Akreditovaná certifikační autorita e-Identity

D10.2 Certifikační politika - QSC

Verze:	1.1
Odpovídá:	Jiří Hejl
Datum:	25.8.2005
Utajení:	Veřejný dokument

Schváleno:

Verze	Schválil	
1.1	Ladislav Šedivý	

Historie dokumentu:

Verze	Datum	Autor	Poznámka
1.0	20.02. 2005	Jiří Hejl	komplexní verze
1.1	25.8. 2005	Jiří Hejl	zjednodušení poskytovaných služeb, konsolidace pojmů, rejstřík zkratek

OBSAH

1 ÚVOD

Tato Certifikační politika pro kvalifikované systémové certifikáty obsahuje zásady a postupy související se zajištěním činnosti akreditovaného poskytovatele certifikačních služeb podle zákona č. 227/2000 Sb. a předpisů souvisejících.

Tato Certifikační politika stanovuje zásady, které poskytovatel certifikačních služeb uplatňuje při zajišťování kvalifikovaných certifikačních služeb:

- vydání kvalifikovaného systémového certifikátu,
- vydání následného kvalifikovaného systémového certifikátu.

Pojem kvalifikovaný systémový certifikát je popsán v zákoně 227/2000 Sb. a využívá se k ověření elektronické značky fyzické osoby, právnické osoby nebo organizační složky státu.

Tato Certifikační politika je určena žadatelům o poskytnutí výše vyjmenované služby, všem spoléhajícím se stranám a jiným účastníkům PKI.

Tato Certifikační politika nevyžaduje na straně označující osoby používání prostředku pro bezpečné vytváření elektronických značek.

Struktura tohoto dokumentu vychází z dokumentu RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Systém ACAeID je budován a provozován ve shodě s právním prostředím České republiky.

1.1 Přehled

Postupy, pravidla, technologie a ostatní skutečnosti popsané v této CP dokladují důvěryhodnost a integritu řešení ACAeID při poskytování certifikačních služeb a to po celou dobu životního cyklu certifikátů či jiných produktů, poskytovaných provozovatelem.

Informace o dalších provozovaných službách jsou popsány v jejich projektové dokumentaci, jejich Certifikačních politikách a na internetových stránkách provozovatele.

Zajištění bezpečného provozovaní všech kvalifikovaných certifikačních služeb je popsáno v Certifikační prováděcí směrnici – QS.

Ve veřejné části webového prostoru provozovatele jsou umístěny informace, které umožní zájemci či žadateli kvalifikovaně se rozhodnout o poskytovaných službách, svých povinnostech a právech. K dispozici mu je také tato Certifikační politika a další dokumenty.

1.2 Název a identifikace dokumentu

Český normalizační institut přidělil společnosti eIdentity a.s. OID ve tvaru 1.2.203.27112489.

Podtřída 1.2.203.27112489.1. je interně určena pro dokumentaci ACAeID, její další členění je určeno číslem dokumentu a jeho verzí, tedy např. 10.2.1.1 značí dokument D10.2 ve verzi 1.1.

Tato Certifikační politika - QSC má tyto identifikační znaky:

Identifikační znak	Význam identifikačního znaku	Hodnota
Název dokumentu	Název dokumentu v čitelné podobě	Certifikační politika ACAeID - QSC
OID	Identifikace dokumentu v rámci prostoru OID eIdentity a.s.	1.2.203.27112489.1.10.2.1.1

1.3 Subjekty participující na PKI

1.3.1 Certifikační autority

ACAeID eIdentity a.s. tvoří kořenová autorita (RCA) a autorita vydávající kvalifikované certifikáty pro podepisující a označující osoby (QCA). Kořenová autorita RCA vydává certifikáty pouze podřízeným certifikačním autoritám a vydala tedy i kvalifikovaný systémový certifikát pro vydávající certifikační autoritu QCA.

Tato vydávající autorita QCA nevydává certifikáty pro žádné podřízené certifikační autority, ale jen jednotlivým žadatelům.

Společnost eIdentity a.s. provozuje i další certifikační autority, které se řídí svými Certifikačními politikami a provozními předpisy.

1.3.2 Registrační autority

Jako Registrační autority pracují důvěryhodní Operátoři registračního místa, kteří provádějí proces ověření skutečností nutných pro vydání certifikátu, případně přijímají žádost o zneplatnění certifikátu. S každým Operátorem registračního místa je uzavřena Smlouva o činnosti, operátoři jsou pravidelně školeni a kontrolováni. Operátorem se může stát pouze osoba, která dosáhla určitých kvalit a splnila kvalifikační předpoklady.

1.3.3 Držitelé kvalifikovaných certifikátů –označující osoby

Označující osobou se stává každá fyzická osoba, právnická osoba nebo organizační složka státu, která je využívá prostředku pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou založenou na kvalifikovaném systémovém certifikátu, vydaného QCA podle zákona 227/2000 Sb.

1.3.4 Spoléhající se strany

Spoléhající se stranou je každý jedinec nebo skupina, která využívá kvalifikovaných systémových certifikátů vydaných QCA a/nebo elektronických značek s nimi souvisejících.

1.3.5 Jiní účastníci

Další účastníci jsou orgány dozoru podle zákona 227/2000 Sb. a orgány činné v trestním řízení, případně další orgány, kterým to ze zákona přísluší.

1.4 Použití certifikátu

Kvalifikované systémové certifikáty vydané podle této Certifikační politiky se mohou použít jen k účelům, které stanovuje zákon 227/2000 Sb.

1.4.1 Přípustné použití certifikátu

Typickými aplikacemi, které je možné použít v souvislosti s kvalifikovanými systémovými certifikáty, vydávanými podle této politiky, jsou aplikace umožňující vytvářet a ověřovat elektronické značky jako například systémy elektronické pošty, podepisovací a ověřovací aplikace pro elektronické značkování (tj. vytváření elektronických značek podle zákona 227/2000Sb.) dokumentů a jiných typů souborů obecně, pokud jsou v souladu s požadavky zákona 227/2000 Sb.

1.4.2 Nepřípustné použití certifikátu

Kvalifikované systémové certifikáty se nesmí používat v rozporu s účelem, ke kterému byly vydány a to jak z technického hlediska (např. podle omezení KeyUsage) tak i z právního hlediska (např. v rozporu se zákonem 227/2000 Sb.).

Takovým nepřípustným použitím kvalifikovaného systémového certifikátu může být například jeho použití pro šifrování či identifikaci účastníka šifrované komunikace v prostředí protokolu SSL/TLS.

1.5 Správa politiky

Za údržbu tohoto dokumentu odpovídá předseda Výboru pro politiky.

1.5.1 Organizace spravující dokument

eIdentity a.s.
Vinohradská 184
130 00 Praha 3

Česká republika

1.5.2 Kontaktní osoba

Předseda Výboru pro politiky
eIdentity a.s.
Vinohradská 184
130 00 Praha 3
Česká republika

Tel: +420 222 866 150
Fax: +420 222 866 190
Email: PAA-manager@acaeid.cz

1.5.3 Subjekt odpovědný za rozhodování o souladu dokumentace

Soulad Certifikační politiky s jí odpovídající Certifikační prováděcí směrnicí schvaluje Výbor pro politiky na základě schůze Výboru a v souladu s jednacím řádem tohoto orgánu.

1.5.4 Postupy schvalování

Postupy jsou určeny jednacím řádem Výboru pro politiky.

1.6 Přehled použitých pojmů a zkratek

Zákon	Zákon 227/2000 Sb. o elektronickém podpisu
ACAeID, ACA	Informační systém eIdentity a.s., poskytující kvalifikované certifikační služby
RCA	Kořenová certifikační autorita, jako součást ACAeID
QCA	Vydávající certifikační autorita, jako součást ACAeID
RM	Registrační místo
ORM	Operátor registračního místa
CP	Certifikační politika
CPS	Certifikační prováděcí směrnice
QC	Kvalifikovaný certifikát
QSC	Kvalifikovaný systémový certifikát
RQSC	Kořenový kvalifikovaný systémový certifikát
CRL	Seznam zneplatněných certifikátů
poskytovatel, PCS	Poskytovatel certifikačních služeb
EVI	Evidenční část informačního systému PCS
soukromý klíč	Data pro vytváření elektronických podpisů nebo značek
veřejný klíč	Data pro ověřování elektronických podpisů nebo značek
revokace	zneplatnění certifikátu
DN	Distinguished Name – Jednoznačná identifikace držitele certifikátu

2 ODPOVĚDNOST ZA PUBLIKOVÁNÍ A ÚLOŽIŠTĚ

QCA zveřejňuje seznam vydaných kvalifikovaných certifikátů a seznam zneplatněných certifikátů včetně kvalifikovaných systémových certifikátů.

Každý žadatel o poskytnutí služby či označující osoba má navíc přístup do svého místa u provozovatele, kde má k dispozici seznam všech svých poskytnutých či právě poskytovaných služeb a může jejich stav sledovat a měnit v rozsahu své autorizace v systému.

2.1 Úložiště

V informačním systému ACAeID jsou zpracovávány a uchovávány informace v souladu se zákonem 227/2000 Sb. a zákonem 101/2000 Sb. tak, aby záznamy nebo jejich změny mohly provádět pouze pověřené osoby, aby bylo možno kontrolovat správnost záznamů a aby jakékoliv technické nebo programové změny, porušující tyto bezpečnostní požadavky, byly zjevné. Zveřejňované informace jsou určeny zejména spoléhajícím se třetím stranám, aby bylo možné rozhodnout o platnosti kvalifikovaného systémového certifikátu s požadovaným stupněm důvěry.

2.2 Zveřejňování informací

K veřejným informacím je možné přistupovat pomocí webových služeb.

Vydané kvalifikované systémové certifikáty jsou zveřejněny v Seznamu vydaných kvalifikovaných certifikátů, který je dostupný na adresách

- http://www.acaeid.cz/aca/certs,
- http://pub1.acaeid.cz/aca/certs,
- http://pub2.acaeid.cz/aca/certs.

Veřejně dostupné jsou tyto položky certifikátu:

- Sériové číslo certifikátu
- Platnost od – do

U certifikátů, k jejichž zveřejnění dal držitel souhlas, jsou veřejně dostupné ještě tyto položky:

- Držitel (Subject)
- Vlastní certifikát ve formátu DER, PEM a TXT

Kvalifikované systémové certifikáty, které byly zneplatněny, jsou zveřejněny v Seznamu zneplatněných kvalifikovaných certifikátů. Aktuální seznam (poslední platný) bude dostupný (vždy nejméně na jednom místě) v elektronické formě ve formátu CRL na adresách:

- http://www.acaeid.cz/aca/crl/actual.crl
- http://pub1.acaeid.cz/aca/crl/actual.crl

- http://pub2.acaeid.cz/aca/crl/actual.crl

Součástí zveřejněných informací bude i informace o pořadí a době zveřejnění aktuálního CRL a historie zveřejněných CRL.

Informace o době zveřejnění aktuálního CRL bude poskytnuta v souboru

- http://www.acaeid.cz/aca/crl/actual-date.txt
- http://pub1.acaeid.cz/aca/crl/actual-date.txt
- http://pub2.acaeid.cz/aca/crl/actual-date.txt

a bude ve tvaru YYYYMMDDHHMMSS.

V osobním účtu Žadatele může žádající osoba získat další podrobnější informace o stavu své žádosti či o odebíraných službách. Tyto informace jsou však neveřejné a jsou dostupné jen příslušné osobě Žadatele.

Součástí veřejně dostupných informací je také dokument Certifikační politika - QSC, který je zveřejněn ve formátu PDF na adresách:

- http://www.acaeid.cz/aca/cp-qsc.pdf
- http://pub1.acaeid.cz/aca/cp-qsc.pdf
- http://pub2.acaeid.cz/aca/cp-qsc.pdf

Na této adrese je dostupná platná verze Certifikační politiky. Historie verzí je přístupná na webových stránkách provozovatele spolu s vyznačením období platnosti.

Zveřejněn na webových stránkách poskytovatele je také kvalifikovaný systémový certifikát kořenové (RCA) a vydávající (QCA) certifikační autority. Pro ověření správnosti těchto certifikátů jsou tyto také zveřejněny na stránkách Ministerstva informatiky ČR a ve Věstníku tohoto ministerstva.

Dále jsou na webových stránkách poskytovatele zveřejněny i procesní, obchodní a další pomocné informace, které se vztahují k poskytovaným službám.

2.3 Periodicita zveřejňování

Certifikační politika je schválena dříve, než je podle ní možné vydat první certifikát. Periodicita zveřejňování dalších informací není určena a závisí na nutnosti udržovat informace v aktuálním stavu. Periodicita zveřejňování CRL je popsána v kapitole 4.9.7.

2.4 Řízení přístupu k úložišti

Publikování CP schvaluje a odpovědnou osobu určuje Výbor pro politiky v souladu s jednacím řádem tohoto Výboru.

Zveřejnění a aktualizaci Seznamu vydaných kvalifikovaných certifikátů a Seznamu

zneplatněných kvalifikovaných certifikátů provádí obsluha ACAeID s frekvencí, která je v souladu s tímto dokumentem.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Kvalifikované systémové certifikáty vydávající QCA eIdentity a.s. obsahují v polích Subject a Issuer jména ve formátu podle doporučení X.501.

3.1.1.1 Vydávající certifikační autorita QCA

Položka Subject vydávající certifikační autority se sestává z komponent uvedených v následující tabulce.

Atribut	**Pravidlo vyplnění**	**Hodnota**
Country (C)	pevný text	„CZ“
Organization (O)	pevný text	„eIdentity a.s.“
Organizational Unit (OU)	pevný text	„Akreditovaný poskytovatel certifikačních služeb“
Locality (L)	pevný text	„Vinohradská 184, 130 00 Praha 3“
Common Name (CN)	pevný text	„ACAeID – Qualified Issuer Certificate (kvalifikovaný systémový certifikát vydávající CA)“

Položka Issuer vydávající certifikační autority se sestává z komponent uvedených v následující tabulce:

Atribut	**Pravidlo vyplnění**	**Hodnota**
Country (C)	pevný text	„CZ“
Organization (O)	pevný text	„eIdentity a.s.“
Organizational Unit (OU)	pevný text	„Akreditovaný poskytovatel certifikačních služeb“
Locality (L)	pevný text	„Vinohradská 184, 130 00 Praha 3“
Common Name (CN)	pevný text	„ACAeID – Qualified Root Certificate (kvalifikovaný systémový certifikát kořenové CA)“

3.1.1.2 Vydávané certifikáty

Kvalifikované systémové certifikáty žadatelů obsahují DN (Distinguished Name) v poli Subject, které se skládá z komponent v následující tabulce.

Atribut	**Význam**	**Čím se dokládá**	**Omezení**	**Hodnota – „příklad“**
Country (C)	Kód státu, kde má žadatel trvalý pobyt nebo kde má sídlo	Identifikační průkaz, cestovní pas, výpis z obchodního rejstříku, zřizovací listina apod.	podle ISO 3166	„CZ“
Organization (O)	Název organizace žadatele	Výpis z obchodního rejstříku, živnostenský list, zřizovací listina, prohlášení osoby s oprávněním za organizaci jednat. Název organizace může být doplněn o identifikační číslo, které bude uvedeno za mezerou v hranatých závorkách, uvozené IČ a mezerou	Pro osoby stojící mimo organizaci vyplní tuto položku poskytovatel. Může být vyznačena jen jedna organizace.	„eIdentity a.s. [IČ 27112489]“
Organizational Unit (OU)	Organizační jednotka	Např. prohlášením osoby s oprávněním za organizaci jednat	Certifikát uživatele může obsahovat jeden nebo více těchto atributů. Nepovinné.	„Elektronická podatelna“

Atribut	Význam	Čím se dokládá	Omezení	Hodnota – „příklad“
Locality (L)	Adresa sídla organizace pro žadatele - právnickou osobu Adresa bydliště pro žadatele - fyzickou osobu	Výpis z obchodního rejstříku, živnostenský list, zřizovací listina, prohlášení osoby s oprávněním za organizaci jednat, identifikační průkaz, cestovní pas, další uznaný osobní doklad.	Povinné.	„Vinohradská 22, 130 00 Praha 3“
Name (Name)	Celé jméno žadatele včetně případných titulů	Identifikační průkaz, cestovní pas, další uznaný osobní doklad.	Nepovinné	„JUDr. Jan Tadeáš Novák“
Given Name	Jméno označující osoby	Identifikační průkaz, cestovní pas, další uznaný osobní doklad.	Nepovinné Obsahuje jméno (jména) žadatele	„Jan Tadeáš“
Surname	Příjmení označující osoby	Identifikační průkaz, cestovní pas, další uznaný osobní doklad.	Nepovinné Příjmení žadatele	Novák
Common Name (CN)	Obsahem pole je celé jméno označující osoby.	Osobní doklad, prohlášení odpovědné osoby za organizaci.	Přenáší se Name nebo Given Name (pokud je vyplněno) a po přidané mezeře Surname	

Atribut	Význam	Čím se dokládá	Omezení	Hodnota – „příklad“
Email Address (E)	Kontaktní emailová adresa.	prohlášením majitele domény či držitele emailové adresy v případě veřejných domén	Nepovinné	jan.novak@eidentity.cz
Title (Title)	Titul či pracovní role nebo označení prostředku pro vytváření elektronických značek	Prohlášením osoby s oprávněním jednat za organizaci či dokladem nebo prohlášením žadatele	Nepovinné.	

Atribut	Význam	Čím se dokládá	Omezení	Hodnota – „příklad“
SerialNumber	Pro fyzickou osobu obsahuje údaj spravovaný ústředním orgánem státní správy, na základě kterého je možné osobu jednoznačně identifikovat uvozený zkratkou správce a pomlčkou nebo hodnotu, přidělenou poskytovatelem certifikačních služeb - v tomto případě je uvozena řetězcem QCA-nebo údaj přidělený žadateli od MPSV, uvozený řetězcem MPSV-.	Rozhodnutím o přidělení ústředním orgánem státní správy		
	Pro právnickou osobu nebo organizační složku státu obsahuje IČ organizace nebo hodnotu, přidělenou poskytovatelem certifikačních služeb - v tomto případě je uvozena řetězcem QCA-	Výpisem z obchodního rejstříku, živnostenským listem, zřizovací listinou, prohlášením osoby s oprávněním za organizaci jednat.		

3.1.2 Požadavek na sémantický význam jmen

Všechna pojmenování uvedená v DN certifikátu musí být smysluplná a doložitelná.

3.1.3 Anonymita a používání pseudonymu

QCA nevydává anonymní certifikáty. Kvalifikovaný systémový certifikát nelze ani vystavit na pseudonym.

3.1.4 Pravidla pro interpretaci různých forem pojmenování

Tam, kde to RFC3280 dovoluje, lze použít národní znakové sady v kódování UTF8.

3.1.5 Jednoznačnost jmen

QCA eIdentity zaručuje automatickou kontrolou unikátnost vazby DN v poli Subject certifikátu na jednoho konkrétního uživatele či prostředek na vytváření elektronických značek. Uživatel však může mít více certifikátů se stejným či jiným DN v poli Subject.

3.1.6 Rozpoznávání, autentizace a význam obchodních značek

Všechny údaje uvedené v kvalifikovaném systémovém certifikátu uživatele se musí prokazatelně vztahovat k jeho osobě. QCA eIdentity tuto skutečnost ověřuje. To vylučuje možnost zneužití obchodní značky třetí osoby.

3.2 Počáteční ověření identity

3.2.1 Metody důkazu vlastnictví (POP - proof of possession) soukromého klíče

Žadatel o kvalifikovaný certifikát musí prokázat vlastnictví soukromého klíče odpovídajícímu veřejnému klíči, který má být uveden v kvalifikovaném systémové certifikátu. Za prokazatelnou se považuje žádost ve formátu PKCS#10, nebo ekvivalentní metoda (např. SPKAC). Principem je předání veřejného klíče spolu s případnými dalšími daty certifikační autoritě tak, aby tento balík nebo jeho otisk byl podepsán odpovídajícím soukromým klíčem. Většinou se taková zpráva vytváří prostředky prostředí, ve kterém se klíče a kvalifikovaný systémový certifikát budou používat.

3.2.2 Prokázání identity právnické osoby

Identitu prokazuje právnická osoba předložením originálu nebo notářsky ověřené kopie výpisu z obchodního rejstříku, živnostenského listu či jiné listiny, na základě které byla organizace zřízena. Z dokladu musí být patrno úplné obchodní jméno organizace, přidělené identifikační číslo, sídlo a statutární orgán. Pro účely jednání s eIdentity a.s. může statutární orgán

zplnomocnit na základě notářsky ověřené plné moci další osobu.

3.2.3 Prokázání identity fyzické osoby

Fyzická osoba prokazuje svoji identitu platným osobním dokladem a pro účely vydání kvalifikovaného certifikátu prokazuje svoje identifikační údaje dvěma osobními doklady. Jako základní osobní doklad se přijímá Občanský průkaz u občanů ČR nebo cestovní pas u občanů jiných zemí. Jako další doklad se přijímá cestovní pas, národní identifikační průkaz cizinců nebo řidičský průkaz. Pokud nemá fyzická osoba požadované doklady vystaveny, musí o jejich vystavení požádat v souladu s právními předpisy a to v dostatečném předstihu před podáním žádosti o kvalifikovaný systémový certifikát.

3.2.4 Neověřované informace

Všechny informace uvedené v certifikátu od QCA jsou ověřené.

3.2.5 Ověřování specifických práv

V případě, že žadatel požaduje umístit do kvalifikovaného systémového certifikátu informaci o pracovní pozici označující osoby v organizaci, dokládá tuto skutečnost souhlasem organizace, který je v písemné podobě a je podepsán statutárním orgánem nebo osobou, která má zmocnění ke komunikaci s eIdentity a.s.

3.2.6 Kritéria pro interoperaci (spolupráci)

QCA eIdentity může spolupracovat s CA třetích stran pouze na základě písemné smlouvy.

3.3 Identifikace a autentizace pro požadavky na výměnu klíče (Re-key)

3.3.1 Identifikace a autentizace při rutinní výměně klíče

Služba se neposkytuje.

3.3.2 Identifikace a autentizace pro výměnu klíče po zneplatnění

Služba se neposkytuje.

3.4 Identifikace a autentizace pro požadavek na zneplatnění

O zneplatnění kvalifikovaného systémového certifikátu může požádat držitel nebo označující osoba, tj. právnická nebo fyzická osoba, které byl kvalifikovaný systémový certifikát vydán.

Certifikát zneplatňuje poskytovatel

- na základě přijaté žádosti o zneplatnění
- pokud žadatel kvalifikovaný systémový certifikát nepřevezme
- pokud žadatel požádá o ukončení zpracování osobních údajů
- na základě uvědomění držitele nebo označující osoby, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických značek
- v případě, že byl kvalifikovaný systémový certifikát vydán na základě nepravdivých nebo chybných údajů
- dozví-li se prokazatelně, že držitel nebo označující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil
- dozví-li se prokazatelně, že údaje, na jejichž základě byl kvalifikovaný systémový certifikát vydán, pozbyly pravdivosti
- pokud mu Ministerstvo informací nařídí zneplatnění kvalifikovaného systémového certifikátu jako předběžné opatření, pokud existuje důvodné podezření, že kvalifikovaný systémový certifikát byl padělán nebo pokud byl vydán na základě nepravdivých údajů nebo v případě, kdy bylo zjištěno, že označující osoba používá prostředek pro vytváření elektronických značek, které vykazuje bezpečnostní nedostatky, které umožňují padělání elektronických značek nebo změnu podepisovaných nebo označovaných údajů.

Žádost o zneplatnění nebo uvědomění držitele musí být v písemné formě a musí obsahovat

- Sériové číslo certifikátu
- Označení držitele, kterému byl kvalifikovaný systémový certifikát vydán
- Heslo pro zneplatnění certifikátu

Pokud si heslo nepamatuje nebo ho nezná, musí uvést dokumenty, kterými prokázal identitu při podání žádosti, a těmito dokumenty také prokázat svoji totožnost při osobním podání této žádosti nebo žádost musí být podepsána statutárním orgánem nebo osobou, která má oprávnění za organizaci jednat s eIdentity a.s. Tuto žádost lze pak podat jen osobně na RM.

Žádost o zneplatnění nebo uvědomění držitele lze podat (nejméně jedna možnost je vždy dostupná)

- Osobně na RM
- Elektronicky ve svém osobním účtu
- Faxem na číslo dle kapitoly 1.5.2 této certifikační politiky

Pokyn pro zneplatnění může podat označující osoba nebo držitel pro své certifikáty nebo odpovědná osoba eIdentity a.s. pro ostatní případy.

4 FUNKČNÍ POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může podat žádost o vydání certifikátu

O kvalifikovaný systémový certifikát může žádat každá fyzická a právnické osoba nebo organizační složka státu v zastoupení fyzickou osobou na základě plné moci (viz. kapitola 3.2.2), která je povinna uvádět pouze pravdivé informace a tyto také odpovídajícím způsobem doložit. Žádat může pouze ten, kterého soud způsobilosti k právním úkonům nezbavil nebo neomezil.

4.1.2 Registrační proces a odpovědnosti

Vlastní registrace žádosti je rozdělena do dvou oblastí. První oblastí je správa žadatelů a výběr služby. Druhou oblast tvoří prokázání skutečností uvedených ve fázi správy žadatelů a, pokud je prokázání dostatečné, dojde k vydání certifikátu.

Vyplnění údajů je plně v zodpovědnosti žadatele. Žadatel je zodpovědný za to, že uváděné údaje jsou správné, úplné a pravdivé. Uvedené údaje pak prokazuje v procesu ověření na registračním místě.

Za ověření údajů zodpovídá Operátor registračního místa, který je také plně zodpovědný za schválení těchto údajů a za vystavení certifikátu. Operátor registračního místa pracuje podle seznamu úkonů Procesu registračního místa, který je připraven na základě struktury uváděných údajů. O průběhu Procesu registračního místa je pořízen Zápis o průběhu registračního procesu, který podepisují Operátor registračního místa a Žadatel. Tento zápis je vyhotoven ve dvou kopiích, jedna zůstává přílohou žádosti a druhou dostává Žadatel.

Operátor registračního místa je oprávněn žádost zrušit a kvalifikovaný systémový certifikát nevydat pokud není plně přesvědčen, že uváděné údaje jsou odpovídajícím způsobem doloženy. Žadatel může reklamovat práci Operátora registračního místa u vedení eIdentity a.s. s uvedením podrobností případu.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

4.2.1.1 Zájem o službu

Vybere se webový formulář, který je přístupný přes SSL/TLS a jehož obsahem je vysvětlení

pravidel, účelu a použití kvalifikovaného systémového certifikátu, včetně podmínek pro jeho užívání (doporučený HW, SW apod.) na straně žadatele a požadavky na držitele vyplývající ze zákona 227/2000 Sb.

Zájemce vyplní:

- Jméno (včetně dalšího jména apod.)
- Příjmení
- V systému unikátní email adresa s výhradním právem přístupu zájemce
- V systému unikátní přihlašovací jméno

Na uvedenou emailovou adresu následně přijde email s URL a heslem, kde zájemce pokračuje v procesu žádosti. Tím se ověří platnost emailové adresy. Tato emailová adresa bude dále používána ke komunikaci s klientem a budou na ni zasílány informace, týkající se procesu zpracování žádosti, návrhy smluv, výzvy k platbě a další servisní informace.

Heslo má omezenou platnost 5 dní. Přihlašovací jméno se emailem nepřenáší, zájemce si ho musí pamatovat či stránku si vytisknout.

Pokud uvedená emailová adresa již je evidována u jiného žadatele, dojde zde k jejímu odmítnutí. Systém nedovolí také duplicitu přihlašovacích jmen. Na stránce bude také specifikován povolený formát vstupních dat s uvedením příkladu vyplnění. Emailové adresy, které jsou společné pro více žadatelů lze volit až dodatečně v průběhu evidence žadatele.

Pokud nedojde k přihlášení zájemce do systému do konce omezené platnosti hesla nebo na příkaz operátora, záznam o zájemci se ze systému odstraní. Na takto pořízené údaje se hledí tak, jako by nebyly použity – mohou se tedy opět použít dalším zájemcem.

4.2.1.2 Vyplnění identifikačních údajů žadatele

Webový formulář je dostupný na URL, který je uveden v zaslaném emailu. Přístup je přes SSL/TLS, autentizace přihlašovacím jménem a zaslaným heslem. Autentizace může být také certifikátem od komerční CA eIdentity a.s.

Žadatel osoba vyplní:

- Jméno – pevně vyplněno z minulého kroku
- Příjmení – pevně vyplněno z minulého kroku
- Email spojení – pevně vyplněno z minulého kroku
- Celé jméno – vznikne z Jména a Příjmení
- Adresa bydliště
- Číslo OP nebo pasu
- Typ dalšího dokladu – pas, řidičský průkaz, národní identifikační průkaz cizinců – ten, který bude předložen při osobní návštěvě u registrační autority.
- Číslo dalšího dokladu
- Registrované další emailové adresy (po zadání nové emailové adresy na ni bude zaslán textový řetězec, který uživatel zadá do formuláře ověření adresy).

Takto je popsán subjekt žadatele pro účely zákona. Tomuto subjektu – žadateli se vytvoří účet v informačním systému, ve kterém jsou vedeny informace o historii jeho žádostí o certifikáty a o jeho vydaných certifikátech. Bude zde i možnost měnit identifikační údaje (je vedena i jejich historie) s následným posouzením operátorem, zda tato změna má či nemá vliv na již vydané certifikáty (zda dojde k administrativnímu zneplatnění apod.) a zda je případně nutná opětovná osobní návštěva na registračním místě.

Zde je možné také měnit přístupové heslo k účtu žadatele.

4.2.1.3 Účet žadatele

Tento webový formulář tvoří zejména dvě tabulky. V první je seznam vydaných kvalifikovaných certifikátů pro podepisující osobu a ve druhé je seznam vydaných kvalifikovaných systémových certifikátů pro označující osobu. V obou tabulkách je jako poslední řádek Žádost o další certifikát. V tabulkách je také informace o stavu, ve kterém se certifikát nachází, např. vydaný a v době platnosti, revokován (zneplatněn), v procesu žádosti (podrobnější info o stavu zpracování – např. žádost podána, proběhla formální kontrola žádosti a je k dispozici Smlouva, proběhla platba a je možné přistoupit ke generování klíčů, žádost zamítnuta apod.). Webový formulář bude mít v záhlaví identifikační údaje z minulého kroku.

Vydání následného certifikátu je možné vyřídit elektronicky. Žadatel bude upozorněn zprávou na primární emailovou adresu o blížícím se termínu vypršení platnosti kvalifikovaného certifikátu. Pokud se nezměnily skutečnosti, které uvedl při žádosti o kvalifikovaný certifikát, bude mu na jeho žádost, kterou tímto ještě platným certifikátem podepíše, vydán následný certifikát se stejnými údaji. Takový certifikát bude mít však odlišné některé položky obsahu, například dobu platnosti, jiné sériové číslo certifikátu, bude vytvořen pro nový veřejný klíč žadatele a mohou být změněny i informace o akreditované vystavující (QCA) či kořenové (RCA) certifikační autoritě.

V osobním účtu žadatele bude také možné požádat o zneplatnění certifikátu či zrušit probíhající žádost o vydání.

Účet žadatele může být doplněn o tabulku dalších nabízených služeb.

4.2.1.4 Žádost o vydání kvalifikovaného systémového certifikátu

Na tento webový formulář se přejde z odkazu Žádosti o další certifikát z tabulky seznamu kvalifikovaných systémových certifikátů žadatele. Žadatel může mít k dispozici jeden či více bonů, které budou označovat nestandardní platební podmínky

Předvyplněno bude:

- Označení, že je certifikát vydán jako kvalifikovaný systémový certifikát podle zákona 227/2000 Sb.
- Název obchodní firmy kvalifikovaného poskytovatele a stát, ve kterém je poskytovatel

usazen
- Elektronická značka kvalifikovaného poskytovatele založená na kvalifikovaném systémovém certifikátu poskytovatele
- CDP– odkaz, kde lze přistoupit k CRL
- Politika, podle které došlo k vydání kvalifikovaného systémového certifikátu

Poskytovatel doplní dodatečně v okamžiku vydání kvalifikovaného systémového certifikátu:

- Správný datum a čas počátku a konce platnosti kvalifikovaného systémového certifikátu
- Unikátní číslo vydávaného kvalifikovaného systémového certifikátu
- Data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby

Žadatel vyplní:

- Jednoznačnou identifikaci držitele
- Jednoznačnou identifikaci označující osoby, případně také prostředku pro vytváření elektronických značek
- Emailová adresa - výběr ze seznamu registrovaných emailových adres nebo žádná
- Omezení kvalifikovaného systémového certifikátu podle povahy a rozsahu jen pro určité použití (KeyUsage)
- Označení kuponu (bonu) na speciální cenu či akci
- Vyjádření souhlasu se zveřejněním certifikátu
- Heslo pro zneplatnění.

Po vyplnění bude žádost odeslána k formální kontrole. Formální kontrola prozkoumá jednak obsah připravovaného kvalifikovaného systémového certifikátu a také platnost kuponu na speciální cenu či akci ve vztahu k vydávanému kvalifikovanému systémovému certifikátu. Formální kontrola také určí, jaké skutečnosti bude muset žadatel doložit (a také jak) při vydávání kvalifikovaného systémového certifikátu.

4.2.1.5 Smlouva a platba

Po úspěšné formální kontrole (a případných opravách žádosti) je připraven návrh smlouvy na vydání odpovídajícího kvalifikovaného systémového certifikátu a bude generována výzva k zálohové platbě za službu a oba dokumenty budou zaslány žadateli. Po obdržení platby na účet a odsouhlasení smlouvy o poskytnutí služby žadatelem bude uvolněno generování klíčů a zaslání žádosti o certifikát dle PKCS#10 nebo obdobným způsobem. Teprve nyní, po doplnění zaznamenaných údajů do formátu podle PKCS#10 (nebo obdobného) se na tyto údaje pohlíží jako na úplnou Žádost o poskytnutí služby. Žádost se přenáší do vnitřního systému CA, kde dochází k registračnímu procesu a k vlastnímu vydání certifikátu.

Ve smlouvě žadatel stvrdí mimo jiné, že

- poskytl přesné a kompletní informace podle požadavku CP
- používá výhradně klíčového páru v souladu s ostatním omezením
- učinil účelná opatření k zabránění neautorizovanému použití soukromého klíče
- generoval klíče

    - algoritmem určeným pro účely vydání kvalifikovaného systémového certifikátu
    - délka klíče vyhovuje pro účely vydání kvalifikovaného systémového certifikátu
    - tak, že zůstal výhradním držitelem soukromého klíče

- upozorní bez zbytečného odkladu v době platnosti certifikátu

    - že soukromý klíč byl ztracen, zcizen či existuje možnost zneužití
    - že se soukromý klíč nenachází pod výhradní kontrolou držitele z důvodu možného zneužití aktivačních dat (PIN) nebo z jiných důvodů
    - na nepřesnosti nebo změny údajů, na základě kterých byl certifikát vydán

- v případě kompromitace soukromého klíče ho přestane okamžitě a napořád používat

- zda souhlasí se zveřejněním vydaného kvalifikovaného certifikátu

4.2.1.6 Registrační místo

Operátor registračního místa postupuje podle schváleného postupu a provede kontrolu vyplněných informací oproti předloženým dokumentům. Pokud bude vše v pořádku, pořídí kopie dokladů a dokumentů, na jejichž základě došlo k ověření údajů a doplní je o prohlášení žadatele, že ten souhlasí s jejich archivací.

Operátor uzavře smlouvu s žadatelem o poskytnutí služby, zadá pokyn k vystavení certifikátu a ten po jeho vystavení protokolárně předá žadateli.

Žadatel obdrží Smlouvu o poskytování služby, fakturu za uhrazení ceny služby včetně příjmového dokladu, Zápis o průběhu procesu registračního místa a Protokol o předání a převzetí kvalifikovaného systémového certifikátu.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Pokyn k vystavení certifikátu může vydat Operátor registračního místa na základě uzavřené písemné Smlouvy o poskytování služeb a to pouze v případě, že si je jist správným doložením údajů ze strany Žadatele a splněním jeho dalších povinností (zejména uhrazení ceny za poskytovanou službu na základě Výzvy k platbě, podepsáním Zápisu o průběhu procesu registračního místa apod.).

Při nedostatečnosti při prokazování údajů či při jiném porušení registračního procesu musí

Operátor zamítnout žádost a neposkytnout objednávanou službu. Případné následující kroky (např. forma vrácení zálohové platby apod.) bude řešena se Žadatelem či plátcem individuálně.

4.2.3 Doba zpracování žádosti o certifikát

Časový limit, ve kterém dojde ke zpracování žádosti o certifikát není pevně stanoven. Jedná se o interaktivní proces, jehož délku určuje převážně žadatel. Společnost eIdentity a.s. poskytuje certifikační služby bez zbytečného otálení. Pokud žádost o službu nezruší žadatel či operátor, zůstává žádost stále aktivní.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

Vydáním pokynu k vystavení certifikátu pro interní systém QCA se sestaví obsah certifikátu, spočte se z něj otisk podle schváleného schématu (SHA1) a předá se k vytvoření elektronické značky na Podepisovací pracoviště. Zde dojde k vytvoření elektronické značky otisku a získaná data se odešlou zpět ke konečnému vytvoření certifikátu ve formátech DER, PEM a TXT.

4.3.2 Oznámování vydání certifikátu označující osobě

Certifikát ve výše zmíněných formátech je od tohoto okamžiku k dispozici trvale v osobním účtu žadatele a jeho obsah je součástí Protokolu o předání a převzetí certifikátu.

4.4 Převzetí certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Součástí předání certifikátu je Protokol o předání a převzetí certifikátu, ve kterém žadatel stvrzuje převzetí certifikátu. Certifikát, který byl vydán v souladu s touto CP nelze odmítnout. Žadatel může požádat však ihned o jeho zneplatnění.

Protokol o předání a převzetí certifikátu obsahuje výpis certifikátu i v textové formě, ze které je zřejmý obsah certifikátu, okamžik převzetí a podpis žadatele a ORM. Jednu kopii si odnáší žadatel a druhá kopie zůstává součástí dokumentace žádosti.

4.4.2 Zveřejňování vydaných certifikátů certifikační autoritou

Vydaný kvalifikovaný systémový certifikát je po převzetí umístěn do seznamu vydaných

kvalifikovaných certifikátů. Zveřejněny jsou pouze tyto údaje

- Sériové číslo certifikátu
- Doba platnosti od-do

V případě, že žadatel souhlasil se zveřejněním certifikátu, jsou ještě navíc zobrazeny údaje

- Držitel (Subject)
- Vlastní certifikát ve formátu DER, PEM a TXT

4.4.3 Oznámení vydání certifikátu jiným subjektům

Vnitřní systém QCA informuje o vydání certifikátu odpovídajícího ORM vyhotovením Protokolu o předání a převzetí certifikátu.

4.5 Použití párových klíčů a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem/označující osobou

Soukromý klíč (data pro vytváření elektronických značek), který se vztahuje k vydanému kvalifikovanému systémovému certifikátu může být použit pouze v souladu se Zákonem a se Smlouvou a toto použití je povoleno až po předchozím převzetí odpovídajícího kvalifikovaného systémového certifikátu a musí být ukončeno po uplynutí doby platnosti či při zneplatnění tohoto kvalifikovaného systémového certifikátu.

Označující osoba i držitel jsou povinni zacházet s prostředkem jakož i s daty pro vytváření elektronických značek s náležitou péčí tak, aby nemohlo dojít k jejich neoprávněnému použití a uvědomit neprodleně poskytovatele certifikačních služeb, který vydal kvalifikovaný systémový certifikát, o tom, že hrozí nebezpečí zneužití jejích dat pro vytváření elektronických značek.

Označující osoba je dále povinna zajistit, aby prostředek pro vytváření elektronických značek, který používá, splňoval požadavky stanovené zákonem 227/2000 Sb.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Spoléhající strana může spoléhat pouze na certifikáty a veřejné klíče, které byly vydány a používány v souladu s touto politikou, byly použity v souladu s údaji v certifikátu a které nemají označen za neplatný žádný certifikát ve svém certifikačním řetězci. Spoléhající strana je plně zodpovědna za veškeré úkony, které je musí vykonat před tím, než získá důvěru v platnost certifikátu a veřejného klíče. Doporučený postup je uveden např. v Nařízení vlády č. 495/2004 Sb. a Vyhlášce 496/2004 Sb. nebo na webových stránkách Ministerstva informatiky.

4.6 Obnovení certifikátu

Služba se neposkytuje. Je možné požádat o vydání nového certifikátu.

4.6.1 Okolnosti pro obnovení certifikátu

Služba se neposkytuje.

4.6.2 Kdo může požadovat obnovení

Služba se neposkytuje.

4.6.3 Zpracování požadavku na obnovu certifikátu

Služba se neposkytuje.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli/podepisující osobě

Služba se neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Služba se neposkytuje.

4.6.6 Zveřejňování vydaných obnovených certifikátů certifikační autoritou

Služba se neposkytuje.

4.6.7 Oznámování vydání certifikátu jiným subjektům

Služba se neposkytuje.

4.7 Výměna klíče (re-key) v certifikátu

Služba se neposkytuje.

4.7.1 Okolnosti pro výměnu klíče v certifikátu

Služba se neposkytuje.

4.7.2 Kdo může požadovat výměnu klíče v certifikátu

Služba se neposkytuje.

4.7.3 Provedení požadavku na výměnu klíče

Služba se neposkytuje.

4.7.4 Oznámení o vydání certifikátu s vyměněným klíčem podepisující osobě

Služba se neposkytuje.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným klíčem podepisující osobou

Služba se neposkytuje.

4.7.6 Zveřejňování vydaných certifikátu s vyměněným klíčem

Služba se neposkytuje.

4.7.7 Oznámení o vydání certifikátu s vyměněným klíčem jiným subjektům

Služba se neposkytuje.

4.8 Změna certifikátu (modification)

Služba se neposkytuje.

4.8.1 Okolnosti pro změnu certifikátu

Služba se neposkytuje.

4.8.2 Subjekty oprávněné požadovat změnu certifikátu

Služba se neposkytuje.

4.8.3 Zpracování požadavku na změnu certifikátu

Služba se neposkytuje.

4.8.4 Oznámení o vydání změněného certifikátu podepisující osobě

Služba se neposkytuje.

4.8.5 Úkony spojené s převzetím změněného certifikátu

Služba se neposkytuje.

4.8.6 Zveřejňování vydaných změněných certifikátů

Služba se neposkytuje.

4.8.7 Oznámení o vydání změněného certifikátu jiným subjektům

Služba se neposkytuje.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Okolnosti pro zneplatnění certifikátu

Držitel musí neprodleně požádat o zneplatnění certifikátu v případě, kdy hrozí nebezpečí zneužití dat pro vytváření elektronických značek a v dalších případech v souladu s bodem 3.4. této CP.

Zneplatnit certifikát může i vydavatel v souladu s bodem 3.4. této CP.

Zneplatněný certifikát nemůže být obnoven.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění může požádat pouze držitel certifikátu či označující osoba nebo na základě skutečností dle bodu 3.4 této CP.

4.9.3 Provedení požadavku na zneplatnění certifikátu

Musí být provedeno v souladu s bodem 3.4 této CP.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Tato doba není specifikována.

4.9.5 Maximální doba, za kterou musí CA realizovat požadavek na zneplatnění certifikátu

Certifikát je zneplatněn neprodleně. Informace o zneplatnění certifikátu se objeví v prvním zveřejněném CRL po uplynutí nejdéle 12 hodin od přijetí žádosti o zneplatnění.

4.9.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn

Spoléhající se strany musí kontrolovat platnost všech certifikátů v certifikačním řetězci – viz kapitola 4.5.2 této CP.

4.9.7 Periodicita vydávání CRL

CRL se vydává denně s periodicitou maximálně 12 hodin.

4.9.8 Maximální zpoždění CRL

CRL se zveřejňuje neprodleně.

4.9.9 Možnost ověřování zneplatnění/statusu certifikátu on-line

Služba se neposkytuje.

4.9.10 Požadavky při on-line ověřování zneplatnění/statusu certifikátu

Služba se neposkytuje.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Služba se neposkytuje.

4.9.12 Speciální podmínky při kompromitaci soukromého klíče

Služba se neposkytuje.

4.9.13 Okolnosti pro pozastavení platnosti certifikátu

Služba se neposkytuje.

4.9.14 Kdo může požadovat pozastavení platnosti certifikátu

Služba se neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Služba se neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Služba se neposkytuje.

4.10 Služby statutu certifikátu

4.10.1 Funkční charakteristiky

Tato služba se poskytuje zveřejněním CRL na webových stránkách eIdentity a.s..

4.10.2 Dostupnost služeb

Tato služba se poskytuje nepřetržitě.

4.10.3 Další charakteristiky služeb statutu certifikátu

Služba se neposkytuje.

4.11 Ukončení poskytování služeb pro podepisující osobu

S ukončením platnosti kvalifikovaného systémovéhocertifikátu v případě, že žadatel nepožádal o vystavení následného kvalifikovaného systémového certifikátu, končí obchodní vztah se žadatelem. Osobní konto žadatele a jeho osobní údaje zůstávají nadále aktivní a žadatel může kdykoliv opět požádat o navázání obchodního vztahu objednáním nabízené služby.

Pokud požádá držitel/žadatel/označující osoba o ukončení zpracování osobních údajů, dojde k zneplatnění jeho certifikátů, jeho osobní údaje se přesunou do archivu a přestanou se zpracovávat.

4.12 Úschova klíče u důvěryhodné třetí strany a jeho obnova

Služba se neposkytuje.

4.12.1 Politika a postupy při úschově a obnovování klíče

Služba se neposkytuje.

4.12.2 Politika a postup při zapouzdřování (encapsulation) a obnovování relačního klíče (session key)

Služba se neposkytuje.

5 BUDOVY, MANAGEMENT A PROVOZNÍ ŘÍZENÍ

Tato kapitola je podrobně rozpracována v Certifikační prováděcí směrnici a v další provozní a projektové dokumentaci.

5.1 Kontrola fyzické bezpečnosti

5.1.1 Umístění a konstrukce

Podepisovací pracoviště s kryptografickým modulem a zařízení obsahující a zpracovávající osobní údaje žadatelů je umístěno ve vhodných geograficky vzdálených hlavních a záložních lokalitách. Použité prostory odpovídají svým bezpečnostním vybavením a režimem provozu objektům kategorie „D“ vyžadované zákonem 227/2000 Sb. pro umístění takových zařízení.

5.1.2 Fyzický přístup

Vstup do budovy, včetně do objektu, je pro vstupující možný při prokázání se identifikačním průkazem s fotografií strážní službě a současně při použití čipové karty (otočné turnikety ve vstupní hale). Vstupní dveře do ulice otevírá dálkově pouze strážní služba.

Návštěvy jsou v budově možné pouze s doprovodem zaměstnance po ověření totožnosti nebo samostatně osobám vybavených identifikační kartou.

Čipy je dále řešen vstup do jednotlivých částí komplexu (bez souvislosti s ochranou citlivých aktiv). Turnikety ve vstupní hale jsou nejúčinnějším prostředkem pro řízení pohybu. Dále je instalován systém CCTV, který chrání perimetr budovy a vybrané části prostor PCS.

Bezpečnost je dále v celém prostoru posílena o systém EZS a EPS s vyvedeným výstupem hlášení na stanoviště strážní služby.

5.1.3 Elektřina a klimatizace

Použité prostory jsou vybaveny nezávislým přívodem elektrické energie, záložním zdrojem elektrické energie a generátorem elektrické energie pro zachování napájení objektu elektrickou energií při dlouhodobém výpadku hlavních přívodů.

Prostory jsou klimatizovány a vlhkost je udržována automaticky.

5.1.4 Vlivy vody

V používaných prostorech je odstraněno nebezpečí zalití vodou, místnosti jsou bez oken a bez rozvodu vody.

5.1.5 Protipožární opatření a ochrana

V případě požáru se použité místnosti naplní netečným plynem, který uhasí požár. Po odvětrání jsou prostory opět přístupné.

5.1.6 Ukládání médií

Média s provozními zálohami dat a systému jsou ukládány na dvou geograficky vzdálených místech v tresorech. Přístup k nim je řízen a kontrolován. O pohybu záložních médií je pořizován zápis.

5.1.7 Nakládání s odpady

Při provozu ACAeID nevznikají jiné než běžné odpady pro kancelářský režim práce. Takovéto odpady se likvidují obvyklým způsobem.

5.1.8 Zálohy mimo budovu

Pro zajištění schopnosti dodržet požadované termíny činností ACAeID jsou využity geograficky vzdálené prostory, které umožní v dostatečně krátké době znovu zprovoznit havarovaný nebo jinak nedostupný informační systém.

5.2 Kontrola procedurální bezpečnosti

5.2.1 Důvěryhodné role

Důvěryhodné role jsou:

- statutární zástupce
- ředitel společnosti
- ředitel bezpečnosti
- Provozní manager ICT

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro bezpečnostní operace je vyžadována přítomnost nejméně dvou důvěryhodných osob najednou.

5.2.3 Identifikace a autentizace pro každou roli

Jednotliví uživatelé se do aplikace hlásí pomocí čipových karet.

5.2.4 Role vyžadující rozdělení povinností

Role, které vyžadují rozdělení jsou:

- ředitel provozu
- ředitel bezpečnosti

5.3 Kontroly personální bezpečnosti

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Společnost eIdentity a.s. při práci s lidskými zdroji vybudovala systém, který zabezpečuje, že budou najímáni pouze důvěryhodní zaměstnanci a je dbáno o to, aby jejich loajalita ke společnosti byla podporována a udržována. Personální práce eIdentity a.s. vede k tomu, že lidé si uvědomují zájem společnosti o ně samé, že cítí sounáležitost se svou společností, identifikují se s ní a cítí jasnou přímou úměrnost mezi úspěchem společnosti a svým prospěchem. Pro společnost je základním východiskem důvěra ve vlastní zaměstnance, která má pozitivní vliv na míru akceptování některých omezení. Personální bezpečnost je součástí aktivit spadajících pod řízení lidských zdrojů, je tedy neoddělitelnou součástí práce všech vedoucích pracovníků eIdentity a.s. Personální bezpečnost eIdentity a.s. vnímá jako součást řádné správy společnosti, neboť je vyjádřením péče o svěřená aktiva.

Personální bezpečnost v oblasti ochrany citlivých aktiv tedy eIdentity a.s. vnímá jako zintenzivnění výše uvedeného systému u osob, které jsou určeny k práci s citlivými aktivy. Organicky navazuje na současný systém řízení lidských zdrojů.

Termínem personální bezpečnost eIdentity a.s. označuje souhrn všech postupů, které vedou k ověření důvěryhodnosti zaměstnanců a k jejich vzdělávání vedoucímu k bezpečnostnímu povědomí o možných bezpečnostních hrozbách a rizicích a k jednání, která toto povědomí odráží.

Důvěryhodnost zaměstnanců je jedním ze základních kvalifikačních předpokladů pro výkon pracovní činnosti v rámci eIdentity a.s. Je zárukou toho, že pracovník, který disponuje svěřenými hodnotami, svého postavení nezneužije a nezpůsobí tak poskytovateli ztrátu. Ověření důvěryhodnosti zaměstnance je proces zahrnující shromažďování, ověřování a vyhodnocování informací. Výstupem je rozhodnutí, zda může být daný jmenovaný pracovník (pracovník usilující o jmenování) považován za důvěryhodnou osobu.

5.3.2 Postupy při ověřování zázemí osob

Zdrojem informací jsou pracovník sám a osoby, které zaměstnance znají. Dalším zdrojem jsou veřejně přístupné informační zdroje.

Bezúhonnost se posuzuje podle výpisu z rejstříku trestů.

Pracovník poskytuje informace v průběhu vstupního osobního pohovoru a dále při periodických pohovorech s vedoucími pracovníky společnosti.

Další osoby poskytují informace v situacích (bezpečnostní incident), které vyvolají potřebu ověřit získané informace.

Postup posuzování spočívá v pečlivém zvažování řady proměnných údajů, které sestavují „celkový profil osobnosti“ (whole person concept). V procesu rozhodování jsou zvažovány dostupné, spolehlivé informace o pracovníkovi, příznivé i nepříznivé, ze současné doby i z minulosti.

Každý případ je posuzován odděleně ve své podstatě. Pochybnosti o důvěryhodnosti posuzovaného pracovníka jsou podnětem ke zvažování bezpečnostních rizik, která by vyplynula z realizace hrozeb definovaných v celkové bezpečnostní politice.

Konečné rozhodnutí o tom, zda považovat pracovníka za důvěryhodného a spolehlivého musí být jednoznačně v souladu se zájmy společnosti a musí být rozhodnutím všeobsáhlé zralé úvahy.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Zaměstnanci a ostatní pracovníci ACAeID musí absolvovat vstupní cyklus bezpečnostního a aplikačního vzdělávání.

5.3.4 Požadavky a periodicita školení

Zaměstnanci a ostatní pracovníci ACAeID musí absolvovat průběžný cyklus bezpečnostního a aplikačního vzdělávání. Podrobnější popis je v dokumentu D8 – Obsluha systému.

5.3.5 Periodicita a posloupnost „job rotation“ mezi různými rolemi

Nepředpokládá se, že by probíhala pravidelná změna pracovních pozic zaměstnanců. Pakliže to bude pro zajištění provozu nezbytně nutné, může zaměstnanec dočasně vykonávat jinou roli. Musí však před tím absolvovat patřičné proškolení.

5.3.6 Postihy za neautorizované činnosti zaměstnanců

Vykonávání neautorizované činnosti se považují za hrubé porušení pracovní kázně a sankce

se řídí zákoníkem práce.

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Doporučuje se certifikát NBÚ na stupeň důvěrné.

5.3.8 Dokumentace poskytovaná zaměstnancům

Dokumentace, která se předává zaměstnanci, se týká specifikace jejich pracovní náplně a popisu systémů se kterými pracují na úrovni příručky uživatele.

5.4 Auditní záznamy (logy)

5.4.1 Typy zaznamenávaných událostí

Auditní záznamy obsahují informace o důležitých událostech provozu systému.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou zpracovávány nejméně 1x týdně, jinak bezprostředně po bezpečnostním incidentu.

5.4.3 Doba uchování auditních záznamů

Auditní záznamy se uchovávají po dobu nejméně 10 let.

5.4.4 Ochrana auditních záznamů

Přístup k auditním logům je řízen a logy jsou chráněny proti pozměnění.

5.4.5 Postupy při zálohování auditních záznamů

Auditní logy jsou ukládány a zálohovány stejně jako ostatní informace, tak, aby bylo možné jejich plné obnovení po případné poruše.

5.4.6 Systém shromažďování auditních záznamů

O shromažďování auditních záznamů se vede evidence.

5.4.7 Oznamování subjektu, který způsobil událost

Neposkytuje se.

5.4.8 Hodnocení zranitelnosti

Události s vyšším stupněm závažnosti, jsou eskalovány automaticky emailem odpovědné osobě.

5.5 Archivace záznamů

5.5.1 Typy záznamů, které se archivují

Archivace dat QCA eIdentity je pravidelně provedena jednou měsíčně. Na DVD medium jsou vypáleny soubory obsahující všechny certifikáty, všechna CRL/ARL a auditní logy za dané období. Otisky souborů a čas jejich archivace jsou uvedeny v přiloženém souboru, který je elektronicky podepsán.

5.5.2 Doba uchování archivovaných záznamů

Pro archivaci jsou vybírána media, u kterých výrobce zaručuje minimální dobu čitelnosti 3 roky. Po dvou letech jsou média přepalována. Celková doba archivace dat je 10 let.

5.5.3 Ochrana úložiště archivovaných záznamů

Práva k prohlížení archivu závisí na sledovaných položkách. Certifikáty a CRL může prohlížet každá osoba, která má oprávněný přístup k archivním informacím. Auditní archivní informace jsou přístupné pouze oprávněným osobám prostřednictvím prohlížecí aplikace. Osoby, které mají oprávnění k přístupu jsou poučeny, že v archivu se vyskytují osobní údaje.

5.5.4 Postupy při zálohování archivovaných záznamů

Postupy odpovídají bodu 5.5.1 této CP.

5.5.5 Požadavky na používání časových razítek u archivovaných záznamů

Záznamy v sobě nesou informaci o čase, ve kterém byly pořízeny. Nevyužívá se časových razítek, systémový čas je však navázán na UTC.

5.5.6 Systém shromažďování archivovaných záznamů

Archivní kopie se ukládají do bankovní schránky.

5.5.7 Postupy pro získání a ověření archivních údajů

Součástí archivu je seznam otisků archivovaných souborů včetně záznamu času pořízení, který je elektronicky podepsán v okamžiku pořízení.

5.6 Výměna klíče CA

Výměna klíčů CA se neprovádí.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

V případě bezpečnostního incidentu odpovídajícího rozsahu se postupuje v souladu s dokumentem Plán pro zvládání krizových situací a plán obnovy.

5.7.2 Poškození výpočetních prostředků, softwaru a/nebo dat

Systém je navržen tak, že je možné vyměnit jakoukoliv část poškozené výpočetní techniky, software a dat tak, aby mohl být provoz zachován či obnoven v požadovaném termínu.

5.7.3 Postup při kompromitaci soukromého klíče ACAeID

V případě kompromitace privátního klíče QCA dojde k jeho okamžitému zneplatnění a umístění na seznam zneplatněných certifikátů vydavatele (RCA).

Dojde k zneplatnění všech certifikátů, které byly vydány za pomoci kompromitovaného klíče QCA.

O skutečnosti je informována veřejnost tak, že je situace popsána na stránkách eIdentity a.s., které jsou nepřetržitě dostupné. Každý žadatel je dále na tuto situaci upozorněn doporučeným dopisem případně navíc ještě elektronickým dopisem. Žadatelé mají v tomto případě nárok na vydání nového certifikátu zdarma.

5.7.4 Schopnost pokračovat v činnosti po havárii

V případě bezpečnostního incidentu odpovídajícího rozsahu se postupuje v souladu s dokumentem Plán pro zvládání krizových situací a plán obnovy.

5.7.5 Ukončení činnosti CA nebo RA

Provozovatel informuje Ministerstvo informací nejméně 3 měsíce před předpokládaným ukončením činnosti. Vynaloží veškeré možné úsilí k tomu, aby vedená evidence byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb.

Provozovatel dále informuje doporučeným dopisem každého Žadatele o svém záměru ukončit činnost nejméně 2 měsíce předem.

Provozovatel nejméně 30 dní před ukončením činnosti informuje Ministerstvo informací v případě, že se nepodařilo zajistit převzetí evidence jiným kvalifikovaným poskytovatelem.

Obdobná ustanovení platí i v případě jiných způsobů ukončení činnosti.

6 KONTROLY TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových klíčů

6.1.1 Generování párových klíčů

Pár klíčů CA eIdentity je vygenerován během procesu instalace třemi vyškolenými pracovníky CA. Ke generování je využit nově nainstalovaný software a hardware. Klíč je generován v kryptografickém modulu, který splňuje normu FIPS 140-1 Level 3 nebo novější a je uveden na stánkách Ministerstva, jako nástroj, u kterého byla vyslovena shoda ve smyslu § 8 odst. 3 vyhlášky č. 366/2001 Sb..

Klíče jsou generovány dle předem připraveného procesu popsaného v instalační příručce podepisovacího pracoviště ACA eIdentity.

Klíče ACAeID se mohou použít pouze k podepisování kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a seznamu zneplatněných certifikátů.

Generování klíčů koncových uživatelů je obecně řešeno přímo uživateli. Pro kvalifikované certifikáty je možno použít generování klíčů za pomoci některého internetového prohlížeče.

6.1.2 Předání soukromého klíče podepisující osobě

Žadatelé generují soukromé klíče vlastními prostředky ve svém prostředí.

6.1.3 Předání veřejného klíče certifikační autoritě

Veřejný klíč uživatele je dodán CA eIdentity v podobě PKCS#10 nebo jiného elektronicky podepsaného balíku dat v rámci SSL spojení.

6.1.4 Předání veřejného klíče CA potenciálním spoléhajícím se stranám

Certifikáty CA eIdentity jsou zveřejněny na webových stránkách CA eIdentity, společně s otisky certifikátu pořízenými alespoň dvěma různými algoritmy. Tytéž informace jsou k dispozici na webu MIČR a v tištěné podobě v centru ACA eIdentity.

6.1.5 Délky klíče

Délky klíčů musí být dostatečné vzhledem k aktuálním metodám pro odhalení soukromého klíče kryptografickou analýzou používání klíčů. Současná praxe udává akceptovatelnou bezpečnost pro velikost klíčů 1024 bitů a více. CA eIdentity odmítne vydat certifikát pro klíče velikosti menší než 1024 bitů.

6.1.6 Parametry pro generování veřejného klíče a ověřování kvality

Přijaty budou pouze unikátní veřejné klíče.

6.1.7 Účel použití klíče (pole použití klíče pro X.509 v3)

Viz kapitola 7.1.2.1 této CP - QC.

6.2 Ochrana soukromého klíče a kontroly kryptografického modulu

Tato kapitola je rozpracována v Certifikační prováděcí směrnici. Soukromý klíč QCA je uložen v bezpečném prostředku pro vytváření elektronických podpisů a přístup k němu je řízen. Spustit takový prostředek mohou pouze dvě osoby současně a o provozu prostředku je veden zápis. Součástí provozních postupů je i pravidelná kontrola kryptografického modulu.

6.2.1 Standardy a kontroly kryptografických modulů

Klíče CA eIdentity jsou generovány hardwarovým modulem splňujícím požadavky normy FIPS 140-1 Level 3 nebo novější.

6.2.2 Sdílení tajemství (m z n)

Veškeré citlivé operace CA eIdentity vyžadují přítomnost dvou operátorů. Každý z těchto operátorů zná část kódu, který umožní tyto operace provést.

6.2.3 Úschova soukromých klíčů

Soukromé klíče CA eIdentity a jejích operátorů jsou uloženy výhradně v úložištích jim odpovídajících bezpečnostních předmětů, které mají pod svojí kontrolou. Žádné jiné úložiště soukromých klíčů neexistuje.

6.2.4 Zálohování soukromých klíčů

Soukromý klíč CA eIdentity je zálohován během procesu jeho vytvoření prostředky HSM. Soukromé klíče operátorů a částí systému nejsou zálohovány a pravidelně se obnovují.

6.2.5 Archivace soukromých klíčů

CA eIdentity nearchivuje soukromé klíče.

6.2.6 Transfer soukromých klíčů do/z kryptografického modulu

Všechny páry klíčů CA eIdentity, operátorské CA či operátorů jsou generovány uvnitř kryptografických modulů a jsou označeny jako neexportovatelné.

Jedinou výjimkou uvedeného pravidla jsou klíče systémové, jež jsou generovány nástroji v závislosti na systému, ve kterému budou použity.

6.2.7 Uložení soukromých klíčů v kryptografickém modulu

Soukromé klíče jsou uloženy v kryptografických modulech v šifrované formě.

6.2.8 Postup aktivování soukromého klíče

K aktivaci soukromého klíče CA je zapotřebí dvou operátorů, kteří ve správném pořadí vloží do podepisovacího pracoviště své části PINu.

6.2.9 Postup při deaktivaci soukromého klíče

Soukromý klíč CA eIdentity je deaktivován při procesu vypnutí podepisovacího pracoviště.

6.2.10 Postup při zničení soukromého klíče

Rozhodnutí o zničení soukromého klíče CA eIdentity mohou provést pouze majitelé firmy na základě závažných důvodů, např. jeho kompromitace. Ke zničení klíče musí být přítomni dva operátoři a zástupce vedení společnosti. O zničení klíče je sepsán protokol, podepsaný všemi zúčastněnými.

Pro ničení soukromých klíčů jsou použity nulovací funkce kryptografických modulů.

6.2.11 Hodnocení kryptografických modulů

Použité kryptografické zařízení HSM má prohlášení o shodě v souladu s požadavky zákona 227/2000 Sb.

6.3 Další aspekty klíčového hospodářství

6.3.1 Archivace veřejného klíče

Veřejný klíč QCA eIdentity, veřejné klíče jednotlivých komponent i veřejné klíče operátorů jsou zálohovány a archivovány v rámci standardních procedur zálohování serverů QCA eIdentity.

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující osobě a párových klíčů

Kvalifikované certifikáty vydané QCA eIdentity mají dobu platnosti 1 rok. Rok před skončením platnosti kvalifikovaného systémového certifikátu QCA přestane být tento užíván k vydávání dalších kvalifikovaných certifikátů žadatelů, aby žádný z vydaných kvalifikovaných certifikátů žadatelů neměl dobu platnosti přesahující dobu platnosti certifikátu, za pomoci kterého byl vytvořen.

Období použití klíčů odpovídá době platnosti certifikátu.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data k soukromému klíči QCA eIdentity jsou vytvořena během procesu instalace, kdy dochází mimo jiné i ke generování těchto párových dat a splňují pravidla pro jejich vytváření.

6.4.2 Ochrana aktivačních dat

Pracovníci jsou smluvně vázáni chránit svá aktivační data a nesou za jejich případné zneužití zodpovědnost.

6.4.3 Ostatní aspekty archivačních dat

Aktivační data slouží výhradně k aktivaci soukromého klíče a nesmí být užita k jinému účelu, ani vkládána do jakéhokoli systému nesouvisejícím s určeným použitím. Aktivační data nikdy nesmí být přenášena v otevřené podobě.

V případě podezření na prozrazení aktivačních dat jsou tato bezodkladně znehodnocena jakýmkoli možným způsobem, včetně případného zničení párových dat.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Veřejná část systému ACA eIdentity je přístupná pomocí HTTP a HTTPS protokolu. Všechny komponenty veřejné části kromě registrace nových uživatelů jsou určeny pouze ke čtení a neumožňují vzdálenému uživateli změnu údajů. Registrace uživatelů vyžaduje vstup ze strany zájemce a je vedena striktně pomocí HTTPS protokolu.

Klientská část systému QCA je zpřístupněna uživatelům šifrovaným kanálem HTTPS, kterým jsou předávána veškerá citlivá data. Přístup k údajům uživatele je umožněn až po zadání uživatelského jména hesla. Toto rozhraní je jediným bodem komunikace s veřejností, všechny ostatní systémy QCA eIdentity jsou mimo vnitřní síť CA eIdentity nepřístupné.

Systémy ACAeID jsou fyzicky umístěny v chráněném objektu typu „D“ a přístup k nim mají pouze určené osoby.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení vychází z ČSN/ISO 17799, CEN CWA 14167-1 a ETSI TS 101 456 a soulad s těmito normami je ověřen auditem.

6.6 Technické kontroly životního cyklu

6.6.1 Řízení vývoje systému

Vývoj systému probíhal podle pravidel zabezpečení vývoje.

6.6.2 Kontroly řízení bezpečnosti

Systém QCA eIdentity obsahuje nástroje pro kontrolu integrity aplikace, které jsou pravidelně spouštěny a jejich výstup vyhodnocován. Integrita aplikace je ověřována otisky souborů aplikace na provozních serverech oproti jejich otiskům pořízených vývojáři před jejich uvedením do provozu.

6.7 Řízení síťové bezpečnosti

Pro zajištění síťové bezpečnosti jsou v rámci systému QCA eIdentity použity firewally několika úrovní.

6.8 Časová razítka

Auditní logy a databázové záznamy žádostí o certifikát, žádostí o revokaci certifikátu, CRL a certifikátů obsahují informace o čase. Čas je v rámci vnitřní sítě synchronizován protokolem NTP a je navázán bezpečným způsobem na UTC. Služby časového razítka se pro tyto účely nepoužívají.

7 CERTIFIKÁT, CRL A OCSP PROFILY

7.1 Profil certifikátu

Certifikáty jsou vydávány v souladu s doporučením ITU-T X.509 (June 1997) a RFC3280 (April 2002).

Délka klíče certifikační autority QCA, vydávající kvalifikované systémové certifikáty je 2 048 bitů.

Minimální délka klíče vydávaných kvalifikovaných systémových certifikátů je 1 024 bitů.

Základní položky a popis jejich hodnot uvádí následující tabulka:

Položka	**Hodnota**
Serial Number	Unikátní číslo certifikátu v prostředí vydavatele QCA
Signature Algorithm	OID algoritmu použitého pro elektronickou značku kvalifikovaného systémového certifikátu
Issuer DN	Označení vydavatele kvalifikovaného systémového certifikátu v souladu s kapitolou 3.1.1.1 této CP
Valid From	Formát dle RFC3280, UTC čas začátku platnosti kvalifikovaného systémového certifikátu
Valid To	Formát dle RFC3280, UTC čas konce platnosti kvalifikovaného systémového certifikátu
Subject DN	Označení držitele kvalifikovaného systémového certifikátu v souladu s kapitolou 3.1.1.2 této CP
Subject Public Key	Veřejný klíč držitele kvalifikovaného systémového certifikátu
Signature	Elektronická značka vydavatele kvalifikovaného systémového certifikátu

7.1.1 Číslo verze

Certifikát ACAeID a kvalifikované certifikáty žadatelů jsou vydávány v souladu s doporučením X.509 ve verzi 3.

7.1.2 Rozšíření certifikátu

7.1.2.1 KeyUsage

V souladu s X.509 v3 je toto rozšíření presentováno nastavením odpovídajícího bitu podle následující tabulky:

		Certifikát Certifikační autority ACAeID	Osobní kvalifikované certifikáty
Kritický		Ano	Ano
0	digitalSignature	-	Volitelný
1	nonRepudiation	-	Nastaven - povinný
2	keyEncipherment	-	Volitelný
3	dataEncipherment	-	Volitelný
4	keyAgreement	-	-
5	keyCertSign	Nastaven	-
6	CRLSign	Nastaven	-
7	encipherOnly	-	-
8	decipherOnly	-	-

7.1.2.2 Certificate Policy

Rozšíření Certificate Policies má OID 0.4.0.1456.1.2 a položka obsahuje:

[1]Certificate Policy:
Policy Identifier=1.2.203.27112489.1.10.2.1.1
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CP
Qualifier:
http://www.eidentity.cz/aca/cp-qsc.pdf
[1,2] Policy Qualifier Info:
Policy Qualifier Id=User Notice
Qualifier:
Notice Text=Tento certifikat je vydan jako Kvalifikovany systemovy certifikat podle zakona 227/2000 Sb./This is Qualified System Certificate according to Czech Act No. 227/2000 Coll.

7.1.2.3 qcStatement

Pro označení kvalifikovaného certifikátu:
statementID – s textem prohlášení „Tento certifikat je vydan jako Kvalifikovany systemovy certifikat podle zakona 227/2000 Sb./This is Qualified System Certificate according to Czech Act No. 227/2000 Coll.“

7.1.2.4 Subject Alternative Names

Nekritický atribut v souladu s RFC3280 obsahuje adresu elektronické pošty ze žádosti o vystavení kvalifikovaného systémového certifikátu.

7.1.2.5 BasicConstraints

Certifikát ACAeID má nastaven atribut CA jako TRUE. Ostatní certifikáty mají tento atribut prázdný.

7.1.2.6 ExtendedKeyUsage

	Certifikát Certifikační autority ACAeID	Osobní kvalifikované certifikáty
Kritický	Ne	Ne
ServerAuth	-	-
ClientAuth	-	-
CodeSigning	-	-
EmaiProtection	-	Nastaven
ipsecEndSystem	-	-
ipsecTunnel	-	-
ipsecUser	-	-
TimeStamping	-	-
OCSP Signing	-	-

Microsoft Server Gated Crypto (SGC) OID:1.3.6.1.4.1.311.10.3.3	-	-
Netscape SGC OID: 2.16.840.1.113730.4.1	-	-

7.1.2.7 CRLDistributionPoints

Toto rozšíření obsahuje URL místa, kde spoléhající strany naleznou CRL. Rozšíření není kritické.

7.1.2.8 Authority Key Identifier

Obsahuje 160 bitový SHA1 výtah veřejného klíče certifikační autority ACAeID, která vydává kvalifikované certifikáty. Není to kritické rozšíření.

7.1.2.9 Subject Key Identifier

Obsahuje 160 bitový SHA1 výtah veřejného klíče držitele certifikátu. Není to kritické rozšíření.

7.1.3 Objektové identifikátory (OID) algoritmů

Pro účely vydávání kvalifikovaných certifikátů žadatelů se použije schválené podpisové schéma 001 definované vyhláškou 366/2001 Sb., tedy sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5), definované v RFC 2437 a také viz RFC 3370.

7.1.4 Způsoby zápisu jmen a názvů

Viz kapitola 3.1.

7.1.5 Omezení jmen a názvů

Je zakázáno použití jmen a názvů v rozporu se zákony.

7.1.6 Objektový identifikátor certifikační politiky

Pro CPS byl přidělen OID 1.2.203.27112489.1.21.1.

Pro tuto CP – QSC byl přidělen OID 1.2.203.27112489.1.10.2.1.1.

7.1.7 Rozšiřující položka „policy constraints“

Služba se neposkytuje.

7.1.8 Syntaxe a sémantika/význam rozšiřující položky kvalifikátorů politiky „policy qualifiers“

Služba se neposkytuje.

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz kapitola 7.1.2.2.

7.2 Profil CRL

OID	Kritický	Název	Hodnota
1.2.840.113549.1.1.5		signatureAlgoritmIdentifier	sha1withRSAEncryption
		issuer	DN vydavatele CRL
		thisUpdate	okamžik vydání CRL
		nextUpdate	okamžik vydání dalšího CRL
		revokedCertificate	Seznam zneplatněných kvalifikovaných certifikátů. Každá položka seznamu obsahuje: userCertificate – číslo certifikátu crlEntryExtension – důvod revokace (ReasonCode 2.5.29.21)
2.5.29.20		CRLNumber	pořadové číslo CRL
2.5.29.28	Ano	issuingDistributionPoint	URL adresa CRL
2.5.29.35		AuthorityKeyIdentifier	identifikátor veřejného klíče vydavatele

7.2.1 Číslo verze

Verze CRL je číslo 2.

7.2.2 Rozšíření CRL a CRL entry

Viz kapitola 7.2.

7.3 Profil OCSP

7.3.1 Číslo verze

Služba se neposkytuje.

7.3.2 Rozšíření OCSP

Služba se neposkytuje.

8 AUDIT SHODY A OSTATNÍ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Audit souladu systému s jeho dokumentací a požadavky zákona č. 227/2000 Sb. se provádí nejméně jednou ročně nebo při každé změně konfigurace.

8.2 Identita a kvalifikace hodnotitele

Hodnotitel musí vlastnit certifikát, který ho opravňuje k vykonávání takové činnosti.

8.3 Vztah hodnotitele k hodnocené entitě

Hodnotitel se nesmí podílet na budování či provozování hodnoceného systému.

8.4 Hodnocené oblasti

Seznam témat a způsob jejich hodnocení je dán použitou metodologií hodnocení.

8.5 Postup v případě zjištění nedostatků

Při zjištění nedostatků dojde k úpravě bezpečnostní dokumentace a následně popisu systému, případně implementačních či konfiguračních nastavení tak, aby došlo k odstranění nedostatků.

8.6 Sdělování výsledků hodnocení

Výsledky auditů jsou dostupné statutárnímu zástupci organizace a pracovníkovi, zodpovědnému za bezpečnost provozu.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání, příp. obnovení certifikátu

Výše poplatků za vydání certifikátu je uvedena v Ceníku služeb. Služba obnovení certifikátu se neposkytuje. Lze však vydat následný certifikát.

9.1.2 Poplatky za přístup k certifikátu

Přístup k seznamu vydaných certifikátů (CRL) je zdarma.

9.1.3 Poplatky za informace o stavu certifikátu a o zneplatnění

Přístup k CRL je zdarma.

9.1.4 Poplatky za další služby

Ceny dalších poskytovaných služeb jsou uvedeny v Ceníku služeb.

9.1.5 Jiná ustanovení týkající se poplatků

S ohledem na výše cen účtovaných služeb se nepředpokládá žádné rozložení plateb za odebrané služby.

9.2 Finanční zodpovědnost

9.2.1 Krytí pojištěním

Společnost eIdentity a.s. má uzavřenu pojistku podnikatelských rizik v dostatečné výši, aby byly pokryty případné finanční škody.

9.2.2 Další aktiva

Společnost eIdentity a.s. má připraveny i další kapitálové zdroje, které zajistí poskytování kvalitních certifikačních služeb na požadované úrovni kvality.

9.2.3 Pojištění nebo krytí zárukou pro koncové entity/uživatele

Služba se neposkytuje.

9.3 Důvěrnost obchodních informací

9.3.1 Stupnice (klasifikace) důvěrnosti informací

Za neveřejné obchodní informace se považují zejména informace o odebíraných službách, jejich ceny a obchodní smlouvy s nimi svázané. Za další takové informace se považují i smlouvy s třetími stranami, které se podílejí na provozu či jeho zajištění ACAeID, žádosti o poskytnutí služby, auditní a transakční záznamy, havarijní plány a plány obnovy, certifikační prováděcí směrnice, způsoby ochrany osobních údajů, zabezpečení obsluhy systému ACAeID, bezpečnostní opatření a jejich realizace.

9.3.2 Informace mimo rámec stupnice důvěrnosti informací

Za takové jsou považovány informace, které jsou zveřejněné pomocí webových služeb.

9.3.3 Odpovědnost za ochranu důvěrných informací

Každý pracovník, který přijde s informacemi podle kapitoly 9.3.1 do styku, je nesmí poskytnout třetí straně bez souhlasu odpovědného pracovníka eIdentity a.s.

9.4 Důvěrnost osobních informací

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb..

9.4.1 Plán důvěrnosti

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb..

9.4.2 Osobní údaje

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb..

9.4.3 Informace, které nejsou osobními údaji

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky

zákona 101/2000 Sb..

9.4.4 Odpovědnost za ochranu osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb..

9.4.5 Oznámení a souhlas s používáním osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb..

9.4.6 Zpřístupňování osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb..

9.4.7 Jiné náležitosti zpřístupňování osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 101/2000 Sb..

9.5 Práva duševního vlastnictví

Společnost eIdentity a.s. zachovává veškerá práva na intelektuální vlastnictví týkající se obsahu certifikátu a revokačních dat, obsahu politik, podle kterých se řídí poskytování certifikačních služeb a obsahu jmen, která mohou obsahovat ochranné známky, obchodní či jiné chráněné informace.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

Společnost eIdentity a.s. zaručuje, že:

- Veškeré údaje v certifikátu jsou uvedeny po jejich úspěšném prokázání hodnověrnými dokumenty
- Jsou uvedeny pouze správné a pravdivé údaje
- Certifikáty jsou vydány plně v souladu s touto CP
- Služba zneplatnění je poskytována plně v souladu s CP

Další záruky mohou být specifikovány ve smlouvě o poskytnutí služby.

9.6.2 Zastupování a záruky RA

Společnost eIdentity a.s. zaručuje, že průběh procesu na registračním místě bude plně v souladu s touto CP.

9.6.3 Zastupování a záruky podepisující osoby

Podepisující osoby budou ručit za informace podle smlouvy o poskytnutí služby.

9.6.4 Zastupování a záruky spoléhajících se stran

Předpokládá se, že spoléhající se strany postupují v souladu se zákonem 227/2000 Sb. a jeho prováděcími předpisy.

9.6.5 Zastupování a záruky ostatních účastníků

Neposkytuje se.

9.7 Zřeknutí se záruk

Poskytování služeb se řídí zejména zákonem 227/2000 Sb. a nelze se zříci záruk v něm určeným.

9.8 Hranice (meze) odpovědnosti

Hranice odpovědnosti jsou dány zákonem 227/2000 Sb. a jsou závazné pro všechny prvky PKI.

9.9 Náhrada škody

V případě vydání certifikátu, jehož obsah neodpovídá skutečnostem ověřeným v průběhu zdárného procesu na registračním místě, nebo v případě neoprávněného zneplatnění certifikátu bude poskytnut nový certifikát zdarma.

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

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Certifikační politika zůstává v platnosti do konce doby platnosti posledního kvalifikovaného systémového certifikátu, který byl podle této politiky vydán. Novou verzi schvaluje a vyhlašuje Výbor pro politiky na základě svého jednacího řádu.

9.10.2 Ukončení

Úpravy CP včetně zajištění souladu politik schvaluje Výbor pro politiky.

9.10.3 Důsledky ukončení a přetrvání závazků

CP bude platit nejméně po dobu platnosti posledního podle ní vydaného certifikátu.

9.11 Komunikace mezi účastníky

Pro účely individuální komunikace s jednotlivými subjekty se může využít prostředí jejich osobních účtů nebo emailových adres, telefonických rozhovorů či osobního jednání.

9.12 Změny

9.12.1 Postup při změnách

Postup probíhá řízeným procesem.

9.12.2 Postup při oznámování změn

Postup probíhá řízeným procesem.

9.12.3 Okolnosti, při kterých musí být změněn OID

Postup probíhá řízeným procesem.

9.13 Opatření pro řešení sporů

V případě nesouhlasu s postupem pracovníků eIdentity a.s. je možné se obrátit přímo na statutární orgán společnosti, případně se obrátit na soud místně příslušný sídlu poskytovatele.

9.14 Relevantní právní úprava

Činnost eIdentity a.s. se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Systém je provozován ve shodě s požadavky zákona 227/2000 Sb., 101/2000 Sb. a dalšími a je provozován jako akreditovaný k poskytování kvalifikovaných certifikačních služeb.

9.16 Další ustanovení

Není použito.

9.16.1 Celková dohoda

Není použito.

9.16.2 Postoupení práv

Není použito.

9.16.3 Oddělitelnost

Není použito.

9.16.4 Platby obhájcům a zřeknutí se práv

Není použito.

9.16.5 Vyšší moc

Smlouva o poskytnutí služby může obsahovat ustanovení o působení vyšší moci.

9.17 Další opatření

Není použito.

10 ZÁVĚREČNÁ USTANOVENÍ

Tato CP – QSC byla projednána na jednání Výboru pro politiky a podle zápisu byla přijata a vyhlášena.