# Kvalifikovaný poskytovatel služeb vytvářejících důvěru eIdentity a.s.

## ACAeID10.8 Certifikační politika - Krátkodobý QC – pro Bank iD

| | |
|---|---|
| Verze: | 1.0 |
| Odpovídá: | Jan Stelibský |
| Datum: | 24. 1. 2024 |
| Utajení: | Veřejný dokument |

Schváleno:

| Verze | Schválil | |
|---|---|---|
| 1.0 | Ladislav Šedivý | |

Historie dokumentu:

| Verze | Datum | Autor | Poznámka |
|---|---|---|---|
| 1.0 | 24. 1. 2024 | Jan Stelibský | Certifikační politika popisuje aplikaci bankovní identity při vydávání QC |

## OBSAH

# 1 ÚVOD

Certifikační politika pro kvalifikované certifikáty obsahuje zásady a postupy související se zajištěním činnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru.

Tato Certifikační politika stanovuje zásady, které kvalifikovaný poskytovatel služeb vytvářejících důvěru uplatňuje při zajišťování kvalifikované služby vytvářejících důvěru:

Vydání krátkodobého kvalifikovaného certifikátu ke kvalifikovanému elektronickému podpisu s použitím elektronického ověření totožnosti pomocí prostředků pro elektronickou identifikaci používaných mimo rámec kvalifikovaného systému elektronické identifikace - pomocí Bank iD (pod touto značkou je bankami poskytováno digitální ověření uživatelů), jako služby poskytované pro klienty ve spolupráci se společností Bankovní identita a.s.

Kvalifikovaný certifikát se využívá k ověření kvalifikovaného elektronického podpisu fyzické osoby.

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

Tato Certifikační politika předpokládá na straně podepisující osoby používání jiné identifikační metody uznávané na vnitrostátní úrovni podle Nařízení eIDAS čl. 24, odst. 1 písmeno d)

Struktura tohoto dokumentu vychází z dokumentu RFC 3647- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework a tato Certifikační politika je v souladu s dokumentem Nařízení Evropského parlamentu a Rady (EU) č. 910/2014

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

Společnost eIdentity a.s. provozuje hierarchickou strukturu certifikačních autorit, respektující stanoviska dozorového orgánu.

## 1.1 Přehled

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

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

Zajištění bezpečného provozování kvalifikovaných služeb vytvářejících důvěru je popsáno v Certifikační prováděcí směrnici – QS a v další interní dokumentaci.

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

## 1.2 Název a jednoznačné určení dokumentu

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

Podtřída 1.2.203.27112489.1. je interně určena pro dokumentaci ACAeID, její další členění je určeno číslem dokumentu a jeho verzí, tedy např. 10.1.1.1 značí dokument ACAeID10.1 ve verzi 1.1.

Tato Certifikační politika – QC má tyto identifikační znaky:

| Identifikační znak | Význam identifikačního znaku | Hodnota |
|---|---|---|
| Název dokumentu | Název dokumentu v čitelné podobě | ACAeID10.8 Certifikační politika - Krátkodobý QC – pro Bank iD |
| OID | Identifikace dokumentu v rámci prostoru OID eIdentity a.s. | 1.2.203.27112489.1.10.8.1.0 |

## 1.3 Participující subjekty

### 1.3.1 Certifikační autority (dále „CA“)

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

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

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

### 1.3.2 Registrační autority

Jako registrační autorita dle této CP slouží registrační autorita on-line (dále RA ol). Procesy a postupy této RA ol byly nastaveny tak, aby byly ve shodě s dokumentem MV ČR ze dne 1. 8. 2022 Upřesnění ke kapitole 2-3 a kapitole 3 dokumentu DKP, který upravuje ověření totožnosti žadatelů o vydání QC pomocí prostředků pro elektronickou identifikaci (v souladu s čl. 24 odst. 1 písm. d) nařízení eIDAS). K ověření totožnosti se využívají prostředky pro el. identifikaci používané mimo rámec kvalifikovaného systému el. identifikace – pomocí Bank iD.

Zvolený postup poskytuje, s implementací vhodných bezpečnostních pojistek, záruku spolehlivosti ověření žadatele rovnocenné fyzické přítomnosti žadatele.

Dle takto stanovených postupů vydává eIdentity a.s. krátkodobé kvalifikované certifikáty on-line s využitím přihlášení pomocí Bank iD. Tato služba je využívána z prostředí RA ol aplikace

vyvíjené a provozované, v souladu s podmínkami provozu RA ol eIdentity, společností Bankovní identita, a.s. na základě smlouvy mezi eIdentity a.s. a Bankovní identitou a.s. RA ol pro účely vydání certifikátu opatří se souhlasem žadatele údaje potřebné pro vydání certifikátu, včetně obsahu certifikátu a údajů potřebných pro identifikaci žadatele s garancí aktuálnosti (na základě ověření bankou v základních registrech). Jako bezpečnostní pojistka k zajištění snížení rizika, že prostředek pro el. identifikaci nebyl zneužit jinou osobou, je po vydání QC aplikováno zaslání e-mailu o této skutečnosti na adresu žadatele uvedenou v Bank iD. Součástí e-mailu je odkaz, kde žadatel může požádat o zneplatnění QC. S přihlédnutím k procesnímu omezení použití certifikátu na jednu operaci podpisu opatření před vydáním certifikátu dle této politiky nejsou aplikována.

#### 1.3.3 Držitelé kvalifikovaných certifikátů a podepisující osoby, kteří požádali o vydání kvalifikovaného certifikátu, a kterým byl certifikát vydán

#### 1.3.4 Držitelem certifikátu a podepisující osobou je fyzická osoba, která požádala prostřednictvím RA ol o vydání certifikátu, a které byl certifikát vydán. Současně tato fyzická osoba využívá prostředek pro vytváření elektronických podpisů a jedná jménem svým a používá kvalifikovaný certifikát, vydaný ACAeID této osobě k tomuto prostředku.Spoléhající se strany

Spoléhající se stranou je každý subjekt, který využívá kvalifikovaných certifikátů vydaných ACAeID a/nebo elektronických podpisů s nimi souvisejících.

#### 1.3.5 Jiné participující subjekty

Další účastníci jsou orgány dozoru a orgány činné v trestním řízení, případně další orgány, kterým to ze zákona přísluší.

### 1.4 Použití certifikátu

Kvalifikované certifikáty vydané podle této Certifikační politiky se mohou použít jen k účelům stanoveným v této certifikační politice.

#### 1.4.1 Přípustné použití certifikátu

Typickými aplikacemi, které je možné použít v souvislosti s kvalifikovanými certifikáty vydávanými podle této politiky, jsou aplikace umožňující vytvářet a ověřovat elektronické podpisy jako například systémy elektronické pošty, podepisovací a ověřovací aplikace pro podepisování dokumentů a jiných typů souborů obecně, pokud jsou v souladu s požadavky Nařízení Evropského parlamentu a Rady (EU) č. 910/2014.

#### 1.4.2 Omezení použití certifikátu

Certifikáty se nesmí používat v rozporu s účelem, ke kterému byly vydány, a to jak z technického hlediska (např. podle omezení KeyUsage) tak i z právního hlediska.

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

## 1.5 Správa politiky

Za údržbu a schválení tohoto dokumentu odpovídá Výbor pro politiky.

### 1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

eIdentity a.s.
Vinohradská 184
130 00 Praha 3
Česká republika

### 1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

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

Tel: +420 222 866 150
Fax: +420 222 866 159
Email: PAA-manager@eidentity.cz

### 1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele a postupy jiných poskytovatelů služeb vytvářejících důvěru

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

### 1.5.4 Postupy při schvalování souladu podle 1.5.3.

Postupy jsou určeny jednacím řádem Výboru pro politiky.

## 1.6 Přehled použitých pojmů a zkratek

| | |
|---|---|
| eIDAS | Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 |
| ACAeID, ACA | Informační systém eIdentity a.s., poskytující služby vytvářející důvěru |
| RCA | Kořenová certifikační autorita, jako součást ACAeID |
| QCA | Vydávající certifikační autorita, jako součást ACAeID |
| RA ol | Registrační autorita online |
| RM | Registrační místo |

| | |
|---|---|
| ORM | Operátor registračního místa |
| CP | Certifikační politika |
| CPS | Certifikační prováděcí směrnice |
| QC | Kvalifikovaný certifikát pro elektronický podpis |
| QSC | Kvalifikovaný certifikát pro elektronickou pečeť |
| RQSC | Kořenový kvalifikovaný certifikát pro elektronickou pečeť |
| CRL | Seznam zneplatněných certifikátů |
| poskytovatel, PSVD | Poskytovatel služeb vytvářejících důvěru |
| EVI | Evidenční část informačního systému PCS |
| soukromý klíč | Data pro vytváření elektronických podpisů nebo pečetí |
| veřejný klíč | Data pro ověřování elektronických podpisů nebo pečetí |
| revokace | zneplatnění certifikátu |
| DN | Distinguished Name – Jednoznačná identifikace subjektu certifikátu |
| Bank iD | Bankami poskytovaná metoda digitálního ověření totožnosti |
| ZR | Základní registry |
| DIA | Digitální a informační agentura |

# 2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

ACAeID zveřejňuje seznam zneplatněných certifikátů.

Každý QC vydaný podle této certifikační politiky je možno dohledat podle sériového čísla a zjistit jeho stav.

## 2.1 Úložiště informací a dokumentace

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

## 2.2 Zveřejňování informací a dokumentace

K veřejným informacím je možné přistupovat pomocí webových služeb.
Veřejně dostupné jsou tyto položky certifikátu:

Sériové číslo certifikátu
Platnost od – do
Stav certifikátu

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

http://www.acaeid.cz/aca3.1/crl/actual.crl
http://pub1.acaeid.cz/aca3.1/crl/actual.crl
http://pub2.acaeid.cz/aca3.1/crl/actual.crl

http://www.acaeid.cz/aca3.2/crl/actual.crl
http://pub1.acaeid.cz/aca3.2/crl/actual.crl
http://pub2.acaeid.cz/aca3.2/crl/actual.crl

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

Informace o době zveřejnění aktuálního CRL bude poskytnuta v souboru

http://www.acaeid.cz/aca3.1/crl/actual-date.txt
http://pub1.acaeid.cz/aca3.1/crl/actual-date.txt
http://pub2.acaeid.cz/aca3.1/crl/actual-date.txt

http://www.acaeid.cz/aca3.2/crl/actual-date.txt
http://pub1.acaeid.cz/aca3.2/crl/actual-date.txt
http://pub2.acaeid.cz/aca3.2/crl/actual-date.txt

a bude ve tvaru YYYYMMDDHHMMSS.

Součástí veřejně dostupných informací je také dokument Certifikační politika – QC, který je zveřejněn ve formátu PDF na webových stránkách eIdentity a.s.

Zde je dostupná právě platná verze Certifikační politiky. Historie verzí je přístupná na webových stránkách provozovatele spolu s vyznačením období platnosti.

Zveřejněn na webových stránkách poskytovatele je také certifikát kořenové (RCA) a vydávající (QCA) certifikační autority. Pro ověření správnosti těchto certifikátů jsou tyto také zveřejněny na stránkách Digitální a informační agentury (dále jen DIA).

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

### 2.3 Periodicita zveřejňování informací

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

### 2.4 Řízení přístupu k jednotlivým typům úložišť

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

Zveřejnění a aktualizaci Seznamu vydaných kvalifikovaných certifikátů a Seznamu zneplatněných kvalifikovaných certifikátů provádí obsluha ACAeID s frekvencí, která je v souladu s tímto dokumentem.

# 3 IDENTIFIKACE A AUTENTIZACE

## 3.1 Pojmenování

### 3.1.1 Typy jmen

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

#### 3.1.1.1 Vydávající certifikační autorita ACAeID

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

| Atribut | Pravidlo vyplnění | Hodnota |
|---|---|---|
| Country (C) | pevný text | „CZ“ |
| Organization (O) | pevný text | „eIdentity a.s. “ |
| OrganizationIdentifier | Pevný text | VATCZ-27112489 |
| Organizational Unit (OU) | pevný text | „Qualified Trust Service Provider“ |
| Common Name (CN) | pevný text | „ACAeID3.x - Issuing Certificate “. |

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

| Atribut | Pravidlo vyplnění | Hodnota |
|---|---|---|
| Country (C) | pevný text | „CZ“ |
| Organization (O) | pevný text | „eIdentity a.s. “ |
| OrganizationIdentifier | Pevný text | VATCZ-27112489 |
| Organizational Unit (OU) | pevný text | „Qualified Trust Service Provider“ |
| Common Name (CN) | pevný text | „ACAeID3 – Root Certificate “ |

#### 3.1.1.2 Vydávané certifikáty

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

| Atribut | Význam | Čím se dokládá | Omezení | Hodnota – „příklad“ |
|---|---|---|---|---|
| Country (C) | Kód státu, kde má žadatel trvalý pobyt nebo kde má sídlo | Bank iD | podle ISO 3166 | „CZ“ |
| Locality (L) | Adresa bydliště pro žadatele – fyzickou osobu | Bank iD | Nepovinné. | „Vinohradská 22, 130 00 Praha 3“ |
| Name (Name) | Celé jméno žadatele včetně případných titulů | Bank iD | Nepovinné | „JUDr. Jan Tadeáš Novák“ |
| Given Name | Jméno | Bank iD | Obsahuje jméno (jména) žadatele | „Jan Tadeáš“ |
| Surname | Příjmení | Bank iD | Příjmení žadatele | Novák |
| Common Name (CN) | Obsahem pole je celé jméno | Bank iD | Přenáší se Name (pokud je vyplněno) nebo Given Name a po přidané mezeře Surname | |
| Email Address (E) | Emailová adresa uživatele. | Bank iD | Nepovinné | jan.novak@eidentity.cz |
| Pseudonym (Pseudonym) | Nepoužívá se | Neprokazuje se. | | |
| Title (Title) | Nepoužívá se | | Nepovinné. | |
| SerialNumber | Obsahuje identifikátor dokladu žadatele dle ETSI 319-412-1 V1.4.4. | Bank iD | | IDCCZ-Test123456 |

| Atribut | Význam | Čím se dokládá | Omezení | Hodnota – „příklad“ |
|---|---|---|---|---|
| Bank iD Pseudonym<br><br>1.3.6.1.4.1.58356.3 | Hodnota specifická pro použití Bank iD | Nedokládá se | | |

Certifikát uživatele musí obsahovat alespoň jeden z atributů CN.

#### 3.1.2 Požadavek na významnost jmen

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

#### 3.1.3 Anonymita a používání pseudonymu

QCA nevydává anonymní certifikáty. Kvalifikovaný certifikát vystavený na základě ověření totožnosti Bank iD není vydáván s možností uvedení pseudonymu.

#### 3.1.4 Pravidla pro interpretaci různých forem jmen

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

#### 3.1.5 Jednoznačnost jmen

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

#### 3.1.6 Obchodní značky

Všechny údaje uvedené v kvalifikovaném certifikátu uživatele se musí prokazatelně vztahovat k fyzické osobě.

### 3.2 Počáteční ověření identity

#### 3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických podpisů odpovídající datům pro ověřování elektronických podpisů

Soukromý klíč bude generován přímo.v rámci HSM spravovaného eIdentity a.s prostřednictvím ACAeID.

#### 3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Identita právnické osoby nebo organizační složky státu se neprokazuje.

### 3.2.3 Ověřování identity fyzické osoby

. Identifikace totožnosti se provádí v souladu s Nařízením eIDAS čl. 24, odst. 1 písmeno d) pomocí prostředků pro el. identifikaci používaných mimo rámec kvalifikovaného systému el. identifikace, konkrétně pomocí Bank iD.

Pouze občan ČR nebo držitel Průkazu o povolení pobytu v ČR může používat tento způsob vydávání QC.

Na základě smlouvy mezi eIdentity a.s. a Bankovní identita a.s. garantuje Bankovní identita a.s. pro účely vydání certifikátu se souhlasem žadatele údaje potřebné pro vydání certifikátu, včetně obsahu certifikátu a údajů potřebných pro identifikaci žadatele s garancí aktuálnosti (na základě ověření bankou v základních registrech). Bezpečnost ověření identity fyzické osoby před vydáním certifikátu se zvýší tím, že uvedené údaje jsou ověřovány v ZR cestou Bank iD, prostřednictvím jednotlivých bank.

Dojde-li v době platnosti certifikátu ke změně údajů, je Bankovní identita a.s. povinna oznámit poskytovateli změnu údajů. V případě, že se jedná o změnu údajů uvedených v certifikátu, dojde ke zneplatnění certifikátu.

Ve shodě s dokumentem MV ČR ze dne 1. 8. 2022 Upřesnění ke kapitole 2-3 a kapitole 3 dokumentu DKP, který upravuje ověření totožnosti žadatelů o vydání QC pomocí prostředků pro elektronickou identifikaci, pro zvýšení bezpečnosti ověření identity fyzické osoby po vydání certifikátu CA odešle na email žadatele informaci o vydaném certifikátu, uzavřenou smlouvu a protokol o převzetí certifikátu, s odkazem na možnost certifikát zneplatnit

### 3.2.4 Neověřované informace vztahující se k držiteli certifikátu nebo podepisující či pečetící osobě

Všechny informace uvedené v certifikátu od QCA jsou ověřené nebo jsou použity v souladu s předcházejícími pravidly.

### 3.2.5 Ověřování specifických práv

Nepředpokládá se.

### 3.2.6 Kritéria pro interoperabilitu

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

### 3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických podpisů

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

Služba se neposkytuje.

#### 3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Služba se neposkytuje.

### 3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Certifikáty jsou vydávány s maximální délkou platnosti maximálně 90 dní.

O zneplatnění kvalifikovaného certifikátu může požádat držitel certifikátu, podepisující osoba nebo Bank iD na základě důvodného podezření na zneužití identifikačních údajů použitých pro autentizaci žadatele.

Kvalifikovaný certifikát poskytovatel zneplatní:

- na základě údajů o ztrátě/změně Bank iD nahlášené Bankovní identitou a.s.
- na základě přijaté žádosti o zneplatnění
- pokud žadatel kvalifikovaný certifikát nepřevezme
- pokud žadatel požádá o ukončení zpracování osobních údajů
- na základě uvědomění držitele nebo podepisující osoby, že hrozí nebezpečí zneužití jejich dat pro vytváření elektronických podpisů
- v případě, že byl kvalifikovaný certifikát vydán na základě nepravdivých nebo chybných údajů
- dozví-li se prokazatelně, že podepisující osoba zemřela nebo zanikla nebo ji soud způsobilosti k právním úkonům zbavil nebo omezil
- dozví-li se prokazatelně, že údaje, na jejichž základě byl kvalifikovaný certifikát vydán, pozbyly pravdivosti
- pokud mu dozorový orgán (DIA) nařídí zneplatnění kvalifikovaného certifikátu jako předběžné opatření, pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán nebo pokud byl vydán na základě nepravdivých údajů nebo v případě, kdy bylo zjištěno, že podepisující osoba používá prostředek pro vytváření podpisu, který vykazuje bezpečnostní nedostatky, které umožňují padělání elektronických podpisů nebo změnu podepisovaných údajů.

Pokyn pro zneplatnění může podat podepisující osoba pro své certifikáty, Bankovní identita a.s. nebo odpovědná osoba eIdentity a.s. pro ostatní případy.

Žádost o zneplatnění QC ze strany držitele QC je realizována v systému QCA eIdentity

pomocí odkazu dostupného v informačním e-mailu, který je zaslán držiteli QC poskytovatelem služeb vytvářejících důvěru při vydání QC.

Žádost o zneplatnění nebo uvědomění podepisující osoby lze podat i (nejméně jedna možnost je vždy dostupná):

Osobně na RM
Elektronicky podepsaným e-mailem
Faxem na číslo dle kapitoly 1.5.2 této certifikační politiky

Žádost podaná faxem je zpracována následující pracovní den po doručení žádosti poskytovateli.

# 4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

## 4.1 Žádost o vydání certifikátu

### 4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

O kvalifikovaný certifikát může žádat každá fyzická osoba s českým občanstvím nebo fyzická osoba, která je držitelem Průkazu o povolení k pobytu v ČR, která je povinna uvádět prostřednictvím Bank iD pouze pravdivé informace a tyto také odpovídajícím způsobem doložit. Žádat může pouze ten, koho soud způsobilosti k právním úkonům nezbavil nebo neomezil. O tento typ certifikátu je možno požádat pouze pomocí RA ol provozovaném ve spolupráci se společností Bankovní identita a.s. – dle postupu v 3.2.3.

### 4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Vyplnění údajů je plně v zodpovědnosti žadatele. Žadatel je zodpovědný za to, že údaje uváděné prostřednictvím Bank iD jsou správné, úplné a pravdivé. Uvedené údaje jsou ověřovány v ZR cestou Bank iD, prostřednictvím jednotlivých bank.
Za ověření údajů zodpovídá poskytovatel služby Bank iD a poskytovatel služeb vytvářejících důvěru, který odpovídá za kontrolu přijatých opatření pro snížení rizika vydání certifikátů neoprávněné osobě (po vydání QC zasílá informace o vydání certifikátu žadateli).

Žadatel může reklamovat výsledek registračního procesu u vedení eldentity a.s. s uvedením podrobností případu.

## 4.2 Zpracování žádosti o certifikát

### 4.2.1 Identifikace a autentizace

#### 4.2.1.1 Zájem o službu

Provádí se v prostředí Bank iD a jeho prostřednictvím.

#### 4.2.1.2 Vyplnění identifikačních údajů žadatele

Provádí se v prostředí Bank iD.

Z Bank iD se převezmou tyto údaje:

Jméno
Příjmení
E-mail spojení
Celé jméno – vznikne ze Jména a Příjmení, nelze měnit
Adresa bydliště
Číslo primárního osobního dokladu (OP nebo cestovní pas u občanů ČR, Průkaz o povolení k pobytu u cizinců)
Služba Bank iD zajistí správnost údajů.

#### 4.2.1.3 Účet žadatele

Účet žadatele se při vydávání QC podle této CP nevytváří.

#### 4.2.1.4 Žádost o vydání kvalifikovaného certifikátu

Po splnění všech kontrol se po přijetí žádosti z RA ol automaticky přejde k vydání QC.

Předvyplněno bude:

- Označení, že je certifikát vydán jako kvalifikovaný certifikát.
- Název obchodní firmy kvalifikovaného poskytovatele a stát, ve kterém je poskytovatel usazen
- Elektronická pečeť kvalifikovaného poskytovatele služeb vytvářejících důvěru založená na certifikátu poskytovatele
- CDP – odkaz, kde lze přistoupit k CRL
- Politika, podle které došlo k vydání
- Celé jméno

Poskytovatel svým aplikačním vybavením doplní dodatečně v okamžiku vydání kvalifikovaného certifikátu:

- Správný datum a čas počátku a konce platnosti kvalifikovaného certifikátu
- Unikátní číslo vydávaného kvalifikovaného certifikátu v prostředí poskytovatele služeb vytvářejících důvěru
- Data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby

#### 4.2.1.5 Smlouva a platba

Platba je řešena smlouvou mezi eIdentity a.s. a Bankovní identitou a. s.,
Po odsouhlasení návrhu smlouvy o poskytnutí služby žadatelem v RA ol vygeneruje aplikace klíče a PKCS#10 žádost o vydání certifikátu do HSM spravovaného eIdentity a.s., se zajištěním výhradního přístupu ke klíči pouze pro žadatele a pouze v rámci jednoho

uživatelského sezení. Teprve nyní, po doplnění zaznamenaných údajů do formátu podle PKCS#10 (nebo obdobného) se na tyto údaje pohlíží jako na úplnou Žádost o poskytnutí služby. Žádost se přenáší do vnitřního systému eIdentity a.s., kde dochází k registračnímu procesu a k vlastnímu vydání certifikátu.

Ve smlouvě o vydání certifikátu žadatel stvrdí mimo jiné, že

- poskytl přesné a kompletní informace podle požadavku CP
- používá výhradně klíčového páru v souladu s ostatním omezením
- učinil účelná opatření k zabránění neautorizovaného použití jeho bankovní identity
- souhlasí s dotazem na svou identitu ze strany poskytovatele služby prostřednictvím banky
- upozorní bez zbytečného odkladu v době platnosti certifikátu
    - na nepřesnosti nebo změny údajů, na základě kterých byl certifikát vydán
- v případě kompromitace soukromého klíče ho přestane okamžitě a napořád používat

#### 4.2.1.6 Registrační proces

Proces vydání certifikátu prochází těmito kroky:

- Uživatel v aplikaci RA ol projeví vůli vytvořit elektronický podpis a za tímto účelem vydat kvalifikovaný certifikát a poskytne souhlas s provedením potřebných úkonů – identifikace a předání údajů.
- Uživatel potvrdí rámcovou smlouvu s eIdentity, a.s., pokud takovou smlouvu již nemá uzavřenu.
- RA ol vytvoří pár klíčů a předá údaje společně s žádostí o certifikát CA, která vydá certifikát.
- CA odešle na email žadatele informaci o vydaném certifikátu, uzavřenou smlouvu a protokol o převzetí certifikátu, s odkazem na možnost certifikát zneplatnit. Uzavřená smlouva a všechny související požadavky jsou archivovány, včetně podpisů zajišťujících integritu předaných požadavků.
- Aplikace RA ol provede elektronický podpis, pro který byl certifikát vydán, a vytvořené klíče zničí.

Aplikace RA ol je vyvíjena a provozována pro eIdentity společností Bankovní identita a.s. v souladu s požadavky eIdentity a.s., které jsou dohlíženy a kontrolovány řízeným procesem.

### 4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Aplikace on-line registrační místo vystaví certifikát na základě údajů předaných pomocí Bank iD, údajů zadaných žadatelem a provedených kontrol.

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

Aplikace on-line registrační místo zamítnout žádost a neposkytnout objednávanou službu. Případné následující kroky budou řešeny s Bankovní identitou a.s. v souladu se smlouvou.

#### 4.2.3 Doba zpracování žádosti o certifikát

Časový limit, ve kterém dojde ke zpracování žádosti o certifikát, není pevně stanoven. Jedná se o interaktivní proces, jehož délku určuje převážně žadatel. Společnost eIdentity a.s. poskytuje certifikační služby bez zbytečného odkladu.

### 4.3 Vydání certifikátu

#### 4.3.1 Úkony CA v průběhu vydávání certifikátu

Vydáním pokynu k vystavení certifikátu pro interní systém QCA se sestaví obsah certifikátu, spočte se z něj otisk podle schváleného schématu elektronické pečeti a předá se k vytvoření elektronické pečeti aplikaci on-line registrační místo. Zde dojde k vytvoření elektronické pečeti otisku a získaná data se odešlou zpět ke konečnému vytvoření obrazu certifikátu ve formátech DER, PEM a TXT.

#### 4.3.2 Oznamování o vydání certifikátu držiteli certifikátu, podepisující osobě

Certifikát ve výše zmíněných formátech je od tohoto okamžiku žadateli k dispozici a jeho obsah je součástí Protokolu o převzetí certifikátu.

### 4.4 Převzetí certifikátu

#### 4.4.1 Úkony spojené s převzetím certifikátu

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

Protokol o převzetí certifikátu obsahuje výpis certifikátu i v textové formě, ze které je zřejmý obsah certifikátu, datum převzetí a podpis žadatele a ORM.
Protokol je vygenerován eIdentity a.s. při vydání certifikátu a zaslán v informačním emailu žadateli a zároveň je součástí elektronicky archivované dokumentace žádosti.

#### 4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Vydaný kvalifikovaný certifikát je po převzetí možno dohledat podle sériového čísla. Zveřejněny jsou pouze tyto údaje:

- Sériové číslo certifikátu
- Doba platnosti od-do
- Stav certifikátu

#### 4.4.3 Oznámení o vydání certifikátu jiným subjektům

Vnitřní systém CA informuje o vydání certifikátu odpovídajícího ORM vyhotovením Protokolu o převzetí certifikátu.

### 4.5 Použití párových dat a certifikátu

#### 4.5.1 Použití dat pro vytváření elektronických podpisů a certifikátu držitelem certifikátu nebo podepisující osobou

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

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

Spoléhající strana může spoléhat pouze na certifikáty a veřejné klíče, které byly vydány a používány v souladu s touto politikou, byly použity v souladu s údaji v certifikátu, a které nemají označen za neplatný žádný certifikát ve svém certifikačním řetězci. Spoléhající strana je plně zodpovědná za veškeré úkony, které musí vykonat před tím, než získá důvěru v platnost certifikátu a veřejného klíče.

### 4.6 Obnovení certifikátu

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

#### 4.6.1 Podmínky pro obnovení certifikátu

Služba se neposkytuje.

#### 4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

Služba se neposkytuje.

#### 4.6.3 Zpracování požadavku na obnovení certifikátu

Služba se neposkytuje.

#### 4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu, podepisující osobě

Služba se neposkytuje.

#### 4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Služba se neposkytuje.

#### 4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

Služba se neposkytuje.

#### 4.6.7 Oznamování o vydání obnoveného certifikátu jiným subjektům

Služba se neposkytuje.

### 4.7 Výměna dat pro ověřování elektronických podpisů v certifikátu

Služba se neposkytuje.

#### 4.7.1 Podmínky pro výměnu dat pro ověřování elektronických podpisů v certifikátu

Služba se neposkytuje.

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

Služba se neposkytuje.

#### 4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických podpisů

Služba se neposkytuje.

#### 4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů nebo podepisující osobě

Služba se neposkytuje.

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

Služba se neposkytuje.

#### 4.7.6 Zveřejňování vydaných certifikátu s vyměněnými daty pro ověřování elektronických podpisů

Služba se neposkytuje.

#### 4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických podpisů jiným subjektům

Služba se neposkytuje.

### 4.8 Změna údajů v certifikátu

Služba se neposkytuje.

#### 4.8.1 Podmínky pro změnu údajů v certifikátu

Služba se neposkytuje.

#### 4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Služba se neposkytuje.

#### 4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Služba se neposkytuje.

#### 4.8.4 Oznámení o vydání certifikátu se změněnými údaji podepisující í osobě

Služba se neposkytuje.

#### 4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Služba se neposkytuje.

#### 4.8.6 Zveřejňování vydaných certifikátu se změněnými údaji

Služba se neposkytuje.

#### 4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Služba se neposkytuje.

### 4.9 Zneplatnění a pozastavení platnosti certifikátu

#### 4.9.1 Podmínky pro zneplatnění certifikátu

Podepisující osoba nebo držitel kvalifikovaného certifikátu musí neprodleně požádat o zneplatnění certifikátu v případě, kdy hrozí nebezpečí zneužití dat pro vytváření elektronického podpisu a v dalších případech v souladu s bodem 3.4 této CP.

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

Zneplatněný certifikát nemůže být obnoven.

#### 4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění může požádat držitel certifikátu, podepisující osoba nebo na základě skutečností dle bodu 3.4 této CP.

#### 4.9.3 Požadavek na zneplatnění certifikátu

Musí být provedeno v souladu s bodem 3.4 této CP.

#### 4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Tato doba není specifikována.

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

Certifikát je po přijetí žádosti o zneplatnění zneplatněn neprodleně. Informace o zneplatnění certifikátu se objeví v zveřejněném CRL po uplynutí nejdéle 24 hodin od přijetí žádosti o zneplatnění.

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

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

#### 4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

CRL se vydává denně s periodicitou minimálně jedenkrát za 24 hodin (zpravidla však každé 4 hodiny).

#### 4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL se zveřejňuje neprodleně.

#### 4.9.9 Možnost ověřování zneplatnění statusu certifikátu on-line (dále „OCSP“)

Tato možnost je poskytována. Viz kapitola 7.3 „Profil OCSP“.

#### 4.9.10 Požadavky při ověřování statusu certifikátu on-line

Viz kapitola 7.3 „Profil OCSP“.

#### 4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Služba se neposkytuje.

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

Služba se neposkytuje.

#### 4.9.13 Podmínky pro pozastavení platnosti certifikátu

Služba se neposkytuje.

#### 4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

Služba se neposkytuje.

#### 4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

Služba se neposkytuje.

#### 4.9.16 Omezení doby pozastavení platnosti certifikátu

Služba se neposkytuje.

### 4.10 Služby související s ověřováním statutu certifikátu

#### 4.10.1 Funkční charakteristiky

Tato služba se poskytuje zveřejněním CRL na webových stránkách eIdentity a.s. nebo pomocí OCSP dle této Certifikační politiky.

#### 4.10.2 Dostupnost služeb

Tato služba se poskytuje nepřetržitě.

#### 4.10.3 Další charakteristiky služeb statutu certifikátu

Služba se neposkytuje.

### 4.11 Ukončení poskytování služeb pro držitele certifikátu, podepisující nebo pečetící osobu

Platnost smluvního vztahu je definována ve smlouvě s žadatelem a je časově omezena. Po ukončení je pro poskytování služeb nutné uzavřít smlouvu novou.

Pokud požádá držitel/podepisující osoba o ukončení zpracování osobních údajů, dojde k zneplatnění jeho certifikátů, jeho osobní údaje se přesunou do archivu a přestanou se zpracovávat. eIdentity a.s. informuje o ukončení smlouvy i Bankovní identitu a.s. e-mailovou zprávou na kontaktní adresu dle smlouvy.

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

Služba se neposkytuje.

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

Služba se neposkytuje.

#### 4.12.2 Politika a postup při zapouzdřování a obnovování šifrovacího klíče pro relaci

Služba se neposkytuje.

# 5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

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

## 5.1 Fyzická bezpečnost

### 5.1.1 Umístění a konstrukce

Zařízení s aplikací on-line registrační místo, kryptografickým modulem a zařízení obsahující a zpracovávající osobní údaje žadatelů je umístěno ve vhodných geograficky vzdálených hlavních a záložních lokalitách. Použité prostory odpovídají svým bezpečnostním vybavením a režimem provozu požadavkům NÚKIB pro významné IS.

### 5.1.2 Fyzický přístup

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

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

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

Bezpečnost je dále v celém prostoru posílena o systém EZS a EPS s vyvedeným výstupem hlášení na stanoviště strážní služby. Současně jsou racky pronajaté eIdentity a.s. pokryty kamerami.

### 5.1.3 Elektřina a klimatizace

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

Prostory jsou klimatizovány a vlhkost je udržována automaticky.

### 5.1.4 Vlivy vody

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

### 5.1.5 Protipožární opatření a ochrana

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

#### 5.1.6 Ukládání médií

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

#### 5.1.7 Nakládání s odpady

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

#### 5.1.8 Zálohy mimo budovu

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

### 5.2 Procesní bezpečnost

#### 5.2.1 Důvěryhodné role

Důvěryhodné role jsou:

statutární zástupce
ředitel společnosti
ředitel bezpečnosti (Security Officer)
Provozní manager ICT

#### 5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

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

#### 5.2.3 Identifikace a autentizace pro každou roli

Jednotliví uživatelé se do aplikace hlásí pomocí čipových karet.

#### 5.2.4 Role vyžadující rozdělení povinností

Role, které vyžadují rozdělení, jsou:

ředitel provozu
ředitel bezpečnosti

## 5.3 Personální bezpečnost

### 5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

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

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

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

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

### 5.3.2 Posouzení spolehlivosti osob

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

Bezúhonnost se posuzuje podle výpisu z rejstříku trestů.

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

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

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

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

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

#### 5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

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

#### 5.3.4 Požadavky a periodicita školení

Zaměstnanci a ostatní pracovníci ACAeID musí absolvovat průběžný cyklus bezpečnostního a aplikačního vzdělávání. Podrobnější popis je v dokumentu ACAeID 8 – Obsluha systému.

#### 5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

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

#### 5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Vykonávání neautorizované činnosti se považuje za hrubé porušení pracovní kázně a sankce se řídí zákoníkem práce.

#### 5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Doporučuje se osvědčení podnikatele pro přístup k utajovaným informacím do stupně utajení VYHRAZENÉ vydané NBÚ.

#### 5.3.8 Dokumentace poskytovaná zaměstnancům

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

### 5.4 Auditní záznamy (logy)

#### 5.4.1 Typy zaznamenávaných událostí

Auditní záznamy obsahují informace o všech důležitých událostech provozu systému.

#### 5.4.2 Periodicita zpracování záznamů

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

#### 5.4.3 Doba uchování auditních záznamů

Auditní záznamy se uchovávají po dobu nejméně 10 let.

#### 5.4.4 Ochrana auditních záznamů

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

#### 5.4.5 Postupy pro zálohování auditních záznamů

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

#### 5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

O shromažďování auditních záznamů se vede evidence.

#### 5.4.7 Postup při oznamování události subjektu, který ji způsobil

Neposkytuje se.

#### 5.4.8 Hodnocení zranitelnosti

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

### 5.5 Uchovávání informací a dokumentace

#### 5.5.1 Typy informací a dokumentace, které se archivují

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

#### 5.5.2 Doba uchování uchovávaných informací a dokumentace

Pro archivaci jsou vybírána media, u kterých výrobce zaručuje minimální dobu čitelnosti 3 roky. Po dvou letech jsou média přepalována. Celková doba archivace dat je 15 let.

#### 5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

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

#### 5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Postupy odpovídají bodu 5.5.1 této CP.

#### 5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

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

#### 5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

Archivní kopie se ukládají do bankovní schránky.

#### 5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

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

### 5.6 Výměna dat pro ověřování elektronických pečetí v nadřízeném kvalifikovaném certifikátu poskytovatele

Výměna klíčů CA se neprovádí.

### 5.7 Obnova po havárii nebo kompromitaci

#### 5.7.1 Postup v případě incidentu a kompromitace

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

#### 5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

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

### 5.7.3 Postup při kompromitaci dat pro vytváření elektronických pečetí poskytovatele

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

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

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

### 5.7.4 Schopnost obnovit v činnosti po havárii

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

## 5.8 Ukončení činnosti CA nebo RA

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

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

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

Obdobná ustanovení platí i v případě jiných způsobů ukončení činnosti.

# 6 TECHNICKÁ BEZPEČNOST

## 6.1 Generování a instalace párových klíčů

### 6.1.1 Generování párových klíčů

Pár klíčů CA eIdentity je vygenerován během procesu instalace nejméně třemi vyškolenými pracovníky CA. Ke generování je využit nově nainstalovaný software a hardware. Klíč je generován v kryptografickém modulu, který slouží jako zařízení pro vytváření elektronických pečetí (SealCD).
Klíče jsou generovány dle předem připraveného procesu popsaného v instalační příručce podepisovacího pracoviště ACA eIdentity.

Klíče ACAeID se mohou použít pouze k pečetění kvalifikovaných certifikátů a seznamu zneplatněných certifikátů.

Generování klíčů koncových uživatelů je řešeno aplikací on-line registrační autorita.

### 6.1.2 Předání dat pro vytváření elektronických podpisů

Generování soukromých klíčů je řešeno aplikací on-line registrační místo, která je přenese na HSM.

### 6.1.3 Předání dat pro ověřování elektronických podpisů poskytovateli služeb vytvářejících důvěru

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

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

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

### 6.1.5 Délky párových dat

Délky klíčů musí být dostatečné vzhledem k aktuálním metodám pro odhalení soukromého klíče kryptografickou analýzou používání klíčů. Současná praxe udává akceptovatelnou bezpečnost pro velikost klíčů pro algoritmus RSA 2048 bitů a více, pro EC 384 a více. CA eIdentity odmítne vydat certifikát pro klíče menší velikosti. .

### 6.1.6 Omezení pro použití dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí

Viz kapitola 7.1.2.1 této CP - QC.

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

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

### 6.2.1 Standardy a podmínky použití kryptografických modulů

Klíče CA eIdentity jsou generovány hardwarovým modulem splňujícím požadavky Common Criterií EAL4+.

### 6.2.2 Sdílení tajemství

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

### 6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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

### 6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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

### 6.2.5 Úschova dat pro vytváření elektronických podpisů

CA eIdentity nearchivuje soukromé klíče.

### 6.2.6 Transfer dat pro vytváření elektronických pečetí do kryptografického modulu nebo z kryptografického modulu

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

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

#### 6.2.7 Uložení dat pro vytváření elektronických pečetí v kryptografickém modulu

Soukromé klíče jsou uloženy v kryptografických modulech v šifrované formě.

#### 6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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

#### 6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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

#### 6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

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

Pro ničení soukromých klíčů jsou použity nulovací funkce kryptografických modulů.

#### 6.2.11 Hodnocení kryptografických modulů

Použité kryptografické zařízení HSM má prohlášení o shodě v souladu s požadavky Nařízení eIDAS a prováděcími předpisy.

### 6.3 Další aspekty správy párových dat

#### 6.3.1 Uchovávání dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí

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

#### 6.3.2 Maximální doba platnosti certifikátu vydaného podepisující nebo pečetící osobě a párových dat

Kvalifikované certifikáty QCA eIdentity vydané pomocí Bank iD mají dobu platnosti stanovenou smlouvou mezi eIdentity a.s. a Bank iD maximálně 90 dnů. Před skončením platnosti kvalifikovaného certifikátu QCA přestane být tento užíván k vydávání dalších kvalifikovaných certifikátů žadatelů, aby žádný z vydaných kvalifikovaných certifikátů žadatelů

neměl dobu platnosti přesahující dobu platnosti certifikátu, za pomocí kterého byl vytvořen.

Období použití klíčů odpovídá době platnosti certifikátu.

## 6.4 Aktivační data

### 6.4.1 Generování a instalace aktivačních dat

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

### 6.4.2 Ochrana aktivačních dat

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

### 6.4.3 Ostatní aspekty archivačních dat

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

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

## 6.5 Počítačová bezpečnost

### 6.5.1 Specifické technické požadavky na počítačovou bezpečnost

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

Komunikace mezi ACAeID a Bank iD je zabezpečena šifrovaným kanálem HTTPS a je garantována smlouvou mezi eIdentity a.s. a Bankovní identitou a.s.

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

Systémy ACAeID jsou od internetového provozu odděleny vhodným bezpečnostním zařízením (např. firewall) a prostupný provoz je řízen a kontrolován.

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

#### 6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení vychází z níže uvedených norem a soulad s těmito normami je ověřen auditem:

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 ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky
ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací
ČSN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací.
ČSN EN ISO 19011 - Směrnice pro auditování systému managementu jakosti a/nebo systému environmentálního managementu.

### 6.6 Bezpečnost životního cyklu

#### 6.6.1 Řízení vývoje systému

Vývoj systému probíhal podle pravidel zabezpečení vývoje.

#### 6.6.2 Kontroly řízení bezpečnosti

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

#### 6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti probíhá v uzavřeném cyklu:

Analýza požadavků a definice systému
Návrh a řešení systému
Integrace
Implementace
Provoz (užívání)
Nepřetržité hodnocení provozu

Nepřetržité školení uživatelů

### 6.7 Síťová bezpečnost

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

### 6.8 Časová razítka

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

# 7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OSCP

## 7.1 Profil certifikátu

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

Délka klíče certifikační autority QCA vydávající kvalifikované certifikáty je 3072 bitů

Minimální délka klíče vydávaných kvalifikovaných certifikátů je 2048 bitů v případě RSA klíčů, 384 bitů v případě EC algoritmu.

Základní položky a popis jejich hodnot uvádí následující tabulka:

| Položka | Hodnota |
|---|---|
| Serial Number | Unikátní číslo kvalifikovaného certifikátu v prostředí poskytovatele služeb vytvářejících důvěru |
| Signature Algorithm | OID algoritmu použitého pro elektronickou pečeť kvalifikovaného certifikátu |
| Issuer DN | Označení vydavatele kvalifikovaného certifikátu v souladu s kapitolou 3.1.1.1 této CP |
| Valid From | Formát dle RFC3280, UTC čas začátku platnosti kvalifikovaného certifikátu |
| Valid To | Formát dle RFC3280, UTC čas konce platnosti kvalifikovaného certifikátu |
| Subject DN | Označení držitele kvalifikovaného certifikátu v souladu s kapitolou 3.1.1.2 této CP |
| Subject Public Key | Veřejný klíč držitele kvalifikovaného certifikátu |
| Signature | Elektronická pečeť vydavatele kvalifikovaného certifikátu |

### 7.1.1 Číslo verze

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

### 7.1.2 Rozšiřující položky v certifikátu

#### 7.1.2.1 KeyUsage

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

| | Certifikát Certifikační autority ACAeID | Osobní kvalifikované certifikáty |
|---|---|---|

| | | | |
|---|---|---|---|
| Kritický | | Ano | Ano |
| 0 | digitalSignature | - | Nastaven - povinný |
| 1 | nonRepudiation | - | Nastaven - povinný |
| 2 | keyEncipherment | - | Nastaven - povinný |
| 3 | dataEncipherment | - | Nastaven - povinný |
| 4 | keyAgreement | - | - |
| 5 | keyCertSign | Nastaven | - |
| 6 | CRLSign | Nastaven | - |
| 7 | encipherOnly | - | - |
| 8 | decipherOnly | - | - |

#### 7.1.2.2 Certificate Policy

Rozšíření Certificate Policies má OID 0.4.0.1456.1.2 a položka obsahuje:

[1]Certificate Policy:
Policy Identifier=1.2.203.27112489.1.10.8.1.0
[1,1]Policy Qualifier Info:
Policy Qualifier Id=CP
Qualifier:
http://www.acaeid.cz/aca3.1/cp-qc-bi.pdf
[1,2] Policy Qualifier Info:
Policy Qualifier Id=User Notice
Qualifier:
Notice Text= **Tento kvalifikovany certifikat pro elektronicky podpis byl vydan v souladu s narizenim EU c. 910/2014.This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.**

#### 7.1.2.3 qcStatements

Rozšíření qcStatements bude mít odpovídající hodnotu:

- statementID, které odpovídá kvalifikovanému certifikátu (esi4-qcStatement-1)
- statementID, označující certifikát splňující přílohu 1 Nařízení, tj. kvalifikovaný certifikát pro elektronický podpis (esi4-qcStatement-6 s QcType id-etsi-qct-esign)
- statementID s odkazem na PKI Disclosure Statement (esi4-qcStatement-5)
- statementID esi4-qcStatement-4, indikující certifikát vydaný do QSCD (esi4- qcStatement-4

#### 7.1.2.4 4Authority Info Access

Toto rozšíření obsahuje adresu OCSP serveru pro daný certifikát.

#### 7.1.2.5 Subject Alternative Names

Nekritický atribut v souladu s RFC3280. Obsahuje adresu elektronické pošty ze žádosti.

#### 7.1.2.6 BasicConstraints

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

| | Certifikát Certifikační autority ACAeID | Osobní kvalifikované certifikáty |
|---|---|---|
| Kritický | Ne | Ne |
| ServerAuth | - | - |
| ClientAuth | - | - |
| CodeSigning | - | - |
| EmaiProtection | - | Nastaven |
| ipsecEndSystem | - | - |
| ipsecTunnel | - | - |
| ipsecUser | - | - |
| TimeStamping | - | - |
| OCSP Signing | - | - |
| Microsoft Server Gated Crypto (SGC) OID:1.3.6.1.4.1.311.10.3.3 | - | - |
| Netscape SGC OID: 2.16.840.1.113730.4.1 | - | - |

#### 7.1.2.7 CRLDistributionPoints

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

#### 7.1.2.8 Authority Key Identifier

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

#### 7.1.2.9 Subject Key Identifier

Obsahuje výtah veřejného klíče držitele certifikátu. Není to kritické rozšíření.

#### 7.1.2.10 Bank iD rozšíření

Obsahuje „envelope name“ a „envelope hash“ jako dvě rozšíření s OID „1.3.6.1.4.1.58356.1“ a

„1.3.6.1.4.1.58356.2“ specifická pro použití s Bankovní identitou a.s..

#### 7.1.3 Objektové identifikátory (dále „OID“) algoritmů

Pro účely vydávání kvalifikovaných certifikátů žadatelů se použijí podpisová schémata dle platné legislativy, respektive dle příslušných technických standardů, na které legislativa odkazuje.

#### 7.1.4 Způsoby zápisu jmen a názvů

Viz kapitola 3.1.

#### 7.1.5 Omezení jmen a názvů

Je zakázáno použití jmen a názvů v rozporu se zákony. Za případné zneužití jmen a názvů je zodpovědný žadatel.

#### 7.1.6 OID certifikační politiky

Viz kapitola 1.2.

#### 7.1.7 Rozšiřující položka „Policy Constraints“

Viz kapitola 7.1.2.2.

#### 7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Viz kapitola 7.1.2.2..

#### 7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Viz kapitola 7.1.2.2.

### 7.2 Profil seznamu zneplatněných certifikátů

| OID | Kritický | Název | Hodnota |
|---|---|---|---|
| 1.2.840.113549.1.1.5 | | signatureAlgoritmIdentifier | Identifikátor a parametry algoritmu, použitého pro elektronickou pečeť vydávaného CRL |

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

#### 7.2.1 Číslo verze

Verze CRL je číslo 3.

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

Viz kapitola 7.2.

### 7.3 Profil OCSP

#### 7.3.1 Číslo verze

Služba je poskytována dle RFC 6950 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ ve verzi 1. Odpovědi jsou opečetěny certifikátem vydávající autority. Algoritmus podpisu OCSP odpovědí je stejný, jako algoritmus pečetě certifikátů dle této politiky.

#### 7.3.2 Rozšiřující položky OCSP

Služba podporuje Nonce rozšíření.

# 8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

## 8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Audit souladu systému s jeho dokumentací a požadavky se provádí nejméně jednou ročně nebo při každé změně konfigurace.

## 8.2 Identita a kvalifikace hodnotitele

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

## 8.3 Vztah hodnotitele k hodnocenému subjektu

Hodnotitel se nesmí podílet na budování či provozování hodnoceného systému.

## 8.4 Hodnocené oblasti

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

## 8.5 Postup v případě zjištění nedostatků

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

## 8.6 Sdělování výsledků hodnocení

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

# 9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

## 9.1 Poplatky

### 9.1.1 Poplatky za vydání nebo obnovení certifikátu

Je řešeno smlouvou mezi Bankovní identitou a.s. a eIdentity a.s. Služba obnovení certifikátu se neposkytuje.

### 9.1.2 Poplatky za přístup k certifikátu

Přístup je zdarma.

### 9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Přístup k CRL je zdarma.

### 9.1.4 Poplatky za další služby

Ceny dalších poskytovaných služeb jsou uvedeny v Ceníku služeb.

### 9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

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

## 9.2 Finanční odpovědnost

### 9.2.1 Krytí pojištěním

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

### 9.2.2 Další aktiva a záruky

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

### 9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Služba se neposkytuje.

## 9.3 Citlivost obchodních údajů

### 9.3.1 Výčet citlivých informací

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

### 9.3.2 Informace mimo rámec citlivých informací

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

### 9.3.3 Odpovědnost za ochranu citlivých informací

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

## 9.4 Ochrana osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. A rovněž s nařízením Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

### 9.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění. Za ochranu osobních údajů ve společnosti eIdentity a.s. odpovídá DPO.

### 9.4.2 Osobní údaje

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

### 9.4.3 Údaje, které nejsou považovány za citlivé

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

### 9.4.4 Odpovědnost za ochranu osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

#### 9.4.5 Oznámení o používání důvěrných informací a souhlas s použitím citlivých informací

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

#### 9.4.6 Poskytnutí citlivých informací pro soudní či správní účely

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

#### 9.4.7 Jiné okolnosti zpřístupňování osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je řešena v souladu s požadavky zákona 110/2019 Sb. v aktuálním znění.

### 9.5 Práva duševního vlastnictví

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

### 9.6 Zastupování a záruky

#### 9.6.1 Zastupování a záruky CA

Společnost eIdentity a.s. zaručuje, že:

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

Další záruky mohou být specifikovány ve smlouvě o poskytnutí služby.

#### 9.6.2 Zastupování a záruky RA

Společnost eIdentity a.s. zaručuje, že průběh procesů v Aplikaci on-line registrační místo bude plně v souladu s touto CP.

#### 9.6.3 Zastupování a záruky držitele certifikátu, podepisující osoby

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

#### 9.6.4 Zastupování a záruky spoléhajících se stran

Předpokládá se, že spoléhající se strany postupují v souladu s Nařízením Evropského parlamentu a Rady (EU) č. 910/2014.

#### 9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Neposkytuje se.

### 9.7 Zřeknutí se záruk

Poskytování služeb se řídí zejména Nařízením Evropského parlamentu a Rady (EU) č. 910/2014.

### 9.8 Omezení odpovědnosti

Hranice odpovědnosti jsou dány Nařízením Evropského parlamentu a Rady (EU) č. 910/2014.

### 9.9 Odpovědnost za škodu, náhrada škody

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

### 9.10 Doba platnosti, ukončení platnosti

#### 9.10.1 Doba platnosti

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

#### 9.10.2 Ukončení platnosti

Úpravy CP včetně zajištění souladu politik schvaluje Výbor pro politiky.

#### 9.10.3 Důsledky ukončení a přetrvání závazků

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

## 9.11 Komunikace mezi zúčastněnými subjekty

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

## 9.12 Změny

### 9.12.1 Postup při změnách

Postup probíhá řízeným procesem.

### 9.12.2 Postup při oznamování změn

Postup probíhá řízeným procesem.

### 9.12.3 Okolnosti, při kterých musí být změněn OID

Postup probíhá řízeným procesem.

## 9.13 Řešení sporů

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

## 9.14 Rozhodné právo

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

## 9.15 Shoda s právními předpisy

Systém je provozován ve shodě s požadavky zákonů a předpisů, zároveň je provozován jako akreditovaný k poskytování kvalifikovaných služeb vytvářejících důvěru.

## 9.16 Další ustanovení

Není použito.

### 9.16.1 Rámcová dohoda

Není použito.

### 9.16.2 Postoupení práv

Není použito.

### 9.16.3 Oddělitelnost ustanovení

Není použito.

### 9.16.4 Zřeknutí se práv

Není použito.

### 9.16.5 Vyšší moc

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

## 9.17 Další opatření

Není použito.

# 10 ZÁVĚREČNÁ USTANOVENÍ

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