incode psc

Politika vzdáleného podepisování a prováděcí směrnice

Verze	Upraveno podle	Provedené změny	Datum úpravy
1.0	LV	Obsah	20/04/2025
1.1	LV	• Upřesnění doby uchovávání	19/06/2025

OBSAH

1 Úvodní stránka

Tento dokument popisuje zásady a provozní pokyny, kterými se společnost Incode Czech Republic s.r.o. (dále jen Incode) řídí při poskytování služby dálkového podpisu.

Popisuje také povinnosti a činnosti vyžadované od koncového uživatele v souvislosti s vydáváním a správou kvalifikovaného elektronického certifikátu spojeného s touto službou.

Služba je primárně určena pro elektronické podepisování dokumentů pomocí kvalifikovaných certifikátů vydaných společností Incode.

V rámci procesu podepisování je kvalifikovaný certifikát bezpečně uložen v zařízení pro vytváření kvalifikovaných podpisů (QSCD), které zůstává pod výhradní kontrolou společnosti Incode, čímž je zajištěn soulad s platnými regulačními a bezpečnostními požadavky.

Zákonné požadavky týkající se služby jsou definovány v:

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění;
- Zákon ČR č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce;
- Právní předpisy týkající se ochrany osobních údajů v souladu s nařízením Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

1.1 Přehled

Tento dokument s názvem **Prohlášení o zásadách dálkového podepisování** vypracovává společnost Incode a definuje v něm zásady řízení při poskytování služby dálkového podepisování.

Tento dokument slouží jako prohlášení o povinnostech, které společnost QTSP přijala pro zákazníky využívající její službu dálkového elektronického podpisu. Je důležité poznamenat, že tento dokument nepředstavuje právní dohodu mezi společností Incode a jejími zákazníky, ale spíše poskytuje:

- Technické, obchodní a právní požadavky na službu infrastruktury veřejného klíče (PKI) poskytovanou společností Incode.

- Pravidla a postupy ověřování pro zákazníky využívající službu elektronického ověřování nabízenou společností Incode QTSP, jakož i práva a povinnosti zákazníků, kteří se této služby účastní.
- Úroveň záruky spojená s digitálním certifikátem vydaným službou QTSP a spolehlivost digitálních podpisů vytvořených pomocí těchto certifikátů.
- Informace pro spoléhající se stranu týkající se úrovně důvěryhodnosti a jistoty poskytované certifikátem vydaným QTSP.

Tento dokument upravuje výhradně poskytování vzdáleného elektronického podpisu a nevztahuje se na jiné služby poskytované společností Incode.

1.2 Název a identifikace dokumentu

Název dokumentu: Prohlášení o politice vzdáleného podpisu.

Podporované OID: 0.4.0.19431.2.1.2 (eu-advanced-x509, AdES založený na certifikátech X.509) a

0.4.0.19431.1.1.3 (politika EU SSASC) - v případě ukládání podpisových klíčů v QSCD.

1.2.1 Politika vytváření podpisů

V daném okamžiku je v rámci služby podporována jediná politika vytváření podpisu. Použitá verze politiky vytváření podpisů je určena časem, kdy byl konkrétní elektronický podpis vytvořen.

1.2.2 Podporované formáty a základní linie podpisu

1.2.2.1 Základní linie

B-B	Minimální a standardizovaný profil zajišťující interoperabilitu bez zahrnutí časového razítka.
B-T	Zajišťuje generování a zahrnutí tokenu časového razítka pro existující podpis, který prokazuje, že podpis sám skutečně existoval k určitému datu a času.
B-LT	Poskytuje začlenění tokenu časového razítka a informace o stavu odvolání podpisového certifikátu.
B-LTA	Poskytuje začlenění tokenů časových razítek, které umožňují ověření platnosti podpisu dlouhou dobu po jeho vytvoření. Cílem této úrovně je řešit dlouhodobou dostupnost a integritu ověřovacího materiálu.

1.2.2.2 Formáty

1.2.2.2.1 PAdES

PAdES (PDF Advanced Electronic Signature) je standard, který definuje způsob vkládání elektronických podpisů do dokumentů PDF bezpečným a právně vyhovujícím způsobem. PAdES vychází z ETSI a je sladěn s eIDAS a zajišťuje pravost, integritu a dlouhodobou platnost podepsaných dokumentů PDF. Podporuje různé úrovně, od základních podpisů až po podpisy s časovým razítkem a plně ověřené podpisy pro dlouhodobou archivaci.

Incode podporuje použití viditelné a neviditelné verze podpisu.

Viditelný podpis lze do dokumentu umístit třemi různými způsoby:

1. Pouze text
2. Pouze obrázek
3. Text a obrázek

1.3 Účastníci PKI

1.3.1 Poskytovatel služby

Incode Czech Republic s.r.o. jako kvalifikovaný poskytovatel služeb vytvářejících důvěru.

1.3.2 Spoléhající se strany

Jakýkoli subjekt spoléhající se na vytváření elektronického podpisu pomocí služby vzdáleného podpisu Incode.

1.3.3 Ostatní účastníci

Dalšími zúčastněnými stranami jsou orgány vyšetřování, stíhání a rozhodování, orgány dohledu a další subjekty, které za takové uznává platná legislativa.

1.4 Použití služby

1.4.1 Vhodné použití služby

Služby vzdáleného podepisování poskytované podle této politiky jsou určeny k podpoře operací elektronického podepisování, při nichž je bezpečně spravován soukromý klíč podepisující osoby a operace podepisování je prováděna na dálku

uživatelem prostřednictvím bezpečných autentizačních mechanismů ve prospěch podepisující osoby a/nebo zúčastněných třetích stran v souladu s platnými právními předpisy.

1.4.2 Zakázaná použití služby

Vzdálené podepisování podle této politiky nesmí být použito v rozporu se schválenými užitími popsanými v oddíle 1.4.1 nebo v rozporu se zákonem. Nesmí být rovněž použito k následujícím účelům:

1. použití neoprávněnými nebo neověřenými osobami
2. automatizované nebo delegované podepisování bez výslovného souhlasu
3. použití mimo definovaný rozsah služby

1.5 Správa zásad

1.5.1 Organizace odpovědná za politiku

Tuto politiku spravuje společnost Incode Czech Republic s.r.o.

1.5.2 Kontaktní osoba

Kontaktní osobou společnosti Incode ve vztahu k této politice je manažer CA. Platí kontaktní údaje uvedené v kapitole 2.2.

1.5.3 Osoba určující vhodnost této politiky

Ředitel CA je jedinou osobou odpovědnou za rozhodování o souladu postupů společnosti Incode Czech Republic, s.r.o. stanovených v tomto dokumentu.

Přezkum postupů stanovených v tomto dokumentu bude prováděn nejméně jednou ročně. V případě potřeby budou provedeny aktualizace a případné změny spolu s aktualizovaným prohlášením budou zveřejněny na určeném portálu, který společnost Incode k tomuto účelu poskytuje.

V rámci každoročních přezkumů a úprav platných postupů a zásad je ředitel CA odpovědný za stanovení použitelnosti policejního prohlášení o vzdáleném podpisu a souvisejících zásad.

1.6 Definice a zkratky

1.6.1 Definice

Pojmy	Vysvětlení
Init kód	QR kód nebo odkaz URL sloužící k inicializaci služby pro konkrétního klienta.
Identita podepisujícího	Identita od podepisující osoby získaná prostřednictvím procesu vzdáleného ověření identity poskytovaného společností Incode.
Utajované informace Zákon o ochraně utajovaných informací	Zákon České republiky č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti.
Elektronický podpis	Zlepšený elektronický podpis nebo kvalifikovaný elektronický podpis poskytovaný podle právních předpisů o službách vytvářejících důvěru.
Elektronický podpis na dálku	Elektronický podpis vytvořený pomocí soukromého klíče uloženého v zařízení provozovaném, spravovaném a zabezpečeném společností Incode. Tento soukromý klíč je pod výhradní kontrolou klienta.
Důvěryhodná služba / kvalifikovaná důvěryhodná služba	Definováno právními předpisy o službách vytvářejících důvěru.
Dozorčí orgán	Orgán vykonávající dohled nad poskytovateli kvalifikovaných služeb vytvářejících důvěru.

1.6.2 Zkratky

Symbol	Úplný název
AdES	Pokročilý elektronický podpis
CR	Česká republika
eIDAS	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, v platném znění.
CS	Evropská norma, typ normy ETSI
ETSI	Evropský institut pro telekomunikační normy, evropský normalizační institut pro informační a komunikační technologie
HSM	Hardwate Security Module
OID	Identifikátor objektu
PAdES	PDF Pokročilé elektronické podpisy
XAdES	XML pokročilé elektronické podpisy

2 Odpovědnost za zveřejnění a uložení

2.1 Uložení

Incode je odpovědný za udržování dostupnosti úložišť, kde jsou zveřejněny informace o jeho zásadách a veřejných informacích.

2.2 Zveřejňování certifikačních informací

Sídlo společnosti Incode Czech Republic, s.r.o., pro účely získávání informací o její činnosti, je následující:

- Pujmanové 1753/10a, Nusle, 140 00 Praha 4.
- https://psc.incode.com/eu/
- tsp@incode.com

Elektronická adresa pro styk veřejnosti s Incode Czech Republic s.r.o. info@incode.com.

Datová schránka společnosti Incode Czech Republic s.r.o. ID je 76gmkd8.

2.3 Četnost zveřejňování informací

Incode zveřejňuje informace následujícím způsobem:

- Politika služby. Po schválení a vydání nové verze.

2.4 Kontroly přístupů na úložiště

Společnost Incode nevyžaduje autentizaci pro přístup třetích stran k této politice prostřednictvím určené online adresy pro zveřejňování informací.

3 Identifikace a ověřování

3.1 Počáteční ověření totožnosti

3.1.1 Jak prokázat vlastnictví tajného klíče

Všechny soukromé klíče jsou generovány interně v rámci procesu podepisování certifikační autoritou vydavatele Incode a bezpečně uloženy v hardwarovém bezpečnostním modulu (HSM).

Pokud certifikační autorita vydavatele nebo RA nevygeneruje klíčový pár subjektu, musí certifikační autorita nebo RA ověřit:

a) elektronický podpis obsažený v žádosti o podepsání certifikátu PKCS #10 (CSR), aby se ujistil, že odpovídá veřejnému klíči žadatele.
b) integritu podepsaných dat v CSR.

3.1.2 Identifikace a ověření jednotlivých subjektů

Ověřování totožnosti jednotlivce se řídí procesem ověřování totožnosti na dálku, aby byla zajištěna bezpečnost, shoda a účinnost. Tento proces obvykle zahrnuje následující kroky:

1. Iniciace žádosti o certifikát

- Žadatel iniciuje proces žádosti o certifikát nebo dokončení transakce vzdáleného podpisu. Doba platnosti se může lišit v závislosti na konkrétním procesu a požadavcích.

2. Předložení dokladů totožnosti

- Žadatel musí předložit státem vydaný doklad totožnosti (např. cestovní pas, občanský průkaz, řidičský průkaz, vízum).
- Doklad se pořizuje pomocí mobilního zařízení prostřednictvím zabezpečeného webového portálu nebo mobilní aplikace Incode.
- Technologie optického rozpoznávání znaků (OCR) vytáhne a ověří údaje z dokladu.
    - Systém shromažďuje identifikační údaje, jako je celé jméno, datum platnosti, země vydání a další relevantní informace z poskytnutých dokladů.
- Provádějí se pokročilé kontroly pravosti dokumentů (např. detekce vodoznaku, ověření hologramu, MRZ skenování), aby se zabránilo podvodům.

3. Vzdálené ověřování živosti a biometrické ověřování

- Žadatel musí absolvovat kontrolu živosti zahrnující následující metody:
    - Snímání selfie s pasivní detekcí živosti řízenou umělou inteligencí.
    - Biometrická shoda mezi selfie a fotografií dokladu totožnosti.
- Technologie rozpoznávání obličeje založená na umělé inteligenci Incodes zajišťuje, že žadatel je fyzicky přítomen a nepoužívá zmanipulované snímky nebo deepfakes.

4. Křížové ověřování dat a kontroly prevence podvodů

- Získané údaje se křížově kontrolují:
    - vládními databázemi (pokud je to relevantní).

  - Seznamy sankcí a sledované seznamy (za účelem dodržování pravidel AML/KYC).
  - Předchozí pokusy o ověření s cílem odhalit anomálie nebo nesrovnalosti.
- Systém označuje potenciální podvody s identitou, duplicitní identity nebo podezřelé chování.

5. Vydávání certifikátů

- Pokud je ověření úspěšné, je vydán signatářský certifikát s konkrétními:
  - definovanou dobou platnosti.
  - Omezený rozsah použití (např. jedna transakce, jedna relace, podepisování dokumentů).

5. Vzdálený podpis

  - Po vydání certifikátu a se souhlasem držitele certifikátu jsou předložené dokumenty podepsány.

7. Vypršení platnosti a automatické odvolání

- Platnost krátkodobého certifikátu automaticky vyprší po uplynutí stanovené doby platnosti.
- Pokud je po vydání zjištěna podezřelá aktivita, lze certifikát okamžitě odvolat prostřednictvím odpovědí protokolu OCSP (Online Certificate Status Protocol).

3.2 Modifikace dat

Po vydání certifikátu není možné data v něm upravovat. Pokud je třeba údaje změnit nebo pokud držitel certifikátu požaduje nový certifikát, je třeba postupovat podle postupu popsaného v části 3.1.2.

4 Provozní požadavky na životní cyklus služby

V následujících oddílech bude podrobně popsán životní cyklus služby vzdáleného podpisu. Čtenáři této politiky získají přehled o klíčových procesech, technických požadavcích a úvahách o shodě v každé fázi životního cyklu služby.

4.1 Aktivace služby

Služba je aktivována, když uživatel obdrží od třetí strany Init kód a zahájí proces ověření identity.

4.1.1 Proces registrace a odpovědnosti

Proces ověření totožnosti musí být proveden podle definice v oddíle 3.1.2 pokaždé, když uživatel použije službu vzdáleného podpisu.

Uživatel je mimo jiné povinen provést následující úkony:

- Seznámit se s touto politikou a CPS pro vydávání kvalifikovaných certifikátů pro vzdálené elektronické podpisy.
- používat službu v souladu s oddílem 1.4.
- Poskytnout pravdivé a úplné informace pro nastavení služby.
- Zkontrolovat, zda jsou údaje z předložených dokumentů správné a odpovídají požadovaným údajům.

Incode je povinen plnit mimo jiné následující povinnosti:

- Informovat uživatele o podmínkách před zahájením procesu vzdáleného podepisování.
- Během procesu ověřování totožnosti ověřit všechny platné údaje podle předložených dokumentů.
- Vydat podpisový certifikát, který obsahuje správné údaje na základě informací poskytnutých uživatelem.
- Zveřejněte certifikáty vydávající a kořenové certifikační autority.

4.1.2 Provádí přijetí konstitutivního certifikátu

Uživatel potvrdí přijetí tím, že:

- Implicitní přijetí, ke kterému může dojít, pokud odběratel použije certifikát k určenému účelu (např. podepsání dokumentu).
- U procesů vzdáleného digitálního podpisu je přijetí potvrzeno před procesem podepisování, takže není třeba provádět žádné další kroky.

4.2 Odvolání a pozastavení platnosti certifikátu

4.2.1 Odvolání certifikátu

Odvolání certifikátu je trvalé zneplatnění digitálního certifikátu před vypršením jeho platnosti. Jednou zrušený certifikát nelze obnovit a musí být v případě potřeby nahrazen novým.

Digitální certifikát může být odvolán z různých bezpečnostních, compliance nebo provozních důvodů, např:

1. Kompromitace soukromého klíče – soukromý klíč spojený s certifikátem byl ztracen, odcizen nebo odhalen, což může vést k jeho neoprávněnému použití.
2. Neoprávněné použití klíče – soukromý klíč je používán k účelům, které nejsou povoleny v souladu s určením certifikátu.

3. Kryptografická slabina – Kryptografické algoritmy nebo délky klíčů certifikátu již nejsou bezpečné v důsledku pokroku v kryptoanalýze nebo nově objevených zranitelností.
4. Dobrovolné odvolání certifikátu – Odběratel požádá o odvolání, protože již certifikát nepotřebuje.
5. Ztráta nebo zneužití soukromého klíče odběratele – Předplatitel ztratí kontrolu nad svým soukromým klíčem, a proto je nutné certifikát zrušit, aby se zabránilo jeho zneužití.
6. Změna údajů o odběrateli – změní se právní název odběratele, údaje o organizaci nebo jiné důležité informace, čímž se stávající certifikát stane neplatným.
7. Zfalšované nebo nesprávné informace – Certifikát byl vydán na základě nepřesných, neúplných nebo podvodných informací.
8. Porušení podmínek a zásad – Odběratel porušil Certifikační politiku (CP), Certifikační prováděcí směrnici (CPS) nebo Smlouvu o poskytování služeb.
9. Zneužití nebo neoprávněné použití certifikátu – Certifikát je používán způsobem, který porušuje jeho zamýšlený účel a potenciálně ohrožuje bezpečnost.
10. Certifikační autorita zjistí riziko pro bezpečnost nebo pověst – Certifikační autorita (CA) nebo kvalifikovaný poskytovatel důvěryhodných služeb (QTSP) identifikuje certifikát jako potenciální hrozbu pro bezpečnost, spolehlivost nebo pověst.
11. Zapojení do podvodu, kybernetické kriminality nebo škodlivé činnosti – Certifikát je spojen s podvodnými aktivitami, phishingovými útoky, hackerskými útoky nebo jinými nezákonnými činnostmi.
12. Odběratel nedodržuje tuto politiku – Odběratel neplní průběžné požadavky uvedené v CPS nebo v platných předpisech.
13. Předplatitel jako fyzická osoba je mrtvý nebo prohlášený za nezvěstného – Pokud odběratel zemřel nebo byl soudem právoplatně prohlášen za nezvěstného, musí být jeho certifikát zrušen.

4.2.1.1 Kdo může o zrušení požádat?

Žádost o zrušení digitálního certifikátu mohou podat následující oprávněné subjekty:

1. Vlastník klíče certifikátu.
2. Certifikační autorita, certifikační autorita vydavatele nebo RA.
3. Vládní agentura, soud nebo regulační orgán.
4. Zaměstnavatel nebo organizace.

4.2.1.2 Postup pro podání žádosti o zrušení certifikátu

Standardní žádost o zrušení certifikátu

- Uživatel musí zaslat e-mail s žádostí o odvolání.
- E-mail musí být digitálně podepsán pomocí soukromého klíče certifikátu (za předpokladu, že je certifikát stále platný a nevypršela jeho platnost).

- Tím je zajištěna pravost a zabráněno neoprávněným žádostem o odvolání.

Nouzová žádost o odvolání

- Pokud uživatel nemůže odeslat digitálně podepsaný e-mail (např. z důvodu kompromitace nebo ztráty klíče), lze žádost o odvolání nahlásit přímo RA nebo certifikační autoritě vydavatele QTSP.
- V takových případech je třeba použít alternativní postupy ověření totožnosti, aby se potvrdila oprávněnost požadavku.

4.2.1.3 Odkladná lhůta pro podání žádosti o zrušení

Pokud existuje podezření na kompromitaci klíče nebo jiný důvod pro odvolání uvedený v oddíle 4.2.1, musí uživatel podat žádost o odvolání co nejdříve v přiměřené lhůtě. Opožděné podání žádosti zvyšuje riziko neoprávněného použití kompromitovaného klíče.

Certifikační autorita neodpovídá za škody vzniklé v důsledku nezákonného nebo neoprávněného použití soukromého klíče odběratele před odvoláním certifikátu. Předplatitel je výhradně odpovědný za ochranu svého soukromého klíče a za neprodlené ohlášení jakéhokoli podezření na kompromitaci.

4.3 Používání služby

Incode poskytuje službu pro vzdálené vytváření elektronických podpisů. Dokumenty, které mají být podepsány, zasílají třetí strany a postup je následující:

1. Třetí strana vytvoří podpisový tok, který obsahuje dokument, jenž má být podepsán, a zašle Incode uživateli.
2. Uživatel přistupuje k toku pomocí Init kódu poskytnutého třetí stranou a dokončí proces ověření de identity.
3. Uživatel si prohlédne obsah dokumentu, který má být podepsán, prezentovaný v aplikaci.
4. Pokud se uživatel rozhodl souhlasit s obsahem podepisovaného dokumentu, stiskne tlačítko "podepsat".
5. Uživatel musí zaškrtnout políčka přítomná v toku, aby vyjádřil souhlas s procesem, vydáním kvalifikovaného certifikátu a podpisem dokumentu vydaným certifikátem.
6. Po označení všech zaškrtávacích políček uživatel stiskne tlačítko "Pokračovat".

7. CA vydá kvalifikovaný certifikát pro elektronický podpis, který bude uložen v zabezpečeném kryptografickém zařízení.
8. Vzdálený elektronický podpis se dokončí pomocí soukromého klíče vytvořeného v kroku 7.

5 Řídicí, provozní a fyzické kontroly .

5.1 Kontrola na fyzické úrovni

Provoz QTSP a RA probíhá v chráněném fyzickém prostředí, které je navrženo tak, aby se zabránilo neoprávněnému přístupu, použití nebo vyzrazení citlivých informací a aby se tyto informace odhalily. Toto prostředí je v souladu s bezpečnostními požadavky QTSP a standardy testování QTSP.

Bezpečnostní požadavky jsou částečně založeny na bezpečnostních opatřeních fyzické úrovně, která zahrnují:

- ochranu obvodu, jako jsou ploty, uzamčené dveře a kontrolované přístupové body, které zajišťují, že pouze oprávněné osoby mohou přejít do další bezpečnostní vrstvy.
- Každá vrstva poskytuje stále omezenější přístup a nabízí vyšší fyzickou bezpečnost proti neoprávněnému vstupu.
- Struktura zabezpečení se řídí vrstevnatým přístupem, kdy je každá vnitřní vrstva plně uzavřena ve vnější vrstvě, čímž vzniká progresivní model zabezpečení.

Minimální úroveň fyzického zabezpečení vyžadovaná QTSP a RA je určena nejvyšší úrovní zabezpečení certifikátu, kterou prosazují.

5.1.1 Fyzický přístup

Servery RA a CA jsou umístěny v kontrolovaném prostředí s omezeným přístupem, který je vynucován prostřednictvím individuálních přístupových práv. Podpisový systém certifikační autority pracuje na vyhrazeném počítači a soukromý klíč je v době, kdy se nepoužívá, bezpečně uložen, aby byla zajištěna jeho ochrana a integrita.

5.1.2 Klimatizace a napájení

- Servery poskytující online služby jsou provozovány v řádně klimatizovaném prostředí a nejsou restartovány s výjimkou nezbytné údržby.
- Servery systému QTSP jsou chráněny systémem UPS a záložním generátorem pro případ výpadku elektrické sítě.

5.1.3 Kontakt s vodou

Umístění zařízení systému Incode QTSP je vhodně zvoleno a je vypracován preventivní plán, který zabraňuje vniknutí vody a záplav do systému.

5.1.4 Protipožární ochrana a prevence

Datová centra, v nichž se nachází infrastruktura CA společnosti Incode, mají v souladu se zprávou SOC 2 zavedeny zásady a postupy protipožární ochrany, které zajišťují, že zařízení infrastruktury zůstane v případě požáru chráněno.

5.1.5 Úložná média

Všechna média obsahující produkční software a data, auditní záznamy, archivy nebo záložní informace jsou uložena v rámci účtu AWS společnosti Incode, přičemž jsou zavedeny příslušné logické kontroly přístupu, které omezují přístup oprávněným pracovníkům. Data jsou navíc chráněna zásadami zálohování, aby se zabránilo jejich ztrátě nebo poškození.

5.1.6 Zpracování a likvidace odpadu

Nakládání s odpadem v zařízeních datového centra podléhá zásadám a předpisům stanoveným společností AWS.

Pokud jde o nakládání s odpady v rámci řízených postupů společnosti Incode, zejména těch, které se týkají nakládání s médii, společnost Incode se řídí zásadami nakládání s médii, které definují postupy dezinfekce požadované pro fyzická a elektronická média. Tyto postupy zajišťují bezpečné zničení médií a zabraňují jakémukoli vystavení uložených informací nebo jejich opětovnému použití.

5.1.7 Vzdálené zálohování

Procesy a systémy QTSP společnosti Incode mají automatizované mechanismy zálohování, které umožňují okamžité body obnovy v případě selhání. Tyto zálohy jsou

bezpečně uloženy s redundancí v regionech zpracování dat, kde společnost Incode působí v rámci cloudu AWS, v souladu s jejími zásadami zálohování.

5.2 Procedurální kontroly

5.2.1 Důvěryhodní členové

Zaměstnance, dodavatele a konzultanty lze považovat za důvěryhodné osoby pracující v důvěryhodné pozici. Osoby vybrané jako důvěryhodné pracují na důvěryhodném místě, které splňuje požadavky CPS.

Všichni zaměstnanci mají právo přístupu nebo kontroly nad šifrovanými operacemi, které mohou primárně ovlivnit vydávání, používání, odvolávání, rušení/zrušování digitálních certifikátů, včetně přístupu do vyhrazené kontrolní oblasti certifikační autority.

Pověřenci jsou všichni zaměstnanci, inženýři a konzultanti, jejichž přístup nebo kontrola procesu ověřování nebo šifrování může významně ovlivnit:

- Proces kontroly informací v žádosti o digitální certifikát.
- Přijetí, zamítnutí nebo jiné zpracování žádosti o digitální certifikát, žádosti o odvolání, žádosti o obnovení nebo informací o registraci.
- Vydávání a rušení certifikátů zaměstnanců, kteří mají přístup do vyhrazených částí systému.

Mezi důvěryhodné osoby patří (nikoli pouze):

- Pracovníci zákaznického servisu.
- Správce systému.
- Projektový inženýr.
- Specialisté na redundanci a její prosazování zajišťují správu zařízení vytvářejících důvěru.

5.2.2 Počet osob potřebných pro každou pracovní pozici

Společnost Incode má zavedeny robustní bezpečnostní mechanismy a postupy, které zajišťují, že žádný jednotlivec nemůže samostatně provádět kritické operace CA. Tento přístup zvyšuje bezpečnost, odpovědnost a provozní integritu prostřednictvím oddělení povinností a kontroly více osob.

1. Kontrola více osob a oddělení povinností
    - Operace CA nikdy neprovádí jediná osoba, aby se zabránilo neoprávněným činnostem a bezpečnostním rizikům.
    - Tato zásada zajišťuje sdílenou odpovědnost, rozdělení znalostí a kolektivní kontrolu kritických bezpečnostních funkcí.
2. Přidělení povinností na základě rolí
    - Zásady a postupy určují přidělování povinností na základě rolí a bezpečnostních prověrek.
    - Vysoce citlivé úkoly, jako je přístup ke kryptografickým hardwarovým systémům a jejich správa a provádění operací správy klíčů, vyžadují zapojení více důvěryhodných osob.
3. Interní kontrolní postupy pro přístup ke kryptografickému hardwaru
    - Na jakémkoli fyzickém nebo logickém přístupu ke kryptografickému hardwaru, který vyžaduje přísnou kontrolu šifrování, se musí podílet nejméně tři důvěryhodné osoby.
    - Citlivé kryptografické operace, jako je generování, podepisování a ničení klíčů, se provádějí pod dohledem více osob, aby se zabránilo narušení bezpečnosti.
    - Od počátečního příjmu a ověření až po závěrečný krok logického nebo fyzického zničení se na procesu podílí více důvěryhodných pracovníků, kteří zajišťují shodu, bezpečnost a transparentnost celého procesu.

5.3 Personální kontroly

Společnost Incode udržuje zdokumentované zásady personální kontroly a zabezpečení systémů CA a RA. Soulad s těmito zásadami zahrnuje požadavky na nezávislý audit, který zajišťuje dodržování bezpečnostních standardů.

Tyto dokumenty obsahují citlivé a důvěrné informace a jsou přístupné pouze stranám účastnícím se služby QTSP, a to s výslovným souhlasem společnosti Incode.

5.3.1 Kompetence, zkušenosti a další požadavky

Všichni zaměstnanci společnosti Incode musí absolvovat odpovídající školení a mít zkušenosti s provozem infrastruktury veřejných klíčů (PKI) spolu s potřebnou technickou a odbornou způsobilostí.

Společnost Incode rovněž vyžaduje, aby zaměstnanci měli ověřenou a bezúhonnou minulost, čímž je zajištěn soulad s požadavky na bezpečnost a důvěryhodnost.

5.3.2 Postup prověřování minulosti

Před nástupem zaměstnance do důvěryhodné role provádí QTSP důkladné prověření, které zahrnuje:

- Ověření historie předchozích zaměstnání.
- Prověření referenčních informačních zdrojů.
- Potvrzení příslušné odborné kvalifikace a osvědčení.
- Ověření životopisu (CV) uchazeče.
- Posouzení finanční a úvěrové historie.

V rámci procesu prověřování mohou být některá zjištění považována za důvod k odmítnutí kandidáta na důvěryhodnou pozici nebo k přijetí disciplinárního opatření vůči stávajícím zaměstnancům na důvěryhodných pozicích.

5.3.3 Požadavky na školení

Společnost Incode organizuje potřebné školicí programy, aby zajistila, že zaměstnanci budou své povinnosti vykonávat profesionálně a efektivně.

Pravidelné vyhodnocování a posilování těchto školicích programů je nezbytné pro udržení kompetencí a dodržování předpisů.

Školicí programy jsou přizpůsobeny konkrétním pracovním povinnostem každého zaměstnance, což zajišťuje, že obdrží relevantní a pro danou roli specifické znalosti.

5.3.4 Cyklus proškolování

Společnost Incode své zaměstnance pravidelně proškoluje a aktualizuje s odpovídající úrovní a frekvencí, aby si zaměstnanci udržovali důvěru a dobře vykonávali svou práci.

Přeškolení je nutné, když se v systému používá nový software nebo funkce a zavádějí se organizační postupy.

5.3.5 Disciplína za nezákonné činnosti

Společnost Incode zavádí, udržuje a prosazuje zásady proti nezákonným činnostem. Disciplinární opatření nebo ukončení smlouvy v závislosti na závažnosti nezákonné činnosti.

5.3.6 Požadavky na nezávislé smluvní partnery

Nezávislí dodavatelé nebo konzultanti mohou být považováni za správce. Na každého takového dodavatele nebo konzultanta se vztahují stejné funkce a obdobné bezpečnostní standardy, jaké platí pro zaměstnance společnosti Incode na srovnatelné pozici.

5.3.7 Poskytování dokumentů zaměstnancům

Společnost Incode poskytuje veškeré potřebné dokumenty k řádnému výkonu jejich práce.

5.4 Postupy protokolování auditů

5.4.1 Typy protokolů událostí

Zaznamenávají se následující události:

- Na serverech s certifikáty:
  - Spuštění a vypnutí;
  - Přihlášení, odhlášení;
  - Vytvoření a podepsání certifikátu.
- Na online serverech QTSP:
  - Přijmutí žádosti o certifikát od RA;
  - Přidání záznamu do databáze certifikační autority;
  - Zapsat žádosti o certifikát do externího paměťového zařízení;
  - Předávání certifikátů v souladu s požadavky zainteresovaných stran;
  - Uložení certifikátu do online úložiště;
  - Přijetí žádosti o stažení;
  - Uvolnění seznamu CRL.

5.4.2 Frekvence zpracování protokolu událostí

Záznamy o auditu jsou prověřovány za účelem identifikace relevantních a neopakujících se alarmů v systému CA/RA.

Centra zpracování porovnávají protokoly auditu s manuálními nebo elektronickými záznamy poskytnutými zákazníky QTSP a servisními centry, aby prošetřila případnou podezřelou aktivitu.

Zpracování auditních protokolů zahrnuje:

- Přezkoumání protokolů auditu za účelem identifikace anomálií a bezpečnostních událostí.
- Zdokumentování příčiny všech významných událostí v přehledu auditu.
- Zajištění integrity dat ověřením, že informace nebyly změněny nebo smíchány.
- Opětovnou kontrolu všech zaznamenaných údajů z hlediska přesnosti a konzistence.
- Analýza alarmů nebo neobvyklých záznamů v protokolu s cílem odhalit potenciální bezpečnostní hrozby.
- Přijímání vhodných opatření na základě zjištění z kontroly auditních protokolů.

5.4.3 Doba uchovávání záznamů auditu

Minimální doba uchovávání záznamů z auditu je 10 let.

5.4.4 Ochrana záznamů o auditu

Záznamy o auditu budou chráněny elektronickým systémem záznamů o auditu, který zahrnuje mechanismy na ochranu záznamů o auditu před neoprávněným přístupem, změnou, vymazáním nebo manipulací. Auditní záznamy jsou přístupné pouze operačnímu systému a správě certifikační autority.

5.4.5 Postup zálohování auditních protokolů

Auditní protokoly budou zálohovány denně se změnami a přírůstky a týdně s úplnými zálohami.

5.4.6 Systém sběru akreditací (interní a externí)

Není specifikováno.

5.4.7 Oznámení o příčině události

Není specifikováno.

5.4.8 Posouzení slabých míst

Není specifikováno.

5.5 Archivace záznamů

5.5.1 Typy uložených záznamů

- Jak je popsáno v kapitole 5.4.1.
- Informace o elektronické žádosti o certifikát.
- Dokumentace k žádostem o certifikát
- Informace o životním cyklu elektronických certifikátů, například informace o odvolání a obnově certifikátu.

5.5.2 Doba uchovávání dokumentů

Minimální doba uchovávání záznamů z auditu je 10 let.

5.5.3 Zabezpečené archivy

- Přístup k archivům je přísně omezen na oprávněné výkonné a administrativní pracovníky společnosti Incode.
- Veškerá uložená data jsou chráněna proti neoprávněnému přístupu, prohlížení, pozměňování, mazání, úpravám nebo zničení v rámci důvěryhodných a zabezpečených systémů.
- Nosiče dat a související aplikace používané ke zpracování dat jsou průběžně udržovány, aby bylo zajištěno, že uložené informace zůstanou přístupné a neporušené po celou dobu uchovávání stanovenou v CPS.

5.5.4 Postupy zálohování

- Incode pravidelně zálohuje elektronická data související s vydanými certifikáty, aby byla zajištěna integrita a bezpečnost dat.
- Provádějí se přírůstkové zálohy, které zachycují a ukládají změny provedené v datech souvisejících s certifikáty.
- Kromě toho se každý týden provádí úplné zálohování všech elektronických dat obsahujících informace o certifikátech, aby se zachoval komplexní a obnovitelný záznam.

5.5.5 Vyžádejte si časová razítka pro data

Všechny protokoly událostí musí být opatřeny časovými razítky.

5.6 Kompromitace a zotavení po havárii

5.6.1 Postupy pro řešení úniků klíčů a incidentů

Pokud dojde ke ztrátě nebo kompromitaci soukromého klíče odběratele, je třeba neprodleně informovat registrační autoritu QTSP (RA) a požádat ji o zrušení dotčeného digitálního certifikátu. Kromě toho by měly být o situaci informovány všechny důvěryhodné strany, které o kompromitovaném klíči vědí a spoléhají na něj.

Pokud je soukromý klíč QTSP kompromitován, musí manažer certifikační autority okamžitě přijmout následující opatření:

1. Informovat odběratele a registrační autority – Zajistit, aby byli o kompromitaci informováni všichni dotčení odběratelé a registrační autority.
2. Zastavit vydávání certifikátů a distribuci seznamů odvolaných certifikátů (CRL) - Pozastavit vydávání všech certifikátů a zastavit distribuci seznamů odvolaných certifikátů (CRL), dokud nebude problém vyřešen.
3. Zrušit platnost kompromitovaného certifikátu – Podat žádost o zrušení platnosti kompromitovaného certifikátu, aby se zabránilo jeho dalšímu používání.
4. Vygenerovat nový pár klíčů a certifikát – Vydat nový klíč a certifikát QTSP a zajistit, aby byl veřejně dostupný v úložišti QTSP.
5. Zrušení všech certifikátů podepsaných kompromitovaným klíčem – Zneplatnit a zrušit všechny aktivní certifikáty dříve vydané s použitím kompromitovaného klíče certifikační autority.
6. Zveřejnit aktualizovaný seznam CRL – Aktualizovat a zveřejnit seznam CRL (Certificate Revocation List), který odráží odvolané certifikáty v úložišti QTSP.
7. Informovat bezpečnostní agentury a regulační orgány – Informovat Národní dozorový orgán a příslušné bezpečnostní agentury o narušení bezpečnosti.
8. Uvědomit důvěryhodné strany a ostatní certifikační autority – Zajistit, aby o narušení věděly všechny spoléhající se strany, poskytovatelé služeb vytvářejících důvěru a spolupracující certifikační autority.

5.6.2 Negativní chování vůči počítačovým zdrojům, softwaru a datům

Společnost Incode vynaloží veškeré úsilí na zavedení preventivních opatření a usnadnění rychlé obnovy v případě selhání systému. Pro minimalizaci výpadků a co

nejrychlejší obnovení provozu po selhání systému Incode budou přijata následující opatření:

- Zálohování softwaru - Každá softwarová komponenta společnosti Incode je zálohována na bezpečná paměťová média ihned po instalaci nové verze jakékoli komponenty společnosti Incode.
- Zálohování dat CA - Všechny aktivní datové soubory CA jsou po každé aktualizaci nebo změně zálohovány na vyměnitelná paměťová média.
- Pokud dojde k selhání hardwaru nebo softwaru podepisovacího serveru, bude problém co nejrychleji diagnostikován a vyřešen.
- V případě nejistoty ohledně rozsahu neopraveného poškození bude server kompletně přeinstalován od začátku s použitím původního vybavení a certifikovaného softwaru.
- Pokud dojde k poškození dat, společnost Incode diagnostikuje rozsah poškození a obnoví postižená data z poslední zálohy.

5.6.3 Schopnost zachovat kontinuitu provozu po havárii

Společnost Incode zajišťuje bezpečnostní opatření pro vývoj, testování a údržbu svého podpisu. V případě potřeby společnost Incode zavede plán obnovy po havárii, který je navržen tak, aby účinně obnovil kritické obchodní funkce a informační systémy.

- Plán obnovy po havárii upřednostňuje obnovu základních služeb, aby bylo zajištěno minimální narušení.
- Místo obnovy po havárii bude mít fyzickou úroveň zabezpečení definovanou společností Incode, aby byla chráněna infrastruktura a data.
- Místo obnovy po havárii je navrženo tak, aby bylo možné obnovit nebo obnovit data do 24 hodin od vzniku havárie.
- Databáze pro obnovu po havárii je pravidelně synchronizována s produkční databází, aby byla zajištěna konzistence dat.

5.7 Ukončení činnosti poskytovatele služeb

Ukončení činnosti poskytovatele služeb vyžaduje formální proces vyřazení z provozu, aby byl zajištěn bezpečný přechod, odvolání a archivace digitálních certifikátů a kryptografických materiálů při zachování souladu s předpisy.

V případě, že společnost Incode ukončí poskytování služeb QTSP, budou provedeny následující kroky:

1. Oznámení a dodržování předpisů
   - Oznámení národnímu regulačnímu orgánu za účelem zahájení a dokončení oficiálních postupů pro ukončení poskytování služeb.
   - Informování odběratelů a RA co nejdříve, aby měli dostatek času na přechod k alternativnímu poskytovateli.
   - Vydejte rozsáhlé veřejné oznámení, abyste transparentně informovali o ukončení provozu.
2. Ukončení vydávání certifikátů a pokračování podpůrných služeb
   - Okamžitě po potvrzení ukončení provozu ukončete vydávání nových digitálních certifikátů.
   - Pokračujte v udržování základních služeb, jako jsou např:
     - vydávání seznamů CRL pro podporu spoléhajících se stran.
     - Udržování služeb OCSP pro ověření stavu.
   - Zrušení všech nevypršených nebo dříve nezrušených certifikátů odběratela, pokud to bude považováno za nezbytné z hlediska bezpečnosti nebo shody s předpisy.
3. Finanční a administrativní povinnosti
   - Zpracovávat náhrady pro odběratele, jejichž certifikáty ještě nevypršely, pokud to vyžadují zásady nebo předpisy.
   - Zničit všechny kopie soukromého klíče QTSP bezpečným způsobem podle osvědčených kryptografických postupů, aby se zabránilo jeho neoprávněnému použití.
4. Minimální výpovědní lhůta a uchovávání záznamů
   - V případě plánovaného ukončení služby bude před jejím pozastavením dodržena minimálně 60denní výpovědní lhůta.
   - Správci certifikační autority v době ukončení odpovídají za:
     - uchovávání všech záznamů podle požadavků oddílu 5.5.2 CPS.
     - Provedení strukturovaného předání služby CA jiným CA, které fungují na základě stávající dohody, pokud je to relevantní.

6 Technická bezpečnostní kontrola

6.1 Kryptografie, soukromé klíče a jejich ochrana

1. Generování páru klíčů QTSP
    - Klíče kořenové certifikační autority a certifikační autority vydavatele jsou generovány v hardwarovém bezpečnostním modulu (HSM) úrovně 3 standardu FIPS 140-2.
2. Generování páru klíčů poskytovatele digitálních podpisových služeb
    - V rámci modelu vzdáleného digitálního podepisování je poskytovatel digitální podpisové služby:
        - Generuje klíčový pár odběratele, který zahrnuje veřejný a soukromý klíč, v souladu s článkem 3 vyhlášky 130/2018/ND-CP.
3. Bezpečnost a soulad pro generování klíčů
    - Aby bylo zaručeno, že páry klíčů jsou náhodné, jedinečné a bezpečné, proces generování klíčů Incode:
        - zabraňuje tomu, aby byl soukromý klíč odvozen z veřejného klíče.
        - Dodržuje standard PKCS #1 verze 2.1 pro generování kryptografických klíčů.
4. Ukládání klíčových párů a vydávání digitálních certifikátů
    - Klíčový pár odběratele je generován v systému Incode a bezpečně uložen v HSM.
    - Společnost Incode vydává digitální certifikáty s minimální délkou klíče RSA 2048 bitů, což zajišťuje silné šifrování a zabraňuje odvození soukromého klíče z veřejného klíče.

6.2 Kontrola počítačové bezpečnosti

6.2.1 Specifické technické požadavky na počítačovou bezpečnost

Společnost Incode zajišťuje, aby systémy obsahující software certifikační autority a datové soubory byly bezpečné a odolné proti neoprávněnému přístupu. Kromě toho prosazuje přísné řízení přístupu k hlavnímu serveru, které omezuje přístup pouze na oprávněné pracovníky. Běžní uživatelé nemají na hlavním serveru účty.

Počítačová síť je logicky rozdělena do samostatných vrstev, což zabraňuje neoprávněnému přístupu s výjimkou přístupu prostřednictvím předem definovaných aplikací pro zpracování.

Všechny relace vyžadují pro přihlášení autentizaci pomocí hesel nebo proxy certifikátů.

Přímý fyzický přístup do sítě Incode je omezen na důvěryhodné pracovníky, přičemž přístupová oprávnění jsou udělována na základě pracovních rolí a odpovědností.

6.2.2 Hodnocení bezpečnosti

Společnost Incode splňuje požadavky normy ISO 27001 týkající se bezpečnosti počítačových systémů. Posuzování a kontrolní práce se provádějí pravidelně a nepravidelně na základě aktuální situace. Útvar řízení systému je odpovědný za zpracování inspekčních zpráv z průzkumů a poskytování opatření, plánů a realizace k řešení problémů v inspekčních zprávách.

6.3 Kontroly bezpečnosti v průběhu životního cyklu

6.3.1 Kontrola vývoje systému

Pro zajištění bezpečnosti, spolehlivosti a souladu s předpisy společnost Incode při návrhu a údržbě softwaru pro své certifikační autority a RA provádí následující kontroly:

- Dodržuje strukturovaný životní cyklus bezpečného vývoje (SDLC), který zahrnuje bezpečnostní opatření v každé fázi (plánování, vývoj, testování, nasazení a údržba).
- Zajišťuje soulad s průmyslovými normami (např. eIDAS, ETSI EN 319 411, ISO/IEC 27001 a NIST SP 800-53).
- Zavádí řízení přístupu na základě rolí (RBAC) k omezení přístupu k vývojovým prostředím na základě pracovních rolí.
- Používá vícefaktorové ověřování (MFA) pro všechny vývojáře a správce přistupující k systému.
- Provádí pravidelnou statickou a dynamickou analýzu kódu s cílem identifikovat zranitelnosti.
- Zavádí osvědčené postupy bezpečného kódování s cílem zmírnit běžné hrozby (např. SQL injection, buffer overflow, cross-site scripting).

- Udržuje verzování kódu a sledování změn prostřednictvím zabezpečených úložišť.

6.4 Kontrola zabezpečení sítě

Funkce certifikační autority (CA) a registrační autority (RA) fungují v rámci zabezpečené sítě a řídí se bezpečnostními zásadami a standardními dokumenty o shodě, aby se zabránilo neoprávněnému přístupu, manipulaci a útokům na službu.

Pro zajištění spolehlivosti a ověřování jsou veškerá komunikace a kritické informace chráněny pomocí šifrování mezi body a digitálních podpisů pro ověřování.

Kromě toho jsou všechny ostatní systémy CA chráněny prostřednictvím:

- Firewally, které omezují neoprávněný přístup.
- Systémy detekce a prevence narušení (IDS/IPS) pro monitorování a zmírnění hrozeb.
- Odstranění nepotřebných služeb, aby se minimalizovala zranitelnost.

6.5 Časové razítko

Společnost Incode provozuje autoritu časových razítek, která je v souladu s RFC 3161.

Společnost Incode zajišťuje přesnou synchronizaci hodin, a to i během přestupných sekund, aby byla zachována přesnost a spolehlivost serveru časových razítek. Server je nejméně jednou za 24 hodin synchronizován se zdrojem času UTC(k), čímž je zajištěn soulad s mezinárodními časovými standardy.

V zájmu zachování přesnosti server časových razítek nepřetržitě monitoruje odchylky hodin nebo anomálie v synchronizaci s UTC. Pokud dojde k jakékoli úpravě hodin o jednu sekundu nebo více, je klasifikována jako auditovatelná událost. Stejně tak podléhají auditu veškeré úpravy provozních procesů serveru časových razítek.

Kromě toho, aby byla zachována kryptografická integrita, musí být algoritmus digestu používaný k podepisování tokenů časových razítek totožný s algoritmem používaným k podepisování certifikátu časového razítka. Tím je zajištěna konzistence, bezpečnost a důvěryhodnost procesu časových razítek.

7 Audity shody a další hodnocení

Společnost Incode bude po svém provozním nasazení provádět pravidelné audity, aby zajistila trvalý soulad se standardy služby QTSP. Tyto standardy budou také sloužit jako základ pro hodnocení, inspekce a hodnocení řízení rizik, čímž bude zajištěna integrita a bezpečnost provozu společnosti Incode.

Klíčová opatření pro dodržování předpisů a audity:

- Interní a externí inspekce:
  - Standardy služeb Incode budou použity k hodnocení provozu QTSP a firemních odběratelů.
  - Pokud audit odhalí, že společnost Incode nesplňuje požadované standardy, budou přijata nápravná opatření.
  - V závislosti na závažnosti a dopadu nedodržení norem může být subjektu povoleno pokračovat v činnosti nebo může být služba pozastavena či ukončena.

Posouzení řízení rizik:

- Standardy služby Incode budou uplatňovány při posuzování rizik prováděném samotnou společností QTSP nebo jejími odběrateli.
  - Tato posouzení pomohou identifikovat problémy s nedodržováním předpisů a odlehlé výsledky auditů dodržování předpisů.
  - Budou také začleněna do celkového rámce řízení rizik společnosti Incode.

Audity subjektů třetích stran:

- Standardy služeb QTSP budou využívány k auditu, hodnocení a kontrole subjektů třetích stran nebo externích auditorských firem.
- Subjekty, u nichž je prováděn audit, musí plně spolupracovat s QTSP, aby byl zajištěn transparentní a důkladný proces hodnocení.

7.1 Četnost a případy posuzování

- Audity shody Incode CPS budou prováděny nejméně jednou ročně.
- Společnost Incode provádí kontroly dodržování CPS u každé RA s účinnou CPS nejméně jednou ročně.

7.2 Totožnost a schopnosti auditora

Auditorská společnost slouží jako třetí strana odpovědná za provádění auditů procesů dodržování předpisů společnosti Incode.

Počáteční posouzení a audit budou dále přezkoumány a potvrzeny buď:

1. certifikovanou účetní firmou specializující se na audity počítačové bezpečnosti, nebo
2. Renomovaní odborníci na počítačovou bezpečnost jmenovaní určeným bezpečnostním poradním sborem.

Kromě toho musí společnost podstupovat pravidelné audity zaměřené na bezpečnost IT a implementaci PKI, aby byl zajištěn trvalý soulad s průmyslovými normami a regulačními požadavky.

7.3 Vztah mezi auditorem a auditovaným subjektem

Audity prováděné externí auditorskou firmou budou provádět subjekty, které jsou na auditované organizaci nezávislé. Nesmí dojít ke střetu zájmů, který by mohl narušit objektivitu nebo integritu procesu auditu.

7.4 Subjekty v procesu hodnocení

Oblasti, které mají být hodnoceny při hodnocení vyžadovaném podle právních předpisů o službách vytvářejících důvěru, jsou uvedeny v těchto předpisech, při jakémkoli jiném hodnocení jsou uvedeny v technických standardech, podle kterých se hodnocení provádí.

7.5 Opatření přijatá v důsledku nedostatků.

Incode musí přijmout okamžitá opatření, pokud při posuzování zjistí porušení požadavků uvedených v Certifikační prováděcí směrnici (CPS).

Pokud má porušení přímý dopad na důvěryhodnost certifikátu, bude dotčený certifikát okamžitě zrušen, aby byla zachována integrita a bezpečnost infrastruktury veřejných klíčů (PKI).

7.6 Oznámení o výsledku

Oznámení výsledků hodnocení podléhá požadavkům právních předpisů o službách vytvářejících důvěru a příslušných technických norem.

Výsledky hodnocení jsou oznamovány formou písemné zprávy, kterou hodnotitel předává generálnímu řediteli a bezpečnostnímu manažerovi společnosti Incode.

8 Další obchodní a právní záležitosti

8.1 Poplatky

8.1.1 Poplatky za služby

Poplatky za službu jsou dány smlouvou uzavřenou mezi Incode a konkrétní třetí stranou (může se jednat o paušální poplatek za časové období, platbu za úspěšné vytvoření elektronického podpisu apod.)

8.1.2 Poplatky za další služby

Nevztahují se na rozsah tohoto dokumentu.

8.1.3 Pravidla pro vracení poplatků

Nevztahuje se na rozsah tohoto dokumentu.

8.2 Finanční odpovědnost

8.2.1 Pojištění

Společnost Incode bude udržovat komerčně přiměřené krytí pro případy vad nebo opomenutí, a to buď prostřednictvím pojistných smluv s pojišťovnami třetích stran, nebo prostřednictvím mechanismů samopojištění.

Tyto nároky se však nevztahují na politické organizace.

8.2.2 Ostatní vlastnosti

Společnost Incode má finanční autonomii, aby mohla udržovat své operace a plnit své závazky. Kromě toho je právně odpovědná za řízení rizik spojených s odběrateli a důvěryhodnými partnery.

8.3 Důvěrnost obchodních informací

8.3.1 Rozsah důvěrných informací

Následující údaje o odběratelích budou důvěrné a soukromé:

- Údaje o žádostech CA, ať už schválené nebo neschválené.
- Údaje o registraci certifikátu předložené odběratelem.
- Podnikové soukromé klíče odběratele spravované v rámci PKI spolu s pověřeními potřebnými pro obnovení klíče.
- Transformační údaje, včetně úplných datových záznamů a auditních protokolů souvisejících s transformacemi.
- Údaje o auditu shromážděné v rámci procesů zabezpečení a dodržování předpisů.
- Plány obnovy po incidentech a haváriích zajišťující kontinuitu provozu a bezpečnost.
- Zásady řízení bezpečnosti, kterými se řídí provoz hardwaru, softwaru, správců a certifikačních služeb, jakož i dalších kritických bezpečnostních služeb.

Společnost Incode zajišťuje, aby tyto kategorie citlivých dat zůstaly chráněny a aby k nim měli přístup pouze oprávnění pracovníci v souladu s požadavky bezpečnostních politik a norem pro dodržování předpisů.

8.3.2 Informace nespadají do procesu utajení

Veřejné informace jsou označeny jako veřejné.

8.3.3 Odpovědnost za ochranu důvěrných informací

Společnost Incode zajišťuje bezpečnost soukromých informací tak, aby nebyly vystaveny nebo zpřístupněny třetí straně, s výjimkou případů, kdy si to vyžádají bezpečnostní agentury, orgány státní správy na ověřovacích službách.

8.4 Důvěrné osobní údaje

8.4.1 Zásady ochrany osobních údajů

Společnost Incode bude prosazovat přísnou politiku ochrany osobních údajů s cílem chránit informace o účastnících. Společnost Incode nezveřejní jméno ani jiné údaje související s žádostí o certifikát odběratele žádné externí straně, s výjimkou případů, kdy to vyžadují příslušné orgány v souladu s právními nebo regulačními povinnostmi.

8.4.2 Informace, které jsou považovány za soukromé

Všechny informace o odběrateli, které nejsou veřejně dostupné, včetně vydaných certifikátů, adresářů certifikátů a online seznamů CRL, jsou považovány za soukromé informace.

8.4.3 Informace, které nejsou považovány za soukromé

Informace obsažené v certifikátech a CRL vydaných společností Incode nejsou považovány za soukromé. Při žádosti o certifikát od společnosti Incode odběratel souhlasí s tím, že tyto informace budou součástí vydaného certifikátu.

8.4.4 Odpovědnost za ochranu soukromí

Společnost Incode je odpovědná za ochranu soukromí svých odběratelů a musí dodržovat zákony na ochranu soukromí ve své jurisdikci.

8.4.5 Upozornění a povolení k použití důvěrných informací

V případě, že si společnost Incode přeje použít soukromé informace, musí získat povolení od vlastníka těchto informací.

8.4.6 Poskytnutí soukromých informací v případě, že je to vyžadováno zákonem nebo pro administrativní procesy.

Společnost Incode odpovídá za zajištění soukromí informací o účastnících, s výjimkou následujících případů:

- Pokud je to vyžadováno příslušným právním orgánem nebo pokud je zveřejnění nařízeno platnými zákony a předpisy.
- Když je přístup k informacím požadován pro administrativní účely, například žádosti o ověření nebo žádosti o vytvoření dokumentu.

8.5 Práva duševního vlastnictví

Mezi smluvními stranami si společnost Incode ponechává veškerá práva, tituly a zájmy ke svým službám, softwaru a technologiím, včetně všech aktualizací, dokumentace, produktů, děl a dalších práv duševního a morálního vlastnictví, která s nimi souvisejí nebo která společnost Incode vytvořila, používá nebo poskytuje pro účely smlouvy s odběratelem. To zahrnuje kopie a odvozená díla založená na výše uvedených prostředcích.

Smlouva nepředstavuje prodej práv ke službám, softwaru nebo technologiím společnosti Incode. Namísto toho uděluje odběrateli právo používat tato aktiva v souladu s podmínkami smlouvy. Smlouva nepřevádí vlastnictví jakýchkoli práv ke službám, softwaru nebo technologii společnosti Incode nebo s nimi souvisejících, včetně všech aktualizací, dokumentace, produktů, děl a práv duševního vlastnictví, které zůstávají výhradním vlastnictvím společnosti Incode.

Kromě toho jsou název a logo společnosti Incode, jakož i názvy jejích produktů spojených s jejími službami, softwarem a technologií, ochrannými známkami a/nebo obchodními názvy společnosti Incode. K jejich používání nejsou udělována žádná práva ani licence, pokud to není výslovně uvedeno v obchodní smlouvě s odběratelem.

8.6 Prohlášení a záruky

8.6.1 Prohlášení a záruky CA

Společnost Incode neposkytuje žádné záruky, garance ani ujištění týkající se jejích produktů nebo služeb, s výjimkou těch, které jsou výslovně uvedeny v tomto dokumentu nebo v právně závazné smlouvě s odběrateli. Jakékoli popisy, prohlášení nebo implicitní závazky, které nejsou výslovně uvedeny v tomto dokumentu nebo ve formální smlouvě, by neměly být vykládány jako prohlášení o závazcích, schopnostech nebo zárukách služeb společnosti Incode.

Povinnosti a závazky společnosti Incode jsou přísně omezeny na ty, které jsou uvedeny v řídících smlouvách a zásadách.

8.6.2 Zástupce důvěryhodných partnerů a otázky záruk

Smlouva s důvěryhodným partnerem vyžaduje, aby důvěryhodný partner měl dostatek informací k tomu, aby se mohl rozhodnout na základě informací v certifikátu. Je odpovědný za rozhodnutí, zda informacím obsaženým v listině důvěřovat, či nikoli. Důvěryhodní partneři nesou odpovědnost za porušení ustanovení o povinnostech důvěryhodného partnera obsažených v CPS.

8.6.3 Zastupování ostatních zúčastněných stran a záležitosti týkající se ručení

Žádná ustanovení.

8.7 Zřeknutí se záruk

- Certifikační autorita nezaručuje, že její služby vydávání, ověřování a odvolávání certifikátů budou nepřetržité, bezchybné nebo trvale dostupné.
- Dostupnost služeb mohou ovlivnit technické poruchy, plánovaná údržba nebo události vyšší moci.
- Certifikační autorita neposkytuje žádnou záruku, že její certifikáty nebo služby budou vhodné pro jakýkoli konkrétní účel kromě těch, které jsou výslovně uvedeny v těchto CPS.
- Odběratelé a spoléhající se strany odpovídají za posouzení vhodnosti certifikátů pro zamýšlené použití.
- Všechny certifikáty a veškerý související software a služby jsou poskytovány "tak, jak jsou" a "tak, jak jsou k dispozici".
- V rozsahu povoleném zákonem mohou smlouvy o předplatném a smlouvy s důvěryhodnými partnery odmítnout záruku QTSP.

8.8 Omezení odpovědnosti

- Tento dokument podléhá systému místních a národních zákonů, pravidel, úprav, nařízení, vyhlášek a příkazů, ale není omezen ani omezen na vývoz softwaru, hardwaru a technických informací.
- Odpovědnost smluvních stran je upravena a omezena v souladu s podepsanou smlouvou.
- Oddělitelnost ustanovení: V případě, že bude některé ustanovení nebo dodatek tohoto dokumentu CPS shledáno soudem či jiným příslušným orgánem jako nevymahatelné, zůstávají ostatní ustanovení tohoto dokumentu nadále v platnosti a účinnosti.

8.9 Odškodnění

Reklamace / nárok na náhradu

Pokud to vyžaduje zákon, zákazník odškodní QTSP v následujících případech:

- Neplatné informace poskytnuté zákazníkem o vydavateli certifikátu.
- Chyba zákazníka odhalí prvky související s žádostí o certifikát, opomenutí z nedbalosti nebo s podvodnými účely.
- Selhání zákazníka při ochraně soukromého klíče, používání důvěryhodného systému nebo nepřijetí nezbytných opatření, aby se předešlo následkům.

- Používání jména zákazníka (mimo jiné včetně obecného jména, názvu domény nebo e-mailové adresy) porušuje práva duševního vlastnictví třetích stran.
- Smlouvy se zákazníky mohou obsahovat příslušné dodatky.

Problém odškodnění prodejců

Pokud to zákon umožňuje, smlouva se zprostředkovatelem vyžaduje, aby zprostředkovatel odškodnil společnost QTSP:

- Nesplnění povinnosti obchodního zástupce protistranou.
- Důvěra zástupce v digitální certifikát není v některých případech splněna.
- Chyba zástupce při kontrole stavu certifikátu za účelem zjištění, zda platnost certifikátu vypršela nebo zda je certifikát odvolán.
- Smlouva se zástupcem bude obsahovat řadu dalších povinností.

8.10 Doba platnosti a Ukončení platnosti

8.10.1 Termín

Tento dokument nabývá účinnosti okamžikem zveřejnění v archivu služby QTSP. Zveřejněním z archivu nabývají účinnosti i další změny tohoto dokumentu.

8.10.2 Ukončení

Tento dokument je platný, dokud není nahrazen novější verzí.

8.10.3 Účinek ukončení a poškození

Po vypršení platnosti dokumentu nebudou jednotlivé komponenty služby Incode omezeny platnými podmínkami vydaného certifikátu.

8.11 Soukromá výpověď a komunikace mezi stranami

Incode bude pro komunikaci se zúčastněnými stranami používat komerčně přijatelné metody komunikace. Pokud je navíc v podepsané smlouvě výslovně uveden konkrétní způsob komunikace nebo časový rámec, bude společnost Incode při veškeré příslušné komunikaci dodržovat podmínky uvedené v této smlouvě.

8.12 Změna

8.12.1 Postupy pro změny

Změny tohoto dokumentu bude provádět příslušné oddělení společnosti Incode. Tyto změny mohou být vydány buď jako:

1. samostatný dokument s podrobným popisem všech změn dokumentu, nebo
2. aktualizovaná verze dokumentu obsahující změny.

Na revidovanou nebo aktualizovanou verzi bude odkaz v sekci Oznámení a aktualizace v archivu služby QTSP, který je k dispozici na adrese https://psc.incode.com/qtsp-legal-repository/.

8.12.2 Případy, kdy je vyžadována změna identifikace objektu (OID)

Této politice není přiřazen žádný OID, vztahuje se na OID definované v kapitole 1.2. Jakákoli změna této Politiky vede k nové verzi dokumentu.

8.13 Řešení sporů

V rozsahu povoleném platnými právními předpisy musí všechny dohody s odběrateli a dohody se spoléhajícími se stranami obsahovat ustanovení o řešení sporů.

Pokud společnost Incode neschválí jinak, musí spory týkající se společnosti Incode probíhat podle strukturovaného procesu řešení, který se skládá z:

1. počáteční lhůta pro vyjednávání v délce šedesáti (60) dnů pro pokus o smírné řešení.
2. Pokud k řešení nedojde, může spor postoupit k soudnímu řízení u příslušného soudu.

Spory související s CPS

- Spory vyplývající z Certifikační prováděcí směrnice (CPS) bude řešit manažer CPS společnosti QTSP.

Smluvní spory

- Spory mezi společností QTSP, spolupracovníky a odběrateli musí být řešeny v souladu s podmínkami příslušné smlouvy.
- Spory mezi společností QTSP a jejími zástupci musí být řešeny podle podmínek smlouvy o spolupráci.
- Pokud se nepodaří dosáhnout řešení během 60denní lhůty pro jednání, může být záležitost postoupena soudu s příslušnou jurisdikcí.

8.14 Rozhodné právo

Provoz Incode musí být v souladu s právními předpisy České republiky, včetně:

- příslušnými vnitrostátními právními předpisy upravujícími činnost Incode
- zákony České republiky o elektronickém obchodování

Veškeré spory vyplývající z:

- podmínek a ustanovení těchto CPS
- činnosti CA a RA
- využívání služeb QTSP
- Vydání, přijetí nebo používání jakéhokoli certifikátu vydaného společností Incode

budou řešeny v souladu s platnými zákony České republiky a prostřednictvím postupů řešení sporů uvedených v příslušných smlouvách.

8.15 Dodržování platných právních předpisů

Veškeré činnosti související s touto CPS musí být v souladu s právními předpisy České republiky.

8.16 Smíšené podmínky

Neuplatňují se.

8.17 Ostatní ustanovení

Neuplatňují se.