ACAeID 10.8 Certifikační politika - krátkodobý QC pro BankID

Kvalifikovaný poskytovatel služeb vytvářejících důvěru

Klasifikace dokumentu: TLP:CLEAR

Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze: 1.0.3
Datum: 12. 05. 2026
Vlastník dokumentu: LŠiroký (eIdentity, a.s.)
Schválil: Ing. Ladislav Šedivý

---

1 Úvod

Tato certifikační politika stanovuje zásady a postupy, které společnost eIdentity a.s. jako kvalifikovaný poskytovatel služeb vytvářejících důvěru uplatňuje při vydávání krátkodobých kvalifikovaných certifikátů pro elektronický podpis v rámci služby Bank iD / QSIGN.

Kvalifikovaná služba podle této certifikační politiky spočívá ve vydání krátkodobého kvalifikovaného certifikátu pro elektronický podpis fyzické osoby, který je použit pro vytvoření kvalifikovaného elektronického podpisu v rámci jedné podpisové transakce.

Ověření totožnosti fyzické osoby je prováděno s využitím prostředku pro elektronickou identifikaci poskytovaného v rámci Bank iD, tj. bankami poskytované metody digitálního ověření totožnosti. Služba je poskytována ve spolupráci se společností Bankovní identita a. s. na základě smluvního a technického integračního rámce mezi eIdentity a.s. a Bankovní identitou a.s.

Kvalifikovaný certifikát vydaný podle této certifikační politiky se využívá k ověření kvalifikovaného elektronického podpisu fyzické osoby. Certifikát je určen pro jednorázové použití v rámci podporované podpisové transakce a není určen k samostatnému opakovanému používání podepisující osobou.

Tato certifikační politika je určena zejména žadatelům o vydání krátkodobého kvalifikovaného certifikátu, podepisujícím osobám, spoléhajícím se stranám a dalším účastníkům PKI.

Tato certifikační politika předpokládá, že ověření identity podepisující osoby je prováděno v souladu s čl. 24 odst. 1a písm. c) nařízení eIDAS, s využitím metody elektronické identifikace, která v kombinaci s dalšími kontrolami a bezpečnostními opatřeními zajišťuje spolehlivé určení totožnosti fyzické osoby.

Struktura tohoto dokumentu vychází z dokumentu RFC 3647 – *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*. Tato certifikační politika je zpracována v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910 /2014, ve znění pozdějších předpisů, a souvisejícími právními a normativními požadavky.

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

Společnost eIdentity a.s. provozuje hierarchickou strukturu certifikačních autorit v souladu s požadavky na kvalifikované služby vytvářející důvěru a s požadavky příslušného orgánu dohledu.

1.1 Přehled

Postupy, pravidla, technologie a další skutečnosti popsané v této certifikační politice dokládají důvěryhodnost a integritu řešení ACAeID při vydávání krátkodobých kvalifikovaných certifikátů pro elektronický podpis v rámci služby Bank iD / QSIGN.

Tato certifikační politika vymezuje zejména:

- účel a rozsah použití krátkodobého kvalifikovaného certifikátu;
- participující subjekty;
- způsob ověření identity fyzické osoby;
- životní cyklus certifikátu;
- pravidla pro vydání, použití, zneplatnění a ověřování statutu certifikátu;

- základní provozní, bezpečnostní a právní požadavky vztahující se k vydávání certifikátu.

Informace o dalších službách poskytovaných eIdentity a.s. jsou popsány v příslušných certifikačních politikách, provozní dokumentaci a na internetových stránkách poskytovatele.

Zajištění bezpečného provozování kvalifikovaných služeb vytvářejících důvěru je popsáno v certifikační prováděcí směrnici, v souvisejících certifikačních politikách, v politice služby vzdáleného podpisu podle ACAeID 10.9 a v další interní bezpečnostní a provozní dokumentaci eIdentity.

Ve veřejné části webového prostoru poskytovatele jsou zpřístupněny informace, které umožňují zájemci, žadateli, podepisující osobě nebo spoléhající se straně seznámit se s poskytovanou službou, podmínkami jejího použití, svými povinnostmi a právy. K dispozici je zejména tato certifikační politika a další související veřejné 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, například `10.1.1.1` označuje dokument ACAeID 10.1 ve verzi 1.1.

Tato certifikační politika má tyto identifikační znaky:

Identifikační znak	Význam identifikačního znaku	Hodnota
Název dokumentu	Název dokumentu v čitelné podobě	ACAeID 10.8 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

ACAeID eIdentity a.s. tvoří kořenová certifikační autorita a podřízené vydávající certifikační autority.

Kořenová certifikační autorita vydává certifikáty pouze podřízeným certifikačním autoritám. Vydávající certifikační autorita QCA vydává kvalifikované certifikáty podle příslušných certifikačních politik, včetně krátkodobých kvalifikovaných certifikátů pro elektronický podpis podle této certifikační politiky.

Vydávající certifikační autorita QCA nevydává certifikáty dalším podřízeným certifikačním autoritám.

Společnost eIdentity a.s. provozuje také další certifikační autority a služby vytvářející důvěru, které se řídí vlastními certifikačními politikami, provozní dokumentací a příslušnými právními a normativními požadavky.

1.3.2 Registrační autority

Pro vydávání certifikátů podle této certifikační politiky se využívá online registrační proces podporovaný Bank iD.

Registrační proces je nastaven tak, aby umožnil ověření totožnosti žadatele o vydání krátkodobého kvalifikovaného certifikátu prostřednictvím prostředku pro elektronickou identifikaci Bank iD a dalších kontrol stanovených touto certifikační politikou, certifikační prováděcí směrnicí a související provozní dokumentací.

Ověření totožnosti je prováděno na základě údajů poskytnutých prostřednictvím Bank iD se souhlasem žadatele. Údaje potřebné pro vydání certifikátu zahrnují zejména identifikační údaje žadatele a další údaje nezbytné pro naplnění profilu kvalifikovaného certifikátu podle této certifikační politiky.

Aktuálnost údajů je zajišťována prostřednictvím banky zapojené do schématu Bank iD, zejména na základě ověření nebo aktualizace údajů vůči základním registrům nebo jiným zákonem předpokládaným zdrojům.

Vydání krátkodobého kvalifikovaného certifikátu probíhá online a je omezeno na konkrétní podpisovou transakci. Certifikát je vydán po splnění podmínek této certifikační politiky, po ověření identity žadatele a po potvrzení souhlasu s vydáním certifikátu a vytvořením kvalifikovaného elektronického podpisu.

Jako bezpečnostní opatření je podepisující osoba informována o provedeném podpisu a vydání certifikátu způsobem stanoveným touto certifikační politikou, politikou služby vzdáleného podpisu a související provozní dokumentací.

1.3.3 Držitelé kvalifikovaných certifikátů a podepisující osoby

Držitelem certifikátu a podepisující osobou je fyzická osoba, která požádala prostřednictvím podporovaného online procesu o vydání krátkodobého kvalifikovaného certifikátu pro elektronický podpis a které byl tento certifikát vydán.

Podepisující osoba jedná vlastním jménem a využívá krátkodobý kvalifikovaný certifikát výhradně k vytvoření kvalifikovaného elektronického podpisu v rámci konkrétní podpisové transakce.

Data pro vytváření elektronického podpisu jsou generována a používána v prostředí QSCD a nejsou podepisující osobě předávána jako samostatný prostředek.

1.3.4 Spoléhající se strany

Spoléhající se stranou je fyzická nebo právnická osoba, která se spoléhá na kvalifikovaný certifikát vydaný podle této certifikační politiky nebo na kvalifikovaný elektronický podpis vytvořený s využitím tohoto certifikátu.

Okruh subjektů, které připravují nebo předkládají podepisující osobě dokument určený k podpisu s využitím krátkodobého kvalifikovaného certifikátu podle této certifikační politiky, může být omezen na důvěryhodné spoléhající se strany nebo smluvní partnery zapojené do podporovaného procesu.

Za důvěryhodnou spoléhající se stranu nebo předkladatele dokumentu se považuje zejména subjekt, který má zavedená organizační a technická opatření zabraňující zneužití identity uživatele, řízený proces přípravy a předložení dokumentu k podpisu, mechanismy pro prevenci a řešení podvodného jednání a který splňuje podmínky stanovené smluvní dokumentací nebo pravidly integračního prostředí Bank iD / QSIGN.

Spoléhající se strany jsou povinny ověřovat platnost kvalifikovaného certifikátu a kvalifikovaného elektronického podpisu způsobem stanoveným touto certifikační politikou, právními předpisy a příslušnými technickými standardy.

1.3.5 Jiné participující subjekty

Dalšími participujícími subjekty jsou zejména:

- Bankovní identita a.s. jako provozovatel a integrátor prostředí Bank iD;
- banky zapojené do schématu Bank iD;
- orgán dohledu nad poskytovateli služeb vytvářejících důvěru;
- subjekt posuzování shody;
- orgány veřejné moci a orgány činné v trestním řízení, pokud jim to přísluší podle právních předpisů;
- další subjekty uvedené v související smluvní nebo provozní dokumentaci.

1.4 Použití certifikátu

Kvalifikované certifikáty vydané podle této certifikační politiky se mohou používat pouze k účelům stanoveným v této certifikační politice.

Certifikáty vydané podle této certifikační politiky jsou určeny pro jednorázové použití v rámci konkrétní podpisové transakce. Certifikát je vydán a použit pro vytvoření kvalifikovaného elektronického podpisu dokumentu předloženého podepisující osobě v rámci podporovaného procesu.

Kvalifikované certifikáty vydané podle této certifikační politiky mohou mít právní účinky úředně ověřeného podpisu za předpokladu, že certifikát obsahuje údaje o čísle a typu dokladu podle požadavků stanovených příslušným metodickým nebo technickým dokumentem Digitální a informační agentury a jsou splněny další podmínky stanovené právními předpisy.

1.4.1 Přípustné použití certifikátu

Kvalifikovaný certifikát vydaný podle této certifikační politiky lze použít výhradně pro vytvoření kvalifikovaného elektronického podpisu fyzické osoby v rámci služby QSIGN, resp. služby vzdáleného podpisu podporované Bank iD.

Certifikát je použitelný pouze v rámci podpisové transakce, pro kterou byl vydán.

1.4.2 Omezení použití certifikátu

Certifikát vydaný podle této certifikační politiky nesmí být použit v rozporu s účelem, pro který byl vydán, ani mimo podporovaný proces služby QSIGN / vzdáleného podpisu.

Certifikát nesmí být použit zejména:

- pro šifrování;
- pro autentizaci serveru nebo klienta v prostředí SSL/TLS;
- pro opakované nebo samostatné podepisování mimo konkrétní podpisovou transakci;
- pro jiné účely, které nejsou výslovně povoleny touto certifikační politikou.

Omezení použití certifikátu je dáno právními podmínkami služby, touto certifikační politikou, příslušným profilem certifikátu a technickými omezeními, zejména rozšířením KeyUsage.

1.5 Správa politiky

Za údržbu, přezkum a schválení tohoto dokumentu odpovídá Výbor pro politiky eIdentity a.s.

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

eIdentity a.s.
Hvožďanská 2053/3
148 00 Praha 4
Česká republika

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Předseda Výboru pro politiky eIdentity a.s.
E-mail: 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 jednání Výboru a v souladu s jeho jednacím řádem.

1.5.4 Postupy při schvalování souladu podle 1.5.3

Postupy při schvalování souladu certifikační politiky, certifikační prováděcí směrnice a souvisejících změn jsou určeny jednacím řádem Výboru pro politiky.

1.6 Přehled použitých pojmů a zkratek

Pojem / zkratka	Význam
ACAeID	Informační systém eIdentity a.s. poskytující služby vytvářející důvěru
Bank iD	Bankami poskytovaná metoda digitálního ověření totožnosti
CA	Certifikační autorita
CP	Certifikační politika
CPS	Certifikační prováděcí směrnice
CRL	Certificate Revocation List; seznam zneplatněných certifikátů
DIA	Digitální a informační agentura
DN	Distinguished Name; jednoznačná identifikace subjektu certifikátu
eIDAS	Nařízení Evropského parlamentu a Rady (EU) č. 910/2014
ISZR	Informační systém základních registrů
OID	Object Identifier; objektový identifikátor
PKI	Public Key Infrastructure; infrastruktura veřejných klíčů
PSVD / TSP	Poskytovatel služeb vytvářejících důvěru / Trust Service Provider
QC	Kvalifikovaný certifikát pro elektronický podpis
QCA	Vydávající certifikační autorita jako součást ACAeID
QSCD	Qualified Signature Creation Device; kvalifikovaný prostředek pro vytváření elektronických podpisů
QSIGN	Služba kvalifikovaného elektronického podpisu na dálku
RA online	Online registrační autorita / online registrační proces
RCA	Kořenová certifikační autorita jako součást ACAeID
SSL/TLS	Kryptografické protokoly pro zabezpečení komunikace v síti
ZR	Základní registry
Data pro vytváření elektronických podpisů	Jedinečná data používaná podepisující osobou k vytváření elektronických podpisů

Data pro ověřování elektronických podpisů	Data používaná k ověření elektronického podpisu
Revokace	Zneplatnění certifikátu

2 Odpovědnost za zveřejňování a úložiště informací a dokumentace

ACAeID zveřejňuje informace nezbytné pro ověření statutu kvalifikovaných certifikátů vydaných podle této certifikační politiky, zejména seznam zneplatněných certifikátů a další informace určené spoléhajícím se stranám.

Každý kvalifikovaný certifikát vydaný podle této certifikační politiky je možné dohledat podle sériového čísla a ověřit jeho stav prostřednictvím zveřejněných revokačních informací nebo jiných služeb ověřování statutu certifikátu, pokud jsou pro daný typ certifikátu poskytovány.

2.1 Úložiště informací a dokumentace

V informačním systému ACAeID jsou zpracovávány a uchovávány informace související s vydáváním, správou, použitím a zneplatněním kvalifikovaných certifikátů v souladu s právními předpisy, příslušnými normami, touto certifikační politikou a certifikační prováděcí směrnicí.

Záznamy a jejich změny mohou provádět pouze pověřené osoby nebo určené systémové komponenty v rozsahu svých oprávnění. Systém je navržen a provozován tak, aby bylo možné kontrolovat správnost záznamů, dohledat relevantní činnosti a identifikovat technické nebo programové změny, které by mohly porušit bezpečnostní požadavky.

Zveřejňované informace jsou určeny zejména spoléhajícím se stranám, aby mohly rozhodnout o platnosti a důvěryhodnosti kvalifikovaného certifikátu a kvalifikovaného elektronického podpisu s požadovanou mírou důvěry.

2.2 Zveřejňování informací a dokumentace

K veřejně dostupným informacím je možné přistupovat prostřednictvím webových služeb poskytovatele.

Veřejně dostupné mohou být zejména tyto informace vztahující se ke kvalifikovanému certifikátu:

- sériové číslo certifikátu;
- údaj o době platnosti certifikátu;
- stav certifikátu;
- revokační informace nezbytné pro ověření platnosti certifikátu.

Kvalifikované certifikáty, které byly zneplatněny, jsou uvedeny v seznamu zneplatněných kvalifikovaných certifikátů. Aktuální seznam zneplatněných certifikátů je dostupný v elektronické formě ve formátu CRL alespoň na jednom z níže uvedených míst:

- `https://www.acaeid.cz/aca3.3/crl/actual.crl`
- `https://pub1.acaeid.cz/aca3.3/crl/actual.crl`
- `https://pub2.acaeid.cz/aca3.3/crl/actual.crl`
- `https://www.acaeid.cz/aca3.2/crl/actual.crl`
- `https://pub1.acaeid.cz/aca3.2/crl/actual.crl`
- `https://pub2.acaeid.cz/aca3.2/crl/actual.crl`

Součástí zveřejněných informací je také informace o pořadí a době zveřejnění aktuálního CRL a historie zveřejněných CRL.

Informace o době zveřejnění aktuálního CRL je poskytována v souboru:

- `https://www.acaeid.cz/aca3.3/crl/actual-date.txt`
- `https://pub1.acaeid.cz/aca3.3/crl/actual-date.txt`
- `https://pub2.acaeid.cz/aca3.3/crl/actual-date.txt`
- `https://www.acaeid.cz/aca3.2/crl/actual-date.txt`
- `https://pub1.acaeid.cz/aca3.2/crl/actual-date.txt`
- `https://pub2.acaeid.cz/aca3.2/crl/actual-date.txt`

Údaj o době zveřejnění aktuálního CRL je uváděn ve tvaru `YYYYMMDDHHMMSS`.

Součástí veřejně dostupných informací je také tato certifikační politika, která je zveřejněna ve formátu PDF na webových stránkách eIdentity a.s. Na webových stránkách poskytovatele je dostupná právě platná verze certifikační politiky. Historie verzí je přístupná společně s vyznačením období platnosti jednotlivých verzí.

Na webových stránkách poskytovatele jsou dále zveřejněny certifikáty kořenové certifikační autority a vydávající certifikační autority. Pro ověření správnosti těchto certifikátů mohou být tyto certifikáty nebo údaje o nich zveřejněny také prostřednictvím důvěryhodného seznamu nebo webových stránek Digitální a informační agentury.

Na webových stránkách poskytovatele mohou být dále zveřejněny procesní, obchodní, uživatelské a další podpůrné informace vztahující se k poskytovaným službám.

2.3 Periodicita zveřejňování informací

Certifikační politika je schválena a zveřejněna dříve, než je podle ní možné vydat první kvalifikovaný certifikát.

Zveřejňované informace jsou aktualizovány podle potřeby tak, aby odpovídaly aktuálnímu stavu poskytované služby, platné dokumentaci a požadavkům právních předpisů.

Periodicita zveřejňování CRL je stanovena v kapitole 4.9.7 této certifikační politiky.

2.4 Řízení přístupu k jednotlivým typům úložišť

Publikování certifikační politiky schvaluje Výbor pro politiky. Odpovědnou osobu za zveřejnění a správu publikovaných dokumentů určuje Výbor pro politiky v souladu se svým jednacím řádem.

Zveřejnění a aktualizaci revokačních informací, zejména seznamu zneplatněných kvalifikovaných certifikátů, zajišťuje obsluha ACAeID nebo k tomu určené systémové komponenty s frekvencí a způsobem stanoveným touto certifikační politikou, certifikační prováděcí směrnicí a provozní dokumentací.

Přístup k neveřejným úložištím, interní dokumentaci, auditním záznamům a provozním informacím je omezen pouze na oprávněné osoby podle jejich role, odpovědnosti a principu nezbytné potřeby.

---

3 Identifikace a autentizace

3.1 Pojmenování

3.1.1 Typy jmen

Kvalifikované certifikáty vydávané QCA eIdentity a.s. obsahují v polích `Subject` a `Issuer` jména ve formátu odpovídajícím požadavkům X.500/X.501 a profilu certifikátu podle příslušných ETSI norem.

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 vydávané podle této certifikační politiky obsahují v poli `Subject` DN (*Distinguished Name*) podepisující osoby. DN se skládá z komponent uvedených v následující tabulce.

Atribut	Význam	Zdroj / ověření	Omezení	Příklad hodnoty

Country (`C`)	Kód státu vztahující se k identifikované osobě	Bank iD	podle ISO 3166	`CZ`
Locality (`L`)	Adresa bydliště fyzické osoby	Bank iD	nepovinné	`Vinohradská 22, 130 00 Praha 3`
Name (`name`)	Celé jméno osoby včetně případných titulů	Bank iD	nepovinné	`JUDr. Jan Tadeáš Novák`
Given Name (`givenName`)	Jméno nebo jména osoby	Bank iD	obsahuje jméno nebo jména osoby	`Jan Tadeáš`
Surname (`surname`)	Příjmení osoby	Bank iD	povinné, pokud je předáno jako samostatný údaj	`Novák`
Common Name (`CN`)	Celé jméno osoby	Bank iD	vyplňuje se hodnotou `name` , pokud je dostupná, nebo kombinací `givenName` a `surname`	`JUDr. Jan Tadeáš Novák`
Email Address (`E`)	E-mailová adresa osoby	Bank iD	nepovinné	`jan.novak@example.cz`
Pseudonym (`pseudonym`)	Pseudonym osoby	nepoužívá se	certifikáty podle této politiky nejsou vydávány na pseudonym	—
Title (	Titul osoby	nepoužívá se jako samostatný atribut,	nepovinné	—

`title`)		pokud není stanoveno profilem certifikátu		
SerialNumber (`serialNumber`)	Identifikátor dokladu nebo jiný identifikátor podle ETSI EN 319 412-1	Bank iD	vyplňuje se podle profilu certifikátu a dostupných údajů	`IDCCZ-Test123456`, `IR:CZ-123456789`
Bank iD pseudonym / specifický atribut	Hodnota specifická pro použití Bank iD	Bank iD / integrační prostředí	podle technického profilu služby; OID `1.3.6.1.4.1.58356.3`	—

Certifikát podepisující osoby musí obsahovat alespoň atribut `Common Name (CN)` nebo jiný jednoznačný identifikační údaj vyžadovaný příslušným profilem kvalifikovaného certifikátu.

Specifický atribut Bank iD pseudonym je používán v souladu s technickým profilem služby Bank iD / QSIGN a slouží k technické vazbě certifikátu na identifikační a podpisovou transakci. Význam, obsah a zpracování tohoto atributu jsou určeny technickou, smluvní a provozní dokumentací služby.

3.1.2 Požadavek na významnost jmen

Všechna pojmenování uvedená v DN certifikátu musí být smysluplná, přesná, doložitelná a musí se vztahovat k identifikované fyzické osobě.

Údaje uvedené v certifikátu musí odpovídat údajům získaným a ověřeným prostřednictvím Bank iD nebo jiným postupem stanoveným touto certifikační politikou, certifikační prováděcí směrnicí a příslušným profilem certifikátu.

3.1.3 Anonymita a používání pseudonymu

QCA eIdentity nevydává podle této certifikační politiky anonymní certifikáty.

Kvalifikovaný certifikát vystavený na základě ověření totožnosti prostřednictvím Bank iD není vydáván s možností uvedení pseudonymu podepisující osoby.

3.1.4 Pravidla pro interpretaci různých forem jmen

Pro uvádění jmen a dalších údajů v certifikátu se používají formáty a kódování přípustné podle příslušných technických norem a profilu certifikátu.

Tam, kde to příslušné normy a profil certifikátu umožňují, lze použít národní znakové sady v kódování UTF-8.

3.1.5 Jednoznačnost jmen

QCA eIdentity zajišťuje, aby údaje uvedené v certifikátu umožňovaly jednoznačnou identifikaci podepisující osoby v rozsahu požadovaném touto certifikační politikou a právními předpisy.

Podepisující osoba může mít v průběhu času více krátkodobých kvalifikovaných certifikátů vydaných podle této certifikační politiky. Tyto certifikáty mohou mít shodné nebo obdobné údaje v poli `Subject`, přičemž každý certifikát je jednoznačně identifikován zejména svým sériovým číslem a údaji vydávající certifikační autority.

3.1.6 Obchodní značky

Údaje uvedené v kvalifikovaném certifikátu vydaném podle této certifikační politiky se vztahují k fyzické osobě. Tato certifikační politika nepředpokládá uvádění obchodních značek, obchodních názvů ani údajů právnické osoby v certifikátu podepisující osoby.

3.2 Počáteční ověření identity

3.2.1 Ověřování souladu dat pro vytváření a ověřování elektronických podpisů

Data pro vytváření elektronických podpisů jsou generována v prostředí QSCD / HSM spravovaném eIdentity a.s. prostřednictvím systému ACAeID.

Odpovídající data pro ověřování elektronických podpisů jsou použita pro vytvoření žádosti o vydání krátkodobého kvalifikovaného certifikátu a jsou svázána s certifikátem vydaným podle této certifikační politiky.

Data pro vytváření elektronických podpisů nejsou předávána podepisující osobě jako samostatný prostředek. Jejich použití je omezeno na konkrétní podpisovou transakci a je řízeno službou vzdáleného podpisu podle příslušné politiky služby.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Podle této certifikační politiky se nevydávají kvalifikované certifikáty právnickým osobám ani organizačním složkám státu.

Identita právnické osoby nebo organizační složky státu se proto v rámci této certifikační politiky neověřuje.

3.2.3 Ověřování identity fyzické osoby

Ověření identity fyzické osoby pro účely vydání krátkodobého kvalifikovaného certifikátu podle této certifikační politiky se provádí v souladu s čl. 24 odst. 1a písm. c) nařízení eIDAS.

Ověření identity je založeno na použití prostředku pro elektronickou identifikaci podle § 38ab odst. 1 zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, tj. bankovní identity, v kombinaci s dalšími kontrolami a bezpečnostními opatřeními stanovenými touto certifikační politikou a související dokumentací.

Vydání bankovní identity bankou je podmíněno předchozím ověřením totožnosti klienta, zejména ověřením totožnosti za fyzické přítomnosti, ověřením totožnosti prostřednictvím prostředku pro elektronickou identifikaci s úrovní záruky vysoká, ověřením prostřednictvím Národního bodu pro identifikaci a autentizaci nebo ověřením v informačním systému veřejné správy.

Dalšími bezpečnostními opatřeními podporujícími spolehlivost procesu ověření identity jsou zejména:

- omezení okruhu důvěryhodných předkladatelů dokumentů nebo spoléhajících se stran;
- smluvní a technické řízení integračního prostředí Bank iD / QSIGN;
- ověřování aktuálnosti údajů prostřednictvím bank zapojených do Bank iD;
- ověřování nebo aktualizace údajů vůči základním registrům nebo jiným zákonem předpokládaným zdrojům;
- informování podepisující osoby o procesu podpisu prostřednictvím SMS notifikací a e-mailových zpráv;

- možnost iniciovat zneplatnění certifikátu v případě popření žádosti nebo podezření na zneužití.

Tento způsob vydávání krátkodobého kvalifikovaného certifikátu mohou využít pouze osoby, u nichž lze provést ověření prostřednictvím Bank iD v rozsahu požadovaném touto certifikační politikou. Typicky se jedná o občana České republiky nebo držitele průkazu o povolení pobytu v České republice, pokud jsou splněny podmínky Bank iD a této certifikační politiky.

Na základě smlouvy mezi eIdentity a.s. a Bankovní identitou a.s. jsou pro účely vydání certifikátu se souhlasem žadatele předávány údaje potřebné pro vydání certifikátu, včetně údajů potřebných pro identifikaci žadatele a údajů vyžadovaných profilem kvalifikovaného certifikátu.

Aktuálnost údajů je zajištěna prostřednictvím Bank iD a bank zapojených do schématu Bank iD, zejména na základě ověření údajů v základních registrech nebo zpracování notifikací ze základních registrů.

Dojde-li v době platnosti certifikátu ke změně údajů, které byly použity pro vydání certifikátu, a poskytovatel se o této změně prokazatelně dozví, posoudí dopad této změny na platnost certifikátu. Pokud se změna týká údajů uvedených v certifikátu nebo údajů podstatných pro jeho vydání, poskytovatel zajistí zneplatnění certifikátu.

Po vydání kvalifikovaného certifikátu a vytvoření podpisu je podepisující osoba informována na e-mailovou adresu a telefonní číslo získané nebo potvrzené prostřednictvím Bank iD nebo jiným postupem stanoveným provozní dokumentací. Informace obsahuje údaje o vydaném certifikátu nebo podpisové transakci a způsob, jak postupovat v případě, že podepisující osoba žádost o vydání certifikátu nebo podpis popírá.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu nebo podepisující osobě

Všechny informace uvedené v certifikátu vydaném podle této certifikační politiky jsou ověřeny prostřednictvím postupů stanovených touto certifikační politikou, certifikační prováděcí směrnicí, technickým profilem certifikátu a související provozní dokumentací, nebo jsou použity v souladu s těmito pravidly.

3.2.5 Ověřování specifických práv

Tato certifikační politika nepředpokládá ověřování specifických práv podepisující osoby jednat jménem jiné osoby nebo právnické osoby.

Certifikát je vydáván fyzické osobě jednající vlastním jménem pro účely vytvoření kvalifikovaného elektronického podpisu.

3.2.6 Kritéria pro interoperabilitu

QCA eIdentity může spolupracovat s certifikačními autoritami třetích stran, Bankovní identitou a.s., bankami zapojenými do schématu Bank iD nebo jinými relevantními subjekty pouze na základě smluvního vztahu nebo jiného právního a technického rámce zajišťujícího požadovanou úroveň bezpečnosti, důvěryhodnosti a interoperability.

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

3.3.1 Identifikace a autentizace při rutinní výměně párových dat

Výměna dat pro ověřování elektronických podpisů v již vydaném certifikátu se podle této certifikační politiky neposkytuje.

Krátkodobý kvalifikovaný certifikát je vydáván pro konkrétní podpisovou transakci. V případě potřeby nové podpisové transakce je generován nový podpisový klíč a vydán nový krátkodobý kvalifikovaný certifikát podle této certifikační politiky.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

Výměna párových dat po zneplatnění certifikátu se podle této certifikační politiky neposkytuje.

Po zneplatnění certifikátu nelze certifikát obnovit ani v něm měnit data pro ověřování elektronických podpisů.

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

Certifikáty vydávané podle této certifikační politiky jsou krátkodobé a jsou vydávány s maximální dobou platnosti nejvýše 3 měsíce.

O zneplatnění kvalifikovaného certifikátu může požádat zejména:

- držitel certifikátu nebo podepisující osoba;
- Bankovní identita a.s. nebo banka zapojená do schématu Bank iD, pokud je k tomu oprávněna podle smluvního nebo provozního rámce;
- odpovědná osoba eIdentity a.s.;
- jiný subjekt, pokud tak stanoví právní předpis, rozhodnutí příslušného orgánu nebo smluvní dokumentace.

Poskytovatel kvalifikovaný certifikát zneplatní zejména v těchto případech:

- na základě údajů o ztrátě, změně, zneužití nebo kompromitaci prostředku Bank iD nebo souvisejících autentizačních údajů, pokud jsou poskytovateli oznámeny Bankovní identitou a.s. nebo jiným oprávněným subjektem;
- na základě přijaté a řádně autentizované žádosti o zneplatnění;
- pokud podpisová transakce nebyla dokončena nebo certifikát nebyl použit v souladu s procesem stanoveným touto certifikační politikou;
- pokud podepisující osoba účinně popře žádost o vydání certifikátu nebo vytvoření podpisu;
- pokud podepisující osoba požádá o ukončení zpracování osobních údajů v rozsahu, který znemožňuje další vedení nebo použití certifikátu, pokud je takový postup v souladu s právními předpisy;
- na základě uvědomění držitele certifikátu nebo podepisující osoby, že hrozí nebezpečí zneužití dat pro vytváření elektronických podpisů nebo procesu vydání certifikátu;
- v případě, že byl kvalifikovaný certifikát vydán na základě nepravdivých, chybných nebo neúplných údajů;
- dozví-li se poskytovatel prokazatelně, že podepisující osoba zemřela nebo byla omezena ve svéprávnosti způsobem relevantním pro použití certifikátu;
- dozví-li se poskytovatel prokazatelně, že údaje, na jejichž základě byl kvalifikovaný certifikát vydán, pozbyly pravdivosti nebo aktuálnosti;
- pokud příslušný orgán dohledu nebo jiný oprávněný orgán nařídí zneplatnění certifikátu;

- pokud existuje důvodné podezření, že kvalifikovaný certifikát byl padělán, byl vydán na základě nepravdivých údajů, nebo pokud bylo zjištěno, že prostředek nebo proces použitý pro vytváření podpisu vykazuje bezpečnostní nedostatky umožňující padělání elektronických podpisů nebo změnu podepisovaných údajů.

Pokyn ke zneplatnění může podat podepisující osoba pro své certifikáty, Bankovní identita a.s., banka zapojená do schématu Bank iD, odpovědná osoba eIdentity a.s. nebo jiný oprávněný subjekt podle právních předpisů, smluvního rámce nebo provozní dokumentace.

Žádost o zneplatnění kvalifikovaného certifikátu ze strany držitele certifikátu nebo podepisující osoby může být realizována zejména prostřednictvím odkazu dostupného v informačním e-mailu zaslaném při vydání certifikátu nebo po provedení podpisové transakce.

Žádost o zneplatnění nebo oznámení podepisující osoby o podezření na zneužití lze podat také jiným způsobem stanoveným poskytovatelem, například:

- osobně na registračním místě, pokud je tento způsob pro danou službu poskytován;
- elektronicky podepsanou zprávou;
- prostřednictvím doručeného URL odkazu do e-mailové schránky podepisující osoby;
- jiným postupem stanoveným provozní dokumentací nebo zveřejněnými podmínkami služby.

Každá žádost o zneplatnění musí být před provedením posouzena z hlediska oprávněnosti žadatele, dostatečné autentizace a relevance důvodu zneplatnění.

Žádosti podané kanálem, který neumožňuje dostatečnou autentizaci žadatele, mohou být zpracovány až po doplnění nebo ověření potřebných údajů. V případě důvodného podezření na zneužití může poskytovatel přijmout přiměřená ochranná opatření i před úplným dokončením ověření.

---

4 Požadavky na životní cyklus certifikátu

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

O vydání krátkodobého kvalifikovaného certifikátu podle této certifikační politiky může požádat fyzická osoba, která splňuje podmínky pro ověření identity prostřednictvím Bank iD podle kapitoly 3.2.3 této certifikační politiky.

O certifikát může požádat pouze fyzická osoba, která:

- má elektronickou identitu použitelnou v rámci Bank iD;
- může být identifikována v rozsahu požadovaném touto certifikační politikou;
- je občanem České republiky nebo držitelem průkazu o povolení k pobytu v České republice, pokud tento údaj odpovídá pravidlům Bank iD a technickému profilu služby;
- nebyla omezena ve svéprávnosti způsobem, který by bránil platnému právnímu jednání souvisejícímu s vydáním certifikátu a vytvořením podpisu;
- poskytuje pouze pravdivé, úplné a aktuální údaje.

O tento typ certifikátu je možné požádat pouze prostřednictvím online registračního procesu provozovaného ve spolupráci se společností Bankovní identita a.s. podle pravidel uvedených v této certifikační politice, certifikační prováděcí směrnici a související provozní dokumentaci.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

Žadatel odpovídá za to, že údaje použité v rámci procesu Bank iD jsou správné, úplné a pravdivé. Žadatel je dále povinen používat prostředek Bank iD v souladu s podmínkami jeho vydavatele a přijmout přiměřená opatření proti jeho zneužití.

Údaje potřebné pro vydání certifikátu jsou předávány prostřednictvím Bank iD se souhlasem žadatele. Tyto údaje jsou ověřovány nebo aktualizovány vůči základním registrům nebo jiným zákonem předpokládaným zdrojům prostřednictvím bank zapojených do schématu Bank iD.

Za zajištění odpovídajícího procesu ověření identity a předání údajů odpovídají subjekty zapojené do procesu Bank iD v rozsahu stanoveném právními předpisy, smluvní dokumentací a provozními pravidly Bank iD.

eIdentity a.s. jako kvalifikovaný poskytovatel služeb vytvářejících důvěru odpovídá za posouzení splnění podmínek pro vydání kvalifikovaného certifikátu, za vydání certifikátu v souladu s touto certifikační politikou a za přijetí přiměřených opatření ke snížení rizika vydání certifikátu neoprávněné osobě.

Součástí bezpečnostních opatření je zejména informování podepisující osoby o vydání certifikátu a provedení podpisové transakce způsobem stanoveným touto certifikační politikou a související provozní dokumentací.

Žadatel může reklamovat výsledek registračního procesu u eIdentity a.s. s uvedením podrobností případu. Reklamace se vyřizuje podle interních pravidel eIdentity a příslušných smluvních podmínek.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Identifikace a autentizace žadatele probíhá prostřednictvím Bank iD a navazujícího online registračního procesu podle kapitoly 3.2.3 této certifikační politiky.

4.2.1.1 Zájem o službu

Zájem o použití služby je vyjádřen v rámci podporovaného procesu Bank iD / QSIGN. Podepisující osoba je před vytvořením podpisu seznámena s dokumentem určeným k podpisu a s podmínkami použití služby.

4.2.1.2 Vyplnění identifikačních údajů žadatele

Identifikační údaje žadatele jsou získány prostřednictvím Bank iD.

Z Bank iD mohou být převzaty zejména tyto údaje:

- jméno;
- příjmení;
- celé jméno;
- e-mailová adresa;
- adresa bydliště;
- číslo a typ primárního osobního dokladu, pokud je tento údaj dostupný a vyžadovaný profilem certifikátu;
- další údaje nezbytné pro vydání kvalifikovaného certifikátu podle této certifikační politiky a technického profilu certifikátu.

Rozsah předávaných údajů je určen právními předpisy, pravidly Bank iD, touto certifikační politikou, technickým profilem certifikátu a souhlasem nebo jiným právním titulem zpracování údajů.

4.2.1.3 Účet žadatele

Samostatný účet žadatele v systému eIdentity se při vydávání krátkodobých kvalifikovaných certifikátů podle této certifikační politiky nevytváří.

4.2.1.4 Žádost o vydání kvalifikovaného certifikátu

Po splnění všech stanovených podmínek, kontrol a potvrzení souhlasů je žádost o vydání krátkodobého kvalifikovaného certifikátu předána do interního systému eIdentity.

Žádost obsahuje nebo umožňuje doplnit zejména:

- označení, že certifikát má být vydán jako kvalifikovaný certifikát pro elektronický podpis;
- identifikační údaje podepisující osoby;
- identifikaci kvalifikovaného poskytovatele služeb vytvářejících důvěru a státu, ve kterém je poskytovatel usazen;
- údaje pro ověření platnosti certifikátu a přístup k revokačním informacím;
- identifikaci certifikační politiky, podle které je certifikát vydáván;
- data pro ověřování elektronického podpisu odpovídající datům pro vytváření elektronického podpisu;
- další údaje vyžadované profilem kvalifikovaného certifikátu.

Poskytovatel svým aplikačním vybavením doplní při vydání kvalifikovaného certifikátu zejména:

- datum a čas počátku a konce platnosti certifikátu;
- unikátní sériové číslo vydávaného certifikátu;
- údaje vydávající certifikační autority;
- elektronickou pečeť nebo podpis certifikační autority;
- příslušná rozšíření certifikátu podle profilu certifikátu.

4.2.1.5 Smlouva a platba

Platba za službu je řešena smluvním vztahem mezi eIdentity a.s. a Bankovní identitou a.s. nebo jiným smluvním partnerem podle obchodního modelu služby.

Před vydáním certifikátu podepisující osoba potvrdí příslušné smluvní podmínky, zejména smlouvu nebo rámcovou smlouvu o poskytnutí služby, pokud již nebyla dříve uzavřena.

Po potvrzení příslušných smluvních podmínek a souhlasů je v prostředí QSCD / HSM spravovaném eIdentity vygenerován podpisový pár klíčů. Data pro vytváření elektronického podpisu jsou vázána na konkrétní podpisovou transakci a nejsou předávána podepisující osobě.

Žádost o vydání certifikátu je následně předána do interního systému eIdentity, kde proběhne registrační proces a vlastní vydání krátkodobého kvalifikovaného certifikátu.

Ve smlouvě nebo smluvních podmínkách žadatel potvrzuje zejména, že:

- poskytl přesné, úplné a pravdivé informace podle požadavků této certifikační politiky;
- používá službu a vydaný certifikát pouze v souladu s jejich určeným účelem;
- učinil přiměřená opatření k zabránění neoprávněnému použití své bankovní identity;
- souhlasí s ověřením své identity prostřednictvím Bank iD a s předáním údajů nezbytných pro vydání certifikátu;
- bez zbytečného odkladu upozorní na nepřesnosti nebo změny údajů, na jejichž základě byl certifikát vydán;
- bez zbytečného odkladu oznámí podezření na zneužití Bank iD, podpisové transakce nebo údajů použitých pro vydání certifikátu.

4.2.1.6 Registrační proces

Proces vydání certifikátu probíhá zejména v těchto krocích:

1. Podepisující osoba v podporovaném rozhraní projeví vůli vytvořit kvalifikovaný elektronický podpis a za tímto účelem vydat krátkodobý kvalifikovaný certifikát.
2. Podepisující osoba je seznámena s dokumentem určeným k podpisu a potvrdí souhlas s vytvořením podpisu.
3. Podepisující osoba je přesměrována do prostředí Bank iD, kde proběhne ověření identity, autentizace a předání údajů potřebných pro vydání certifikátu.
4. Podepisující osoba potvrdí smluvní podmínky nebo rámcovou smlouvu s eIdentity a. s., pokud již taková smlouva nebyla uzavřena.
5. Systém v prostředí QSCD / HSM vygeneruje podpisový pár klíčů.
6. Interní systém eIdentity zpracuje žádost a vydá krátkodobý kvalifikovaný certifikát.
7. Certifikát je použit pro vytvoření kvalifikovaného elektronického podpisu v rámci konkrétní podpisové transakce.
8. Podepisující osoba je informována o vydání certifikátu a provedení podpisu.

9. Data pro vytváření elektronického podpisu jsou po dokončení podpisové transakce odstraněna z QSCD / HSM bez možnosti obnovy.
10. Záznamy související s žádostí, vydáním certifikátu, podpisovou transakcí a souhlasy jsou archivovány v souladu s touto certifikační politikou a interní dokumentací eIdentity.

Aplikace a integrační prostředí podporující online registrační proces jsou provozovány ve spolupráci se společností Bankovní identita a.s. v souladu se smluvním rámcem a požadavky eIdentity a.s. Plnění těchto požadavků je řízeno a kontrolováno stanoveným procesem.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

Žádost o vydání certifikátu je přijata pouze tehdy, pokud byly splněny podmínky této certifikační politiky, bylo provedeno ověření identity a autentizace podepisující osoby, byly předány údaje nezbytné pro vydání certifikátu a byly potvrzeny požadované souhlasy a smluvní podmínky.

Žádost musí být zamítnuta zejména v případě, že:

- není možné dostatečně ověřit identitu žadatele;
- nejsou předány údaje nezbytné pro vydání certifikátu;
- předané údaje jsou neúplné, rozporné nebo neodpovídají požadavkům profilu certifikátu;
- dojde k porušení registračního procesu;
- nejsou potvrzeny požadované souhlasy nebo smluvní podmínky;
- existuje důvodné podezření na zneužití identity, Bank iD nebo podpisové transakce.

Případné následné kroky jsou řešeny podle provozních pravidel eIdentity a smluvního rámce s Bankovní identitou a.s. nebo jiným relevantním smluvním partnerem.

4.2.3 Doba zpracování žádosti o certifikát

Zpracování žádosti o certifikát probíhá v rámci interaktivního online procesu. Délka procesu závisí zejména na činnosti podepisující osoby, dostupnosti Bank iD, dostupnosti systémů eIdentity a splnění požadovaných kontrol.

eIdentity a.s. poskytuje certifikační služby bez zbytečného odkladu po splnění všech podmínek pro vydání certifikátu.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

Po přijetí platné žádosti o vydání certifikátu interní systém QCA sestaví obsah certifikátu podle příslušného profilu certifikátu a této certifikační politiky.

Certifikát obsahuje zejména údaje podepisující osoby, data pro ověřování elektronického podpisu, identifikaci vydávající certifikační autority, dobu platnosti, sériové číslo certifikátu, identifikaci certifikační politiky a další povinná rozšíření podle profilu kvalifikovaného certifikátu.

Certifikát je vydán vydávající certifikační autoritou QCA a je opatřen elektronickou pečetí nebo podpisem certifikační autority v souladu s používanou technologií a profilem certifikátu.

Výsledný certifikát může být veden nebo zpřístupněn ve formátech odpovídajících provozní dokumentaci, zejména DER, PEM nebo jiném podporovaném formátu.

4.3.2 Oznamování o vydání certifikátu držiteli certifikátu a podepisující osobě

Podepisující osoba je informována o vydání certifikátu a provedení podpisové transakce způsobem stanoveným touto certifikační politikou, politikou služby vzdáleného podpisu a související provozní dokumentací.

Informace může obsahovat zejména údaje o vydaném certifikátu, identifikaci podpisové transakce, potvrzení o uzavření nebo použití smluvního vztahu, protokol o převzetí certifikátu nebo jiný důkaz o průběhu transakce.

4.4 Převzetí certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Certifikát vydaný podle této certifikační politiky je vydán a použit v rámci jedné podpisové transakce. Certifikát ani data pro vytváření elektronického podpisu nejsou podepisující osobě předávány jako samostatný prostředek.

Součástí dokumentace transakce může být protokol o převzetí certifikátu nebo jiný záznam potvrzující vydání certifikátu, jeho obsah, okamžik vydání a vazbu na konkrétní podpisovou transakci.

Certifikát vydaný v souladu s touto certifikační politikou nelze v rámci transakce odmítnout jako samostatně převzatý certifikát. Podepisující osoba však může bez zbytečného odkladu požádat o jeho zneplatnění, zejména pokud popírá žádost o vydání certifikátu nebo vytvoření podpisu.

Protokol nebo jiný záznam o vydání certifikátu je uchováván v elektronické archivní dokumentaci žádosti a podpisové transakce.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Vydaný kvalifikovaný certifikát lze po jeho vydání dohledat podle sériového čísla.

Veřejně dostupné mohou být zejména tyto údaje:

- sériové číslo certifikátu;
- doba platnosti certifikátu od–do;
- stav certifikátu;
- revokační informace nezbytné pro ověření platnosti certifikátu.

Zveřejňování údajů o certifikátu probíhá v rozsahu nezbytném pro ověření platnosti certifikátu a kvalifikovaného elektronického podpisu.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

O vydání certifikátu mohou být informovány pouze subjekty, které jsou k tomu oprávněny podle právních předpisů, smluvní dokumentace nebo provozních pravidel služby.

Informace o vydání certifikátu může být předána zejména:

- podepisující osobě;
- Bankovní identitě a.s. nebo bance zapojené do schématu Bank iD, pokud je to stanoveno smluvním nebo provozním rámcem;
- spoléhající se straně nebo předkladateli dokumentu v rozsahu nezbytném pro dokončení podpisové transakce;
- interním systémům eIdentity pro účely evidence, auditních záznamů a archivace.

4.5 Použití párových dat a certifikátu

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

Data pro vytváření elektronického podpisu vztahující se k vydanému kvalifikovanému certifikátu mohou být použita pouze pro vytvoření kvalifikovaného elektronického podpisu v rámci konkrétní podpisové transakce, pro kterou byl certifikát vydán.

Použití dat pro vytváření elektronického podpisu je povoleno až po splnění podmínek této certifikační politiky, ověření identity podepisující osoby, potvrzení příslušných souhlasů a vydání kvalifikovaného certifikátu.

Data pro vytváření elektronického podpisu jsou generována a používána v prostředí QSCD / HSM a nejsou předávána podepisující osobě. Po provedení podpisové transakce je jejich používání ukončeno a data jsou odstraněna bez možnosti obnovy.

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

Spoléhající se strana se může spoléhat pouze na certifikáty a data pro ověřování elektronických podpisů, které byly vydány a použity v souladu s touto certifikační politikou, příslušnou politikou služby vzdáleného podpisu a právními předpisy.

Před tím, než spoléhající se strana získá důvěru v platnost certifikátu a elektronického podpisu, musí provést přiměřené ověření, zejména:

- ověřit platnost certifikátu;
- ověřit, zda certifikát nebyl zneplatněn;
- ověřit celý certifikační řetězec;
- ověřit, zda certifikát nebyl použit v rozporu s jeho účelem nebo omezeními;
- ověřit kvalifikovaný elektronický podpis podle příslušných technických standardů.

Spoléhající se strana odpovídá za úkony, které musí provést před tím, než se na certifikát nebo podpis spolehne.

4.6 Obnovení certifikátu

Obnovení certifikátu se podle této certifikační politiky neposkytuje.

Krátkodobý kvalifikovaný certifikát je vydáván pro konkrétní podpisovou transakci. Pro další podpisovou transakci je nutné vydat nový kvalifikovaný certifikát podle této certifikační politiky.

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 nebo 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

Výměna dat pro ověřování elektronických podpisů v certifikátu se podle této certifikační politiky neposkytuje.

Pro další podpisovou transakci je generován nový podpisový pár klíčů a vydán nový krátkodobý kvalifikovaný certifikát.

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 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 certifikátů 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

Změna údajů v již vydaném certifikátu se podle této certifikační politiky neposkytuje.

Pokud dojde ke změně údajů, které jsou uvedeny v certifikátu nebo které byly podstatné pro jeho vydání, postupuje poskytovatel podle pravidel pro zneplatnění certifikátu. Pro další podpisovou transakci je nutné vydat nový kvalifikovaný certifikát.

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 osobě

Služba se neposkytuje.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Služba se neposkytuje.

4.8.6 Zveřejňování vydaných certifikátů 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 certifikátu musí bez zbytečného odkladu požádat o zneplatnění certifikátu v případě, kdy hrozí nebezpečí zneužití údajů použitých pro vydání certifikátu, zneužití Bank iD, zneužití podpisové transakce nebo jiné okolnosti uvedené v kapitole 3.4 této certifikační politiky.

Certifikát může zneplatnit také poskytovatel, pokud nastane některý z důvodů uvedených v kapitole 3.4 této certifikační politiky nebo v právních předpisech.

Zneplatněný certifikát nemůže být obnoven.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat držitel certifikátu, podepisující osoba, Bankovní identita a.s., banka zapojená do schématu Bank iD, odpovědná osoba eIdentity a.s. nebo jiný oprávněný subjekt podle kapitoly 3.4 této certifikační politiky.

4.9.3 Požadavek na zneplatnění certifikátu

Požadavek na zneplatnění certifikátu musí být podán, autentizován a zpracován v souladu s kapitolou 3.4 této certifikační politiky a související provozní dokumentací.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

Doba odkladu požadavku na zneplatnění certifikátu není stanovena. Požadavky na zneplatnění jsou zpracovávány bez zbytečného odkladu.

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

Certifikát je po přijetí oprávněné žádosti o zneplatnění zneplatněn neprodleně.

Informace o zneplatnění certifikátu se objeví ve zveřejněném CRL nejpozději do 24 hodin od přijetí oprávněné žádosti o zneplatnění.

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

Spoléhající se strany musí před spolehnutím se na certifikát nebo elektronický podpis ověřit stav certifikátu a platnost celého certifikačního řetězce podle kapitoly 4.5.2 této certifikační politiky.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

CRL se vydává denně s periodicitou nejméně jedenkrát za 24 hodin, zpravidla však každé 4 hodiny.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

CRL se zveřejňuje bez zbytečného odkladu po jeho vydání.

4.9.9 Možnost ověřování zneplatnění statusu certifikátu online

Ověřování statutu certifikátu online je poskytováno prostřednictvím OCSP. Podrobnosti jsou uvedeny v kapitole 7.3 „Profil OCSP“.

4.9.10 Požadavky při ověřování statusu certifikátu online

Požadavky při ověřování statusu certifikátu online jsou uvedeny v kapitole 7.3 „Profil OCSP “.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Jiné způsoby oznamování zneplatnění certifikátu se podle této certifikační politiky neposkytují.

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

Při kompromitaci nebo podezření na kompromitaci dat pro vytváření elektronických podpisů se postupuje podle kapitoly 3.4 této certifikační politiky a interních pravidel pro řízení bezpečnostních incidentů.

S ohledem na to, že data pro vytváření elektronických podpisů jsou generována a používána v prostředí QSCD / HSM pouze pro konkrétní podpisovou transakci a po jejím dokončení jsou odstraněna bez možnosti obnovy, se úschova ani obnova těchto dat neposkytuje.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Pozastavení platnosti certifikátu se podle této certifikační politiky 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

Ověřování statutu certifikátu je poskytováno prostřednictvím zveřejněného CRL a prostřednictvím OCSP podle této certifikační politiky.

4.10.2 Dostupnost služeb

Služby související s ověřováním statutu certifikátu jsou poskytovány nepřetržitě.

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou podle této certifikační politiky stanoveny.

4.11 Ukončení poskytování služeb pro držitele certifikátu nebo podepisující osobu

Platnost smluvního vztahu je stanovena smlouvou nebo smluvními podmínkami. Po ukončení smluvního vztahu je pro další využití služby nutné uzavřít nový smluvní vztah nebo znovu potvrdit příslušné smluvní podmínky, pokud to provozní model služby vyžaduje.

Pokud držitel certifikátu nebo podepisující osoba požádá o ukončení zpracování osobních údajů, eIdentity posoudí žádost podle pravidel ochrany osobních údajů a právních povinností vztahujících se k poskytování kvalifikovaných služeb vytvářejících důvěru.

Pokud je to s ohledem na stav certifikátu relevantní, může dojít ke zneplatnění certifikátu. Osobní údaje a záznamy, které je eIdentity povinna uchovávat z důvodu právních, regulatorních, smluvních, auditních nebo bezpečnostních požadavků, jsou nadále uchovávány v nezbytném rozsahu a po stanovenou dobu.

O ukončení smluvního vztahu nebo jiných relevantních skutečnostech může být informována Bankovní identita a.s. nebo jiný smluvní partner, pokud je to stanoveno smluvní dokumentací nebo je to nezbytné pro poskytování, ukončení nebo vypořádání služby.

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

Úschova dat pro vytváření elektronických podpisů u důvěryhodné třetí strany a jejich obnova se podle této certifikační politiky neposkytují.

Data pro vytváření elektronických podpisů jsou generována a používána v prostředí QSCD / HSM pouze pro konkrétní podpisovou transakci a po jejím dokončení jsou odstraněna bez možnosti obnovy.

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 stanovuje základní požadavky na fyzickou, procesní, personální, provozní a dokumentační bezpečnost související s vydáváním krátkodobých kvalifikovaných certifikátů podle této certifikační politiky.

Podrobné postupy jsou stanoveny v certifikační prováděcí směrnici, v interních bezpečnostních politikách, provozní dokumentaci, dokumentaci řízení incidentů, dokumentaci řízení změn, dokumentaci řízení přístupů a v další řízené dokumentaci eIdentity.

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Technologické komponenty podporující vydávání krátkodobých kvalifikovaných certifikátů, zpracování osobních údajů žadatelů, provoz QCA, provoz QSCD / HSM a související služby jsou umístěny v chráněných provozních lokalitách a datových centrech.

Používané prostory jsou voleny a provozovány tak, aby odpovídaly požadavkům na ochranu služeb vytvářejících důvěru, požadavkům systému řízení bezpečnosti informací a relevantním právním, regulatorním a normativním požadavkům.

Kritické technologické komponenty mohou být provozovány ve více geograficky oddělených lokalitách, aby byla zajištěna dostupnost, kontinuita a obnova služby v případě mimořádné události.

5.1.2 Fyzický přístup

Fyzický přístup do prostor, ve kterých jsou umístěny systémy a technologie podporující poskytování služby, je řízen a omezen pouze na oprávněné osoby.

Přístup do chráněných prostor je zajištěn kombinací organizačních a technických opatření, zejména:

- identifikací a evidencí vstupujících osob;
- řízením vstupu prostřednictvím přístupových prostředků;
- režimem návštěv a doprovodu;
- dohledem nebo ostrahou podle charakteru prostoru;
- monitorováním vybraných prostor a perimetru;
- zabezpečovacím a požárním systémem.

Přístup k technologiím eIdentity mají pouze osoby s odpovídajícím oprávněním a v rozsahu nezbytném pro výkon jejich role.

5.1.3 Elektřina a klimatizace

Používané prostory jsou vybaveny odpovídajícím napájením, záložními zdroji elektrické energie a klimatizací.

Napájení je zajištěno tak, aby byla minimalizována rizika výpadku služby v důsledku poruchy hlavního přívodu elektrické energie. Pro kritické technologie jsou využívány záložní zdroje, zejména UPS nebo náhradní zdroje elektrické energie.

Provozní prostředí je klimatizováno a je sledováno tak, aby byly zachovány podmínky potřebné pro bezpečný a spolehlivý provoz technologií.

5.1.4 Vlivy vody

Prostory určené pro provoz kritických technologií jsou chráněny proti rizikům způsobeným vodou. Jsou přijata opatření ke snížení rizika průniku vody, zaplavení nebo poškození technologií vodou.

5.1.5 Protipožární opatření a ochrana

Provozní prostory jsou chráněny proti požáru odpovídajícími technickými a organizačními opatřeními.

Používané prostory jsou vybaveny detekcí požáru a prostředky protipožární ochrany odpovídajícími charakteru prostoru a provozovaných technologií.

5.1.6 Ukládání médií

Média obsahující provozní zálohy, archivní kopie, auditní záznamy nebo jiné neveřejné informace jsou ukládána v chráněných úložištích s řízeným přístupem.

Přístup k médiím je omezen pouze na oprávněné osoby. O manipulaci s médii, pokud je relevantní, se vede evidence.

5.1.7 Nakládání s odpady

Odpady vznikající při provozu jsou likvidovány způsobem odpovídajícím jejich povaze a klasifikaci.

Média, dokumenty nebo jiné nosiče obsahující neveřejné, osobní nebo bezpečnostně citlivé informace jsou likvidovány bezpečným způsobem tak, aby nemohlo dojít k neoprávněnému zpřístupnění informací.

5.1.8 Zálohy mimo budovu

Pro zajištění obnovy služby a uchování záznamů jsou zálohy a archivní kopie ukládány také odděleně od produkčního prostředí nebo v jiné chráněné lokalitě.

Způsob ukládání záloh mimo hlavní provozní lokalitu je stanoven interními pravidly pro zálohování, archivaci, obnovu a kontinuitu činností.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Důvěryhodné role jsou role, které mají významný vliv na bezpečnost, provoz, správu nebo audit služeb vytvářejících důvěru.

Mezi důvěryhodné role patří zejména:

- statutární zástupce;
- ředitel společnosti;
- bezpečnostní ředitel / CISO / manažer kybernetické bezpečnosti;
- provozní ředitel nebo provozní manažer ICT;
- architekt kybernetické bezpečnosti;
- administrátor;
- auditor;
- další role stanovené interní dokumentací eIdentity.

Odpovědnosti, pravomoci, obsazení a neslučitelnosti důvěryhodných rolí jsou stanoveny v interní dokumentaci bezpečnostních a provozních rolí.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro vybrané bezpečnostně významné operace může být vyžadována účast nejméně dvou důvěryhodných osob.

Rozsah činností, pro které se uplatní pravidlo více osob, je stanoven certifikační prováděcí směrnicí, interní provozní dokumentací nebo dokumentací bezpečnostních rolí.

5.2.3 Identifikace a autentizace pro každou roli

Osoby v důvěryhodných, administrátorských a provozních rolích se do systémů přihlašují individuálně s využitím přidělených autentizačních prostředků.

Sdílení účtů nebo autentizačních prostředků není přípustné.

Přístupová oprávnění jsou přidělována podle role, odpovědnosti a principu nezbytné potřeby. Přístupy jsou evidovány a přezkoumávány podle interních pravidel eIdentity.

5.2.4 Role vyžadující rozdělení povinností

Rozdělení povinností se uplatňuje u rolí, jejichž souběh by mohl vést ke střetu zájmů, obcházení kontrol, neoprávněným změnám nebo snížení nezávislosti bezpečnostního dohledu.

Oddělení rolí se uplatňuje zejména mezi:

- provozními rolemi;
- bezpečnostními rolemi;
- administrátorskými rolemi;
- auditními rolemi;
- rolemi odpovědnými za schvalování a provádění změn.

Konkrétní neslučitelnosti rolí jsou stanoveny v interní dokumentaci bezpečnostních a provozních rolí.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

eIdentity zajišťuje, aby osoby podílející se na poskytování, správě, bezpečnosti nebo auditu služeb vytvářejících důvěru měly odpovídající kvalifikaci, zkušenosti, důvěryhodnost a znalosti potřebné pro výkon svěřené role.

Důvěryhodnost zaměstnanců a dalších osob je jedním ze základních předpokladů pro výkon činností, při nichž dochází k přístupu k citlivým aktivům, systémům, informacím nebo bezpečnostně významným operacím.

Personální bezpečnost zahrnuje zejména výběr vhodných osob, ověřování jejich spolehlivosti, školení, stanovení odpovědností, řízení přístupů a postupy při změně nebo ukončení pracovního nebo smluvního vztahu.

5.3.2 Posouzení spolehlivosti osob

Spolehlivost osob je posuzována přiměřeně povaze jejich role, odpovědnostem a oprávněním.

Zdrojem informací mohou být zejména:

- informace poskytnuté posuzovanou osobou;
- veřejně dostupné informace;

- reference;
- interní záznamy;
- další podklady v souladu s právními předpisy.

Bezúhonnost může být ověřována výpisem z rejstříku trestů, pokud je to přiměřené a v souladu s právními předpisy.

Při posuzování spolehlivosti se zohledňují relevantní informace o osobě, povaze role, rozsahu přístupu k aktivům a rizicích spojených s výkonem dané role.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Zaměstnanci a další osoby podílející se na provozu ACAeID musí před zahájením výkonu své role absolvovat vstupní bezpečnostní a aplikační školení v rozsahu odpovídajícím jejich roli.

Školení zahrnuje zejména základní bezpečnostní pravidla, ochranu informací, ochranu osobních údajů, pravidla používání systémů, povinnosti související s rolí a postupy pro hlášení bezpečnostních událostí.

5.3.4 Požadavky a periodicita školení

Zaměstnanci a další osoby podílející se na provozu ACAeID absolvují pravidelné bezpečnostní a aplikační školení.

Periodicita a obsah školení jsou stanoveny interní dokumentací eIdentity a přizpůsobují se povaze role, změnám v dokumentaci, změnám systémů, výsledkům auditů, bezpečnostním incidentům a regulatorním požadavkům.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Pravidelná rotace pracovníků mezi rolemi se obecně nepředpokládá.

Pokud je pro zajištění provozu nezbytné, aby pracovník dočasně vykonával jinou roli, musí být k této roli oprávněn, proškolen a musí mu být přidělena pouze oprávnění nezbytná pro její výkon.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Neoprávněná činnost, zneužití oprávnění nebo porušení bezpečnostních pravidel se posuzuje podle závažnosti.

Takové jednání může být řešeno jako porušení pracovních nebo smluvních povinností, bezpečnostní incident nebo jiný delikt podle právních předpisů.

Sankce se řídí pracovněprávními předpisy, smluvními podmínkami a interními pravidly eIdentity.

5.3.7 Požadavky na nezávislé zhotovitele a dodavatele

Dodavatelé a jiné externí osoby, které se podílejí na poskytování, správě nebo bezpečnosti služeb vytvářejících důvěru, musí splňovat bezpečnostní, smluvní a organizační požadavky stanovené eIdentity.

Přístup dodavatelů k systémům, informacím, prostorám nebo bezpečnostně významným činnostem je řízen, evidován a omezen pouze na nezbytný rozsah.

Podle povahy činnosti mohou být po dodavateli požadována dodatečná bezpečnostní opatření, smluvní závazky, prohlášení o mlčenlivosti, doložení kvalifikace nebo jiné důkazy způsobilosti.

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnancům a dalším osobám je poskytována dokumentace nezbytná pro výkon jejich role.

Tato dokumentace může zahrnovat zejména:

- popis pracovní náplně;
- bezpečnostní politiky a provozní postupy;
- uživatelskou nebo administrátorskou dokumentaci systémů;
- pravidla pro ochranu informací a osobních údajů;
- postupy pro hlášení incidentů a bezpečnostních událostí.

5.4 Auditní záznamy

5.4.1 Typy zaznamenávaných událostí

Auditní záznamy obsahují informace o důležitých událostech provozu systému a služby.

Zaznamenávány jsou zejména události související s:

- žádostí o vydání certifikátu;

- ověřením identity a autentizací žadatele;
- předáním údajů prostřednictvím Bank iD;
- vydáním certifikátu;
- vytvořením kvalifikovaného elektronického podpisu;
- zneplatněním certifikátu;
- přístupy oprávněných osob k systémům;
- administrátorskými zásahy;
- změnami konfigurace;
- bezpečnostními událostmi a incidenty;
- provozem revokačních a validačních služeb.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou pravidelně zpracovávány a vyhodnocovány.

Události s vyšší závažností, bezpečnostní události a podezření na incident jsou vyhodnocovány bez zbytečného odkladu.

5.4.3 Doba uchování auditních záznamů

Auditní záznamy se uchovávají po dobu nejméně 10 let, není-li právními předpisy, regulatorními požadavky, příslušnými normami nebo interní dokumentací stanovena delší doba uchování.

5.4.4 Ochrana auditních záznamů

Přístup k auditním záznamům je řízen a omezen pouze na oprávněné osoby.

Auditní záznamy jsou chráněny proti neoprávněné změně, zničení, smazání, ztrátě nebo neoprávněnému zpřístupnění.

5.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy jsou ukládány a zálohovány tak, aby bylo možné jejich obnovení v případě technické poruchy, poškození dat, bezpečnostního incidentu nebo jiné mimořádné události.

Zálohy auditních záznamů jsou chráněny obdobně jako primární auditní záznamy.

5.4.6 Systém shromažďování auditních záznamů

Auditní záznamy jsou shromažďovány v interních systémech eIdentity nebo v určených systémech pro log management, monitoring a archivaci.

O shromažďování auditních záznamů se vede evidence v rozsahu stanoveném interní dokumentací.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Oznamování události subjektu, který ji způsobil, se standardně neposkytuje, pokud právní předpis, smluvní závazek nebo interní postup nestanoví jinak.

Události, které mohou mít dopad na bezpečnost, důvěryhodnost, dostupnost nebo právní účinky služby, jsou řešeny podle pravidel řízení bezpečnostních událostí a incidentů.

5.4.8 Hodnocení zranitelnosti

Události s vyšším stupněm závažnosti jsou eskalovány odpovědným osobám.

Zjištěné zranitelnosti jsou evidovány, vyhodnocovány, prioritizovány a řešeny v souladu s interním procesem řízení zranitelností a změnového řízení.

5.5 Uchovávání informací a dokumentace

5.5.1 Typy informací a dokumentace, které se archivují

eIdentity uchovává informace a dokumentaci vztahující se k vydávání, použití, správě a zneplatnění kvalifikovaných certifikátů tak, aby bylo možné zpětně prokázat řádné provedení jednotlivých úkonů a splnění požadavků této certifikační politiky.

Uchovávají se zejména:

- údaje a záznamy související s žádostí o vydání certifikátu;
- údaje získané prostřednictvím Bank iD v rozsahu nezbytném pro vydání certifikátu;
- záznamy o ověření identity a autentizaci podepisující osoby;
- záznamy o souhlasu s vydáním certifikátu a vytvořením podpisu;
- vydané certifikáty;
- záznamy o vytvoření podpisu;
- záznamy o zneplatnění certifikátu;
- CRL, OCSP záznamy a související revokační informace;
- auditní a provozní záznamy;

- smluvní a uživatelská dokumentace související s vydáním certifikátu;
- záznamy potřebné pro řešení reklamací, sporů, incidentů, auditů a posuzování shody.

Archivované záznamy jsou chráněny tak, aby byla zajištěna jejich integrita, důvěrnost, dostupnost a ověřitelnost po celou dobu uchování.

5.5.2 Doba uchování uchovávaných informací a dokumentace

Záznamy a dokumentace vztahující se k vydávání certifikátů podle této certifikační politiky jsou uchovávány po dobu stanovenou právními předpisy, regulatorními požadavky, příslušnými normami, touto certifikační politikou a interní dokumentací eIdentity.

Není-li stanovena delší doba, jsou záznamy a dokumentace uchovávány po dobu nejméně 15 let.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Uchovávané informace a dokumentace jsou chráněny proti neoprávněnému přístupu, změně, zničení, ztrátě nebo neoprávněnému zpřístupnění.

Přístup k archivním záznamům je řízen podle typu záznamu, jeho klasifikace a oprávnění konkrétní osoby.

Certifikáty a revokační informace mohou být zpřístupněny v rozsahu stanoveném touto certifikační politikou. Auditní, provozní, bezpečnostní, smluvní a transakční záznamy jsou přístupné pouze oprávněným osobám.

Osoby s oprávněním k přístupu k archivním záznamům jsou poučeny o povinnosti zachovávat důvěrnost informací a o tom, že archivní záznamy mohou obsahovat osobní údaje, důvěrné informace, provozní informace a bezpečnostně citlivé informace.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Záznamy a dokumentace jsou pravidelně zálohovány v souladu s interními pravidly zálohování, archivace a obnovy.

Zálohy jsou ukládány a chráněny tak, aby bylo možné obnovit záznamy v případě technické poruchy, poškození dat, bezpečnostního incidentu nebo jiné mimořádné události.

Integrita archivovaných dat je ověřována prostřednictvím kontrolních mechanismů, zejména kryptografických otisků, elektronických podpisů, elektronických pečetí, časových údajů nebo jiných odpovídajících prostředků.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Záznamy obsahují údaj o čase, ve kterém byly pořízeny nebo zpracovány.

Systémový čas relevantních systémů je synchronizován s důvěryhodným zdrojem času navázaným na UTC.

U vybraných archivních záznamů mohou být pro posílení prokazatelnosti, integrity a časového určení použity elektronické podpisy, elektronické pečetě, elektronická časová razítka nebo jiné odpovídající technické prostředky.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace

Záznamy a dokumentace jsou shromažďovány a uchovávány v systémech eIdentity určených pro provozní evidenci, auditní záznamy, bezpečnostní monitoring a archivaci.

Archivní kopie mohou být uchovávány v elektronické podobě na zabezpečených úložištích, případně na oddělených archivních médiích nebo v jiném řízeném úložišti, pokud tento způsob splňuje požadavky na integritu, dostupnost, důvěrnost a obnovitelnost záznamů.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Uchovávané informace lze získat pouze řízeným postupem a pouze osobami, které k tomu mají oprávnění.

Ověření integrity archivovaných informací se provádí zejména porovnáním kryptografických otisků, ověřením elektronického podpisu, elektronické pečeti, časového údaje nebo jiného mechanismu použitého při archivaci.

5.6 Výměna dat pro ověřování elektronických podpisů v certifikátu vydávající certifikační autority

Výměna dat pro ověřování elektronických podpisů v certifikátu vydávající certifikační autority se v rámci této certifikační politiky neprovádí.

Změna nebo výměna klíčů certifikační autority se řídí příslušnou certifikační politikou, certifikační prováděcí směrnicí a interní provozní dokumentací eIdentity.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup v případě incidentu a kompromitace

V případě bezpečnostního incidentu, kompromitace nebo podezření na kompromitaci se postupuje podle interní politiky řízení incidentů, plánu pro zvládání krizových situací, plánu obnovy a dalších souvisejících dokumentů eIdentity.

Incident je evidován, klasifikován, analyzován, řešen a vyhodnocen v souladu s interními pravidly a použitelnými právními a regulatorními požadavky.

Pokud incident může mít dopad na důvěrnost, integritu nebo dostupnost služby, na vydané certifikáty, na data pro vytváření elektronických podpisů nebo na důvěryhodnost poskytované služby, jsou přijata přiměřená nápravná a ochranná opatření.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Systém je navržen a provozován tak, aby bylo možné v případě poškození výpočetních prostředků, softwaru nebo dat obnovit poskytování služby v požadovaném rozsahu a čase.

Obnova může zahrnovat zejména výměnu poškozených technických prostředků, obnovu softwaru, obnovu konfigurací, obnovu dat ze záloh nebo aktivaci náhradních provozních postupů.

5.7.3 Postup při kompromitaci klíčů vydávající certifikační autority

V případě kompromitace nebo podezření na kompromitaci soukromého klíče vydávající certifikační autority nebo jiného klíče poskytovatele, který má dopad na důvěryhodnost vydaných certifikátů, eIdentity přijme bez zbytečného odkladu opatření k omezení dopadů.

Tato opatření mohou zahrnovat zejména:

- zneplatnění dotčeného certifikátu vydávající certifikační autority;
- zveřejnění informace o zneplatnění prostřednictvím příslušných revokačních informací;
- posouzení dopadu na certifikáty vydané kompromitovaným klíčem;
- zneplatnění dotčených vydaných certifikátů, pokud je to nezbytné;

- informování orgánu dohledu a dalších oprávněných subjektů;
- informování dotčených osob nebo spoléhajících se stran přiměřeným způsobem;
- obnovení služby s využitím náhradních nebo nově vytvořených důvěryhodných komponent.

Podrobnosti jsou stanoveny v certifikační prováděcí směrnici, plánu obnovy, politice řízení incidentů a další interní provozní dokumentaci.

5.7.4 Schopnost obnovit činnost po havárii

eIdentity udržuje postupy a opatření pro obnovu činnosti po havárii nebo jiné mimořádné události.

Postupy obnovy jsou stanoveny v interní dokumentaci pro kontinuitu činností, zvládání krizových situací a obnovu služeb.

Postupy obnovy jsou pravidelně přezkoumávány a podle potřeby testovány tak, aby byla zajištěna schopnost obnovit poskytování služby v požadovaném čase a rozsahu.

5.8 Ukončení činnosti CA nebo RA

eIdentity v případě plánovaného ukončení činnosti CA, RA nebo poskytování služby postupuje řízeným způsobem tak, aby byla zachována ochrana uživatelů, dostupnost potřebných záznamů, informování příslušných orgánů a minimalizace dopadů na spoléhající se strany.

eIdentity informuje Digitální a informační agenturu nejméně 3 měsíce před předpokládaným ukončením činnosti. Současně vynaloží veškeré možné úsilí k tomu, aby vedená evidence byla převzata jiným kvalifikovaným poskytovatelem služeb vytvářejících důvěru, pokud je to relevantní a proveditelné.

eIdentity dále informuje dotčené žadatele, podepisující osoby, spoléhající se strany nebo smluvní partnery o záměru ukončit činnost v přiměřené lhůtě a způsobem odpovídajícím povaze poskytované služby, smluvním podmínkám a právním požadavkům.

Pokud se nepodaří zajistit převzetí evidence jiným kvalifikovaným poskytovatelem služeb vytvářejících důvěru, eIdentity informuje Digitální a informační agenturu nejméně 30 dní před ukončením činnosti.

Obdobná ustanovení platí i v případě jiných způsobů ukončení činnosti nebo ukončení poskytování služby.

---

6 Technická bezpečnost

6.1 Generování a instalace párových klíčů

6.1.1 Generování párových klíčů

Párová data certifikačních autorit eIdentity jsou generována řízeným postupem podle certifikační prováděcí směrnice, instalační dokumentace a interních provozních pravidel ACAeID.

Generování párových dat certifikační autority probíhá za účasti určeného počtu vyškolených a oprávněných osob v důvěryhodných rolích. Ke generování se používá schválený hardware, software a kryptografický modul splňující požadavky stanovené právními předpisy, příslušnými normami a interní bezpečnostní dokumentací eIdentity.

Data pro vytváření elektronických pečetí nebo podpisů používaná certifikační autoritou jsou generována a uchovávána v kryptografickém modulu určeném pro provoz certifikační autority. Tato data se používají pouze k účelům stanoveným příslušnou certifikační politikou, zejména k vydávání kvalifikovaných certifikátů a k vydávání seznamů zneplatněných certifikátů.

Generování dat pro vytváření elektronických podpisů podepisujících osob podle této certifikační politiky probíhá v rámci podporovaného online registračního a podpisového procesu. Tato data jsou generována v prostředí QSCD / HSM a jsou určena pouze pro konkrétní podpisovou transakci.

6.1.2 Předání dat pro vytváření elektronických podpisů

Data pro vytváření elektronických podpisů podepisující osoby jsou generována v prostředí QSCD / HSM spravovaném eIdentity a.s. prostřednictvím systému ACAeID a související služby vzdáleného podpisu.

Data pro vytváření elektronických podpisů nejsou předávána podepisující osobě jako samostatný prostředek a nejsou exportována mimo prostředí určené pro jejich bezpečné použití.

Použití těchto dat je omezeno na konkrétní podpisovou transakci, pro kterou byl vydán krátkodobý kvalifikovaný certifikát podle této certifikační politiky.

6.1.3 Předání dat pro ověřování elektronických podpisů poskytovateli služeb vytvářejících důvěru

Data pro ověřování elektronických podpisů odpovídající datům pro vytváření elektronických podpisů jsou předána certifikační autoritě v rámci žádosti o vydání kvalifikovaného certifikátu.

Žádost o vydání certifikátu je vytvářena a předávána způsobem stanoveným provozní dokumentací, zejména ve formátu PKCS#10 nebo v jiném technicky odpovídajícím formátu. Přenos žádosti probíhá zabezpečeným komunikačním kanálem.

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

Data pro ověřování elektronických podpisů podepisující osoby jsou součástí vydaného kvalifikovaného certifikátu.

Certifikáty certifikačních autorit eIdentity jsou zveřejněny na webových stránkách eIdentity a.s. společně s údaji umožňujícími ověření jejich pravosti, zejména s otisky certifikátů pořízenými vhodnými kryptografickými algoritmy.

Certifikáty certifikačních autorit nebo údaje o nich mohou být dostupné také prostřednictvím důvěryhodného seznamu nebo webových stránek Digitální a informační agentury.

6.1.5 Délky párových dat

Délky klíčů musí být zvoleny tak, aby poskytovaly dostatečnou kryptografickou odolnost po celou dobu zamýšleného použití s ohledem na aktuální stav poznání, platná bezpečnostní doporučení, technické normy a schválené kryptografické profily.

CA eIdentity odmítne vydat certifikát pro klíče menší než 3072 bitů v případě algoritmu RSA nebo pro klíče s nižší než ekvivalentní bezpečnostní úrovní v případě algoritmů založených na eliptických křivkách.

Délky párových dat a použité kryptografické algoritmy musí být v souladu s profilem certifikátu, certifikační prováděcí směrnicí, interní kryptografickou politikou a požadavky vztahujícími se ke kvalifikovaným službám vytvářejícím důvěru.

Data pro vytváření elektronických podpisů podepisující osoby vydávaná podle této certifikační politiky jsou určena pouze pro konkrétní podpisovou transakci. I v tomto případě musí použitý algoritmus a délka klíče splňovat minimální požadavky uvedené výše.

6.1.6 Omezení pro použití dat pro ověřování elektronických podpisů

Omezení pro použití dat pro ověřování elektronických podpisů jsou stanovena profilem certifikátu, příslušnými rozšířeními certifikátu, zejména `KeyUsage`, a touto certifikační politikou.

Krátkodobý kvalifikovaný certifikát vydaný podle této certifikační politiky je určen výhradně pro ověření kvalifikovaného elektronického podpisu vytvořeného v rámci konkrétní podpisové transakce.

Podrobnosti profilu certifikátu jsou uvedeny v kapitole 7 této certifikační politiky.

6.2 Ochrana dat pro vytváření elektronických podpisů a bezpečnost kryptografických modulů

Tato kapitola je podrobně rozpracována v certifikační prováděcí směrnici, technické dokumentaci, provozní dokumentaci a dokumentaci kryptografických modulů.

Data pro vytváření elektronických podpisů podepisující osoby jsou generována a používána v prostředí QSCD / HSM. Jejich použití je řízeno tak, aby bylo umožněno pouze v rámci konkrétní podpisové transakce a po potvrzení příslušných souhlasů podepisující osoby.

Soukromé klíče certifikačních autorit eIdentity jsou uloženy v kryptografických modulech a jejich použití je řízeno interními bezpečnostními pravidly, pravidly důvěryhodných rolí a postupy pro aktivaci, provoz, zálohování, obnovu a ukončení životního cyklu klíčů.

6.2.1 Standardy a podmínky použití kryptografických modulů

Kryptografické moduly používané pro činnosti certifikační autority a pro podporu služby podle této certifikační politiky splňují požadavky stanovené nařízením eIDAS, souvisejícími prováděcími předpisy, příslušnými ETSI normami a dalšími relevantními technickými specifikacemi.

Použité kryptografické moduly jsou voleny a provozovány tak, aby poskytovaly odpovídající úroveň ochrany dat pro vytváření elektronických podpisů, dat certifikační autority a dalších kryptografických aktiv.

6.2.2 Sdílení tajemství

Vybrané citlivé operace certifikační autority vyžadují účast více oprávněných osob nebo použití mechanismů rozdělení oprávnění.

Rozsah operací, u kterých se uplatňuje pravidlo více osob, je stanoven certifikační prováděcí směrnicí a interní provozní dokumentací.

6.2.3 Úschova dat pro vytváření elektronických podpisů

Data pro vytváření elektronických podpisů podepisujících osob nejsou archivována ani předávána do úschovy třetí straně.

Tato data jsou generována a používána v prostředí QSCD / HSM pouze pro konkrétní podpisovou transakci a po jejím dokončení jsou odstraněna bez možnosti obnovy.

Soukromé klíče certifikačních autorit a souvisejících komponent jsou uloženy pouze v určených bezpečnostních prostředcích a chráněny v souladu s interními pravidly eIdentity.

6.2.4 Zálohování dat pro vytváření elektronických podpisů

Data pro vytváření elektronických podpisů podepisujících osob vydávaná podle této certifikační politiky se nezálohují, protože jsou určena pouze pro jednorázové použití v rámci konkrétní podpisové transakce.

Soukromé klíče certifikačních autorit mohou být zálohovány v rámci řízeného postupu prostředky kryptografického modulu, pokud je to povoleno příslušným bezpečnostním profilem, certifikační prováděcí směrnicí a interními pravidly eIdentity.

6.2.5 Archivace dat pro vytváření elektronických podpisů

eIdentity nearchivuje data pro vytváření elektronických podpisů podepisujících osob vydaná nebo použitá podle této certifikační politiky.

Archivovány jsou pouze záznamy o žádosti, vydání certifikátu, podpisové transakci, použití certifikátu, zneplatnění certifikátu a další auditní a provozní záznamy podle této certifikační politiky.

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

Data pro vytváření elektronických podpisů podepisujících osob jsou generována uvnitř QSCD / HSM a nejsou exportována mimo toto prostředí.

Pokud je v rámci provozu certifikační autority nezbytný transfer kryptografických aktiv, provádí se pouze řízeným a bezpečným způsobem stanoveným certifikační prováděcí směrnicí, dokumentací kryptografického modulu a interní provozní dokumentací.

6.2.7 Uložení dat pro vytváření elektronických podpisů v kryptografickém modulu

Data pro vytváření elektronických podpisů jsou po dobu svého použití uložena v kryptografickém modulu způsobem odpovídajícím jeho bezpečnostním vlastnostem a konfiguraci.

Uložení a použití těchto dat je chráněno proti neoprávněnému přístupu, exportu, změně nebo zneužití.

6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat certifikační autority

Data pro vytváření elektronických podpisů podepisující osoby mohou být použita pouze po splnění podmínek podpisové transakce, zejména po ověření identity podepisující osoby, potvrzení souhlasu s vydáním certifikátu a potvrzení souhlasu s vytvořením podpisu.

Aktivace soukromého klíče certifikační autority nebo jiných klíčů poskytovatele probíhá podle certifikační prováděcí směrnice a interních provozních pravidel, která stanoví požadavky na oprávněné osoby, autentizaci a případné použití pravidla více osob.

6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat certifikační autority

Použití dat pro vytváření elektronických podpisů podepisující osoby je ukončeno po dokončení podpisové transakce.

Soukromé klíče certifikační autority nebo jiné klíče poskytovatele jsou deaktivovány postupy stanovenými provozní dokumentací, zejména při ukončení příslušného provozního režimu, změně konfigurace nebo při bezpečnostní události.

6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat certifikační autority

Data pro vytváření elektronických podpisů podepisující osoby jsou po dokončení podpisové transakce zničena nebo odstraněna z QSCD / HSM bez možnosti obnovy.

Zničení soukromého klíče certifikační autority nebo jiného klíče poskytovatele se provádí pouze na základě schváleného řízeného postupu a za účasti určených oprávněných osob. O zničení klíče se pořizuje záznam.

Pro ničení kryptografických dat se používají bezpečné funkce kryptografických modulů nebo jiné odpovídající technické prostředky.

6.2.11 Hodnocení kryptografických modulů

Použité kryptografické moduly a prostředky mají odpovídající prohlášení, certifikaci nebo jiné důkazy shody podle požadavků nařízení eIDAS, prováděcích předpisů a příslušných technických norem.

Dokumentace k hodnocení kryptografických modulů je uchovávána jako součást řízené dokumentace eIdentity a je předkládána při posuzování shody v rozsahu požadovaném auditorem nebo orgánem dohledu.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických podpisů

Data pro ověřování elektronických podpisů podepisující osoby jsou součástí vydaného kvalifikovaného certifikátu.

Veřejné klíče certifikačních autorit, veřejné klíče vybraných komponent a další data pro ověřování elektronických podpisů nebo pečetí jsou zálohovány a archivovány v rámci standardních postupů zálohování a archivace eIdentity.

6.3.2 Maximální doba platnosti certifikátu vydaného podepisující osobě a párových dat

Kvalifikované certifikáty vydané podle této certifikační politiky mají maximální dobu platnosti nejvýše 3 měsíce, pokud příslušný profil certifikátu nebo smluvní dokumentace nestanoví kratší dobu.

Data pro vytváření elektronických podpisů podepisující osoby jsou určena pouze pro konkrétní podpisovou transakci. Období jejich použití je omezeno na dobu nezbytnou pro vytvoření kvalifikovaného elektronického podpisu v rámci této transakce.

Před skončením platnosti certifikátu vydávající certifikační autority přestane být tento certifikát používán k vydávání dalších certifikátů tak, aby žádný z vydaných certifikátů neměl dobu platnosti přesahující dobu platnosti certifikátu, kterým byl vydán.

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data k soukromým klíčům certifikační autority jsou vytvářena během řízeného procesu instalace nebo inicializace kryptografického modulu.

Aktivační data k použití dat pro vytváření elektronických podpisů podepisující osoby jsou součástí řízeného podpisového procesu a jsou vázána na konkrétní podpisovou transakci, ověření identity a potvrzení souhlasu podepisující osoby.

6.4.2 Ochrana aktivačních dat

Osoby, kterým jsou svěřena aktivační data nebo prostředky umožňující použití kryptografických aktiv, jsou povinny tato data a prostředky chránit před ztrátou, prozrazením, zneužitím nebo neoprávněným použitím.

Tato povinnost je stanovena smluvně, interní dokumentací a bezpečnostními pravidly eIdentity.

6.4.3 Ostatní aspekty aktivačních dat

Aktivační data slouží výhradně k účelu, pro který byla vytvořena nebo přidělena. Nesmí být používána k jinému účelu ani vkládána do systému, který nesouvisí s jejich určeným použitím.

Aktivační data nesmí být přenášena v otevřené podobě.

V případě podezření na prozrazení, ztrátu nebo zneužití aktivačních dat jsou přijata přiměřená ochranná opatření, včetně zneplatnění, změny nebo zničení aktivačních dat, případně i zneplatnění nebo vyřazení souvisejících kryptografických aktiv.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Veřejně dostupné části systému ACAeID a služby Bank iD / QSIGN jsou zpřístupněny prostřednictvím zabezpečeného komunikačního kanálu HTTPS. Případný provoz prostřednictvím protokolu HTTP je omezen pouze na veřejné informace nebo je přesměrován na HTTPS tak, aby nedocházelo k přenosu citlivých údajů nezabezpečeným kanálem.

Komponenty veřejné části systému, které slouží pouze k poskytování veřejných informací, jsou určeny pouze ke čtení a neumožňují vzdálenému uživateli provádět změny údajů v systému.

Veškeré úkony, při nichž dochází ke zpracování osobních údajů, údajů pro vydání certifikátu, údajů souvisejících s autentizací uživatele nebo údajů souvisejících s vytvořením elektronického podpisu, jsou prováděny výhradně prostřednictvím zabezpečených komunikačních kanálů.

Komunikace mezi ACAeID a Bank iD je zabezpečena šifrovaným komunikačním kanálem HTTPS. Podmínky integrace, bezpečnosti komunikace, odpovědností a předávání údajů jsou upraveny smlouvou mezi eIdentity a.s. a Bankovní identitou a.s.

Systémy ACAeID a související komponenty služby jsou odděleny od veřejného internetového provozu pomocí bezpečnostních síťových prvků, zejména firewallů a dalších mechanismů řízení a kontroly síťového provozu. Přístup z veřejné sítě je omezen pouze na nezbytná rozhraní služby.

Přístupové servery, veřejná rozhraní a další relevantní komponenty služby jsou pravidelně testovány na známé zranitelnosti. Zjištěné zranitelnosti jsou vyhodnocovány a řešeny v souladu s interním procesem řízení zranitelností a změnového řízení.

Systémy ACAeID a související technologické komponenty jsou provozovány v chráněném datovém centru s řízeným fyzickým přístupem. Přístup k technologiím mají pouze určené a oprávněné osoby v souladu s pravidly fyzické bezpečnosti, řízení přístupů a bezpečnostních a provozních rolí.

6.5.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti systému pro vydávání kvalifikovaných certifikátů podle této certifikační politiky vychází z požadavků právních předpisů, technických norem a veřejně dostupných specifikací vztahujících se k poskytování kvalifikovaných služeb vytvářejících důvěru, vydávání kvalifikovaných certifikátů, vzdálenému vytváření kvalifikovaných elektronických podpisů a řízení bezpečnosti informací.

Soulad s těmito požadavky je ověřován v rámci interních přezkumů, bezpečnostních kontrol a auditů, včetně posouzení shody prováděného subjektem posuzování shody.

Pro hodnocení počítačové bezpečnosti jsou relevantní zejména následující normy, specifikace a předpisy:

- **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 27002** – Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací;
- **ČSN ISO/IEC 27005** – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací;
- **ČSN EN ISO 19011** – Směrnice pro auditování systémů managementu;
- **ETSI EN 319 401** – *Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers*;

- **ETSI EN 319 411-1** – *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*;
- **ETSI EN 319 411-2** – *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*;
- **ETSI EN 319 412** – *Electronic Signatures and Trust Infrastructures (ESI); Certificate Profiles*;
- **ETSI TS 119 431-1** – *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev*;
- **ETSI TS 119 461** – *Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects*;
- **Prováděcí nařízení Komise (EU) 2025/1567**, pokud je relevantní pro službu vzdáleného vytváření kvalifikovaných elektronických podpisů nebo správu vzdálených QSCD.

Požadavky uvedených norem a předpisů jsou naplňovány prostřednictvím technických, organizačních a provozních opatření popsaných v této certifikační politice, v souvisejících certifikačních politikách, certifikační prováděcí směrnici, politice služby vzdáleného podpisu, interních bezpečnostních politikách a provozní dokumentaci eIdentity.

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Vývoj, úpravy a údržba systému pro vydávání certifikátů a související služby Bank iD / QSIGN probíhají podle interních pravidel zabezpečeného vývoje, řízení změn a provozního nasazování.

Změny systému, které mohou mít dopad na bezpečnost, dostupnost, integritu, důvěryhodnost služby nebo soulad s touto certifikační politikou, podléhají řízenému procesu posouzení, schválení, testování a dokumentace.

Produkční prostředí je odděleno od vývojového a testovacího prostředí. Nasazení změn do produkčního prostředí provádějí pouze oprávněné osoby v souladu s pravidly řízení přístupů, bezpečnostních a provozních rolí a změnového řízení.

6.6.2 Kontroly řízení bezpečnosti

Systém QCA eIdentity a související komponenty služby obsahují technické a organizační mechanismy pro ověřování integrity, řízení konfigurací, sledování bezpečnostních událostí a kontrolu provozního stavu služby.

Integrita aplikací a vybraných systémových komponent je ověřována pomocí kontrolních mechanismů, zejména kryptografických otisků, kontrol konfigurací nebo jiných prostředků umožňujících zjistit neoprávněnou změnu.

Výstupy kontrol integrity jsou pravidelně vyhodnocovány oprávněnými osobami.

Systémová a aplikační bezpečnost je dále podporována logováním, monitoringem, řízením zranitelností, řízením privilegovaných přístupů a pravidelným přezkumem relevantních bezpečnostních opatření.

6.6.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti probíhá v uzavřeném a opakovaném cyklu, který zahrnuje zejména:

- analýzu požadavků a bezpečnostních potřeb;
- návrh a posouzení bezpečnostní architektury;
- implementaci technických a organizačních opatření;
- integraci a testování;
- schválení změn před jejich nasazením;
- provoz a průběžné sledování bezpečnostního stavu;
- vyhodnocování provozních a bezpečnostních událostí;
- řízení zranitelností a nápravných opatření;
- pravidelné přezkumy, audity a aktualizace bezpečnostní dokumentace;
- školení osob podílejících se na provozu a správě systému.

Bezpečnostní opatření jsou v průběhu životního cyklu pravidelně přezkoumávána s ohledem na změny právních a regulatorních požadavků, změny technologií, výsledky auditů, zjištěné zranitelnosti, bezpečnostní incidenty a změny v architektuře nebo provozu služby.

6.7 Síťová bezpečnost

Síťová bezpečnost systému QCA eIdentity a souvisejících komponent služby je zajišťována vícevrstvým modelem ochrany, který zahrnuje zejména oddělení veřejně dostupných rozhraní od interních systémů, řízení síťového provozu, filtrování komunikace a omezení přístupů pouze na nezbytná komunikační rozhraní.

Systémy ACAeID a související komponenty služby jsou od veřejného internetového provozu odděleny bezpečnostními síťovými prvky, zejména firewally a dalšími mechanismy pro řízení, kontrolu a monitorování síťové komunikace.

Přístup k interním systémům, administrátorským rozhraním a provozním komponentám služby je omezen na oprávněné osoby a vyhrazené komunikační cesty.

Komunikace s Bank iD, spoléhajícími se stranami a dalšími relevantními systémy probíhá prostřednictvím zabezpečených komunikačních kanálů.

Změny síťové konfigurace, bezpečnostních pravidel a komunikačních rozhraní jsou prováděny řízeným způsobem v souladu s procesem změnového řízení.

6.8 Časová razítka

Auditní logy, databázové záznamy žádostí o certifikát, žádostí o zneplatnění certifikátu, CRL, OCSP záznamy, certifikáty a další relevantní provozní záznamy obsahují informace o čase.

Systémový čas relevantních systémů je v rámci vnitřní sítě synchronizován prostřednictvím protokolu NTP nebo jiného odpovídajícího mechanismu a je bezpečným způsobem navázán na UTC.

Služby kvalifikovaných elektronických časových razítek se pro tyto účely standardně nepoužívají, pokud není v konkrétním provozním postupu nebo archivačním mechanismu stanoveno jinak.

---

7 Profily certifikátu, seznamu zneplatněných certifikátů a OCSP

7.1 Profil certifikátu

Certifikáty vydávané podle této certifikační politiky jsou vydávány v souladu s doporučením ITU-T X.509, profilem X.509 podle RFC 5280 a příslušnými profily kvalifikovaných certifikátů podle ETSI EN 319 412.

Délka klíče vydávající certifikační autority QCA odpovídá požadavkům příslušné certifikační politiky, certifikační prováděcí směrnice a aktuálním kryptografickým požadavkům eIdentity.

CA eIdentity odmítne vydat certifikát pro klíče menší než 3072 bitů v případě algoritmu RSA nebo pro klíče s nižší než ekvivalentní bezpečnostní úrovní v případě algoritmů založených na eliptických křivkách.

Certifikáty vydané podle této certifikační politiky jsou určeny pro vytvoření kvalifikovaného elektronického podpisu v rámci konkrétní podpisové transakce. Data pro vytváření elektronického podpisu jsou generována a používána v prostředí QSCD / HSM a nejsou předávána podepisující osobě.

Základní položky certifikátu 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 nebo podpis vydávající certifikační autority
Issuer DN	Označení vydavatele kvalifikovaného certifikátu v souladu s kapitolou 3.1.1.1 této certifikační politiky
Valid From	UTC čas počátku platnosti kvalifikovaného certifikátu ve formátu podle RFC 5280
Valid To	UTC čas konce platnosti kvalifikovaného certifikátu ve formátu podle RFC 5280
Subject DN	Označení držitele kvalifikovaného certifikátu v souladu s kapitolou 3.1.1.2 této certifikační politiky
Subject Public Key	Data pro ověřování elektronického podpisu držitele kvalifikovaného certifikátu
Signature	Elektronická pečeť nebo podpis vydávající certifikační autority nad vydaným certifikátem

7.1.1 Číslo verze

Certifikáty certifikační autority ACAeID a kvalifikované certifikáty vydávané podle této certifikační politiky jsou vydávány jako certifikáty X.509 verze 3.

7.1.2 Rozšiřující položky v certifikátu

7.1.2.1 KeyUsage

Rozšíření `KeyUsage` je v certifikátu uvedeno v souladu s X.509 v3, RFC 5280 a příslušným profilem certifikátu.

Použití	Certifikát certifikační autority ACAeID	Krátkodobý kvalifikovaný certifikát pro elektronický podpis
Kritický	Ano	Ano
digitalSignature	—	Nastaven
nonRepudiation / contentCommitment	—	Nastaven
keyEncipherment	—	Nenastaven
dataEncipherment	—	Nenastaven
keyAgreement	—	Nenastaven
keyCertSign	Nastaven	Nenastaven
cRLSign	Nastaven	Nenastaven
encipherOnly	—	Nenastaven
decipherOnly	—	Nenastaven

Krátkodobý kvalifikovaný certifikát vydaný podle této certifikační politiky je určen pouze pro vytvoření kvalifikovaného elektronického podpisu a nesmí být použit pro šifrování, autentizaci serveru nebo klienta, ani pro jiné účely, které nejsou výslovně povoleny touto certifikační politikou.

7.1.2.2 Certificate Policies

Rozšíření `Certificate Policies` obsahuje identifikátor certifikační politiky, podle které byl certifikát vydán.

Položka	Hodnota
Policy Identifier	`1.2.203.27112489.1.10.8.1.0`
CPS / CP URI	`http://www.acaeid.cz/aca3.3/cp-qc-bi.pdf`
User Notice	Tento kvalifikovaný certifikát pro elektronický podpis byl vydán v souladu s nařízením Evropského parlamentu a Rady (EU) č. 910/2014. / This is a qualified certificate for electronic signature according to Regulation (EU) No 910/2014.

Certifikáty vydávané podle této certifikační politiky jsou v produkčním prostředí vydávány v rámci větve `aca3.3`. Historické větve mohou být nadále uvedeny v revokačních nebo publikačních informacích, pokud je to nezbytné pro ověřování dříve vydaných certifikátů.

7.1.2.3 qcStatements

Rozšíření `qcStatements` obsahuje položky odpovídající kvalifikovanému certifikátu pro elektronický podpis podle eIDAS a příslušných ETSI profilů.

Rozšíření obsahuje zejména:

- `id-etsi-qcs-QcCompliance` – indikace, že certifikát je kvalifikovaným certifikátem;
- `id-etsi-qcs-QcType` s hodnotou `id-etsi-qct-esign` – indikace, že se jedná o kvalifikovaný certifikát pro elektronický podpis;
- `id-etsi-qcs-QcPDS` – odkaz na PKI Disclosure Statement / D35 – Zprávu pro uživatele nebo jiný odpovídající veřejný dokument poskytovatele;
- `id-etsi-qcs-QcSSCD` nebo odpovídající indikace podle aktuálního ETSI profilu – indikace, že data pro vytváření elektronického podpisu jsou uložena a používána v QSCD.

Certifikát vydaný podle této certifikační politiky indikuje použití QSCD v rozsahu odpovídajícím skutečnému technickému profilu certifikátu a použitému prostředku pro vytváření elektronického podpisu.

Odkaz uvedený v `QcPDS` směřuje na veřejný dokument poskytovatele obsahující základní informace pro uživatele a spoléhající se strany. Tímto dokumentem je zejména D35 – Zpráva pro uživatele / PKI Disclosure Statement, případně jeho aktuální zveřejněná verze.

7.1.2.4 Authority Information Access

Rozšíření `Authority Information Access` obsahuje adresu OCSP služby pro ověření statutu certifikátu, případně další informace stanovené profilem certifikátu.

Rozšíření není kritické, pokud příslušný profil certifikátu nestanoví jinak.

7.1.2.5 Subject Alternative Name

Rozšíření `Subject Alternative Name` je nekritické, pokud je v certifikátu použito.

Může obsahovat zejména e-mailovou adresu podepisující osoby, pokud je tento údaj získán prostřednictvím Bank iD, je povolen profilem certifikátu a je relevantní pro účel certifikátu.

7.1.2.6 BasicConstraints

Certifikát certifikační autority ACAeID má v rozšíření `BasicConstraints` nastaven atribut `CA = TRUE`.

Kvalifikované certifikáty vydávané podepisujícím osobám podle této certifikační politiky mají `CA = FALSE`, případně toto rozšíření odpovídá profilu koncového certifikátu podle příslušných norem.

7.1.2.7 ExtendedKeyUsage

Rozšíření `ExtendedKeyUsage` se u kvalifikovaných certifikátů vydávaných podle této certifikační politiky standardně nepoužívá, pokud to nevyžaduje nebo nepřipouští příslušný profil certifikátu.

Certifikát vydaný podle této certifikační politiky není určen pro autentizaci serveru, autentizaci klienta, šifrování e-mailu, podepisování kódu, časová razítka ani OCSP signing.

Použití	**Certifikát certifikační autority ACAeID**	**Krátkodobý kvalifikovaný certifikát pro elektronický podpis**
Kritický	Ne	Ne, pokud je rozšíření použito

serverAuth	—	Nenastaven
clientAuth	—	Nenastaven
codeSigning	—	Nenastaven
emailProtection	—	Nenastaven
timeStamping	—	Nenastaven
OCSPSigning	—	Nenastaven

Technické ověření potvrdilo, že rozšíření `ExtendedKeyUsage` není v krátkodobém kvalifikovaném certifikátu pro Bank iD / QSIGN přítomno.

7.1.2.8 CRLDistributionPoints

Rozšíření `CRLDistributionPoints` obsahuje URL místa, kde spoléhající se strany naleznou seznam zneplatněných certifikátů.

Rozšíření není kritické.

7.1.2.9 Authority Key Identifier

Rozšíření `Authority Key Identifier` obsahuje identifikátor veřejného klíče certifikační autority ACAeID, která certifikát vydala.

Rozšíření není kritické.

7.1.2.10 Subject Key Identifier

Rozšíření `Subject Key Identifier` obsahuje identifikátor veřejného klíče držitele certifikátu.

Rozšíření není kritické.

7.1.2.11 Bank iD rozšíření

Certifikát může obsahovat technická rozšíření a specifické atributy používané v prostředí Bank iD / QSIGN, zejména údaje označované jako `envelope hash`, `envelope name` a Bank iD pseudonym.

Tato rozšíření nebo specifické atributy mohou být uvedeny zejména s následujícími OID:

- `1.3.6.1.4.1.58356.1` – `envelopeHash`;
- `1.3.6.1.4.1.58356.2` – `envelopeName`;
- `1.3.6.1.4.1.58356.3` – Bank iD pseudonym / specifický atribut používaný v `Subject`.

Význam, obsah a zpracování těchto rozšíření a specifických atributů jsou stanoveny technickým profilem služby, smluvní dokumentací a provozní dokumentací mezi eIdentity a.s. a Bankovní identitou a.s.

Tyto údaje slouží k technické vazbě certifikátu na identifikační, certifikační nebo podpisovou transakci v prostředí Bank iD / QSIGN a nejsou určeny k samostatnému použití mimo tento proces.

7.1.3 Objektové identifikátory algoritmů

Pro účely vydávání kvalifikovaných certifikátů podle této certifikační politiky se používají podpisová schémata a kryptografické algoritmy odpovídající platným právním požadavkům, příslušným technickým standardům a interním kryptografickým pravidlům eIdentity.

Použité algoritmy a jejich OID jsou stanoveny technickým profilem certifikátu, certifikační prováděcí směrnicí a konfigurací vydávající certifikační autority.

7.1.4 Způsoby zápisu jmen a názvů

Způsoby zápisu jmen a názvů jsou uvedeny v kapitole 3.1 této certifikační politiky.

7.1.5 Omezení jmen a názvů

Je zakázáno použití jmen, názvů nebo údajů v rozporu s právními předpisy, touto certifikační politikou nebo technickým profilem certifikátu.

Žadatel odpovídá za pravdivost, úplnost a správnost údajů použitých v procesu vydání certifikátu v rozsahu stanoveném touto certifikační politikou a smluvními podmínkami.

7.1.6 OID certifikační politiky

OID této certifikační politiky je uvedeno v kapitole 1.2.

7.1.7 Rozšiřující položka Policy Constraints

Rozšíření `Policy Constraints` se u certifikátů vydávaných podle této certifikační politiky použije pouze v případě, že to vyžaduje příslušný profil certifikátu nebo politika certifikační autority.

7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky Policy Qualifiers

Syntaxe a sémantika kvalifikátorů politiky je uvedena v kapitole 7.1.2.2 této certifikační politiky.

7.1.9 Způsob zápisu kritické rozšiřující položky Certificate Policies

Rozšíření `Certificate Policies` se zapisuje v souladu s profilem certifikátu, touto certifikační politikou a příslušnými technickými normami.

Kritičnost rozšíření je stanovena technickým profilem certifikátu.

7.2 Profil seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je vydáván jako CRL v souladu s X.509, RFC 5280 a příslušnými profily používanými eIdentity.

Základní položky CRL jsou uvedeny v následující tabulce.

OID / položka	Kritický	Název	Hodnota
signatureAlgorithmIdentifier	Ne	Identifikátor podpisového algoritmu	Identifikátor a parametry algoritmu použitého pro elektronickou pečeť nebo podpis vydávaného CRL
issuer	Ne	Vydavatel CRL	DN vydavatele CRL
thisUpdate	Ne	Čas vydání CRL	Okamžik vydání CRL
		Další	

nextUpdate	Ne	plánované vydání CRL	Předpokládaný okamžik vydání dalšího CRL
revokedCertificates	Ne	Seznam zneplatněných certifikátů	Seznam zneplatněných kvalifikovaných certifikátů
userCertificate	Ne	Číslo certifikátu	Sériové číslo zneplatněného certifikátu
`2.5.29.21`	Ne	ReasonCode	Důvod zneplatnění certifikátu, pokud je uváděn
`2.5.29.20`	Ne	CRLNumber	Pořadové číslo CRL
`2.5.29.28`	Ano, pokud je použito jako kritické podle profilu	IssuingDistributionPoint	URL adresa nebo identifikace distribučního místa CRL
`2.5.29.35`	Ne	AuthorityKeyIdentifier	Identifikátor veřejného klíče vydavatele CRL

7.2.1 Číslo verze

CRL je vydáváno ve verzi odpovídající X.509 v2 CRL podle RFC 5280.

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

Rozšiřující položky CRL a položek v CRL jsou uvedeny v kapitole 7.2 této certifikační politiky a v příslušné certifikační prováděcí směrnici.

7.3 Profil OCSP

7.3.1 Číslo verze

Služba OCSP je poskytována podle RFC 6960 – *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* ve verzi 1.

OCSP odpovědi pro koncové krátkodobé kvalifikované certifikáty vydané podle této certifikační politiky jsou podepisovány vydávající certifikační autoritou, pokud technický profil služby nebo interní provozní dokumentace nestanoví jiný způsob odpovídající požadavkům RFC 6960 a příslušným technickým normám.

Pro jiné části hierarchie ACAeID může být použit odlišný OCSP profil, například delegovaný OCSP responder, pokud je to stanoveno příslušnou certifikační politikou, certifikační prováděcí směrnicí nebo technickým profilem služby.

Algoritmus použitý pro podpis nebo pečeť OCSP odpovědí odpovídá aktuálním kryptografickým požadavkům a konfiguraci služby.

7.3.2 Rozšiřující položky OCSP

Služba OCSP podporuje rozšíření `Nonce`, pokud je to v souladu s aktuální konfigurací služby a profilem OCSP.

Další rozšíření OCSP se používají podle technického profilu služby a provozní dokumentace.

---

8 Hodnocení shody a jiná hodnocení

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Soulad systému ACAeID, postupů vydávání krátkodobých kvalifikovaných certifikátů podle této certifikační politiky, certifikační prováděcí směrnice, interní bezpečnostní dokumentace a použitelných právních, regulatorních a normativních požadavků je pravidelně ověřován.

Hodnocení se provádí zejména:

- nejméně jednou ročně v rámci interního přezkumu nebo interního auditu;
- v rámci pravidelného posouzení shody kvalifikované služby prováděného subjektem posuzování shody;
- při významné změně architektury, konfigurace, technického profilu certifikátu, provozního modelu nebo bezpečnostních opatření;

- po významném bezpečnostním incidentu nebo události, která může mít dopad na důvěryhodnost služby, vydaných certifikátů nebo podpisové transakce;
- při změně právních, regulatorních nebo normativních požadavků, pokud taková změna může mít dopad na vydávání certifikátů podle této certifikační politiky;
- v dalších případech stanovených interní dokumentací eIdentity, rozhodnutím Výboru pro politiky nebo požadavkem příslušného orgánu.

Běžné provozní a konfigurační změny jsou posuzovány v rámci změnového řízení. Změny, které mohou mít dopad na bezpečnost, důvěryhodnost, soulad nebo dostupnost služby, podléhají přiměřenému bezpečnostnímu posouzení a podle povahy změny také mimořádnému hodnocení.

8.2 Identita a kvalifikace hodnotitele

Hodnocení shody kvalifikované služby provádí způsobilý subjekt posuzování shody, který splňuje požadavky právních předpisů a příslušných akreditačních pravidel pro posuzování služeb vytvářejících důvěru.

Interní audity a interní bezpečnostní hodnocení provádějí osoby s odpovídající kvalifikací, znalostí systému řízení bezpečnosti informací, požadavků eIDAS, příslušných ETSI norem, této certifikační politiky, certifikační prováděcí směrnice a interní bezpečnostní dokumentace eIdentity.

Hodnotitel musí mít odpovídající odbornou způsobilost, znalost použitelných požadavků a oprávnění k provedení hodnocení v rozsahu daného typu hodnocení.

8.3 Vztah hodnotitele k hodnocenému subjektu

Hodnotitel musí být nezávislý na činnostech, které jsou předmětem hodnocení, a nesmí být v postavení, které by mohlo ohrozit objektivitu nebo nestrannost hodnocení.

Osoba provádějící interní audit nebo interní bezpečnostní hodnocení nesmí hodnotit činnost, za jejíž návrh, implementaci nebo provoz je přímo odpovědná.

V případě externího posouzení shody musí být zachována nezávislost a nestrannost subjektu posuzování shody podle příslušných akreditačních pravidel.

8.4 Hodnocené oblasti

Rozsah hodnocení je určen povahou služby, použitou metodikou hodnocení, požadavky právních předpisů, ETSI norem, certifikačních politik, certifikační prováděcí směrnice a interní dokumentace eIdentity.

Hodnocení se zaměřuje zejména na:

- soulad vydávání krátkodobých kvalifikovaných certifikátů s touto certifikační politikou;
- soulad s certifikační prováděcí směrnicí a související provozní dokumentací;
- ověření identity a autentizaci žadatele prostřednictvím Bank iD;
- předání a zpracování údajů potřebných pro vydání certifikátu;
- proces vydání krátkodobého kvalifikovaného certifikátu;
- profil certifikátu a jeho soulad s příslušnými technickými normami;
- řízení dat pro vytváření a ověřování elektronických podpisů;
- použití QSCD / HSM a souvisejících kryptografických modulů;
- proces zneplatnění certifikátu a dostupnost revokačních informací;
- služby ověřování statutu certifikátu, zejména CRL a OCSP;
- auditní záznamy, logování, archivaci a uchovávání dokumentace;
- řízení přístupů, důvěryhodné role a oddělení povinností;
- řízení změn, zranitelností a bezpečnostních incidentů;
- fyzickou, provozní, síťovou a počítačovou bezpečnost;
- ochranu osobních údajů a důvěrných informací;
- plnění relevantních požadavků eIDAS, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412 a dalších použitelných norem.

8.5 Postup v případě zjištění nedostatků

Zjištěné nedostatky, neshody nebo doporučení jsou evidovány, klasifikovány podle závažnosti a předány odpovědným osobám k řešení.

Pro každý relevantní nedostatek se stanoví nápravné opatření, odpovědná osoba a termín splnění.

Nápravná opatření mohou zahrnovat zejména:

- úpravu certifikační politiky, certifikační prováděcí směrnice nebo jiné řízené dokumentace;
- změnu technického, konfiguračního nebo procesního nastavení;

- doplnění nebo úpravu bezpečnostních opatření;
- doplnění auditních, provozních nebo technických důkazů;
- proškolení odpovědných osob;
- zneplatnění dotčených certifikátů, pokud je to nezbytné;
- opakované ověření účinnosti přijatého opatření.

Realizace nápravných opatření je sledována do jejich vypořádání. Účinnost přijatých opatření je ověřována přiměřeně povaze a závažnosti zjištění.

8.6 Sdělování výsledků hodnocení

Výsledky hodnocení jsou zpřístupněny osobám odpovědným za řízení a bezpečnost služby, zejména statutárnímu zástupci, bezpečnostnímu řediteli, provoznímu řediteli, Výboru pro politiky a dalším určeným osobám podle povahy zjištění.

Výsledky posouzení shody jsou uchovávány jako součást řízené dokumentace eIdentity a jsou poskytovány příslušným orgánům, auditorům nebo subjektu posuzování shody v rozsahu stanoveném právními předpisy, smluvními závazky nebo pravidly posuzování shody.

Informace o zjištěních, která mohou mít dopad na důvěryhodnost, bezpečnost, dostupnost nebo soulad služby, jsou eskalovány odpovědným osobám bez zbytečného odkladu.

---

9 Ostatní obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Poplatky za vydání krátkodobého kvalifikovaného certifikátu podle této certifikační politiky jsou řešeny smluvním vztahem mezi eIdentity a.s. a Bankovní identitou a.s., případně jiným smluvním partnerem podle obchodního modelu služby.

Služba obnovení certifikátu se podle této certifikační politiky neposkytuje.

9.1.2 Poplatky za přístup k certifikátu

Přístup k informacím nezbytným pro ověření certifikátu je poskytován bezplatně, není-li ve smluvních podmínkách stanoveno jinak.

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Přístup k CRL je poskytován bezplatně.

Ověření statutu certifikátu prostřednictvím OCSP je poskytováno v souladu s touto certifikační politikou, provozní dokumentací a případnými smluvními podmínkami.

9.1.4 Poplatky za další služby

Poplatky za další služby, pokud jsou poskytovány, jsou stanoveny příslušnou smlouvou, ceníkem služeb nebo jinými smluvními podmínkami.

9.1.5 Jiná ustanovení týkající se poplatků včetně refundací

Refundace, storna nebo jiné úpravy plateb se řídí příslušnými smluvními podmínkami mezi eIdentity a.s., Bankovní identitou a.s., spoléhající se stranou nebo jiným smluvním partnerem.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

Společnost eIdentity a.s. má sjednáno pojištění podnikatelských rizik v rozsahu přiměřeném povaze poskytovaných kvalifikovaných služeb vytvářejících důvěru.

9.2.2 Další aktiva a záruky

Společnost eIdentity a.s. zajišťuje zdroje potřebné pro poskytování kvalifikovaných služeb vytvářejících důvěru na požadované úrovni kvality, bezpečnosti a dostupnosti.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Samostatné pojištění nebo krytí zárukou pro koncové uživatele se podle této certifikační politiky neposkytuje, pokud není ve smluvních podmínkách stanoveno jinak.

9.3 Důvěrnost obchodních informací

9.3.1 Výčet důvěrných informací

Za neveřejné obchodní informace se považují zejména:

- informace o odebíraných službách;
- ceny služeb a obchodní podmínky;
- obchodní smlouvy a smluvní dokumentace;
- smlouvy s třetími stranami, které se podílejí na provozu nebo zajištění ACAeID;
- žádosti o poskytnutí služby;
- auditní, provozní a transakční záznamy;
- havarijní plány, plány obnovy a dokumentace kontinuity činností;
- certifikační prováděcí směrnice;
- interní bezpečnostní a provozní dokumentace;
- způsoby ochrany osobních údajů;
- informace o zabezpečení obsluhy systému ACAeID;
- bezpečnostní opatření a podrobnosti jejich realizace;
- další informace označené jako neveřejné, důvěrné nebo interní.

9.3.2 Informace mimo rámec důvěrných informací

Za informace mimo rámec důvěrných informací se považují informace, které byly eIdentity a.s. zveřejněny prostřednictvím webových stránek, veřejných dokumentů nebo jiným určeným způsobem.

9.3.3 Odpovědnost za ochranu důvěrných informací

Každá osoba, která přijde do styku s důvěrnými informacemi, je povinna chránit je před neoprávněným zpřístupněním, změnou, ztrátou, zničením nebo zneužitím.

Poskytnutí důvěrných informací třetí straně je možné pouze na základě právního požadavku, smluvního ujednání, oprávnění nebo souhlasu odpovědné osoby eIdentity a.s.

9.4 Ochrana osobních údajů

Ochrana osobních údajů a jiných neveřejných informací je zajišťována v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679, obecným nařízením o ochraně osobních údajů, zákonem č. 110/2019 Sb., o zpracování osobních údajů, a dalšími použitelnými právními předpisy.

9.4.1 Politika ochrany osobních údajů

eIdentity a.s. zpracovává osobní údaje v rozsahu nezbytném pro poskytování kvalifikovaných služeb vytvářejících důvěru, zejména pro ověření identity žadatele, vydání kvalifikovaného certifikátu, vytvoření a ověření kvalifikovaného elektronického podpisu, vedení auditních záznamů, řešení reklamací, sporů, incidentů a plnění právních a regulatorních povinností.

Za oblast ochrany osobních údajů odpovídá určená odpovědná osoba nebo pověřenec pro ochranu osobních údajů, pokud je jmenován.

9.4.2 Osobní údaje

Za osobní údaje se považují veškeré informace o identifikované nebo identifikovatelné fyzické osobě.

V rámci poskytování služby podle této certifikační politiky se mohou zpracovávat zejména:

- identifikační údaje žadatele nebo podepisující osoby;
- kontaktní údaje;
- údaje získané prostřednictvím Bank iD;
- údaje potřebné pro vydání kvalifikovaného certifikátu;
- údaje uvedené v certifikátu;
- údaje o podpisové transakci;
- auditní a provozní záznamy;
- údaje potřebné pro řešení reklamací, sporů, incidentů a posuzování shody.

9.4.3 Údaje, které nejsou považovány za osobní údaje

Za osobní údaje se nepovažují údaje, které se nevztahují k identifikované nebo identifikovatelné fyzické osobě, nebo údaje, které byly anonymizovány tak, že již nelze identifikovat konkrétní fyzickou osobu.

9.4.4 Odpovědnost za ochranu osobních údajů

eIdentity a.s. zajišťuje ochranu osobních údajů prostřednictvím technických a organizačních opatření odpovídajících povaze, rozsahu, kontextu a účelům zpracování a rizikům pro práva a svobody fyzických osob.

Přístup k osobním údajům je omezen pouze na oprávněné osoby a systémy v rozsahu nezbytném pro plnění jejich úkolů.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Podepisující osoba je informována o zpracování osobních údajů v rozsahu stanoveném právními předpisy a příslušnými informačními dokumenty eIdentity a.s.

Pokud je pro konkrétní zpracování vyžadován souhlas, je získáván před zahájením takového zpracování. V ostatních případech je zpracování založeno na jiném odpovídajícím právním titulu, zejména na plnění smlouvy, plnění právní povinnosti nebo oprávněném zájmu, pokud je použitelný.

9.4.6 Poskytnutí osobních údajů pro soudní či správní účely

Osobní údaje mohou být zpřístupněny orgánům veřejné moci, soudům, správním orgánům, orgánům činným v trestním řízení nebo jiným oprávněným subjektům pouze v rozsahu a za podmínek stanovených právními předpisy.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

Osobní údaje mohou být zpřístupněny také dalším subjektům, pokud je to nezbytné pro poskytování služby, splnění právní nebo smluvní povinnosti, řešení incidentů, reklamací nebo sporů, ochranu práv eIdentity a.s., nebo pokud s tím subjekt údajů souhlasil.

9.5 Práva duševního vlastnictví

Společnost eIdentity a.s. zachovává veškerá práva duševního vlastnictví týkající se obsahu certifikátů, revokačních dat, certifikačních politik, certifikační prováděcí směrnice, interní dokumentace, provozních postupů, technických řešení a dalších chráněných prvků souvisejících s poskytováním služeb vytvářejících důvěru.

Práva třetích stran, včetně ochranných známek, obchodních názvů a jiných chráněných označení, nejsou touto certifikační politikou dotčena.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

Společnost eIdentity a.s. zaručuje, že:

- certifikáty vydané podle této certifikační politiky jsou vydány v souladu s touto certifikační politikou, certifikační prováděcí směrnicí a použitelnými právními a normativními požadavky;
- údaje uvedené v certifikátu jsou uvedeny na základě údajů získaných a ověřených postupem podle této certifikační politiky;
- certifikát je vydán jako kvalifikovaný certifikát pro elektronický podpis;
- služba zneplatnění certifikátu a služby ověřování statutu certifikátu jsou poskytovány v souladu s touto certifikační politikou;
- revokační informace jsou zveřejňovány v souladu s touto certifikační politikou.

Další záruky mohou být specifikovány ve smlouvě o poskytnutí služby nebo v jiných smluvních podmínkách.

9.6.2 Zastupování a záruky RA

eIdentity a.s. zajišťuje, že online registrační proces pro vydávání certifikátů podle této certifikační politiky je prováděn v souladu s touto certifikační politikou, certifikační prováděcí směrnicí, smluvním rámcem s Bankovní identitou a.s. a související provozní dokumentací.

9.6.3 Zastupování a záruky držitele certifikátu a podepisující osoby

Držitel certifikátu a podepisující osoba odpovídají za plnění povinností stanovených touto certifikační politikou, smlouvou o poskytnutí služby a příslušnými podmínkami služby.

Podepisující osoba odpovídá zejména za to, že:

- poskytuje pravdivé, úplné a aktuální údaje;
- používá Bank iD a související autentizační prostředky v souladu s jejich podmínkami;
- chrání své autentizační prostředky před zneužitím;
- používá službu pouze k účelu, pro který je určena;
- bez zbytečného odkladu oznámí podezření na zneužití Bank iD, podpisové transakce nebo vydaného certifikátu.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strany jsou povinny postupovat v souladu s nařízením eIDAS, touto certifikační politikou, příslušnými technickými normami a dalšími relevantními právními nebo smluvními požadavky.

Spoléhající se strany odpovídají zejména za ověření platnosti certifikátu, ověření statutu certifikátu, ověření certifikačního řetězce a posouzení, zda byl certifikát a elektronický podpis použit v souladu s účelem certifikátu.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Záruky ostatních zúčastněných subjektů se řídí příslušnými právními předpisy, smluvní dokumentací, provozní dokumentací a pravidly integračního prostředí Bank iD / QSIGN.

9.7 Zřeknutí se záruk

Poskytování služeb podle této certifikační politiky se řídí zejména nařízením eIDAS, touto certifikační politikou, certifikační prováděcí směrnicí, politikou služby vzdáleného podpisu a příslušnými smluvními podmínkami.

eIdentity a.s. neposkytuje jiné záruky nad rámec stanovený právními předpisy, touto certifikační politikou nebo smluvními ujednáními.

9.8 Omezení odpovědnosti

Odpovědnost eIdentity a.s. je stanovena právními předpisy, zejména nařízením eIDAS, a příslušnými smluvními podmínkami.

Omezení odpovědnosti nesmí být v rozporu s kogentními ustanoveními právních předpisů.

9.9 Odpovědnost za škodu a náhrada škody

Náhrada škody a případné odškodnění se řídí příslušnými právními předpisy a smluvními podmínkami.

O výši náhrady škody může rozhodnout příslušný soud, pokud není věc vyřešena jiným právně přípustným způsobem.

9.10 Doba platnosti a ukončení platnosti

9.10.1 Doba platnosti

Tato certifikační politika zůstává v platnosti do jejího nahrazení novější verzí, zrušení nebo ukončení poskytování služby, nejméně však po dobu platnosti posledního kvalifikovaného certifikátu vydaného podle této certifikační politiky, pokud právní nebo regulatorní požadavky nestanoví delší dobu.

Novou verzi certifikační politiky schvaluje a vyhlašuje Výbor pro politiky v souladu se svým jednacím řádem.

9.10.2 Ukončení platnosti

Ukončení platnosti této certifikační politiky nebo její nahrazení novou verzí se provádí řízeným procesem.

Úpravy certifikační politiky, včetně zajištění souladu s certifikační prováděcí směrnicí a navazující dokumentací, schvaluje Výbor pro politiky.

9.10.3 Důsledky ukončení a přetrvání závazků

Ukončením platnosti této certifikační politiky nejsou dotčeny povinnosti uchovávat záznamy, chránit důvěrné informace, chránit osobní údaje, poskytovat informace nezbytné pro ověření certifikátů a plnit povinnosti vyplývající z právních předpisů, smluvních podmínek a auditních požadavků.

9.11 Komunikace mezi zúčastněnými subjekty

Pro účely individuální komunikace se zúčastněnými subjekty může eIdentity a.s. využít zejména:

- e-mailové adresy;
- telefonické spojení;
- prostředí podporované služby nebo uživatelského rozhraní;
- datovou schránku;
- písemnou komunikaci;
- osobní jednání;
- jiné komunikační prostředky stanovené smluvními nebo provozními podmínkami.

9.12 Změny

9.12.1 Postup při změnách

Změny této certifikační politiky probíhají řízeným procesem.

Návrh změny je posuzován z hlediska dopadu na poskytovanou službu, vydané certifikáty, spoléhající se strany, certifikační prováděcí směrnici, související dokumentaci, právní a regulatorní požadavky a technický profil certifikátu.

9.12.2 Postup při oznamování změn

Změny certifikační politiky jsou po schválení zveřejněny způsobem stanoveným touto certifikační politikou.

Změny, které mají významný dopad na žadatele, podepisující osoby, spoléhající se strany nebo způsob poskytování služby, jsou komunikovány přiměřeným způsobem bez zbytečného odkladu po jejich schválení.

9.12.3 Okolnosti, při kterých musí být změněn OID

OID certifikační politiky se mění v případě takové změny politiky, která má zásadní dopad na její účel, rozsah, pravidla vydávání certifikátů, použití certifikátů, profil certifikátu nebo posuzování souladu.

O změně OID rozhoduje Výbor pro politiky.

9.13 Řešení sporů

V případě nesouhlasu s postupem pracovníků eIdentity a.s., s vydáním certifikátu, zneplatněním certifikátu nebo poskytováním služby podle této certifikační politiky se dotčená osoba může obrátit na eIdentity a.s. prostřednictvím určených kontaktních údajů.

Není-li spor vyřešen smírně, může být předložen příslušnému soudu podle právních předpisů České republiky.

9.14 Rozhodné právo

Činnost eIdentity a.s. a poskytování služeb podle této certifikační politiky se řídí právním řádem České republiky a přímo použitelnými právními předpisy Evropské unie.

9.15 Shoda s právními předpisy

Systém ACAeID a vydávání certifikátů podle této certifikační politiky jsou provozovány ve shodě s použitelnými právními a regulatorními požadavky vztahujícími se ke kvalifikovaným službám vytvářejícím důvěru, zejména s nařízením eIDAS a navazujícími předpisy.

Služba je předmětem posuzování shody v rozsahu stanoveném právními předpisy a pravidly pro kvalifikované služby vytvářející důvěru.

9.16 Další ustanovení

Další ustanovení mohou být stanovena ve smluvních podmínkách, certifikační prováděcí směrnici, provozní dokumentaci nebo jiné řízené dokumentaci eIdentity.

9.16.1 Rámcová dohoda

Rámcová dohoda nebo rámcová smlouva může být použita v rozsahu stanoveném smluvními podmínkami služby.

9.16.2 Postoupení práv

Postoupení práv a povinností se řídí příslušnými právními předpisy a smluvními podmínkami.

9.16.3 Oddělitelnost ustanovení

Pokud se některé ustanovení této certifikační politiky nebo smluvních podmínek stane neplatným nebo neúčinným, nemá tato skutečnost vliv na platnost a účinnost ostatních ustanovení, pokud z povahy věci nevyplývá jinak.

9.16.4 Zřeknutí se práv

Neuplatnění určitého práva nebo nároku ze strany eIdentity a.s. nelze bez dalšího považovat za vzdání se tohoto práva nebo nároku do budoucna.

9.16.5 Vyšší moc

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

Události vyšší moci nemají vliv na povinnosti eIdentity a.s. přijmout přiměřená opatření k ochraně záznamů, bezpečnosti, důvěryhodnosti a kontinuity služby v rozsahu, ve kterém je to možné.

9.17 Další opatření

Další opatření mohou být stanovena v certifikační prováděcí směrnici, politice služby vzdáleného podpisu, interní bezpečnostní dokumentaci, smluvních podmínkách, provozní dokumentaci nebo auditní dokumentaci.

---

10 Závěrečná ustanovení

Tato certifikační politika byla projednána Výborem pro politiky eIdentity a.s. a podle zápisu z jednání byla přijata a vyhlášena.

Tato certifikační politika nabývá účinnosti dnem stanoveným při jejím schválení a zůstává platná do jejího nahrazení novou verzí, zrušení nebo ukončení poskytování služby podle této certifikační politiky.

Změny této certifikační politiky se provádějí řízeným postupem podle kapitoly 9.12.

Historie dokumentu

Verze 1.0

Datum: 24. 1. 2024
Autor: Jan Stelibský

Certifikační politika popisuje aplikaci bankovní identity při vydávání kvalifikovaných certifikátů pro elektronický podpis.

Verze 1.0.1

Datum: 9. 10. 2024
Autor: Jan Stelibský

Zapracování změn vyžádaných DIA.

Verze 1.0.2

Datum: 09. 05. 2026
Autor: Libor Široký

Celková revize dokumentu; aktualizace kontaktních údajů; sladění terminologie a procesů s ACAeID 10.9 – Politikou služby vzdáleného podpisu dle eIDAS – Bank iD; zpřesnění pravidel pro vydávání krátkodobých kvalifikovaných certifikátů, ověření identity prostřednictvím Bank iD, použití QSCD/HSM, zneplatnění certifikátů, technickou bezpečnost, profily certifikátu, CRL a OCSP.

Verze 1.0.3

Datum: 12. 05. 2026
Autor: Libor Široký

Zapracování výsledků technického ověření auditní matice ACA-A-38; aktualizace produkční větve `aca3.3` v Certificate Policies URL; doplnění Bank iD OID `1.3.6.1.4.1.58356.3`; sladění doby platnosti certifikátu na „nejvýše 3 měsíce“; upřesnění QcPDS, OCSP profilu a formulací k prostředí QSCD / HSM. Profil `KeyUsage` a minimální délka RSA klíče zůstávají uvedeny v cílovém auditně správném znění a vyžadují uvedení implementace do souladu změnovým řízením.