První certifikační autorita, a.s.

(akreditovaný poskytovatel certifikačních služeb)

CERTIFIKAČNÍ PROVÁDĚCÍ SMĚRNICE

VYDÁVÁNÍ NADŘÍZENÝCH KVALIFIKOVANÝCH SYSTÉMOVÝCH CERTIFIKÁTŮ I.CA

Verze 3.5

Tabulka 1 - Identifikace

Název	Certifikační prováděcí směrnice nadřízených kvalifikovaných systémových certifikátů I.CA
Společnost	První certifikační autorita, a.s.
Schválil	Ředitel společnosti První certifikační autorita, a.s.

Tabulka 2 – Vývoj dokumentu

Verze	**Datum vydání**	**Shrnutí změn**
3.0	03.08.2009	Implementace požadavků ETSI TS 102 176-1 (viz vyhláška České republiky č. 378/2006 Sb.) – rodina SHA2
3.1	04.12.2009	Úprava profilu certifikátu TSU
3.2	01.12.2011	Revize a úprava dokumentu - zejména kapitol 3, 4, 6
3.3	17.12.2012	Aktualizace názvů interních směrnic
3.4	12.01.2015	aktualizace odkazovaných norem a standardů
3.5	22.09.2015	Aktualizace a revize dokumentu

Obsah

1 ÚVOD 9

1.1 PŘEHLED 9
1.2 NÁZEV A IDENTIFIKACE DOKUMENTU 9
1.3 PARTICIPUJÍCÍ SUBJEKTY 10
1.3.1 Certifikační autority (dále "CA") 10
1.3.2 Registrační autority (dále "RA") 10
1.3.3 Držitelé kvalifikovaných certifikátů a podepisující nebo označující osoby, kteří požádali o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu (dále certifikátu) a kterým byl certifikát vydán 10
1.3.4 Spoléhající se strany 10
1.3.5 Jiné participující subjekty 10
1.4 POUŽITÍ CERTIFIKÁTU 10
1.4.1 Přípustné použití certifikátu 10
1.4.2 Omezení použití certifikátu 10
1.5 SPRÁVA POLITIKY 10
1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici 10
1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici 11
1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb 11
1.5.4 Postupy při schvalování souladu s bodem 1.5.3 11
1.6 PŘEHLED POUŽITÝCH POJMŮ A ZKRATEK 11

2 ODPOVĚDNOSTI ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE 13

2.1 ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE 13
2.2 ZVEŘEJŇOVÁNÍ INFORMACÍ A DOKUMENTACE 13
2.3 PERIODICITA ZVEŘEJŇOVÁNÍ INFORMACÍ 13
2.4 ŘÍZENÍ PŘÍSTUPU K JEDNOTLIVÝM TYPŮM ÚLOŽIŠŤ 14

3 IDENTIFIKACE A AUTENTIZACE 15

3.1 POJMENOVÁVÁNÍ 15
3.1.1 Typy jmen 15
3.1.1.1 nQCA 15
3.1.1.2 nQTSA 15
3.1.2 Požadavek na významovost jmen 15
3.1.3 Anonymita a používání pseudonymu 15
3.1.4 Pravidla pro interpretaci různých forem jmen 15
3.1.5 Jedinečnost jmen 15
3.1.6 Obchodní značky 15
3.2 POČÁTEČNÍ OVĚŘENÍ IDENTITY 16
3.2.1 Ověření souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek 16
3.2.2 Ověřování identity právnické osoby nebo organizační složky státu 16
3.2.3 Ověřování identity fyzické osoby 16
3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě 16
3.2.5 Ověřování specifických práv 17
3.2.6 Kritéria pro interoperabilitu 17
3.3 IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKŮ NA VÝMĚNU DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÝCH PODPISŮ NEBO ELEKTRONICKÝCH ZNAČEK V CERTIFIKÁTU 17
3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a jim odpovídajících dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek (dále „párová data") 17
3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu 17
3.4 IDENTIFIKACE A AUTENTIZACE PŘI ZPRACOVÁNÍ POŽADAVKŮ NA ZNEPLATNĚNÍ CERTIFIKÁTU 17

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU 18

4.1 ŽÁDOST O VYDÁNÍ CERTIFIKÁTU 18
4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu 18
4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele 18
4.2 ZPRACOVÁNÍ ŽÁDOSTI O CERTIFIKÁT 18
4.2.1 Identifikace a autentizace 18
4.2.2 Přijetí nebo odmítnutí žádosti o certifikát 18
4.2.3 Doba zpracování žádosti o certifikát 18
4.3 VYDÁNÍ CERTIFIKÁTU 18
4.3.1 Úkony CA v průběhu vydání certifikátu 18
4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující osobě nebo označující osobě 18
4.4 PŘEVZETÍ VYDANÉHO CERTIFIKÁTU 18
4.4.1 Úkony spojené s převzetím certifikátu 18
4.4.2 Zveřejňování vydaných certifikátů poskytovatelem 19
4.4.3 Oznámení o vydání certifikátu jiným subjektům 19
4.5 POUŽITÍ PÁROVÝCH DAT A CERTIFIKÁTU 19
4.5.1 Použití dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a certifikátu držitelem certifikátu, podepisující osobou nebo označující osobou 19
4.5.2 Použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a certifikátu spoléhající se stranou 19
4.6 OBNOVENÍ CERTIFIKÁTU 19
4.6.1 Podmínky pro obnovení certifikátu 19
4.6.2 Subjekty oprávněné požadovat obnovení certifikátu 19
4.6.3 Zpracování požadavku na obnovení certifikátu 19
4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující osobě nebo označující osobě 19
4.6.5 Úkony spojené s převzetím obnoveného certifikátu 20
4.6.6 Zveřejnění vydaných obnovených certifikátů poskytovatelem 20
4.6.7 Oznámení o vydání obnoveného certifikátu ostatním subjektům 20
4.7 VÝMĚNA DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÝCH PODPISŮ NEBO DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÝCH ZNAČEK V CERTIFIKÁTU 20
4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu 20
4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu 20
4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu 20
4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek podepisující nebo označující osobě 20
4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek 20
4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek 20
4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek 21
4.8 ZMĚNA ÚDAJŮ V CERTIFIKÁTU 21
4.8.1 Podmínky pro změnu údajů v certifikátu 21
4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu 21
4.8.3 Zpracování požadavku na změnu údajů v certifikátu 21
4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo označující osobě 21
4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji 21
4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji 21
4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům 21
4.9 ZNEPLATNĚNÍ A POZASTAVENÍ PLATNOSTI CERTIFIKÁTU 21
4.9.1 Podmínky pro zneplatnění certifikátu 21
4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu 22
4.9.3 Požadavek na zneplatnění certifikátu 22

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu *22*
4.9.5 Maximální doba, za kterou musí poskytovatel realizovat požadavek na zneplatnění certifikátu *22*
4.9.6 Povinnosti spoléhajících se stran při ověřování, zda nebyl certifikát zneplatněn *22*
4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů *22*
4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů *22*
4.9.9 Možnost ověřování statutu certifikátu on-line („dále OCSP") *22*
4.9.10 Požadavky při ověřování statutu certifikátu na on-line *22*
4.9.11 Jiné způsoby oznamování zneplatnění certifikátu *23*
4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek *23*
4.9.13 Podmínky pro pozastavení platnosti certifikátu *23*
4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu *23*
4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu *23*
4.9.16 Omezení doby pozastavení platnosti certifikátu *23*
4.10 SLUŽBY SOUVISEJÍCÍ S OVĚŘOVÁNÍM STATUTU CERTIFIKÁTU 23
4.10.1 Funkční charakteristiky *23*
4.10.2 Dostupnost služeb *24*
4.10.3 Další charakteristiky služeb statutu certifikátu *24*
4.11 UKONČENÍ POSKYTOVÁNÍ SLUŽEB PRO DRŽITELE CERTIFIKÁTU, PODEPISUJÍCÍ NEBO OZNAČUJÍCÍ OSOBOU 24
4.12 ÚSCHOVA DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ NEBO DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH ZNAČEK U DŮVĚRYHODNÉ TŘETÍ STRANY A JEJICH OBNOVA 24
4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek *24*
4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci *24*

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST 25

5.1 FYZICKÁ BEZPEČNOST 25
5.1.1 Umístění a konstrukce *25*
5.1.2 Fyzický přístup *25*
5.1.3 Elektřina a klimatizace *25*
5.1.4 Vliv vody *25*
5.1.5 Protipožární opatření a ochrana *26*
5.1.6 Ukládání médií *26*
5.1.7 Nakládání s odpady *26*
5.1.8 Zálohy mimo budovu provozního pracoviště *26*
5.2 PROCESNÍ BEZPEČNOST 26
5.2.1 Důvěryhodné role *26*
5.2.2 Počet osob požadovaných na zajištění jednotlivých činností *26*
5.2.3 Identifikace a autentizace pro každou roli *27*
5.2.4 Role vyžadující rozdělení povinností *27*
5.3 PERSONÁLNÍ BEZPEČNOST 27
5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost *27*
5.3.2 Posouzení spolehlivosti osob *27*
5.3.3 Požadavky na přípravu pro výkon role, vstupní školení *28*
5.3.4 Požadavky a periodicita školení *28*
5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi *28*
5.3.6 Postihy za neoprávněné činnosti zaměstnanců *28*
5.3.7 Požadavky na nezávislé zhotovitele (dodavatele) *28*
5.3.8 Dokumentace poskytovaná zaměstnancům *28*
5.4 AUDITNÍ ZÁZNAMY (LOGY) 28
5.4.1 Typy zaznamenávaných událostí *29*
5.4.2 Periodicita zpracování záznamů *29*
5.4.3 Doba uchovávání auditních záznamů *29*
5.4.4 Ochrana auditních záznamů *30*
5.4.5 Postupy pro zálohování auditních záznamů *30*
5.4.6 Systém shromažďování auditních záznamů (interní nebo externí) *30*

5.4.7 Postup při oznamování události subjektu, který ji způsobil 30
5.4.8 Hodnocení zranitelnosti 30
5.5 UCHOVÁVÁNÍ INFORMACÍ A DOKUMENTACE 30
5.5.1 Typy informací a dokumentace, které se uchovávají 31
5.5.2 Doba uchovávání uchovávaných informací a dokumentace 31
5.5.3 Ochrana úložiště uchovávaných informací a dokumentace 31
5.5.4 Postupy při zálohování uchovávaných informací a dokumentace 31
5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace 31
5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní, externí) 31
5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace 31
5.6 VÝMĚNA DAT PRO OVĚŘOVÁNÍ ELEKTRONICKÝCH ZNAČEK V NADŘÍZENÉM KVALIFIKOVANÉM SYSTÉMOVÉM CERTIFIKÁTU POSKYTOVATELE 32
5.7 OBNOVA PO HAVÁRII NEBO KOMPROMITACI 32
5.7.1 Postup v případě incidentu a kompromitace 32
5.7.2 Poškození výpočetních prostředků, software nebo dat 32
5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek/podpisů poskytovatele 32
5.7.4 Schopnosti obnovit činnost po havárii 33
5.8 UKONČENÍ ČINNOSTI CA 33

6 TECHNICKÁ BEZPEČNOST 36

6.1 GENEROVÁNÍ A INSTALACE PÁROVÝCH DAT 36
6.1.1 Generování párových dat 36
6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek podepisující nebo označující osobě 36
6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek poskytovateli certifikačních služeb 36
6.1.4 Poskytování dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám 37
6.1.5 Délky párových dat 37
6.1.6 Generování parametrů dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a kontrola jejich kvality 37
6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek 37
6.2 OCHRANA DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ NEBO DAT PRO VYTVÁŘENÍ ELEKTRONICKÝCH ZNAČEK A BEZPEČNOST KRYPTOGRAFICKÝCH MODULŮ 37
6.2.1 Standardy a podmínky používání kryptografických modulů 37
6.2.2 Sdílení tajemství 38
6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 38
6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 38
6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 38
6.2.6 Transfer dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu 38
6.2.7 Uložení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek v kryptografickém modulu 38
6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 39
6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 39
6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek 39
6.2.11 Hodnocení kryptografického modulu 39
6.3 DALŠÍ ASPEKTY SPRÁVY PÁROVÝCH DAT 40
6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek 40

6.3.2 Maximální doba platnosti certifikátu označující osoby a párových dat ... 40
6.4 AKTIVAČNÍ DATA ... 40
6.4.1 Generování a instalace aktivačních dat ... 40
6.4.2 Ochrana aktivačních dat ... 40
6.4.3 Ostatní aspekty aktivačních dat ... 40
6.5 POČÍTAČOVÁ BEZPEČNOST ... 40
6.5.1 Specifické technické požadavky na počítačovou bezpečnost ... 40
6.5.2 Hodnocení počítačové bezpečnosti ... 41
6.6 BEZPEČNOST ŽIVOTNÍHO CYKLU ... 42
6.6.1 Řízení vývoje systému ... 42
6.6.2 Kontroly řízení bezpečnosti ... 42
6.6.3 Řízení bezpečnosti životního cyklu ... 42
6.7 SÍŤOVÁ BEZPEČNOST ... 42
6.8 ČASOVÁ RAZÍTKA ... 42

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP ... 43

7.1 PROFIL CERTIFIKÁTU ... 43
7.1.1 Čísla verzí ... 43
7.1.2 Rozšiřující položky v certifikátu ... 43
7.1.3 Objektové identifikátory (dále OID) algoritmů ... 43
7.1.4 Způsoby zápisu jmen a názvů ... 43
7.1.5 Omezení jmen a názvů ... 43
7.1.6 OID certifikační politiky ... 43
7.1.7 Rozšiřující položka „PolicyConstraints“ ... 43
7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „PolicyQualifiers“ ... 43
7.1.9 Způsob zápisu kritické rozšiřující položky „CertificatePolicies“ ... 43
7.2 PROFIL SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ ... 44
7.2.1 Číslo verze ... 44
7.2.2 Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů ... 44
7.3 PROFIL OCSP ... 44
7.3.1 Číslo verze ... 44
7.3.2 Rozšiřující položky OCSP ... 44

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ ... 45

8.1 PERIODICITA HODNOCENÍ NEBO OKOLNOSTI PRO PROVEDENÍ HODNOCENÍ ... 45
8.2 IDENTITA A KVALIFIKACE HODNOTITELE ... 45
8.3 VZTAH HODNOTITELE K HODNOCENÉ ENTITĚ ... 45
8.4 HODNOCENÉ OBLASTI ... 45
8.5 POSTUP V PŘÍPADĚ ZJIŠTĚNÝCH NEDOSTATKŮ ... 46
8.6 SDĚLOVÁNÍ VÝSLEDKŮ HODNOCENÍ ... 46

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI ... 47

9.1 POPLATKY ... 47
9.1.1 Poplatky za vydání nebo obnovení certifikátu ... 47
9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů ... 47
9.1.3 Poplatky za informace o statutu certifikátu a o zneplatnění certifikátu ... 47
9.1.4 Poplatky za další služby ... 47
9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací) ... 47
9.2 FINANČNÍ ODPOVĚDNOST ... 47
9.2.1 Krytí pojištěním ... 47
9.2.2 Další aktiva a záruky ... 47
9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele ... 47
9.3 CITLIVOST OBCHODNÍCH INFORMACÍ ... 48
9.3.1 Výčet citlivých informací ... 48
9.3.2 Informace mimo rámec citlivých informací ... 48
9.3.3 Odpovědnost za ochranu citlivých informací ... 48

9.4 OCHRANA OSOBNÍCH ÚDAJŮ 48
9.4.1 Politika ochrany osobních údajů 48
9.4.2 Osobní údaje 48
9.4.3 Údaje, které nejsou považovány za důvěrné 48
9.4.4 Odpovědnost za ochranu osobních údajů 48
9.4.5 Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací 49
9.4.6 Poskytování citlivých informací pro soudní či správní účely 49
9.4.7 Jiné okolnosti zpřístupňování osobních údajů 49
9.5 PRÁVA DUŠEVNÍHO VLASTNICTVÍ 49
9.6 ZASTUPOVÁNÍ A ZÁRUKY 49
9.6.1 Zastupování a záruky CA 49
9.6.2 Zastupování a záruky RA 49
9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby 49
9.6.4 Zastupování a záruky spoléhajících se stran 50
9.6.5 Zastupování a záruky ostatních zúčastněných subjektů 50
9.7 ZŘEKNUTÍ SE ZÁRUK 50
9.8 OMEZENÍ ODPOVĚDNOSTI 50
9.9 ODPOVĚDNOST ZA ŠKODU, NÁHRADA ŠKODY 50
9.10 DOBA PLATNOSTI, UKONČENÍ PLATNOSTI 50
9.10.1 Doba platnosti 50
9.10.2 Ukončení platnosti 50
9.10.3 Důsledky ukončení a přetrvání závazků 50
9.11 KOMUNIKACE MEZI ZÚČASTNĚNÝMI SUBJEKTY 50
9.12 ZMĚNY 51
9.12.1 Postup při změnách 51
9.12.2 Postup při oznamování změn 51
9.12.3 Okolnosti, při kterých musí být změněno OID 51
9.13 ŘEŠENÍ SPORŮ 51
9.14 ROZHODNÉ PRÁVO 51
9.15 SHODA S PRÁVNÍMI PŘEDPISY 51
9.16 DALŠÍ USTANOVENÍ 51
9.16.1 Rámcová dohoda 51
9.16.2 Postoupení práv 51
9.16.3 Oddělitelnost ustanovení 52
9.16.4 Zřeknutí se práv 52
9.16.5 Vyšší moc 52
9.17 DALŠÍ OPATŘENÍ 52
10 ZÁVĚREČNÁ USTANOVENÍ 53

1 Úvod

1.1 Přehled

Tento dokument, **Certifikační prováděcí směrnice vydávání nadřízených kvalifikovaných systémových certifikátů I.CA** (dále též CPS), vypracovaný společností První certifikační autorita, a. s. (dále též I.CA):

- se zabývá skutečnostmi, které se vztahují na I.CA a které souvisejí s vydáváním nadřízených kvalifikovaných systémových certifikátů I.CA, jejich další správou, použitím, akceptací, ukončením platnosti, zneplatněním a všemi aspekty souvisejícími s nakládáním s párovými daty,
- striktně dodržuje členění dokumentu navržené v RFC 3647, s přihlédnutím k doporučením orgánů EU a k právu ČR v dané oblasti. Jednotlivé kapitoly jsou proto v této CPS zachovány i v případě, že jsou ve vztahu k ní irelevantní,
- může být mimo jiné využit nezávislými institucemi (např. auditorskými společnostmi) jako základ pro potvrzení toho, že kvalifikované certifikační služby poskytované společností První certifikační autorita, a.s., je možné považovat za důvěryhodné.

Nadřízenými kvalifikovanými systémovými certifikáty jsou v souladu s legislativou ČR, vztahující se k problematice elektronického podpisu, kvalifikované systémové certifikáty, které obsahují data pro ověřování elektronických značek odpovídající datům pro vytváření elektronických značek, kterými poskytovatel označuje vydávané kvalifikované certifikáty, kvalifikované systémové certifikáty a seznamy zneplatněných certifikátů (dále též nQCA) a vydávaná kvalifikovaná časová razítka (dále též nQTSA).

Společnost První certifikační autorita, a.s., je akreditovaným poskytovatelem certifikačních služeb v oblastech:

- kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů a kvalifikovaných časových razítek dle zákona České republiky č. 227/2000 Sb., o elektronickém podpisu, a proto jsou v procesech certifikačních služeb využívány oba výše typy nadřízených kvalifikovaných systémových certifikátů,
- kvalifikovaných certifikátů a časových razítek dle zákona Slovenské republiky č. 215/2002 Z.z., o elektronickom podpise, kdy „certifikát pro správu“ je ekvivalentní „nadřízenému kvalifikovanému certifikátu“.

1.2 Název a identifikace dokumentu

Název tohoto dokumentu:	Certifikační prováděcí směrnice vydávání nadřízených kvalifikovaných systémových certifikátů I.CA, verze 3.5
OID dokumentu:	není přiřazeno

Tato CPS se vztahuje k následující CP:

OID	CP
1.3.6.1.4.1.23624.1.1.10.3.4	Certifikační politika vydávání nadřízených kvalifikovaných systémových certifikátů I.CA

1.3 Participující subjekty

1.3.1 Certifikační autority (dále "CA")

Společnost První certifikační autorita, a. s., (dále též I.CA) je akreditovaným poskytovatelem certifikačních služeb v souladu s legislativou České republika a Slovenské republiky, vztahující se k problematice elektronického podpisu.

1.3.2 Registrační autority (dále "RA")

Poskytování služeb společnosti První certifikační autorita, a.s., pro veřejnost se realizuje prostřednictvím veřejných registračních autorit (vlastních nebo smluvních partnerů), které jsou v případě nadřízených kvalifikovaných systémových certifikátů využívány pouze pro případné předání těchto certifikátů, resp. informací o těchto certifikátech veřejnosti.

1.3.3 Držitelé kvalifikovaných certifikátů a podepisující nebo označující osoby, kteří požádali o vydání kvalifikovaného certifikátu nebo kvalifikovaného systémového certifikátu (dále certifikátu) a kterým byl certifikát vydán

Držitelem nadřízených kvalifikovaných systémových certifikátů I.CA je společnost První certifikační autorita, a.s. Oprávněným žadatelem a následně držitelem certifikátů je I.CA jako právnická osoba.

1.3.4 Spoléhající se strany

Spoléhající se stranou mohou být fyzické osoby, právnické osoby nebo organizační složky státu, spoléhající se na vydaný certifikát dle příslušné CP.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány dozoru (viz ZoEP), orgány činné v trestním řízení a další, kterým to ze zákona přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Nadřízené kvalifikované systémové certifikáty vydávané dle této certifikační politiky lze využívat pouze v procesech ověřování elektronické značky, resp. elektronického podpisu vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů, kvalifikovaných časových razítek a v souladu s platnou legislativou (ZoEP, VoEP).

1.4.2 Omezení použití certifikátu

Nadřízené kvalifikované certifikáty nesmí být využívány v rozporu s vydávaným účelem (definovaným touto certifikační politikou), platnou legislativou (ZoEP, VoEP) a dalšími právními předpisy.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

První certifikační autorita, a.s.

Podvinný mlýn 2178/6
190 00 Praha 9
Česká republika

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Pracovník I.CA, jmenovaný ředitelem společnosti První certifikační autorita, a.s., do funkce bezpečnostního manažera.

1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., s postupy jiných poskytovatelů certifikačních služeb, je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování souladu s bodem 1.5.3

V případě, že je potřebné provést změny a tedy i vytvořit novou verzi této CPS, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provádět (viz kapitola 1.5.2). Nabytí platnosti nových verzí CPS předchází jejich schválení ředitelem společnosti První certifikační autorita, a.s.

1.6 Přehled použitých pojmů a zkratek

Tabulka 3 – Pojmy a zkratky

Pojem	Vysvětlení
CP	certifikační politika (veřejný dokument)
CPS	certifikační prováděcí směrnice (neveřejný dokument)
CRL	**C**ertificate **R**evocation **L**ist (seznam zneplatněných certifikátů)
Držitel certifikátu	fyzická osoba, právnická osoba nebo organizační složka státu, která požádala o vydání certifikátu pro sebe nebo pro podepisující osobu a které byl certifikát vydán
Čas	světový čas UTC
Elektronický podpis, resp. elektronická značka	údaje, resp. informace, které splňují požadavky platné legislativy[1]
ETSI	**E**uropean **T**elecommunications **S**tandards **I**nstitute
I.CA	První certifikační autorita, a.s. – akreditovaný poskytovatel certifikačních služeb
Kvalifikovaný certifikát, kvalifikovaný systémový certifikát, nadřízený kvalifikovaný systémový certifikát, kvalifikované časové razítko	viz platná legislativa
MV ČR	Ministerstvo vnitra České republiky
nQCA	certifikáty spojené s vydáváním kvalifikovaných certifikátů a/nebo kvalifikovaných systémových certifikátů vydávaných koncovým uživatelům
nQTSA	certifikáty spojené s vydáváním kvalifikovaných časových razítek, resp. časových razítek
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology

[1] Viz ZoEP

Označující osoba	fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou
Párová data (dvojice soukromý a veřejný klíč)	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky spolu s odpovídajícími daty pro ověřování elektronického podpisu, resp. elektronické značky
Podepisující osoba	fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby
Smluvní partner	poskytovatel certifikačních služeb, který zajišťuje na základě písemné smlouvy pro I.CA certifikační služby nebo jejich části
Soukromý klíč	jedinečná data pro vytváření elektronického podpisu, resp. elektronické značky
Spoléhající se strana	subjekt spoléhající se při své činnosti na certifikát vydaný I.CA
TSS	Time Stamp Service (služba vydávání kvalifikovaných časových razítek)
TSU	Time Stamp Unit (vyhrazený server, generující kvalifikovaná časová razítka)
UTC	**U**niversal **C**o-ordinated **T**ime, Standard přijatý 1. 1. 1972 pro světový koordinovaný čas (Coordinated Universal Time – UTC). Funkci "oficiálního časoměřiče" atomového času pro celý svět vykonává Bureau International de l'Heure (BIH)
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu, resp. elektronické značky
VoEP	vyhláška České republiky č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb, o požadavcích na nástroje elektronického podpisu a o požadavcích na ochranu dat pro vytváření elektronických značek (vyhláška o postupech kvalifikovaných poskytovatelů certifikačních služeb)
ZoEP	aktuální znění zákona České republiky č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu),

2 Odpovědnosti za zveřejňování a úložiště informací a dokumentace

2.1 Úložiště informací a dokumentace

Společnost První certifikační autorita, a.s., s ohledem na požadavky ZoEP zřizuje a provozuje úložiště informací a dokumentace, za která taktéž jako poskytovatel certifikačních služeb odpovídá.

2.2 Zveřejňování informací a dokumentace

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s. (certifikační politiky, zprávy pro uživatele, další informace dle ZoEP a VoEP, ostatní veřejné a aktuální informace a dokumenty atd.), případně odkazy pro zjištění dalších informací, jsou:

a) První certifikační autorita, a.s.

   Podvinný mlýn 2178/6, 190 00 Praha 9, Česká republika

b) internetová adresa http://www.ica.cz

c) sídla registračních autorit

Adresy, které slouží pro kontakt veřejnosti s I.CA, jsou:

a) sídlo registrační autority, která smluvní vztah s I.CA zprostředkovala

b) elektronická poštovní adresa info@ica.cz

I.CA zveřejňuje výše uvedené kontaktní adresy na své internetové adrese a pracovištích vlastních registračních autorit. Pracovníci I.CA a smluvních partnerů jsou rovněž povinni tyto informace na vyžádání sdělit veřejnosti.

V případech odejmutí akreditace nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů nebo kvalifikovaných časových razítek, oznámí I.CA tuto skutečnost na své internetové informační adrese a prostřednictvím nejméně jednoho celostátně distribuovaného deníku.

2.3 Periodicita zveřejňování informací

S ohledem na problematiku nadřízených kvalifikovaných systémových certifikátů I.CA zveřejňuje I.CA informace s následující periodicitou:

- Získání nebo odejmutí akreditace – bezodkladně.
- Nadřízené kvalifikované systémové certifikáty I.CA včetně hashe – před jejich využíváním.
- Informace o zneplatnění certifikátů nadřízených kvalifikovaných systémových certifikátů I.CA s uvedením důvodu zneplatnění (v případě zneužití nebo vzniku důvodné obavy ze zneužití dat pro vytváření elektronických značek, resp. elektronických podpisů, určených pro označování, resp. podepisování vydávaných certifikátů, seznamů zneplatněných certifikátů nebo časových razítek) – bezodkladně.
- Seznam zneplatněných certifikátů (CRL) - maximálně za 24 hodin od vydání předchozího CRL (zpravidla à 8 hodin).
- Ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí odrážet aktuální stav poskytovaných kvalifikovaných certifikačních služeb.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným pracovníkům I.CA, smluvním partnerům nebo subjektům, definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly, uvedenými v interní dokumentaci, zejména:

- ***„Operátor CA“,***
- ***„Směrnice pro pracovníky RA I.CA“,***
- ***„Řízení bezpečnosti informací“,***
- ***„Příručka administrátora“,***
- ***„Bezpečnostní incidenty“,***
- ***„HSM/Private Server“,***
- ***„Správa TSS“,***
- ***„Dokumenty agendy certifikačních služeb“,***
- ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“,***
- ***„Dílčí spisový a skartační plán pro agendy certifikačních služeb“.***

3 Identifikace a autentizace

3.1 Pojmenovávání

3.1.1 Typy jmen

3.1.1.1 nQCA

Tabulka 4 – Issuer, Subject

Položka	Obsah
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName(OU)	I.CA – Accredited Provider of Certification Services
CommonName (CN)	I.CA – Qualified Certification Authority, MM/RRRR
Country (C)	CZ

Pozn.: MM/RRRR je měsíc a rok vydání certifikátu nQCA

3.1.1.2 nQTSA

Issuer – viz Tabulka 4

Tabulka 5 – Subject

Položka	Hodnota
Organization (O)	První certifikační autorita, a.s.
OrganizationUnitName (OU)	I.CA – Accredited Provider of Certification Services
CommonName (CN)	I.CA - Time Stamping Authority, TSS/TSU X, MM/RRRR
Country (C)	CZ

Pozn.: X – číslo TSU, MM/RRRR – měsíc a rok vydání certifikátu nQTSA

3.1.2 Požadavek na významovost jmen

Viz obsah sloupce Hodnota v tabulkách uvedených v kapitole 3.1.1.

3.1.3 Anonymita a používání pseudonymu

Není využíváno.

3.1.4 Pravidla pro interpretaci různých forem jmen

Pokud se jedná o jména nebo jiné skutečnosti, které jsou uvedeny v předkládaných dokumentech, přenášejí se tato jména v té podobě, v jaké jsou v dokumentu uvedena. Vlastní transkripce se neprovádí.

3.1.5 Jedinečnost jmen

Jedinečnost jména Subject a Issuer je zaručena.

3.1.6 Obchodní značky

Ve vydaném nQCA/nQTSA se musí ověřitelné údaje vztahovat k I.CA.

3.2 Počáteční ověření identity

3.2.1 Ověření souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů nebo data pro vytváření elektronických značek odpovídající datům pro ověřování elektronických značek

Vlastnictví dat pro vytváření elektronických značek, resp. elektronických podpisů, odpovídajících datům pro ověřování elektronických značek, resp. elektronických podpisů, která bude daný nQCA/nQTSA obsahovat, se prokazuje v procesu generování párových dat, případně předložením žádosti o certifikát (PKCS#10) ověřujícímu subjektu. Samotný proces generování párových dat je prováděn v souladu s interními směrnicemi a dokumentací výrobce konkrétního HSM.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Jsou vyžadovány listinné dokumenty (originál nebo notářsky ověřená kopie výpisu z obchodního rejstříku), na jejichž základě byla I.CA vytvořena a které musí obsahovat úplné obchodní jméno, identifikační číslo (IČ), statutární orgán a sídlo.

3.2.3 Ověřování identity fyzické osoby

Fyzickou osobou, která může rozhodnout a následně žádat o vydání nQCA/nQTSA, je výhradně ředitel společnosti První certifikační autorita, a.s.

V procesu ověřování identity jsou vyžadovány listinné dokumenty (originál nebo notářsky ověřená kopie), které dokládají jmenování ředitelem I.CA. Dále je vyžadováno předložení následujících údajů:

- celé občanské jméno,
- datum narození (nebo rodné číslo u občanů České republiky, resp. Slovenské republiky),
- číslo předloženého primárního osobního dokladu,
- adresa trvalého bydliště (je-li v primárním dokladu uvedena).

Vyžaduje se předložení originálu platného primárního osobního dokladu a originálu dalšího osobního dokladu (sekundárního). Primární osobní doklad pro občany ČR musí být občanský průkaz, popř. obdobný doklad stejné právní váhy. Primární osobní doklad pro cizince je platný cestovní pas, popř. obdobný doklad stejné právní váhy. Sekundární osobní doklad musí být vydán orgánem veřejné moci nebo jinou organizací, jejíž existenci lze doložit. Sekundární osobní doklad musí obsahovat celé občanské jméno fyzické osoby, vyřizující žádost a dále nejméně jeden z následujících údajů:

- datum narození (nebo rodné číslo u občanů ČR),
- adresu trvalého bydliště žadatele,
- fotografii obličeje.

Údaje požadované v sekundárním osobním dokladu musí být shodné s těmito údaji v primárním osobním dokladu.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu nebo podepisující či označující osobě

Všechny informace musí být ověřeny.

3.2.5 Ověřování specifických práv

Není využíváno.

3.2.6 Kritéria pro interoperabilitu

Není využíváno.

3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů nebo elektronických značek v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a jim odpovídajících dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek (dále „párová data“)

Vydání certifikátu je vždy spojeno s fyzickou generací nových párových dat a vydáním nového certifikátu.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Vydání certifikátu je vždy spojeno s fyzickou generací nových párových dat a vydáním nového certifikátu.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Oprávněným žadatelem o zneplatnění nQCA/nQTSA je výhradně ředitel společnosti První certifikační autorita, a.s.

4 Požadavky na životní cyklus certifikátu

V souladu s legislativou (odkazující se na doporučení technické specifikace ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites je v procesu vydávání nadřízených kvalifikovaných systémových certifikátů využíván algoritmus RSA s SHA-256 (sha256RSA) a délka kryptografického klíče pro algoritmus RSA 2048 bitů.

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Viz kapitola 3.2.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Viz kapitola 3.2.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Viz kapitola 3.2.

4.2.2 Přijetí nebo odmítnutí žádosti o certifikát

Viz kapitola 4.3..

4.2.3 Doba zpracování žádosti o certifikát

Při dodržení všech potřebných podmínek řádově minuty.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydání certifikátu

Viz relevantní podkapitoly kapitoly 3.2.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu, podepisující osobě nebo označující osobě

V procesu vydávání nQCA/nQTSA je ředitel I.CA informován prostřednictvím pracovníků komise (jedná se o kmenové pracovníky I.CA).

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Pokud byly splněny podmínky pro vydání nQCA/nQTSA, je povinností ředitele I.CA tento certifikát přijmout.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

I.CA je povinna zajistit zveřejnění nQCA/nQTSA v souladu s platnou legislativou.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

V případech vydání nQCA/nQTSA získají oznámení o vydání nQCA/nQTSA pracovníci komise. Dále platí ustanovení kapitoly 4.4.2.

4.5 Použití párových dat a certifikátu

4.5.1 Použití dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a certifikátu držitelem certifikátu, podepisující osobou nebo označující osobou

Dáno platnou legislativou.

4.5.2 Použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek a certifikátu spoléhající se stranou

Spoléhající se strany jsou zejména povinny:

- získat z bezpečného zdroje certifikát nQCA/nQTSA a ověřit kontrolní součet tohoto certifikátu,
- provádět veškeré úkony potřebné k tomu, aby si ověřily, že tento certifikát nebyl zneplatněn

4.6 Obnovení certifikátu

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

4.6.1 Podmínky pro obnovení certifikátu

Viz kapitola 4.6.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Viz kapitola 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Viz kapitola 4.6.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující osobě nebo označující osobě

Viz kapitola 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Viz kapitola 4.6.

4.6.6 Zveřejnění vydaných obnovených certifikátů poskytovatelem

Viz kapitola 4.6.

4.6.7 Oznámení o vydání obnoveného certifikátu ostatním subjektům

Viz kapitola 4.6.

4.7 Výměna dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

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

4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Viz kapitola 4.7.

4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Viz kapitola 4.7.

4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek v certifikátu

Viz kapitola 4.7.

4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek podepisující nebo označující osobě

Viz kapitola 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Viz kapitola 4.7.

4.7.6 Zveřejnění vydaných certifikátů s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Viz kapitola 4.7.

4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo daty pro ověřování elektronických značek

Viz kapitola 4.7.

4.8 Změna údajů v certifikátu

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

4.8.1 Podmínky pro změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Viz kapitola 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující nebo označující osobě

Viz kapitola 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Viz kapitola 4.8.

4.8.6 Zveřejnění vydaných certifikátů se změněnými údaji

Viz kapitola 4.8.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Viz kapitola 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

4.9.1 Podmínky pro zneplatnění certifikátu

Podnětem k zneplatnění mohou být zejména:

- existuje-li důvodné podezření, že došlo ke kompromitaci soukromého klíče nQCA/nQTSA,

- nastanou-li skutečnosti uvedené v platné legislativě.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

Viz kapitola 3.4.

4.9.3 Požadavek na zneplatnění certifikátu

Po splnění podmínek na identifikaci a autentizaci je postupováno následujícím způsobem. Žádost musí obsahovat sériové číslo certifikátu buď v dekadickém tvaru nebo hexadecimální (uvozeno řetězcem „0x"), celé občanské jméno ředitele I.CA, kterému byl certifikát vydán a heslo pro zneplatnění. Pokud žádost splňuje výše uvedené požadavky, odpovědný pracovník CA neprodleně certifikát zneplatní. Datum a čas zneplatnění je určen okamžikem přijetí platné žádosti o zneplatnění certifikátu serverem I.CA.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Tyto skutečnosti jsou pro aplikaci tohoto vydání této CPS irelevantní.

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

Reakcí I.CA na přijetí platné žádosti o zneplatnění certifikátu, je jeho okamžité zneplatnění a zveřejnění této informace. CRL obsahující sériové číslo zneplatněného certifikátu musí být vydán neprodleně po zneplatnění tohoto certifikátu.

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

Viz kapitola 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je společností První certifikační autorita, a.s., standardně vydáván v pravidelných intervalech, nejvýše 24 hodin od vydání předchozího CRL (zpravidla à 8 hodin), v případě nutnosti bezodkladně.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

V procesu vydávání CRL je s ohledem na platnou legislativu vždy dodrženo ustanovení kapitoly 4.9.3.

4.9.9 Možnost ověřování statutu certifikátu on-line („dále OCSP")

Není využíváno.

4.9.10 Požadavky při ověřování statutu certifikátu na on-line

Není využíváno.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Dáno platnou legislativou.

4.9.12 Případné odlišnosti postupu zneplatnění v případě kompromitace dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Není využíváno.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Není využíváno.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Není využíváno.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Není využíváno.

4.9.16 Omezení doby pozastavení platnosti certifikátu

Není využíváno.

4.10 Služby související s ověřováním statutu certifikátu

4.10.1 Funkční charakteristiky

Služby související s ověřováním statutu certifikátu nQCA jsou poskytovány:

- prostřednictvím internetových informačních adres I.CA,
- prostřednictvím internetových informačních adres úřadu/úřadů, určených platnou legislativou, resp. v příslušném věstníku,
- o zneplatněných certifikátech:
    - prostřednictvím internetových informačních adres I.CA,
    - prostřednictvím internetových informačních adres úřadu/úřadů, určených platnou legislativou.

Služby související s ověřováním statutu nQTSA jsou poskytovány:

- prostřednictvím internetových informačních adres I.CA,
- prostřednictvím internetových informačních adres úřadu/úřadů, určených platnou legislativou, resp. v příslušném věstníku,
- o zneplatněných certifikátech:
    - na adresách, uvedených v samotném nQTSA,
    - prostřednictvím internetových informačních adres I.CA,
    - prostřednictvím internetových informačních adres úřadu/úřadů, určených platnou legislativou.

4.10.2 Dostupnost služeb

Služba poskytování veřejných certifikátů formou zveřejňování informací je dostupná 7 dní v týdnu 24 hodin denně.

I.CA garantuje zajištění nepřetržité dostupnosti (7 dní v týdnu 24 hodin denně) a integrity seznamu zneplatněných certifikátů (platné CRL).

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou poskytovány. I.CA může bez udání důvodu poskytování charakteristik služeb statutu certifikátu rozšířit, přitom je povinna dodržet příslušná ustanovení ZoEP a VoEP.

4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo označující osobou

Viz kapitola 5.8.

4.12 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek u důvěryhodné třetí strany a jejich obnova

Není využíváno.

4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Není využíváno.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci

Není využíváno.

5 Management, provozní a fyzická bezpečnost

Management bezpečnosti poskytovaných kvalifikovaných certifikačních služeb v oblasti vydávání kvalifikovaných certifikátů a/nebo kvalifikovaných systémových certifikátů je zaměřen především na:

- systémy, které vydávají a elektronicky označují, resp. podepisují výše uvedené certifikáty a seznamy zneplatněných certifikátů,
- veškeré procesy poskytování certifikačních služeb v oblasti vydávaní výše uvedených certifikátů dle ZoEP a VoEP.

5.1 Fyzická bezpečnost

Problematika fyzické bezpečnosti je detailně uvedena v interní dokumentaci, zejména:

- ***„Řízení fyzického přístupu do místností I.CA“,***
- ***„Požární bezpečnost“,***
- ***„Bezpečnostní incidenty“,***
- ***„Příručka administrátora“,***
- ***„Obnova komponenty provozního pracoviště“,***
- ***„Přemístění provozního pracoviště“,***
- ***„HSM/PrivateServer“,***
- ***„Správa TSS“,***
- ***„Kamerový systém – provozní pracoviště“.***

5.1.1 Umístění a konstrukce

Objekty provozního pracoviště jsou umístěny v geograficky odlišných lokalitách, které jsou dále jiné než ředitelství společnosti, obchodní a vývojová pracoviště, pracoviště registračních autorit a obchodních míst.

Zařízení určená k výkonu hlavních certifikačních služeb jsou umístěna ve vyhrazených prostorách provozních pracovišť. Tyto prostory jsou zabezpečené obdobně, jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona o ochraně utajovaných informací.

5.1.2 Fyzický přístup

Požadavky na fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozních pracovišť jsou uvedeny v interní dokumentaci společnosti. Ochrana objektů je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a případně speciálním systémem pro sledování pohybu osob a dopravních prostředků.

5.1.3 Elektřina a klimatizace

V prostorách určených k výkonu hlavních certifikačních služeb je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí 20°C ± 5°C. Přívod elektrické energie je jištěn pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 Vliv vody

Všechny kritické systémy provozních pracovišť jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoletou vodou. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou umístěna zařízení, určená k výkonu hlavních certifikačních služeb, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezorech. Kopie jsou ukládány v jiné geografické lokalitě, než kde je umístěno provozní pracoviště. Papírová média, která je nutno, mj. podle platné legislativy týkající se elektronického podpisu, archivovat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

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

5.1.8 Zálohy mimo budovu provozního pracoviště

Kopie provozních a pracovních záloh jsou uloženy na místě určeném ředitelem I.CA a popsaném v interní dokumentaci.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou ve společnosti I.CA definovány důvěryhodné role, která jsou spolu s odpovídajícími činnostmi a odpovědnostmi definovány v interní dokumentaci, zejména:

- ***„Systémová bezpečnostní politika CA“,***
- ***„Systémová bezpečnostní politika TSA“,***
- ***„Příručka administrátora“.***

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Ve společnosti První certifikační autorita, a.s., jsou pro procesy poskytování kvalifikovaných certifikačních služeb definovány činnosti, které se musí vykonávat jedině za účasti více než jediné osoby. Jedná se zejména o:

- generování párových dat pro vytváření/ověřování elektronické značky I.CA vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek,
- ničení dat pro vytváření elektronické značky I.CA vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek,
- zálohování/obnovu dat pro vytváření elektronické značky I.CA kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek,
- aktivace kryptografického modulu obsahujícího data pro vytváření elektronické značky I.CA vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek.

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

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci a autentizaci - upraveno interní dokumentací, zejména:

- ***„Příručka administrátora“,***
- ***„HSM/PrivateServer“,***
- ***„Správa TSS“.***

5.2.4 Role vyžadující rozdělení povinností

Pro vybrané činnosti jsou ve společnosti I.CA definovány důvěryhodné role, která jsou spolu s odpovídajícími činnostmi a odpovědnostmi definovány v interní dokumentaci, zejména:

- ***„Systémová bezpečnostní politika CA“,***
- ***„Systémová bezpečnostní politika TSA“.***

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenost a bezúhonnost

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

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z registru trestů nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně 3 roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně 5 let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně 1 rok v oblasti poskytování certifikačních služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti,
- v jednotlivých případech lze zkrátit délku uvedené praxe až o jednu třetinu stanovené délky na základě přezkoušení, při němž pracovník prokáže dostatečné znalosti k výkonu důvěryhodné funkce.

Ostatní pracovníci jsou přijímáni na základě následujících kritérií:

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

Problematika je detailně uvedena v interní dokumentaci, zejména ***„Kontrolní činnost, bezúhonnost a odbornost“***.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací všech kmenových pracovníků I.CA jsou:

- sami tito pracovníci,
- osoby, které tyto pracovníky znají,
- veřejné zdroje informací.

Pracovníci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, které aktualizují při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Pracovníci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samopřípravy a metodickým vedením již zaškoleným pracovníkem. Běžná doba na zaškolení je jeden měsíc. Problematika je detailně uvedena v interní dokumentaci, zejména ***„Kontrolní činnost, bezúhonnost a odbornost“***.

5.3.4 Požadavky a periodicita školení

Pro kmenové pracovníky pořádá vedení I.CA minimálně jedenkrát ročně interní výukový seminář, zaměřený na problematiku bezpečnosti informací.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou kmenoví pracovníci I.CA motivováni k získávání znalostí potřebných pro zastávání jiné role v I.CA.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným pracovníkem postupováno způsobem uvedeným v interních dokumentech společnosti, který se řídí zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

I.CA může, nebo musí některé činnosti zajišťovat smluvně. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se o např. o smluvní registrační autority, zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými certifikačními politikami, relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty, a předepsanými normativními dokumenty. V případě porušení těchto povinností jsou vyžadovány smluvní pokuty, případně je s nimi okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

Kmenoví zaměstnanci I.CA mají k dispozici kromě certifikační politiky, certifikační prováděcí směrnice, bezpečnostní a provozní dokumentace veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

5.4 Auditní záznamy (logy)

Problematika spojená s vytvářením, zpracováním a uchováváním auditních logů je detailně řešena v interní dokumentaci, zejména:

- ***„Příručka administrátora“,***
- ***„HSM/Private Server“,***

- ***„Správa TSS“ ,***
- ***„Příprava uchovávaných informací“,***
- ***„Záloha dat provozních systémů“ ,***
- ***„Řízení fyzického přístupu do místností I.CA“.***

5.4.1 Typy zaznamenávaných událostí

Dle požadavků CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements jsou minimálně logovány následující události:

- z hlediska systému významné události prostředí a klíčového hospodářství,
- spuštění a ukončení funkcí auditu,
- změny parametrů auditu,
- akce, prováděné při chybách úložiště auditních záznamů,
- všechny pokusy přístupu k systému

a dále:

- záznam o požadavku na vydání certifikátu,
- záznam o vydání certifikátu,
- záznam o požadavku na zneplatnění certifikátu,
- záznam o zneplatnění certifikátu,
- záznam o zařazení zneplatněného certifikátu do CRL,
- záznam o zveřejnění CRL,
- všechny události vztahující se k životnímu cyklu párových dat a certifikátů CA.

Záznamy v auditním souboru obsahují následující parametry:

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

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

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditní dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech, definovaných v interní bezpečnostní dokumentaci, v případě bezpečnostního incidentu okamžitě - uvedeno v interním dokumentu ***„Příručka administrátora“***.

5.4.3 Doba uchovávání auditních záznamů

Auditní záznamy jsou uchovávány v souladu s požadavky ZoEP.

5.4.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy způsobem, zajišťujícím jejich ochranu před jejich změnami, krádeží a zničení (ať již úmyslnému, tak neúmyslnému).

Auditní záznamy informačních systémů provozního pracoviště jsou ukládány ve dvou kopiích, každá kopie je umístěna v jiné místnosti provozních prostor I.CA. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

Procesy jsou uvedeny v interní dokumentaci, zejména:

- ***„Příručka administrátora“,***
- ***„Příprava uchovávaných informací“,***
- ***„Záloha dat provozních systémů“ ,***
- ***„Dokumenty agendy certifikačních služeb“.***

5.4.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem jako zálohovaní ostatních elektronických informací. Procesy jsou uvedeny v interní dokumentaci, zejména:

- ***„Příručka administrátora“,***
- ***„Záloha dat provozních systémů“.***

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je ve vztahu k I.CA interní, ve vztahu k smluvním partnerům externí.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s., prováděno v periodických intervalech, v případě incidentu majícího vliv na bezpečnost poskytovaných služeb okamžitě.

5.5 Uchovávání informací a dokumentace

Uchovávání informací a dokumentace je u I.CA prováděno dle požadavků ZoEP (ČR). Problematika spojená s uchováváním informací a dokumentace je detailně řešena v interní dokumentaci, zejména:

- ***„Řízení fyzického přístupu do místností I.CA“,***
- ***„Příprava uchovávaných informací“,***
- ***„Záloha dat provozních systémů“ ,***
- ***„Příručka administrátora“.***

5.5.1 Typy informací a dokumentace, které se uchovávají

I.CA uchovává informace a dokumentaci v souladu se ZoEP a VoEP. Tyto informace a dokumenty jsou konkretizovány v interních dokumentech ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“*** a ***„Dokumenty agendy certifikačních služeb“***.

5.5.2 Doba uchovávání uchovávaných informací a dokumentace

Doba uchovávaných informací a dokumentace je uvedena v interním dokumentu ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“***.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Uchovávané informace a dokumentace obsahují i osobní data klientů a proto je vzhledem k zákonu ČR č. 101/2000 Sb. dbáno zvýšené ochrany těchto dat. Prostory, ve kterých se uchovávané informace a dokumentace nacházejí, jsou zabezpečeny formou opatření, vycházejících z požadavků objektové a fyzické bezpečnosti.

Uchovávané informace a dokumentace jsou přístupné oprávněným:

- pracovníkům I.CA,
- kontrolním subjektům, orgánům činných v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy při zálohování uchovávaných informací a dokumentace jsou upraveny výše uvedenou interní dokumentací I.CA.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

V případě, že jsou využívána časová razítka, jedná se vždy o kvalifikovaná časová razítka vydána I.CA.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní, externí)

Informace a dokumentace jsou ukládány na místo, určené ředitelem I.CA. Samotná problematika přípravy a způsobu ukládání informací a dokumentace v elektronické i písemné podobě je upravena interními normami a směrnicemi, uvedenými v záhlaví kapitoly 5.5 a dokumentem ***„Dílčí spisový a skartační řád pro agendy certifikačních služeb“***.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Postupy jsou popsány v interní dokumentaci I.CA, uvedené v záhlaví kapitoly 5.5 a v dokumentu ***„Dokumenty agendy certifikačních služeb“***.

5.6 Výměna dat pro ověřování elektronických značek v nadřízeném kvalifikovaném systémovém certifikátu poskytovatele

V případě standardních situací je výměna dat pro ověřování elektronických značek, resp. elektronických podpisů v nQCA/nQTSA (jedná se o data, sloužící pro ověření elektronické značky, resp. elektronického podpisu vydaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek) s dostatečným časovým předstihem prováděna formou vydání nového certifikátu a vždy ve spojení s fyzickou generací nových párových dat.

V případě nestandardních situací (např. dojde-li k takovému vývoji kryptoanalytických metod, že by mohla být ohrožena bezpečnost procesu tvorby elektronických podpisů, resp. značek, tzn. změny kryptografických algoritmů, délky klíčů atd.) je tato činnost prováděna v adekvátním časovém období.

Jak v případě standardních situací, tak nestandardních situací je výměna dat pro ověřování elektronických značek/podpisů v nQCA/nQTSA veřejnosti s předstihem (je-li to možné) vhodnou formou sdělena.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

V případě výskytu těchto událostí postupuje I.CA v souladu s interním dokumentem ***Plán pro zvládání krizových situací a plán obnovy*** a jím odkazované dokumentaci, zejména:.

- ***„Obnova komponenty provozního pracoviště“,***
- ***„Přemístění provozního pracoviště“,***
- ***„Bezpečnostní incidenty“.***

5.7.2 Poškození výpočetních prostředků, software nebo dat

V případě poškození výpočetních prostředků, softwaru nebo dat postupuje I.CA v souladu s interním dokumentem ***Plán pro zvládání krizových situací a plán obnovy*** a jím odkazované dokumentaci, zejména:

- ***„Obnova komponenty provozního pracoviště“,***
- ***„Přemístění provozního pracoviště“,***
- ***„Bezpečnostní incidenty“.***

5.7.3 Postup při kompromitaci dat pro vytváření elektronických značek/podpisů poskytovatele

V případě vzniku důvodné obavy z kompromitace dat pro vytváření elektronických značek, resp. elektronických podpisů pro označování, resp. podepisování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek I.CA:

- ukončí jejich používání,
- okamžitě a prokazatelně zneplatní příslušný certifikát a jemu odpovídající data pro vytváření elektronických značek, resp. elektronických podpisů,
- zneplatní všechny platné certifikáty, které byly výše uvedenými daty označeny, resp. podepsány,
- bezodkladně o této skutečnosti, včetně důvodu informuje způsobem, uvedeným v kapitole 2.2,
- pokud je to možné, informuje držitele platných certifikátů o zneplatnění těchto certifikátů, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly v žádosti o vydání certifikátu, součástí této informace je důvod ukončení platnosti příslušného certifikátu,

- oznámí příslušnému úřadu informaci o zneplatnění příslušného certifikátu s uvedením důvodu zneplatnění.

V případě vzniku důvodné obavy z kompromitace dat pro vytváření elektronických značek, resp. elektronických podpisů pro označování, resp. podepisování vydávaných kvalifikovaných časových razítek I.CA:

- ukončí jejich používání,
- okamžitě a prokazatelně zneplatní příslušný certifikát a jemu odpovídající data pro vytváření elektronických značek, resp. elektronických podpisů,
- bezodkladně o této skutečnosti, včetně důvodu, informuje způsobem uvedeným v kapitole 2.2,
- pokud je to možné, informuje držitele platných kvalifikovaných časových razítek o zneplatnění příslušného certifikátu, a to prostřednictvím zaslání zprávy elektronickou poštou na elektronickou adresu, kterou tyto osoby uvedly v žádosti o vydání kvalifikovaných časových razítek, součástí této informace je důvod ukončení platnosti příslušného certifikátu,
- oznámí příslušnému úřadu informaci o zneplatnění daného certifikátu s uvedením důvodu zneplatnění,
- vydá nový certifikát relevantnímu TSU - postup je stejný jako při vydání prvotního certifikátu.

Obdobné postupy budou uplatněny i v případě, že dojde k takovému vývoji kryptoanalytických metod (např. změny kryptografických algoritmů, délky klíčů atd.), které by mohly bezprostředně ohrozit bezpečnost procesu certifikačních služeb.

5.7.4 Schopnosti obnovit činnost po havárii

V případě havárie postupuje I.CA v souladu s interním dokumentem ***Plán pro zvládání krizových situací a plán obnovy*** a jím odkazované dokumentaci, zejména:

- ***„Obnova komponenty provozního pracoviště“***
- ***„Přemístění provozního pracoviště“***

5.8 Ukončení činnosti CA

V případě plánovaného ukončení činnosti I.CA jako kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů, tzn. z jiných důvodů, než jsou mimořádné události jakými jsou stávky, občanské nepokoje, válečný stav, přírodní katastrofy celostátního rozsahu nebo jiné výsledky působení vyšší moci, zajistí I.CA provedení následujících činností:

- Certifikáty vydané v souladu s legislativou České republiky:
    - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 3 měsíce před plánovaným ukončením činnosti,
    - vynaloží veškeré možné úsilí pro to, aby evidence vedená dle platné legislativy byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání certifikátů, v případě, že se jí nepodařilo tuto evidenci předat jinému kvalifikovanému poskytovateli certifikačních služeb v oblasti vydávání certifikátů, ohlásí nejpozději 30 dnů před plánovaným datem ukončení činnosti tuto skutečnost příslušnému úřadu a zajistí předání této evidence příslušnému úřadu - tuto informaci zahrne do zprávy odeslané všem svým klientům, kteří jsou držiteli platných smluv o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů, pokud toto bude známo nejméně 2 měsíce před plánovaným ukončením činnosti,
    - zpřístupní informaci o ukončení činnosti I.CA v oblasti vydávání certifikátů na své internetové informační adrese nejméně 2 měsíce před plánovaným ukončením činnosti,
    - ukončí poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů,

- prokazatelné zničí svá data pro vytváření elektronických značek sloužící k označování vydávaných certifikátů a seznamu zneplatněných certifikátů.

- Certifikáty vydané v souladu s legislativou Slovenské republiky:
  - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,
  - ohlásí každému držiteli platného kvalifikovaného certifikátu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání certifikátů nejméně 6 měsíců před plánovaným ukončením činnosti,
  - může se dohodnout s jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání certifikátů o převzetí záznamů o vydaných a zrušených certifikátech a provozní dokumentaci – pokud žádný kvalifikovaný poskytovatel certifikačních služeb v oblasti vydávání certifikátů tyto záznamy nepřevezme:
    - zaniká platnost všech jím vydaných kvalifikovaných certifikátů ke dni zániku tohoto kvalifikovaného poskytovatele certifikačních služeb v oblasti vydávání certifikátů,
    - převezme tyto záznamy úřad.

Pro oblast vydávání časových razítek platí následující:

- v případě České republiky:
  - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek nejméně 3 měsíce před plánovaným ukončením činnosti,
  - vynaloží veškeré možné úsilí pro to, aby evidence vedená dle platné legislativy byla převzata jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání časových razítek, v případě, že se jí nepodařilo tuto evidenci předat jinému kvalifikovanému poskytovateli certifikačních služeb v oblasti vydávání časových razítek, ohlásí nejpozději 30 dnů před plánovaným datem ukončení činnosti tuto skutečnost příslušnému úřadu a zajistí předání této evidence příslušnému úřadu - tuto informaci zahrne do zprávy odeslané všem svým klientům, kteří jsou držiteli platných smluv o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek, pokud toto bude známo nejméně 2 měsíce před plánovaným ukončením činnosti,
  - zpřístupní informaci o ukončení činnosti I.CA v oblasti vydávání kvalifikovaných časových razítek na své internetové informační adrese nejméně 2 měsíce před plánovaným ukončením činnosti,
  - ukončí poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek,
  - prokazatelné zničí svá data pro vytváření elektronických značek sloužící k označování vydávaných kvalifikovaných časových razítek.

- v případě Slovenské republiky:
  - ohlásí příslušnému úřadu záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek nejméně 6 měsíců před plánovaným ukončením činnosti,
  - ohlásí každému držiteli platné smlouvy o poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek záměr ukončit činnost poskytování kvalifikovaných certifikačních služeb v oblasti vydávání časových razítek nejméně 6 měsíců před plánovaným ukončením činnosti,
  - může se dohodnout s jiným kvalifikovaným poskytovatelem certifikačních služeb v oblasti vydávání časových razítek o převzetí záznamů o časových razítkách a provozní dokumentaci – pokud žádný kvalifikovaný poskytovatel certifikačních služeb v oblasti vydávání časových razítek tyto záznamy nepřevezme, převezme tyto záznamy úřad.

V případě odnětí akreditace I.CA bez prodlení informuje o této skutečnosti nejen subjekty, kterým poskytuje své kvalifikované certifikační služby, ale i další dotčené osoby způsobem uvedeným v kapitole 2.2.

6 Technická bezpečnost

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Generování párových dat I.CA, které probíhá v zabezpečené zóně v souladu s dokumentem Systémová bezpečnostní politika CA a o jehož průběhu je vyhotoven písemný protokol, je prováděno v kryptografickém modulu, který splňuje požadavky české, resp. slovenské legislativy, vztahující se k problematice elektronického podpisu. Použitý modul svými vlastnostmi odpovídá požadavkům vyžadovaným ZoEP a VoEP. I.CA používá pro párová data, sloužící k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů délku rovnou 2048 bitů.

V průběhu procesu generování párových dat I.CA, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů, musí být minimálně fyzicky přítomni:

- ředitel I.CA,
- bezpečnostní manager,
- vedoucí provozního pracoviště.

Konkrétní technický postup generace párových dat nQCA/nQTSA a následné vyhotovení odpovídajícího certifikátu je popsán v interní dokumentaci I.CA:

- ***„Řízení fyzického přístupu do místností I.CA“*,**
- ***„HSM/Private Server“,***
- ***„Správa TSS“,***
- ***„Příručka administrátora“.***

O průběhu generování párových dat nQCA/nQTSA je vyhotoven písemný protokol obsahující:

- jmenný seznam přítomných pracovníků s uvedením: jména, příjmení, titulu,
- datum a čas zahájení a ukončení generace párových dat s přesností minimálně na minuty,
- místo, kde ke generaci párových dat došlo,
- popis zařízení, na kterém byla generace prováděna, umožňující jednoznačnou identifikaci tohoto zařízení,
- kompletní výpis certifikátu nQCA/nQTSA,
- datum vyhotovení protokolu,
- vlastnoruční podpisy všech pracovníků, kteří generaci párových dat nQCA/nQTSA prováděli.

6.1.2 Předání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek podepisující nebo označující osobě

Není využíváno - generování párových dat nQCA/nQTSA je prováděno na zařízení a v prostředí, která jsou v okamžiku jejich generování pod výhradní kontrolou I.CA.

6.1.3 Předání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek poskytovateli certifikačních služeb

Není využíváno.

6.1.4 Poskytování dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek certifikační autoritou spoléhajícím se stranám

Data pro ověřování elektronických značek, resp. elektronických podpisů jsou obsažena v nQCA/nQTSA a možnost jeho získání je garantována následujícími způsoby:

- obdržením na RA (osobní návštěva),
- prostřednictvím internetových informačních adres I.CA a příslušného úřadu, případně prostřednictvím věstníku příslušného úřadu,
- každý koncový žadatel o kvalifikovaný certifikát a/nebo kvalifikovaný systémový certifikát obdrží nQCA při získání svého prvotního kvalifikovaného certifikátu a/nebo kvalifikovaného systémového certifikátu na RA.

6.1.5 Délky párových dat

I.CA používá nejprověřenější klasický asymetrický šifrový algoritmus – RSA. Mohutnost klíčů (resp. parametrů daného algoritmu) použitých v procesech poskytování kvalifikovaných certifikačních služeb je 2048 bitů.

6.1.6 Generování parametrů dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a kontrola jejich kvality

Algoritmy použité pro generování celočíselných hodnot nutných pro fungování elektronického podpisu/značky (např. testy prvočíselnosti atd.) musí mít parametry uvedené v platné legislativě, resp. v ní odkazovaných technických standardech nebo normách.

6.1.7 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Uvedeno v kapitole 1.4.1.

6.2 Ochrana dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek a bezpečnost kryptografických modulů

Konkrétní postupy níže uvedených podkapitol jsou popsány v interní dokumentaci I.CA:

- ***„Řízení fyzického přístupu do místností I.CA“*,**
- ***„HSM/Private Server“,***
- ***„Správa TSS“ ,***
- ***„Příručka administrátora“ .***

6.2.1 Standardy a podmínky používání kryptografických modulů

Generování párových dat nQCA/nQTSA, uložení soukromého klíče I.CA sloužícího pro vytváření elektronických značek, resp. elektronických podpisů vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek probíhá v kryptografickém modulu, který splňuje požadavky standardu FIPS PUB 140-2 úroveň 3 a VoEP.

6.2.2 Sdílení tajemství

Ochrana sdílením tajemství je realizována prostředky kryptografického modulu. Při provádění citlivých činností, které souvisejí se zásadními činnostmi I.CA, je nezbytná přítomnost tří pověřených pracovníků I.CA, z nichž dva znají část kódu k provedení těchto činností.

6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Není využíváno.

6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Kryptografické moduly použité pro správu nQCA/nQTSA umožňují zálohování dat pro vytváření elektronických značek, resp. elektronických podpisů. Data v zašifrované podobě jsou zálohována s využitím čipových karet.

6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Po uplynutí doby platnosti soukromého klíče (dat určených k označování, resp. podepisování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek) je tento (včetně záloh) zničen a jeho další zálohování se neprovádí. Uchovávání těchto soukromých klíčů představuje bezpečnostní riziko, a proto je u I.CA zakázáno.

6.2.6 Transfer dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek do kryptografického modulu nebo z kryptografického modulu

Soukromý klíč sloužící pro vytváření elektronických značek vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek je generován přímo v kryptografickém modulu.

Vkládání soukromého klíče do kryptografického modulu v případě, že se jedná o jeho obnovení ze šifrované zálohy, probíhá za přímé osobní účasti nejméně dvou určených pracovníků I.CA. V okamžiku jeho vkládání musí být vyhrazená stanice a kryptografický modul odpojeny od počítačové sítě. O vložení soukromého klíče je pořízen písemný záznam.

6.2.7 Uložení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek v kryptografickém modulu

Soukromé klíče sloužící k vytváření elektronických značek, resp. elektronických podpisů vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek jsou uloženy bezpečným způsobem v kryptografickém modulu splňujícím požadavky platné legislativy.

6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Aktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek, provádí určení pracovníci I.CA prostřednictvím vlastní aktivace kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací. Po aktivaci je systém připraven k označování, resp. podepisování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek a aktivační čipová karta se vyjme. Po aktivaci je zařízení přístupné pouze určeným odpovědným pracovníkům I.CA.

6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Deaktivaci dat pro vytváření elektronických značek, resp. elektronických podpisů vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek po jejich vložení do kryptografického modulu provádí určení pracovníci I.CA prostřednictvím kryptografického modulu a aktivační čipové karty podle přesně určeného postupu, který je upraven interní dokumentací.

O provedení deaktivace dat pro vytváření elektronických značek, resp. elektronických podpisů vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek je pořízen písemný záznam, který podepíší určení pracovníci I.CA.

6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických značek

Data pro vytváření elektronických značek, resp. elektronických podpisů sloužící k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů jsou uložena v kryptografickém modulu. Ničení těchto dat je realizováno prostředky kryptografického modulu. Zálohy těchto dat uložené v zašifrované podobě na externích médiích jsou rovněž zničeny. Ničení spočívá ve fyzické destrukci těchto nosičů.

Při ničení dat pro vytváření elektronických značek, resp. elektronických podpisů, sloužících k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů musí být minimálně fyzicky přítomni:

- ředitel I.CA,
- bezpečnostní manager,
- vedoucí provozního pracoviště.

O průběhu ničení dat pro vytváření elektronických značek, resp. elektronických podpisů, sloužící k označování, resp. podepisování vydávaných certifikátů a seznamů zneplatněných certifikátů je sepsán protokol.

6.2.11 Hodnocení kryptografického modulu

Nástroj elektronického podpisu pro elektronické označování, resp. elektronické podepisování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek byl certifikován na shodu s požadavky standardu FIPS PUB 140-2 úroveň 3.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických značek

Problematika uchovávání dat pro ověřování elektronických značek/podpisů je řešena v souladu s ZoEP a VoEP.

6.3.2 Maximální doba platnosti certifikátu označující osoby a párových dat

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

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou vytvářena v průběhu procesu instalace, kdy jsou generována párová data pro elektronické označování, resp. elektronické podepisování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, seznamů zneplatněných certifikátů a kvalifikovaných časových razítek. Konkrétní postupy jsou popsány v interním dokumentaci, zejména:

- ***„Řízení fyzického přístupu do místností I.CA“*,**
- ***„HSM/Private Server“,***
- ***„Správa TSS“,***
- ***„Příručka administrátora“.***

6.4.2 Ochrana aktivačních dat

Výše uvedená aktivační data jsou chráněna způsobem uvedeným v interní bezpečnostní dokumentaci, zejména:

- ***„Řízení fyzického přístupu do místností I.CA“*,**
- ***„HSM/Private Server“,***
- ***„Správa TSS“,***
- ***„Příručka administrátora“.***

6.4.3 Ostatní aspekty aktivačních dat

Výše uvedená aktivační data jsou určena výhradně pro procesy poskytování kvalifikovaných certifikačních služeb a nesmí být použita k jiným účelům, ani přenášena nebo uchovávána v otevřené podobě.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Specifické technické požadavky na počítačovou bezpečnost jsou definovány ZoEP, resp. VoEP a jimi odkazovanými standardy. Detailní řešení specifických technických požadavků počítačové bezpečnosti je popsáno v interní dokumentaci:

- ***„Systémová bezpečnostní politika CA“,***
- ***„Plán pro zvládání krizových situací a plán obnovy“,***

- ***„Obnova komponenty provozního pracoviště“,***
- ***„Přemístění provozního pracoviště“,***
- ***„Záloha dat provozních systémů“,***
- ***„Příprava uchovávaných dat“,***
- ***„Příručka administrátora“***
- ***„Řízení fyzického přístupu do místností I.CA“,***
- ***„HSM/Private Server“,***
- ***„Správa TSS“.***

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení bezpečnosti je založeno na mezinárodních a národních standardech, zejména:

- CWA 14167-1 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements/Bezpečnostní požadavky na důvěryhodné systémy spravující certifikáty pro elektronický podpis – část 1: Požadavky na bezpečnost systémů,
- ČSN ETSI TS 101 456 - Elektronické podpisy a infrastruktury; Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty,
- ČSN ETSI EN 319 411-2 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 2: Požadavky politiky na certifikační autority vydávající kvalifikované certifikáty,
- ETSI TS 102 042 – Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates,
- ČSN ETSI EN 319 411-3 Elektronické podpisy a infrastruktury (ESI) - Požadavky politiky a bezpečnosti na poskytovatele důvěryhodných služeb vydávající certifikáty - Část 3: Požadavky politiky na certifikační autority vydávající certifikáty veřejného klíče,
- ČSN ETSI TS 102 023 – Elektronické podpisy a infrastruktury; Požadavky na postupy autorit časových razítek,
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky,
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací,
- ČSN ISO/IEC 27003 Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti informací,
- ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky – Řízení rizik bezpečnosti informací,
- ČSN ISO/IEC 15408 Informační technologie – Kritéria pro hodnocení bezpečnosti IT,
- RFC 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (dále též RFC 3647),
- RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP),
- RFC 2630 – Cryptographic message Syntax,
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites[2],
- RFC 5280 - Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile.

[2] Nahrazující ALGO paper (viz http://www.mvcr.cz/clanek/e-podpis-povinne-zverejnovane-informace-kryptograficke-algoritmy-a-jejich-parametry-podle-vyhlasky-c-378-2006-sb.aspx)

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

V případě vývoje systému v oblastech provozní činnosti, systémového programového vybavení, změn v bezpečnostní dokumentační základně atd. je postupováno dle interního dokumentu „***Změnové řízení***".

6.6.2 Kontroly řízení bezpečnosti

Soulad se standardy (viz kapitola 6.5.2), ZoEP a VoEP je ověřován pravidelnými audity systému managementu bezpečnosti informací, prováděnými pracovníky nezávislých firem a kontrolami bezpečnostní shody, prováděnými interními pracovníky I.CA. Tato problematika je popsána v interním dokumentu ***„Kontrolní činnost, bezúhonnost a odbornost"***.

I.CA si vyhrazuje právo provádění i jiných typů kontrol, resp. auditů.

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v I.CA je vytvářeno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití" (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování – definování bezpečnostní politiky, plánů, cílů, procesů a postupů s ohledem na řízení rizik a bezpečnost informací tak, aby byly v souladu s celkovou bezpečnostní politikou,
- implementace a provoz – bezpečnostní politiky, plánů, cílů, procesů a postupů,
- monitorování a přehodnocování – posouzení procesu s ohledem na bezpečnostní politiku a předání poznatků vedení společnosti k posouzení,
- využití – na základě rozhodnutí vedení organizace provedení nápravných opatření.

6.7 Síťová bezpečnost

V prostředí I.CA nejsou prostředky provádějící vlastní kvalifikované certifikační služby přímo dostupné z veřejné sítě Internet. Informační systém je mimo jiné chráněn komerčním produktem typu firewall. Veškerá komunikace mezi RA a provozním pracovištěm certifikační autority je vedena šifrovaně. Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci, zejména:

Detailní řešení řízení síťové bezpečnosti je popsáno v interní dokumentaci:

- ***„Systémová bezpečnostní politika CA",***
- ***„Systémová bezpečnostní politika TSA",***
- ***„Plán pro zvládání krizových situací a plán obnovy",***
- ***„Obnova komponenty provozního pracoviště",***
- ***„Přemístění provozního pracoviště",***
- ***„Řízení fyzického přístupu do místností I.CA"*** **,**
- ***„Příručka administrátora"*****,**
- ***„Firewall – provozní pracoviště".***

6.8 Časová razítka

Uvedeno v kapitole 5.5.5.

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

Profily certifikátu a seznamu zneplatněných certifikátů, odpovídají doporučením RFC 3280, resp. RFC 5280., jsou vždy uvedeny v konkrétní CP. Délka klíče certifikační autority, označujícího vydávané certifikáty a seznamy zneplatněných certifikátů je 2048 bitů.

7.1 Profil certifikátu

Viz kapitola 7.

7.1.1 Čísla verzí

Viz kapitola 7.

7.1.2 Rozšiřující položky v certifikátu

Viz kapitola 7.

7.1.3 Objektové identifikátory (dále OID) algoritmů

Viz kapitola 7.

7.1.4 Způsoby zápisu jmen a názvů

Viz kapitola 7.

7.1.5 Omezení jmen a názvů

Viz kapitola 7.

7.1.6 OID certifikační politiky

Viz kapitola 7.

7.1.7 Rozšiřující položka „PolicyConstraints“

Viz kapitola 7.

7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „PolicyQualifiers“

Viz kapitola 7.

7.1.9 Způsob zápisu kritické rozšiřující položky „CertificatePolicies“

Viz kapitola 7.

7.2 Profil seznamu zneplatněných certifikátů

Viz kapitola 7.

7.2.1 Číslo verze

Viz kapitola 7.

7.2.2 Rozšiřující položky seznamu zneplatněných certifikátů a záznamů v seznamu zneplatněných certifikátů

Viz kapitola 7.

7.3 Profil OCSP

Služba není poskytována.

7.3.1 Číslo verze

Služba není poskytována.

7.3.2 Rozšiřující položky OCSP

Služba není poskytována.

8 Hodnocení shody a jiná hodnocení

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

S ohledem na skutečnost, že společnost První certifikační autorita, a.s. je akreditovaným poskytovatel certifikačních služeb, jsou periodicita hodnocení, včetně okolností pro provádění hodnocení striktně dány požadavky ZoEP a VoEP, jedná se zejména o audit systému řízení bezpečnosti informací, který je prováděn každé dva roky a kontroly bezpečnostní shody v intervalu 4 let (celková), resp. každého roku (částečná).

Společnost První certifikační autorita, a.s. si vyhrazuje právo provádění i jiných forem kontrol.

Problematika hodnocení je upřesněna interním dokumentem ***„Kontrolní činnost, bezúhonnost a odbornost“***.

8.2 Identita a kvalifikace hodnotitele

Identita a kvalifikace hodnotitele je upravena interním dokumentem ***„Kontrolní činnost, bezúhonnost a odbornost“***.

8.3 Vztah hodnotitele k hodnocené entitě

V případě auditu systému managementu bezpečnosti informací je hodnotitelem externí, nezávislá organizace.

V případě celkové kontroly bezpečnostní shody nebo částečné kontroly bezpečnostní shody je hodnotitelem fyzická/právnická osoba, pověřená ředitelem společnosti První certifikační autorita, a.s.

8.4 Hodnocené oblasti

Cílem kontroly bezpečnostní shody je ověření, že společnost První certifikační autorita, a.s.:

- provozuje důvěryhodné systémy v souladu se ZoEP a VoEP,
- provádí změny v důvěryhodných systémech v souladu s bezpečnostní dokumentací, a to jejími částmi upravujícími řízení změn.

Předmětem kontroly bezpečnostní shody:

- jsou všechny důvěryhodné systémy I.CA (celková kontrola bezpečnostní shody), nebo
- jsou všechny změny, které I.CA provedla od provedení předchozí roční kontroly bezpečnostní shody (částečná kontrola bezpečnostní shody) a jejich vliv na důvěryhodné systémy I.CA, nebo
- je v případě, že v důvěryhodných systémech I.CA nenastaly od předchozí částečné kontroly bezpečnostní shody žádné změny, ověření této skutečnosti.

Cílem auditu systému managementu bezpečnosti informací je objektivní a na I.CA nezávislé ověření, že je v důvěryhodných systémech I.CA v oblasti vydávání certifikátů zaveden a uplatňován systém managementu bezpečnosti informací.

8.5 Postup v případě zjištěných nedostatků

V případě nedostatků, zjištěných na základě výsledné zprávy konkrétního hodnocení je bezpečnostní manager povinen do 15 dnů po obdržení zprávy určit, jaká opatření k odstranění nedostatků musí I.CA přijmout.

Zjistí-li příslušný úřad, že I.CA porušuje povinnosti stanovené ZoEP, VoEP uloží jí, aby ve stanovené lhůtě zjednala nápravu a případně určí, jaká opatření k odstranění nedostatků je I.CA povinna přijmout.

8.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli, resp. bezpečnostnímu manažerovi společnosti.

V nejbližším možném termínu svolá bezpečnostní manager schůzi bezpečnostního výboru, na kterém bude vedení společnosti s výsledky hodnocení seznámeno.

Sdělování výsledků hodnocení taktéž podléhá požadavkům ZoEP a VoEP.

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Není využíváno.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Přístup k vydaným veřejným certifikátům elektronickou cestou I.CA nezpoplatňuje.

9.1.3 Poplatky za informace o statutu certifikátu a o zneplatnění certifikátu

Přístup k informacím o zneplatněných certifikátech Služby nebo statutech certifikátů elektronickou cestou formou CRL nebo internetové adresy http://www.ica.cz I.CA nezpoplatňuje.

9.1.4 Poplatky za další služby

Předání nQCA/nQTSA není zpoplatněno.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Není využíváno.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

Společnost První certifikační autorita, a.s., prohlašuje, že má uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční škody.

9.2.2 Další aktiva a záruky

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiné finanční zajištění na provoz v souladu s požadavky uvedenými v relevantní legislativě a s ohledem na riziko vzniku odpovědnosti za škodu.

Podrobné informace o aktivech společnosti První certifikační autorita, a.s., je možno získat z Výroční zprávy I.CA.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Viz kapitoly 9.2.1 a 9.2.2.

9.3 Citlivost obchodních informací

9.3.1 Výčet citlivých informací

Citlivými a důvěrnými informacemi I.CA jsou veškeré informace, které nejsou zveřejňovány způsobem uvedeným v kapitole 2.2, zejména:

- data pro vytváření elektronických značek, resp. elektronických podpisů příslušná k datům pro ověřování elektronických značek, resp. elektronických podpisů obsažených v nQCA/nQTSA,
- data pro vytváření elektronických podpisů příslušná k datům pro ověřování elektronických podpisů obsažených v účelových certifikátech I.CA (např. klíče pro komunikaci s RA),
- ostatní kryptograficky podstatné informace sloužící k provozu I.CA a RA,
- vybrané obchodní informace I.CA,
- veškeré interní informace a dokumentace s ohledem na poskytování kvalifikovaných certifikačních služeb dle ZoEP,
- veškeré osobní údaje.

9.3.2 Informace mimo rámec citlivých informací

Za veřejné se považují typy informací, které nepatří do žádné z uvedených skupin v kapitole 9.3.1.

9.3.3 Odpovědnost za ochranu citlivých informací

Každý pracovník, který přijde do styku s informacemi uvedenými v kapitole 9.3.1, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

Zaměstnanci I.CA, případně jiné fyzické osoby, které přicházejí do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení příslušných prací.

9.4 Ochrana osobních údajů

9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

9.4.2 Osobní údaje

Osobními informacemi jsou veškeré osobní údaje klientů, uživatelů či pracovníků podléhající ochraně ve smyslu příslušných zákonných norem.

9.4.3 Údaje, které nejsou považovány za důvěrné

Informace, které nejsou považovány za důvěrné jsou obecně údaje, zveřejňované způsobem uvedeným v kapitole 2.2.

9.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů a dalších neveřejných informací je odpovědna I.CA.

9.4.5 Oznámení o používání důvěrných informací a souhlas s používáním citlivých informací

Problematika oznamování o používání důvěrných informací a souhlasu s používáním citlivých informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem.

9.4.6 Poskytování citlivých informací pro soudní či správní účely

Poskytování citlivých informací pro soudní, resp. správní účely je v I.CA řešeno v souladu s požadavky příslušných zákonných norem.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně dle požadavků příslušných zákonných norem.

Osoby uvedené v kapitole 9.3.3 může zbavit mlčenlivosti ten, v jehož zájmu tuto povinnost mají, nebo soud.

9.5 Práva duševního vlastnictví

Tato CPS, veškeré související dokumenty, obsah webových stránek, certifikáty CA, klíče I.CA a procedury zajišťující provoz systému poskytujícího kvalifikované certifikační služby v oblasti certifikátů, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

I.CA zaručuje, že:

- použije soukromé klíče příslušné certifikátům nQCA/nQTSA pouze k elektronickému označování, resp. podepisování vydávaných kvalifikovaných certifikátů, kvalifikovaných systémových certifikátů, kvalifikovaných časových razítek a seznamu zneplatněných certifikátů,
- vydávané certifikáty, kvalifikovaná časová razítka a seznamy zneplatněných certifikátů splňují náležitosti požadované platnou legislativou,
- zneplatní certifikát, pokud byla žádost o ukončení jeho platnosti podána způsobem definovaným v odpovídající CP daného certifikátu,
- splní veškeré povinnost plynoucí z platné legislativy vztahující se k problematice elektronického podpisu.

9.6.2 Zastupování a záruky RA

Není využíváno.

9.6.3 Zastupování a záruky držitele certifikátu, podepisující nebo označující osoby

Držitel certifikátu nebo podepisující, resp. označující osoba postupují v souladu s platnou legislativou vztahující se k problematice elektronického podpisu a ručí za informace uvedené ve vydaném certifikátu nQCA/nQTSA.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany postupují v souladu s platnou legislativou vztahující se k problematice elektronického podpisu.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Služba není poskytována.

9.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., se především striktně řídí platnou legislativou vztahující se k problematice elektronického podpisu a nemůže se zříci záruk v něm určených.

9.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti, požadované certifikační politikou, dle které byl certifikát vydán.

9.9 Odpovědnost za škodu, náhrada škody

Není relevantní pro tento dokument, je řešeno v politikách pro vydávání certifikátů koncovým klientům.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CP platí minimálně po dobu platnosti posledního podle ní vydaného certifikátu.

9.10.2 Ukončení platnosti

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této CPS, je ředitel společnosti První certifikační autorita, a.s.

9.10.3 Důsledky ukončení a přetrvání závazků

Uvedeno v kapitole 9.10.1.

9.11 Komunikace mezi zúčastněnými subjekty

Všechny zúčastněné subjekty jsou organizačnímu částmi I.CA a komunikace mezi nimi se řídí interními pravidly I.CA.

9.12 Změny

Postup v případě certifikačních politik je vždy popsán v konkrétní certifikační politice.

9.12.1 Postup při změnách

Certifikační politiky - viz kap. 9.12.

V případě této CPS - postup je realizován řízeným procesem uvedeném v interním dokumentu ***„Změnové řízení“.***

9.12.2 Postup při oznamování změn

Certifikační politiky - viz kap. 9.12.

V případě této CPS - vydání nové verze je vždy oznámeno formou zveřejňování informací.

9.12.3 Okolnosti, při kterých musí být změněno OID

Certifikační politiky - viz kap. 9.12. V případě této CPS - OID není přiřazován.

9.13 Řešení sporů

Není využíváno.

9.14 Rozhodné právo

Obchodní činnost společnosti První certifikační autorita, a.s., se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Systém poskytování kvalifikovaných certifikačních služeb je provozován ve shodě s požadavky ZoEP, VoEP.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Není využíváno.

9.16.2 Postoupení práv

V případě ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb postupuje společnost První certifikační autorita, a.s., v souladu se ZoEP.

9.16.3 Oddělitelnost ustanovení

Není využíváno.

9.16.4 Zřeknutí se práv

Není využíváno.

9.16.5 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývající ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu.

9.17 Další opatření

Není využíváno.

10 Závěrečná ustanovení

Tato CPS vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 22.09.2015.