Jméno	**Certifikační politika – ČSOB EDSS CA**
Typ	Veřejný dokument
Verze	**1.0**
Datum vydání	**13.6.2022**
ID	**Certifikační politika – ČSOB EDSS CA**
Popis	Tento dokument specifikuje použitelnost certifikátů vydaných ČSOB EDSS CA pro konkrétní použití, definuje podmínky životního cyklu certifikátů a také ukládá požadavky na provoz ČSOB EDSS CA.
Vlastník	IT Bezpečnost
Klasifikační stupeň	Veřejné
Prostředí	Produkční
Společnost	ČSOB, a.s.

Změny:

Datum vydání	Verze	Popis změn	Upravil (jméno)
26.4.2022	0.1	Úvodní verze, interní poznámky	Josef Kučera
9.6.2022	0.2	Úprava 5.1, 5.2, odstranění interních informací	Josef Kučera
13.6.2022	1.0	Finální revize	Jiří Vábek

Obsah

1. ÚVOD

1.1 Přehled

Tento dokument specifikuje procedurální a provozní požadavky, které ČSOB požaduje od účastníků PKI při vydávání a správě certifikátů vydaných ČSOB EDSS CA.

Certifikáty vydané ČSOB EDSS CA podle této politiky jsou vydávány pomocí produktu EDSS vyvinutého dodavatelem.

Tento CP je pouze jedním z dokumentů, kterými se řídí ČSOB EDSS CA. Kromě regulačních dokumentů jsou uplatňovány i vnitřní zásady ČSOB.

Aby se zachoval obrys specifikovaný v RFC 3647, mají nadpisy oddílů, které nejsou relevantní, prohlášení „Nepoužije se“ nebo „Žádné ustanovení“.

1.2 Název a identifikace dokumentu

Název a identifikace dokumentu: Certifikační politika – ČSOB EDSS CA, verze 1.0.

OID politiky: 1.3.6.1.4.1.27627.100.1

1.3 Participující subjekty

1.3.1 Certifikační autority

Touto politikou se řídí CA s názvem „ČSOB EDSS CA“. Je to podřízená vydávající CA, kterou vydává offline kořenová CA – „ČSOB EDSS Root CA“.

1.3.2 Registrační autority

Roli Registrační autority zastává Sefira aplikace EDSS, která zodpovídá za identifikaci a autentizaci subjektu/klienta certifikátu.

1.3.3 Držitelé certifikátů

Držitelem vydaného certifikátu ČSOB EDSS CA jsou klienti, kteří jsou v nějakém obchodním vztahu s ČSOB a od kterých ČSOB požaduje, aby podepisovali dokumenty poskytnuté ČSOB prostřednictvím certifikátů vydaných ČSOB EDSS CA.

1.3.4 Spoléhající strany

Spoléhající se stranou jsou subjekty spoléhající se při své činnosti na Certifikáty vydávané podle této CP.

1.3.5 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dohledu a další, kterým to podle právní úpravy pro služby vytvářející důvěru přísluší.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Certifikáty vydané ČSOB EDSS CA slouží k podepisování dokumentů držitelů certifikátů.

1.4.2 Zakázané použití certifikátu

Certifikáty vydané podle tohoto CP nesmějí být použity k jinému účelu, než je uvedeno v 1.4.1. Certifikát pouze potvrzuje, že informace v certifikátu byly při vydání certifikátu ověřeny jako přiměřeně správné, a neposkytuje žádnou jinou záruku.

1.5 Správa politiky

1.5.1 Organizace spravující dokument

Tuto CP spravuje společnost ČSOB.

1.5.2 Kontaktní osoba

Kontaktní osoba pro tuto politiku je aplikační manažer aplikace ČSOB EDSS.

1.5.3 Osoba rozhodující o souladu CPS s certifikační politikou

Žádné ustanovení.

1.5.4 Postupy při schvalování CPS

Žádné ustanovení.

1.6 Pojmy a zkratky

CA	Certifikační autorita. Pokud není uvedeno jinak, jedná se konkrétně o ČSOB EDSS CA.
Certifikát	Elektronický dokument, který používá digitální podpis ke spojení veřejného klíče a identity.
CP	Certifikační politika
CRL	Certificate Revocation List, seznam zneplatněných certifikátů obsahující certifikáty, které již nelze pokládat za platné
ČSOB	Československá obchodní banka, a.s.
ČSOB PKI	Interní ČSOB Public Key Infrastructure, infrastruktura veřejných klíčů
HSM	Hardware Security Module
Soukromý klíč	jedinečná data pro vytváření elektronického podpisu/pečetě
Veřejný klíč	jedinečná data pro ověřování elektronického podpisu/pečetě
RA	Registrační autorita

SDLC	Bezpečný vývojový cyklus

2. ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ

2.1 Úložiště

ČSOB uchovává informace jako certifikáty, zásady a podobně podle vnitřních předpisů a pravidel pro nakládání s informacemi a jejich klasifikaci.

2.2 Zveřejňování certifikačních informací

ČSOB EDSS CA zveřejňuje na veřejných webových stránkách ČSOB (https:\\www.csob.cz\software) následující informace: všechny důvěryhodné certifikáty CA, kořenové certifikáty CA a CP.

2.3 Čas nebo četnost zveřejňování

ČSOB EDSS CA zveřejňuje certifikáty CA a CP co nejdříve po jejich vydání nebo změně.

2.4 Řízení přístupů k jednotlivým typům úložišť

Všechny veřejné informace jsou zveřejňovány bez omezení.

S interními a důvěrnými informacemi je nakládáno v souladu s interními pravidly ČSOB pro nakládání a klasifikaci informací, která jsou v souladu s regulatorními požadavky.

3. IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Veškerá jména jsou konstruována v souladu s platnými technickými standardy a normami.

3.1.2 Požadavek na významnost jmen

Jména v některých polích mají specifický význam, který je popsán u profilu certifikátu (kapitola 7.1.4.).

3.1.3 Anonymita nebo používání pseudonymu držitele certifikátu

Žádné ustanovení.

3.1.4 Pravidla pro interpretaci různých forem jmen

Rozlišující názvy v certifikátech jsou interpretovány pomocí standardů X.500 a syntaxe ASN.1

3.1.5 Jedinečnost jmen

Jedinečnost sériového čísla je vyžadována v každém certifikátu vydaném CA.

3.1.6 Uznávání, ověřování a poslání obchodních značek

Předplatitelé nesmí požadovat Certifikáty s jakýmkoli obsahem, který porušuje práva duševního vlastnictví jiného subjektu. Tato CP nevyžaduje, aby CA ověřovala právo Účastníka používat ochrannou známku.

3.2 Počáteční ověření identity

3.2.1 Ověřování vlastnictví soukromého klíče

Nepoužije se

3.2.2 Ověřování identity organizace

Nepoužije se

3.2.3 Ověřování identity fyzické osoby

Každý jednotlivec jednající s ČSOB musí být autentizován v souladu s principy stanovenými českým a evropským právem, mezinárodními smlouvami jako AML a metodikami a směrnicemi skupiny ČSOB a KBC. Ve věci upisování certifikátu musí být veškerá jednání vedena osobně se všemi účastníky prokazujícími svou totožnost příslušným identifikačním dokladem, a to do doby, než budou zřízeny prostředky důvěryhodné komunikace (může se jednat mimo jiné o šifrovanou e-mailovou komunikaci).

Identifikaci identity klienta provádějí systémy ČSOB, které pro daného klienta vyžadují vystavení certifikátu.

3.2.4 Neověřované informace vztahující se k držiteli certifikátu

Nepoužije se.

3.2.5 Ověřování kompetencí

Viz 3.2.3.

3.2.6 Kritéria pro interoperabilitu

Nepoužije se.

3.3 Identifikace a autentizace při požadavku na výměnu klíče

3.3.1 Identifikace a autentizace při běžném požadavku na výměnu klíče

Nepoužije se.

3.3.2 Identifikace a autentizace při požadavku na výměnu klíče po zneplatnění certifikátu

Nepoužije se.

3.4 Identifikace a autentizace při požadavku na zneplatnění certifikátu

Nepoužije se.

4. POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Kdo může požádat o vydání certifikátu

CA lze kontaktovat interní aplikací ČSOB (k tomu určená backendová aplikační komponenta), která má k tomuto požadavku oprávnění.

4.1.2 Registrační proces a odpovědnosti

Všechny klíčové operace v rámci dané relace pro daného uživatele se provádějí na straně CA.

4.2 Zpracování žádosti o certifikát

4.2.1 Provádění identifikace a autentizace

Popsáno v kapitole 3.2.2 a 3.2.3 pro počáteční identifikaci a autentizaci.

4.2.2 Schválení nebo zamítnutí žádosti o certifikát

Žádné ustanovení.

4.2.3 Doba zpracování žádosti o certifikát

Certifikát pro klienta CA okamžitě vygeneruje.

4.3 Vydání certifikátu

4.3.1 Úkony CA v průběhu vydávání certifikátu

Žádné ustanovení.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu certifikační autoritou

Nepoužije se

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Žádné ustanovení

4.4.2 Zveřejňování certifikátů certifikační autoritou

Nepoužije se.

4.4.3 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Nepoužije se.

4.5 Použití párových dat a certifikátu

4.5.1 Použití soukromého klíče a certifikátu držitelem certifikátu

Soukromý klíč je provozován v bezpečném prostředí ČSOB, které se řídí vnitřními předpisy ČSOB. Po dokončení všech operací podepisování dokumentů bude tento klíč trvale odstraněn. Použití certifikátu viz 1.4.

4.5.2 Použití veřejného klíče a certifikátu spoléhající se stranou

Nepoužije se, viz 1.3.4.

4.6 Obnovení certifikátu

CA generuje krátkodobé klíče a certifikáty (maximálně 30 minut) pro podepisování dokumentů, takže není potřeba certifikát obnovovat.

4.6.1 Podmínky pro obnovení certifikátu

Nepoužije se, viz 4.6.

4.6.2 Kdo může žádat o obnovení

Nepoužije se, viz 4.6.

4.6.3 Zpracování požadavku na obnovení certifikátu

Nepoužije se, viz 4.6.

4.6.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Nepoužije se, viz 4.6.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

Nepoužije se, viz 4.6.

4.6.6 Zveřejňování obnovených certifikátů certifikační autoritou

Nepoužije se, viz 4.6.

4.6.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Nepoužije se, viz 4.6.

4.7 Výměna veřejného klíče v certifikátu

CA generuje krátkodobé klíče a certifikáty (maximálně 30 minut) pro podepisování dokumentů, takže není potřeba znovu klíč.

4.7.1 Podmínky pro výměnu veřejného klíče v certifikátu

Nepoužije se, viz 4.7.

4.7.2 Kdo může žádat o výměnu veřejného klíče v certifikátu

Nepoužije se, viz 4.7.

4.7.3 Zpracování požadavku na výměnu veřejného klíče v certifikátu

Nepoužije se, viz 4.7.

4.7.4 Oznámení o vydání nového certifikátu držiteli certifikátu

Nepoužije se, viz 4.7.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněným veřejným klíčem

Nepoužije se, viz 4.7.

4.7.6 Zveřejňování certifikátů s vyměněným veřejným klíčem certifikační autoritou

Nepoužije se, viz 4.7.

4.7.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Nepoužije se, viz 4.7.

4.8 Změna údajů v certifikátu

CA generuje krátkodobé klíče a certifikáty (maximálně 30 minut) pro podepisování dokumentů, takže není potřeba měnit údaje v certifikátu.

4.8.1 Podmínky pro změnu údajů v certifikátu

Nepoužije se, viz 4.8.

4.8.2 Kdo může požádat o změnu údajů v certifikátu

Nepoužije se, viz 4.8.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Nepoužije se, viz 4.8.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji držiteli certifikátu

Nepoužije se, viz 4.8.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Nepoužije se, viz 4.8.

4.8.6 Zveřejňování certifikátů se změněnými údaji certifikační autoritou

Nepoužije se, viz 4.8.

4.8.7 Oznámení o vydání certifikátu certifikační autoritou jiným subjektům

Nepoužije se, viz 4.8.

4.9 Zneplatnění a pozastavení platnosti certifikátu

CA generuje krátkodobé klíče a certifikáty (maximálně 30 minut) pro podepisování dokumentů, takže není potřeba revokace a pozastavení platnosti.

4.9.1 Podmínky pro zneplatnění

Nepoužije se, viz 4.9.

4.9.2 Kdo může požádat o zneplatnění

Nepoužije se, viz 4.9.

4.9.3 Postup při žádosti o zneplatnění

Nepoužije se, viz 4.9.

4.9.4 Prodleva při požadavku na zneplatnění certifikátu

Nepoužije se, viz 4.9..

4.9.5 Doba zpracování žádosti o zneplatnění

Nepoužije se, viz 4.9.

4.9.6 Povinnosti spoléhajících se stran při kontrole zneplatnění

Nepoužije se, viz 4.9.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Nepoužije se, viz 4.9.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Nepoužije se, viz 4.9.

4.9.9 Dostupnost ověřování stavu certifikátu on-line

Nepoužije se, viz 4.9.

4.9.10 Požadavky při ověřování stavu certifikátu on-line

Nepoužije se, viz 4.9.

4.9.11 Jiné možné způsoby oznamování zneplatnění

Nepoužije se, viz 4.9.

4.9.12 Zvláštní postupy při kompromitaci klíče

Nepoužije se, viz 4.9.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

Nepoužije se, viz 4.9.

4.9.14 Kdo může požádat o pozastavení platnosti

Nepoužije se, viz 4.9.

4.9.15 Postup při žádosti o pozastavení platnosti

Nepoužije se, viz 4.9.

4.9.16 Omezení doby pozastavení platnosti

Nepoužije se, viz 4.9.

4.10 Služby ověřování stavu certifikátu

Neexistují žádné služby stavu certifikátu.

4.10.1 Funkční charakteristiky

Nepoužije se, viz 4.10

4.10.2 Dostupnost služeb

Nepoužije se, viz 4.10.

4.10.3 Další charakteristiky služeb stavu certifikátu

Nepoužije se, viz 4.10.

4.11 Konec smlouvy o vydávání certifikátů

CA generuje krátkodobé certifikáty – expirace 30 minut.

4.12 Úschova a obnova klíčů

4.12.1 Politika a postupy při úschově a obnově klíčů

Nepoužije se.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Nepoužije se

4.13 Politika a postupy při úschově a obnově klíčů

Nepoužije se.

4.13.1 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče relace

Nepoužije se.

5. POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

5.1 Fyzická bezpečnost

Komponenty infrastruktury PKI jsou umístěny buď v datacentrech ČSOB, nebo ve zvláště chráněných lokalitách, podle citlivosti komponenty.

Fyzická bezpečnost lokalit a datových center ČSOB je řízena podle vnitřních pravidel a popsána v interních dokumentech, které podléhají příslušným bankovním předpisům a pravidelným interním i externím auditům. Podrobné informace jsou klasifikovány jako interní / důvěrné.

5.1.1 Umístění a konstrukce

Žádné ustanovení, viz 5.1.

5.1.2 Fyzický přístup

Žádné ustanovení, viz 5.1.

5.1.3 Elektřina a klimatizace

Žádné ustanovení, viz 5.1.

5.1.4 Vlivy vody

Žádné ustanovení, viz 5.1.

5.1.5 Protipožární opatření a ochrana

Žádné ustanovení, viz 5.1.

5.1.6 Ukládání médií

Žádné ustanovení, viz 5.1.

5.1.7 Nakládání s odpady

Žádné ustanovení, viz 5.1.

5.1.8 Zálohy mimo budovu

Žádné ustanovení, viz 5.1.

5.2 Procedurální postupy

Pro administraci CA je vytvořeno několik rolí v rámci interních procesů ČSOB. Jedná se o tyto:

- Konfigurátor EDSS – konfigurace CA
- Aplikační správce EDSS – provádí analýzu logů CA
- Administrátor HSM – konfigurace a analýza logů HSM.

Veškeré postupy konfigurace a správy CA jsou popsány interními směrnicemi ČSOB.

5.2.1 Důvěryhodné role

Žádné ustanovení, viz 5.2.

5.2.2 Počet osob požadovaných pro zajištění jednotlivých činností

Žádné ustanovení, viz 5.2.

5.2.3 Identifikace a autentizace pro každou roli

Žádné ustanovení, viz 5.2.

5.2.4 Role vyžadující rozdělení povinností

Žádné ustanovení, viz 5.2.

5.3 Personální postupy

5.3.1 Požadavky na kvalifikaci, praxi a bezúhonnost

Každá role účastnící se provozu CA musí být kvalifikována podle interní kompetenční matice pro dané pozice.

5.3.2 Posouzení spolehlivosti osob

U nově přijatých zaměstnanců se uplatňují standardní prověrky dle interních HR pravidel ČSOB. Na role související s CA se nevztahují žádné další požadavky.

5.3.3 Požadavky na školení

Žádné ustanovení.

5.3.4 Požadavky a periodicita doškolování

Žádné ustanovení.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Nepoužije se.

5.3.6 Postihy za neoprávněné činnosti

Žádné ustanovení.

5.3.7 Požadavky na nezávislé dodavatele

Požadavky na dodavatele jsou uplatňovány v souladu s interními pravidly ČSOB i v souladu s regulatorními požadavky.

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci CA jsou vybaveni vnitřními předpisy ČSOB a také nezbytnou dokumentací pro jejich postavení k provozování PKI.

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

Všechny události související se zabezpečením jsou protokolovány a podléhají bezpečnostnímu monitorování ze strany SIEM, zejména protokoly auditu týkající se událostí:

- Generování privátního klíče a manipulace s ním

- Žádosti o certifikát – vyžádání a vydání

- Změny parametrů auditu

- Pokusy o autentizaci

- Změny rolí a oprávnění

- Správa EDSS

5.4.2 Periodicita zpracování záznamů

Bezpečnostní monitorování specifikovaných událostí provádí SIEM, revidované 24x7.

Pro klíčové komponenty EDSS je definována perioda rotace logů pro kritické logy.

5.4.3 Doba uchování auditních záznamů

Uchovávání auditních protokolů se liší podle jeho typu a zahrnutých údajů a řídí se vnitřními pravidly ČSOB pro protokolování a audit.

5.4.4 Ochrana auditních záznamů

Kritické protokoly auditu jsou odesílány do SIEM, kde jsou chráněny před neoprávněným přístupem a kontrolovány vyhrazenými operátory.

5.4.5 Postupy pro zálohování auditních záznamů

Audit log je zálohován pomocí interní SIEM.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Pro sběr logů se používá interní systém.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt způsobující událost není o záznamu protokolu informován.

5.4.8 Hodnocení zranitelnosti

Infrastruktura EDSS je pravidelně skenována na zranitelnosti společným nástrojem ČSOB pro hodnocení zranitelnosti a zranitelnosti jsou spravovány v souladu s interními pravidly ČSOB.

5.5 Uchovávání záznamů

5.5.1 Typy uchovávaných záznamů

Elektronické záznamy spojené s CA, které jsou archivovány, jsou nejdůležitější:

- Certifikáty CA a související definovaná data

- dokumentace CP / CPS, smluvní dokumentace

Dokumentace komponent CA, provozní dokumentace, procesní dokumentace

5.5.2 Doba uchování záznamů

Doba uchovávání archivovaných informací je individuální podle vnitřních pravidel ČSOB, právních předpisů a obchodních potřeb pro každý typ informací.

5.5.3 Ochrana úložiště záznamů

Archivované informace jsou chráněny standardními fyzickými a logickými bezpečnostními prostředky definovanými interními standardy ČSOB.

5.5.4 Postupy při zálohování záznamů

Nepoužije se.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

Nepoužije se.

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

CA shromažďuje archivní informace interně.

5.5.7 Postupy pro získání a ověření uchovávaných informací

Informace jsou uchovávány buď v online archivu, jinak se postupuje podle interních postupů ČSOB.

5.6 Výměna klíče

CA pravidelně a včas mění své soukromé klíče, aby se předešlo prostojům operace. Po výměně klíče CA podepíše certifikáty pouze pomocí nového klíče. CA stále chrání své staré soukromé klíče a starý certifikát je k dispozici pro ověřování podpisů, dokud nevyprší platnost všech certifikátů podepsaných starým soukromým klíčem.

5.7 Obnova po havárii nebo kompromitaci

5.7.1 Postup ošetření incidentu nebo kompromitace

Pro případ incidentu jsou ustanoveny interní pravidla a procesy, kterými je průběh incidentu řízen. Tato pravidla jsou dodržována všemi zúčastněnými rolemi včetně CA administrátora.

Specifické procesy a postupy pro obnovu nebo řešení incidentu jsou popsány v provozní dokumentaci CA, která je k dispozici administrátorovi CA.

5.7.2 Poškození výpočetních prostředků, programového vybavení nebo dat

Žádné ustanovení, viz 5.7.1

5.7.3 Postup při kompromitaci soukromého klíče

V případě, že existuje oprávněné podezření, že soukromý klíč CA je kompromitován, měli by správci CA podniknout následující kroky:

- Posoudit riziko kompromitace a určit míru a rozsah potenciálního dopadu narušení bezpečnosti privátního klíče

- Vzhledem k tomu, že spoléhající stranou pro tento CA je samotná ČSOB, je třeba před odvoláním soukromého klíče CA zvážit potenciální interní mitigace.

Pokud je určeno, že soukromý klíč má být odvolán, musí být vydán nový soukromý klíč a operace obnovena v co nejkratším čase a nové certifikáty vydány s možným minimálním dopadem, podle analýzy mitigačních postupů.

5.7.4 Schopnost obnovit činnost po havárii

Hlavní součásti CA jsou provozovány na dvou různých místech, což omezuje pravděpodobnost katastrofy. Také klíčová role Administrátora CA je dostatečně personálně zajištěna, aby byla zajištěna kontinuita provozu CA.

5.8 Ukončení činnosti CA nebo RA

V případě, že CA ukončí své služby, musí být účastníci předem upozorněni, aby byl zajištěn hladký provoz a přechod na jinou službu.

Vzhledem k tomu, že spoléhající stranou pro tuto CA je samotná ČSOB, musí být zajištěna důvěra v Certifikáty CA do doby, než budou poskytnuty související služby nebo bude na místě jiné řešení pro zajištění hladkého fungování.

6. ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Všechny klíče CA, které je třeba bezpečně chránit, jsou generovány pomocí FIPS ověřených HSM. Proces generování klíčů je popsán v interní provozní dokumentaci, kterou má k dispozici role Správce PKI. Provozní procesy musí dodržovat správce PKI a tam, kde je to potřeba, se uplatňuje princip čtyř očí a oddělení rolí

6.1.2 Předávání soukromého klíče jeho držiteli

Nepoužije se.

6.1.3 Předávání veřejného klíče vydavateli certifikátu

Veřejný klíč je předán na CA přes šifrovaný kanál, v podepsaném PKCS#10 formátu.

6.1.4 Poskytování veřejného klíče CA spoléhajícím se stranám

Nepoužije se.

6.1.5 Délky klíčů

Velikost klíče certifikátu CA, který je vydán pomocí algoritmu RSA, je 4096 bitů.

Velikosti klíčů certifikátů vydaných CA podle této zásady, vydaných pomocí algoritmu RSA, mohou být buď 2048 bitů, nebo 4096 bitů.

Kromě toho všechny algoritmy a délky klíčů podléhají interní regulaci kryptografických algoritmů a velikostí klíčů ČSOB a mohou být odpovídajícím způsobem vylepšeny, aby reagovaly na nová rizika a naplňovaly tento interní předpis.

6.1.6 Parametry veřejného klíče a kontrola jeho kvality

Klíče by měly být generovány podle mezinárodních standardů a norem.

6.1.7 Účely použití klíče (dle rozšíření key usage X.509 v3)

Pro odpovídající certifikát je povoleno následující použití klíče:

Certifikát EDSSCA – digitální podpis, keyCertSign.

Certifikát kořenové CA EDSS - keyCertSign.

Pro certifikáty vydané předplatitelům je použití klíče definováno v profilu a je omezeno na digitální podpis a šifrování klíčů.

6.2 Ochrana soukromého klíče a technologie kryptografických modulů

6.2.1 Řízení a standardy kryptografických modulů

K uložení privátního klíče CA se používá HSM, který splňuje standard FIPS 140-2. HSM jsou provozovány podle interní provozní dokumentace a provozovány pouze Správci PKI.

6.2.2 Soukromý klíč pod kontrolou více osob (n z m)

Je zajištěno, že za účelem přístupu a používání soukromých klíčů CA, včetně jakýchkoli záloh soukromých klíčů, musí jednat pouze důvěryhodný personál a je dodržován princip čtyř očí.

6.2.3 Úschova soukromého klíče

Nepoužije se.

6.2.4 Zálohování soukromého klíče

CA Private key je zálohován v samostatném HSM a uložen na bezpečném místě, odlišném od ostatních HSM používaných v provozu.

Přístup k záložnímu HSM je omezen na správce PKI.

6.2.5 Uchovávání soukromého klíče

Soukromý klíč CA, který byl nahrazen novým, se neukládá ani nearchivuje a je smazán.

6.2.6 Transfer soukromého klíče do nebo z kryptografického modulu

Přenos soukromého klíče provádějí pouze správci PKI. Přenos se provádí pouze mezi HSM prostřednictvím zabezpečeného kanálu a klíče nejsou nikdy uloženy mimo schválený HSM.

6.2.7 Uložení soukromého klíče v kryptografickém modulu

Soukromý klíč CA je uložen v HSM, které splňuje standard FIPS 140-2, ve vyhrazeném oddílu.

6.2.8 Postup aktivace soukromého klíče

Zničení/smazání soukromého klíče provádějí správci PKI podle postupů popsaných v provozní dokumentaci prostřednictvím nativních funkcí HSM.

6.2.9 Postup deaktivace soukromého klíče

Nepoužije se.

6.2.10 Postup ničení soukromého klíče

Zničení/smazání soukromého klíče provádějí správci PKI podle postupů popsaných v provozní dokumentaci prostřednictvím nativních funkcí HSM. Fyzická likvidace HW není nutná.

6.2.11 Hodnocení kryptografických modulů

Viz 6.2.1.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání veřejných klíčů

Veřejný klíč CA je po dobu své platnosti uchováván a dále archivován standardními interními prostředky až do konce interní existence PKI.

6.3.2 Doba funkčnosti certifikátu a doba použitelnosti párových dat

Maximální doba platnosti certifikátů (a příslušných klíčů) je uvedena u každého certifikátu a je definována pro každý typ certifikátu takto:

Certifikát CA – 20 let.

Certifikát kořenové CA – 30 let.

U certifikátů vydávaných Účastníkům je doba provozu definována konfigurací CA a nastavena na maximálně 30 minut..

6.4 Aktivační data

6.4.1 Generování a instalace aktivačních dat

Aktivační data pro soukromé klíče nebo operace HSM se generují buď při inicializaci HSM nebo během vytváření soukromého klíče. Jsou spravovány správci PKI podle interních pravidel pro citlivé informace.

6.4.2 Ochrana aktivačních dat

Aktivační údaje jsou spravovány správci PKI podle interních pravidel pro citlivé informace v kombinaci fyzické a logické ochrany přístupu a šifrování.

6.4.3 Ostatní aspekty aktivačních dat

Nepoužije se.

6.5 Řízení počítačové bezpečnosti

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Požadavky na počítačovou bezpečnost a kontroly jsou definovány interními pravidly a zásadami ČSOB. Pro CA jsou specifické požadavky popsány v technické dokumentaci.

6.5.2 Hodnocení počítačové bezpečnosti

Žádné ustanovení.

6.6 Technické řízení životního cyklu

6.6.1 Řízení vývoje systému

Kontroly vývoje systému jsou definovány interními pravidly a zásadami ČSOB a v souladu s postupy SDLC.

6.6.2 Řízení správy bezpečnosti

Řízení bezpečnosti je definováno interními pravidly a politikami ČSOB a je založeno na mezinárodním standardu ISO 27001.

6.6.3 Řízení životního cyklu bezpečnosti

Žádné ustanovení.

6.7 Řízení bezpečnosti sítě

Kontroly zabezpečení sítě jsou definovány interními pravidly a politikami ČSOB podle osvědčených postupů, jako je použití filtrovacích zařízení na různých úrovních modelu vrstvy OSI, segmentace sítě atd.

6.8 Označování časovými razítky

Nepoužije se.

7. PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

7.1.1 Číslo verze

CA vydává certifikáty X.509 verze 3.

7.1.2 Rozšíření certifikátu

Pro vydávání Certifikátů předplatitelům se používají následující rozšíření:

- Authority Key Identifier
- Subject Key Identifier
- Authority Info Access (Policy Information)
- Netscape Comment
- Key Usage

7.1.3 Objektové identifikátory algoritmů

Použité algoritmy jsou navrženy v souladu s mezinárodními standardy a normami.

7.1.4 Tvary jmen

Pro profil používaný pro vydávání Certifikátů předplatitelům se používají následující významy názvů v následujících parametrech:

SERIALNUMBER – náhodně vygenerované číslo

UID – identifikace klienta (ICID)

PSEUDONYM – identifikace klienta (OLI číslo)

GIVENNAME – křestní jméno klienta

PŘÍJMENÍ – příjmení klienta

C – země klientského certifikátu

CN – celé jméno klienta

O - název organizace, pokud je zadán

netscapeComment - nakonfigurovaný text (šablona) s přidaným algoritmem a odpovídajícím otiskem dokumentu

policyInformation – OID a URI, kde je možné najít tuto politiku

CertificateValidity – maximálně 30 minut nebo konfigurační parametr

keyUsage – nastavení na digitalSignature a nonrepudiation

Autorita vydává certifikáty s tvary jmen, vyhovujícími standardu RFC 5280

7.1.5 Omezení jmen

Žádné ustanovení

7.1.6 Objektový identifikátor certifikační politiky

Žádné ustanovení

7.1.7 Použití rozšíření Policy Constraints

Nepoužije se

7.1.8 Syntaxe a sémantika kvalifikátorů politiky

Nepoužije se.

7.1.9 Zpracování sémantiky kritického rozšíření Certificate Policies

Nepoužije se.

7.2 Profil seznamu zneplatněných certifikátů

7.2.1 Číslo verze

Nepoužije se.

7.2.2 Rozšíření CRL a záznamů v CRL

Nepoužije se .

7.3 Profil OCSP

7.3.1 Číslo verze

Nepoužije se.

7.3.2 Rozšíření OCSP

Nepoužije se.

8. HODNOCENÍ SHODY A JINÁ HODNOCENÍ

CA je auditována v rámci obecných požadavků na audit ČSOB, a to jak externím auditem, tak interním auditem, a to buď podle regulatorních požadavků, nebo podle vnitřních pravidel pro audit.

8.1 Periodicita nebo okolnosti hodnocení

Žádné ustanovení, viz 8.

8.2 Identita a kvalifikace hodnotitele

Žádné ustanovení, viz 8.

8.3 Vztah hodnotitele k hodnocenému subjektu

Žádné ustanovení, viz 8.

8.4 Hodnocené oblasti

Žádné ustanovení, viz 8.

8.5 Postup v případě zjištění nedostatků

Žádné ustanovení, viz 8.

8.6 Sdělování výsledků hodnocení

Žádné ustanovení, viz 8.

9. OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

Obecně platí, že CP neslouží jako smlouva nebo součást smlouvy. Předpokládá se, že určité právní podmínky a podmínky odpovědnosti se v případě potřeby objeví v samostatných dokumentech a dohodách s klientem.

9.1 Poplatky

Klientům CA neúčtuje žádné poplatky .

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Nepoužije se.

9.1.2 Poplatky za přístup k certifikátu

Nepoužije se.

9.1.3 Zneplatnění nebo přístup k informaci o stavu certifikátu

Nepoužije se.

9.1.4 Poplatky za další služby

Nepoužije se.

9.1.5 Postup při refundování

Nepoužije se.

9.2 Finanční odpovědnost

Nepoužije se.

9.2.1 Krytí pojištěním

Nepoužije se.

9.2.2 Další aktiva

Nepoužije se.

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Nepoužije se.

9.3 Důvěrnost obchodních informací

S důvěrnými informacemi je nakládáno v souladu s interními pravidly ČSOB pro klasifikaci informací.

9.3.1 Rozsah důvěrných informací

Žádné ustanovení, viz 9.3.

9.3.2 Informace mimo rámec důvěrných informací

Žádné ustanovení, viz 9.3.

9.3.3 Odpovědnost za ochranu důvěrných informací

Žádné ustanovení, viz 9.3.

9.4 Ochrana osobních údajů

S osobními údaji je nakládáno v souladu s regulatorními požadavky jako GDPR a také v souladu s interními pravidly ČSOB, která jsou v souladu s externími předpisy.

9.4.1 Politika ochrany osobních údajů

Žádné ustanovení, viz 9.4.

9.4.2 Informace považované za osobní údaje

Žádné ustanovení, viz 9.4.

9.4.3 Informace nepovažované za osobní údaje

Žádné ustanovení, viz 9.4.

9.4.4 Odpovědnost za ochranu osobních údajů

Žádné ustanovení, viz 9.4.

9.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Žádné ustanovení, viz 9.4.

9.4.6 Poskytování osobních údajů pro soudní či správní účely

Žádné ustanovení, viz 9.4.

9.4.7 Jiné okolnosti zpřístupňování osobních údajů

Žádné ustanovení, viz 9.4.

9.5 Práva duševního vlastnictví

Žádné ustanovení.

9.6 Zastupování a záruky

9.6.1 Zastupování a záruky CA

CA se zavazuje poskytovat služby odpovídajícím způsobem v souladu s tímto CP a vnitřními pravidly a politikami ČSOB. Toto a všechna další prohlášení a záruky, které jsou individuální nebo netýkající se konkrétního obchodního vztahu, jsou stanoveny v odpovídající smlouvě.

9.6.2 Zastupování a záruky RA

Nepoužije se.

9.6.3 Zastupování a záruky držitele certifikátu

Nepoužije se.

9.6.4 Zastupování a záruky spoléhajících se stran

Nepoužije se.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Nepoužije se.

9.7 Zřeknutí se záruk

S výjimkou prohlášení výslovně uvedených v tomto CP nebo omezených zákonem se zříkají všech záruk a závazků souvisejících s tímto CP.

9.8 Omezení odpovědnosti

Nepoužije se, viz 9.

9.9 Záruky a odškodnění

Nepoužije se, viz 9.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Tato CP je platná od data uvedeného v tabulce na straně 2 s historií změn a zůstává platná, dokud není nahrazena novější verzí.

9.10.2 Ukončení platnosti

Tato CP a případné změny zůstávají v platnosti, dokud nebudou nahrazeny novější verzí.

9.10.3 Důsledky ukončení a přetrvání závazků

Ustanovení v tomto CP platí do jejich nahrazení novou verzí CP. Aktualizace CP zohledňuje vydané certifikáty a nemění ustanovení způsobem, který by ovlivnil úpravu potřebnou pro již vydané certifikáty.

.

9.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

Žádné ustanovení

9.12 Novelizace

9.12.1 Postup při novelizaci

Změny provádějí správci CA a schvaluje je vedoucí oddělení.

9.12.2 Postup a periodicita oznamování

Nová verze CP je publikována interně a poskytována na public web ČSOB.

9.12.3 Okolnosti, při kterých musí být změněn OID

Nepoužije se.

9.13 Ustanovení o řešení sporů

Nepoužije se, viz 9.

9.14 Rozhodné právo

Nepoužije se.

9.15 Shoda s platnými právními předpisy

CA je provozována v souladu s platnými zákony a mezinárodními standardy, pokud jsou relevantní.

9.16 Různá ustanovení

9.16.1 Rámcová dohoda

Nepoužije se.

9.16.2 Postoupení práv

Nepoužije se.

9.16.3 Oddělitelnost ustanovení

Nepoužije se.

9.16.4 Vymáhání (poplatky za právní zastoupení a zřeknutí se práv)

Nepoužije se.

9.16.5 Vyšší moc

CA neodpovídá za porušení svých povinností vyplývajících z této CP v případě, že porušení je způsobeno zásahem vyšší moci mimo kontrolu CA.

9.17 Další ustanovení

Žádné ustanovení.