm: sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)

7.1.4 Formy jmen

Položka certifikátu SUBJECT může obsahovat následující položky:

- Stát (countryName);
- Obecné Jméno (commonName);
- Příjmení (surname);
- Křestní Jméno (givenName);
- Firma (organizationName);
- Útvar ve firmě (organizationalUnitName);
- Služební identifikační číslo (title)
- Oblast (stateOrProvinceName);
- Město (localityName);
- Adresa (postalAddress).

Položka SUBJECT musí obsahovat položky uvedené v odstavci 7.1.2 Ostatní položky jsou nepovinné.

Položka Služební identifikační číslo obsahuje služební identifikační číslo žadatele. Tato položka (pokud je použita) není ovlivnitelná žadatelem – slouží k zajištění jednoznačnosti položky SUBJECT.

7.1.5 Omezující pravidla na jména

Jediná použitelná jména jsou uvedena v odstavci 7.1.2 .

7.1.6 Identifikátory CP

Tato certifikační politika je ve vztahu k CA_Root a CA_INTERMEDIATE identifikovatelná následujícím OID: 1.2.203.6947.2.1.1.1.1

Ve vztahu k vydávacím certifikačním autoritám CA_LOCAL lze tuto certifikační politiku lze identifikovat podle následujících OID v závislosti na lokalitě, v níž je umístěna certifikační autorita:

Obecné jméno vydávací certifikační autority	OID
Ministerstvo financi - CA Urad	1.2.203.6947.2.1.2.1.1
Ministerstvo financi - CA Test	1.2.203.6947.2.1.3.1.1
Ministerstvo financi - CA FR Praha mesto	1.2.203.6947.2.1.4.1.1
Ministerstvo financi - CA Celni sprava	1.2.203.6947.2.1.5.1.1
Ministerstvo financi - CA FR v Praze	1.2.203.6947.2.1.6.1.1
Ministerstvo financi - CA FR v Ceskych Budejovicich	1.2.203.6947.2.1.7.1.1
Ministerstvo financi - CA FR v Plzni	1.2.203.6947.2.1.8.1.1
Ministerstvo financi - CA FR v Hradci Kralove	1.2.203.6947.2.1.9.1.1
Ministerstvo financi - CA FR v Ostrave	1.2.203.6947.2.1.10.1.1
Ministerstvo financi - CA FR v Brne	1.2.203.6947.2.1.11.1.1
Ministerstvo financi - CA FR v Usti nad Labem	1.2.203.6947.2.1.12.1.1
Ministerstvo financí – CA Generalni financni reditelstvi	1.2.203.6947.2.1.13.1.1

7.1.7 Použití rozšíření pro omezení politiky

Tyto skutečnosti nejsou relevantní pro tuto CP.

7.1.8 Syntaxe a sémantika pro kvalifikátory politiky

Syntaxe a sémantika pro kvalifikátory politiky se řídí RFC 3280 – kap 4.2.1.5.

7.1.9 Sémantika pro rozhodující rozšíření vztahující se k CP

Sémantika pro rozhodující rozšíření vztahující se k CP není kritická.

7.2 Profil CRL

Profil CRL je podle RFC 3280.

7.2.1 Čísla verzí

CRL jsou vydávány ve verzi 2 podle X.509.

7.2.2 CRL a rozšíření položek CRL

CRL vydávají jednotlivé CA pouze pro certifikáty vydané těmito CA. CRL je vždy vydáváno v úplném rozsahu, vydávání delta CRL není touto CP podporováno. Kromě povinných položek může CRL obsahovat i rozšířené položky:

- Číslo veřejného klíče vydávající CA - položka je obsažena ve všech vydaných CRL, položka je kritická
- Alternativní jméno vydavatele CRL – položka je obsažena, položka není kritická
- Číslo CRL - položka je obsažena, položka není kritická
- Indikátor delta CRL - položka není obsažena, vydávání delta (přírůstkových) CRL není touto CP podporováno
- Vydávací distribuční bod - položka je obsažena, položka je kritická
- Delta CRL distribuční bod - položka není obsažena
- Kód důvodu zneplatnění - položka není obsažena
- Kód instrukce pro zjištění platnosti - položka není obsažena
- Datum kompromitace privátního klíče - položka není obsažena
- Vydavatel certifikátu - položka není obsažena, protože vydavatel CRL je stejný jako vydavatel certifikátu

7.3 Profil OCSP

OCSP není touto CP podporováno.

8 Audit

Audit má za úkol vyhodnotit shodu činnosti konkrétního subjektu v rámci CA MF ČR s CP, příslušnou CPS a dalšími dokumenty, které upravují činnost subjektu. Výstupem auditu je hodnotící zpráva a seznam doporučení, která vedou k nápravě případných nedostatků.

Frekvence provádění auditu je

- 1 x ročně interní audit
- 1 x za 3 roky hloubkový audit nadřízeným orgánem MF ČR
- nepravidelný audit dle rozhodnutí vedoucího CA MF ČR

Další podrobnosti

- 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 příslušných CPS.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

Tyto skutečnosti nejsou relevantní pro tuto CP.

9.2 Finanční odpovědnost

Tyto skutečnosti nejsou relevantní pro tuto CP.

9.3 Důvěrnost obchodních informací

Tyto skutečnosti nejsou relevantní pro tuto CP.

9.4 Důvěrnost osobních informací

9.4.1 Systém ochrany osobních údajů

Systém ochrany osobních údajů je definován ve speciálních směrnicích platných pro celé Ministerstvo financí ČR.

9.4.2 Typy chráněných osobních informací

Chráněnými osobními informacemi CA_Local a příslušných RA jsou veškeré osobní údaje uživatelů podléhající ochraně ve smyslu příslušné zákonné normy – zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů.

9.4.3 Typy osobních informací nepovažovaných za citlivé

Osobní informace nepovažované za citlivé jsou zejména informace pracovního charakteru jako čísla služebních telefonů, názvy funkcí, služební e-mailové adresy o pod., pokud nejsou jiným platným interním předpisem MF ČR explicitně považována za citlivé.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů odpovídají pracovníci, kteří s těmito údaji přímo pracují a dále správce CA_Local.

9.4.5 Případy zpřístupnění osobních údajů

Případy zpřístupnění chráněných osobních údajů jsou

- Žádost odpovědných pracovníků MF ČR v rozsahu jejich pravomocí
- Žádost soudu
- Žádost orgánu činného v trestním řízení

9.4.6 Zpřístupnění osobních údajů orgánům činným v trestním řízení

CA_Local poskytne informace obsahující chráněné osobní údaje třetí straně pouze na základě rozhodnutí soudu. Dále CA_Local poskytne chráněné osobní údaje orgánům činným v trestním řízení pouze na základě rozhodnutí příslušného státního zástupce, a to pouze na základě písemné žádosti vybavené všemi náležitostmi.

9.4.7 Ostatní okolnosti zpřístupnění osobních údajů

Chráněné osobní údaje lze zpřístupnit pouze v případech uvedených v odstavci 9.4.5.

9.5 Duševní vlastnictví

Tato CP 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 CA

CA MF ČR poskytuje u certifikátů vydaných podle této CP záruky na:

- Jednoznačnost sériového čísla vydaných certifikátů,
- Kryptografickou odolnost použitých algoritmů pro výpočet hash a digitálního podpisu,
- Správné použití privátních klíčů příslušných k vydaným nadřízeným certifikátům,
- Vydávání pouze těch certifikátů, které jsou popsány v této CP,

- Vztah mezi držitelem privátního klíče a subjektem uvedeným v certifikátu obsahujícím veřejný klíč který je příslušný k podepisovacímu privátnímu klíči,
- Shodu identifikačních údajů uvedených v žádosti o vydání certifikátu s těmito údaji obsaženými ve vydaném certifikátu,
- Časové limity uvedené v této CP na vydání CRL,
- Přístup ke skladům vydaných certifikátů a CRL,
- Bezpečnost osobních údajů o uživatelích, které byly využity pro vydání osobních certifikátů.

CA MF ČR neposkytuje žádné finanční záruky.

Veškeré záruky je možné uznat jen tehdy, pokud uživatel neporušil povinnosti plynoucí z této CP.

Na používání certifikátu mimo pracovní účely v rámci MF ČR se záruky nevztahují.

9.6.2 Zajištění a záruky RA

RA ručí za to, že všechny žádosti o vydání osobních certifikátů, certifikátů pro aplikace a testovacích certifikátů jí předložené, budou zpracovány a vyhodnoceny podle příslušné platné CP. Rovněž RA ručí, že všechny žádosti o zneplatnění certifikátu jí předložené, budou zpracovány a vyhodnoceny podle této CP. RA ručí za to, že identifikační údaje žadatele uvedené v žádosti o vydání certifikátu jsou shodné s identifikačními údaji, které žadatel RA předložil.

9.6.3 Zajištění a záruky vlastníků certifikátů

Vlastník certifikátu zaručuje, že jeho identifikační údaje uvedené v certifikátu jsou pravdivé. Rovněž musí zajistit svou bezvýhradní kontrolu nad použitím privátního klíče příslušného k danému certifikátu určenému k digitálnímu podepisování a autentizaci.

Vlastník certifikátu vydaného testovací CA ručí za to, že bezprostředně po zániku potřeby používat daný testovací certifikát zajistí jeho zneplatnění a rovněž za to, že daný certifikát bude použit výhradně v testovacím prostředí.

9.6.4 Zajištění a záruky spoléhající strany

Spoléhající strana zaručuje, že v případech, kdy k jejímu dalšímu jednání je potřebné ověření digitálního podpisu pomocí certifikátu, provede po kladném výsledku ověření daného digitálního podpisu akce v souladu s deklarovaným dalším svým jednáním.

9.6.5 Zajištění a záruky ostatních účastníků

Tato CP nedefinuje požadavky na zajištění a záruky ostatních subjektů.

9.7 Zmocněnecké vztahy

Vztah mezi CA MF ČR jakožto poskytovatelem certifikačních služeb a osobami využívajícími jeho služby je v rozsahu definovaném touto CP. CA MF ČR nevystupuje v žádném případě jako zmocněnec nebo jiný zástupce uživatelů svých služeb.

9.8 Limity záruk

Tyto skutečnosti nejsou relevantní pro tuto CP.

9.9 Kompenzace ze strany vlastníků certifikátů a uživatelů

Tyto skutečnosti nejsou relevantní pro tuto CP.

9.10 Lhůty a zánik platnosti CP

9.10.1 Lhůty platnosti

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

9.10.2 Zánik platnosti

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

9.10.3 Důsledky zániku platnosti

V případě jakýchkoliv změn, které mají za následek neplatnost některého z článků této CP, ostatní články zůstávají v platnosti do vydání nové CP. Do té doby se bude rovněž vymáhat odpovědnost za dodržování této CP 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 za účelem poskytování certifikačních služeb je popsána v příslušných odstavcích. Obecná zásada je, že

jde buď o komunikaci přímou nebo komunikaci dálkovou. Při dálkové komunikaci se uvažuje vesměs používání digitálně podepsaných e-mailových zpráv.

9.12 Změny v CP

9.12.1 Postup provádění změn

V době platnosti CP mohou navrhovat změny v CP správci jednotlivých CA a osoby uvedené v odstavci 1.5.3. 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, a takto upravená CP je publikována stejným způsobem jako předchozí verze CP.

9.12.3 Okolnosti za kterých se mění OID

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

9.13 Řešení případných neshod

Právo výkladu této Certifikační politiky 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. Odpovědný pracovník RA
2. Správce CA_Local
3. Vedoucí CA MF ČR
4. Ředitel odboru 33 MF ČR

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

9.14 Právní výkon

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

9.15 Soulad s platnými zákony

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

9.16 Různá smluvní ustanovení

9.16.1 Integrační doložka

Tyto skutečnosti nejsou relevantní pro tuto CP.

9.16.2 Doložka převoditelnosti práv a povinností

Tato CP neumožňuje převod práv a povinností plynoucích z této CP na jiný subjekt.

9.16.3 Doložka o oddělitelnosti jednotlivých článků smlouvy

Tyto skutečnosti nejsou relevantní pro tuto CP.

9.16.4 Doložka o soudním řešení sporů

V případě sporů, které nelze vyřešit prostředky uvedenými v této CP a dotýkají se zájmů chráněných zákonnými předpisy, je jejich řešení přezkoumatelné soudy.

9.16.5 Doložka pro případy vzniklé působením vyšší moci

Jednání v situacích vzniklých vyšší mocí jako války, teroristické akce, státní převraty, globální přírodní katastrofy je v této CP uvažováno pro případ uvedený v odstavci 5.8. Dalšími aspekty dopadů situací vzniklých vyšší mocí se zabývá plán pro zvládání krizových situací a plán obnovy CA

9.17 Závěrečné ustanovení

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