incode psc

Certifikační politika a prováděcí směrnice

Verze	Upraveno podle	Provedené změny	Datum úpravy
1.0	LV	Obsah	12/2024
1.1	LV	Úprava OID, zahrnutí dalších e-mailových adres pro kontakt a upřesnění oddílu 4.10.1.7.	01/03/2025
1.2	LV	Nová definice oddílu 7, konkrétně pododdílu 7.1.	24/03/2025
1.3	LV	• Pro lepší orientaci byla doplněna čísla stránek. • Doplněny odkazy na příslušné předpisy v oddíle 1. • ID datové schránky je zařazeno do oddílu 2.2. • Rozšíření QCP-n již není možné zahrnout. • Upřesněn oddíl 1.4.1 týkající se použití certifikátu. Přidán odkaz na oddíl 7.1.4.	28/03/2025
1.4	LV	• Upřesnění definice v oddílech 6.1.1 a 6.2.1. • Pravopisná oprava v oddílu 6.2.3. • Upřesnění ohledně minimální doby uchování.	19/06/2025

OBSAH

1 Úvodní stránka

Tento dokument definuje zásady a principy, které společnost Incode Czech Republic s.r.o., kvalifikovaný poskytovatel služeb vytvářejících důvěru, dodržuje při vydávání kvalifikovaných certifikátů pro elektronické podpisy fyzickým osobám. Tyto certifikáty slouží jako klíčová součást zajištění pravosti, integrity a právní platnosti elektronických podpisů v souladu s příslušnými předpisy a oborovými normami.

Služba poskytování kvalifikovaných služeb vytvářejících důvěru vydávání kvalifikovaných certifikátů pro elektronické podpisy se opírá o algoritmus RSA. Tím je zajištěno, že vydávané certifikáty si zachovávají vysokou úroveň důvěryhodnosti a splňují nezbytné požadavky na bezpečné elektronické transakce.

Zákonné požadavky týkající se této 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 **Certifikační politika QTSP pro vydávání kvalifikovaných certifikátů pro elektronické podpisy fyzických osob** vypracovává společnost Incode Czech Republic, s.r.o., která definuje politiku řízení při poskytování kvalifikovaných certifikátů pro elektronický podpis. Vymezuje certifikační rámec pro vzdálené digitální podepisování, specifikuje způsob vydávání, správy, používání, rušení a opětovného vydávání digitálních certifikátů.

Požadavky CPS, které mají zajistit bezpečnost a integritu služby QTSP, se vztahují na všechny účastníky ekosystému služby. Tento dokument je strukturován v souladu s RFC 3647 a zároveň zohledňuje platné technické a jiné standardy a normy Evropské unie a příslušné zákony České republiky.

CPS slouží jako prohlášení o závazcích, které QTSP přebírá pro zákazníky využívající jeho službu ověřování digitálních podpisů. Je důležité si uvědomit, že CPS nepředstavuje právní dohodu mezi QTSP a jeho zákazníky, ale 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 QTSP, jakož i práva a povinnosti zákazníků, kteří se této služby účastní.
- Úroveň záruky spojenou s digitálním certifikátem vydaným 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 elektronických certifikátů a nevztahuje se na jiné služby poskytované QTSP.

1.2 Název a identifikace dokumentu

Tento dokument je identifikován identifikátorem objektu (OID).

OID této certifikační politiky je **1.3.6.1.4.1.22635891.1.2.1**, který byl přidělen v souladu s předpisy Národního centra pro certifikaci digitálních podpisů a podle standardního formátu číslování IANA:

1.3.6.1.4.1.[EnterpriseNumber].[TypeCA].[codeCA].[codeCAPS].

Kde:

- Identifikátor TypeCA = 1 (veřejný).
- Identifikátor QTSP codeCA= 2.
- Identifikátor codeCAPS = 1.

Tato struktura zajišťuje jedinečnou a standardizovanou identifikaci certifikační politiky v rámci digitálního podpisu.

Název dokumentu: QTSP Certifikační politika pro vydávání kvalifikovaných certifikátů pro elektronické podpisy fyzických osob.

1.3 Účastníci PKI

1.3.1 Kořenová certifikační autorita Incode

Kořenová certifikační autorita společnosti Incode (Root CA) je subjekt nejvyšší úrovně v rámci PKI společnosti Incode, který je odpovědný za vydávání a správu digitálních certifikátů. Funguje jako kotva důvěry pro celý ekosystém PKI a zajišťuje pravost, integritu a bezpečnost všech certifikátů, které jsou pod ní vydávány.

- Kořenová certifikační autorita Incode obvykle nevydává certifikáty přímo koncovým uživatelům.
- Podepisuje a vydává certifikáty pro zprostředkující (podřízené) certifikační autority, které pak vydávají certifikáty koncovým subjektům (např. jednotlivcům, organizacím nebo zařízením).

1.3.2 Zprostředkující nebo vydávající certifikační autorita Incode

Zprostředkující certifikační autorita Incode (Intermediate CA), známá také jako podřízená certifikační autorita, slouží jako most mezi svou kořenovou certifikační autoritou a certifikáty koncových entit v jejím PKI.

V architektuře Incode je vydávající certifikační autorita specifickým typem zprostředkující certifikační autority, která je přímo odpovědná za vydávání certifikátů koncových entit, jako jsou certifikáty TLS/SSL, digitální podpisy nebo ověřovací certifikáty.

1.3.3 Registrační autorita (RA)

Registrační autority (RA) slouží jako ověřovací subjekty odpovědné za ověřování žádostí o certifikát od zákazníků. Kvalifikovaný poskytovatel služeb vytvářejících důvěru (QTSP) a jeho určené pobočky působící jako RA dohlížejí na vydávání a správu životního cyklu digitálních certifikátů a zajišťují dodržování regulačních a bezpečnostních standardů.

Kromě toho mohou pobočky QTSP uzavírat smluvní dohody s firmami, které si přejí spravovat vydávání certifikátů samy. V takových případech mohou tito firemní klienti fungovat jako svá vlastní RA a ověřovat žádosti pro:

- Sebe sama, pro interní firemní použití.

- Jednotlivce nebo organizace v rámci jejich hierarchie, například zaměstnanci, partneři nebo dceřiné společnosti.

Aby byla zachována nestrannost a soulad s předpisy, musí operátor RA – odpovědný za schvalování provozu služby – pracovat bez střetu zájmů. Tento operátor nesmí být zapojen do procesu iniciace žádosti i schvalování, aby byla zajištěna integrita, neutralita a bezpečnost pracovního postupu vydávání certifikátů.

QTSP nebo jím pověřená přidružená společnost si ponechává celkovou odpovědnost za dodržování certifikačních standardů a přebírá plnou odpovědnost za platnost a bezpečnost všech vydaných certifikátů.

1.3.4 Odběratelé

Odběrateli kvalifikovaných služeb vytvářejících důvěru společnosti Incode mohou být fyzické nebo právnické osoby nebo systém, kterému společnost Incode vydává digitální certifikát. Odběratelé používají tyto certifikáty k provádění bezpečné komunikace, ověřování, šifrování a digitálnímu podepisování v rámci PKI. Odběratel nemusí být subjektem certifikátů, které má pod svou kontrolou.

1.3.4.1 Práva odběratele:

- Odběratelům jsou digitální certifikáty udělovány na základě typu požadovaného certifikátu.
- Digitální certifikát odběratele zůstává platný a aktivní po celou dobu jeho stanovené platnosti.
- Odběratelé jsou oprávněni používat služby digitálního podpisu a ověřovat digitální podpisy podle modelu vzdáleného digitálního podpisu v souladu s dobou platnosti uvedenou ve smlouvě o poskytování služeb.
- Odběratelé mají právo požádat o obnovení nebo zrušení platnosti svých digitálních certifikátů.
- Odběratelé mají právo potvrzovat všechny úkony související s jejich soukromým klíčem prostřednictvím svého registrovaného zařízení.
- Odběratelé mají právo obnovit, pozastavit nebo zrušit službu digitálního podpisu a ověřovat digitální podpisy podle modelu vzdáleného digitálního podpisu.

1.3.4.2 Povinnosti odběratele:

- Veškeré závazky odběratelů uvedené v jejich žádosti o digitální certifikát jsou přesné a pravdivé.
- Veškeré informace poskytnuté objednatelem a obsažené v digitálním certifikátu jsou správné a aktuální.
- Digitální certifikáty musí být používány pouze k zákonným účelům a musí být v souladu s Prohlášením o certifikační praxi (CPS) a předpisy stanovenými příslušnými orgány.
- Odběratelé nesmějí digitální certifikáty QTSP padělat ani s nimi manipulovat.
- Jakékoli změny údajů o odběrateli musí být neprodleně oznámeny QTSP prostřednictvím jím určených kontaktních bodů.
- Odběratelé musí požádat o zrušení digitálních certifikátů v případě chyb nebo bezpečnostních problémů, které mohou ovlivnit integritu digitálních certifikátů QTSP.

1.3.5 Spoléhající se strany

Spoléhající se strana je subjekt, který důvěřuje digitálnímu certifikátu nebo digitálnímu podpisu vydanému QTSP. V závislosti na předpisech upravujících používání digitálních certifikátů může, ale nemusí být odběratel QTSP. Spoléhající se strana:

- Zakládá důvěryhodnost na důvěře v digitální certifikát vydaný QTSP.
- Při ověřování elektronických transakcí rozhoduje, zda certifikát přijme, nebo odmítne.
- Musí dodržovat podmínky uvedené v dohodě o spoléhající se straně (RPA) spojené s certifikátem.

1.3.5.1 Práva příjemce

- Spoléhající se strana má právo ověřit správnost informací o odběrateli obsažených v digitálním certifikátu.
- Spoléhající se strana rozhoduje o dohodách a závazcích na základě ověřených informací v digitálním certifikátu a podrobností uvedených v dokumentu Certifikační prováděcí směrnice (CPS).

1.3.5.2 Povinnosti příjemce

- Přijímat oznámení od QTSP o podmínkách spolupráce pro třetí strany.
- Důvěřovat digitálnímu certifikátu poskytnutému QTSP pouze v případě, že je při kontrole a pravidelné aktualizaci platný.
- Důvěřovat digitálnímu certifikátu pouze v případě, že nebyl odvolán.
- Důvěřovat pouze mobilní aplikaci QTSP poskytované společností QTSP, která je oznámena na oficiálních webových stránkách služby QTSP.
- Neprodleně informuje CA/RA, pokud existuje podezření, že soukromý klíč byl odhalen, odcizen, upraven nebo zničen;
- CA/RA je třeba neprodleně informovat, pokud existuje podezření, že aplikace QTSP v telefonu vykazuje známky poškození, kopírování nebo je odhalen kód PIN.

1.3.6 Ostatní účastníci

Žádné ustanovení.

1.4 Používání certifikátu

Účastníci a spoléhající se strany musí při používání digitálních certifikátů přísně dodržovat příslušné dohody. Vzhledem k různé citlivosti informací chráněných veřejně důvěryhodnými certifikáty nese každá spoléhající se strana plnou odpovědnost za posouzení možných rizik a ověření platnosti certifikátu před tím, než mu začne důvěřovat.

1.4.1 Vhodné používání certifikátů

Digitální certifikáty vydané v souladu s touto CPS lze používat k účelům určeným v polích pro použití klíče (viz oddíl 7.1.4) a v polích pro rozšířené použití klíče definovaných v certifikátu. Citlivost informací, které budou digitálním certifikátem zpracovávány nebo chráněny, však závisí na prostředí, ve kterém je certifikát použit. Každá spoléhající se strana musí před rozhodnutím o použití digitálního certifikátu vydaného v souladu s tímto CPS posoudit prostředí aplikace a související rizika.

Certifikáty jsou vydávány pro různé bezpečnostní funkce, ale jejich použití podle této CPS je klasifikováno následovně:

- **Digitální podpisy** – zajišťují integritu a nepopiratelnost podepsaných dokumentů a transakcí.

Certifikáty musí být používány v souladu s ustanoveními právních předpisů v EU.

1.4.2 Zakázané použití certifikátů

Incode striktně zakazuje používání digitálních podpisů k odporu proti státu, narušování bezpečnosti, pořádku a ochrany, provádění pašeráckých aktivit nebo provozování jiných činností v rozporu se zákonem, společenskou morálkou.

Digitální certifikáty vydané v souladu s touto CPS nelze používat v následujících scénářích:

1. Jako podřízený subjekt certifikační autority Incode

a. Certifikáty vydané podle této politiky nesmí:
b. být použity k podepisování jiných certifikátů.
c. Vystupovat jako certifikační agenti.
d. Fungovat jako certifikační autorita.
e. Podepisovat seznamy odvolaných certifikátů (CRL).
f. Podepisovat služby vydávané v rámci protokolu OCSP (Online Certificate Status Protocol).

2. V aplikacích, které vyžadují bezpečný výkon bez selhání

Certifikáty se nesmí používat v systémech, kde by selhání mohlo způsobit vážné škody, včetně:

a. Provoz elektrických energetických zařízení.
b. Systémy řízení dopravy (pozemní, letecké atd.).
c. Navigační systémy letadel.
d. Jakýkoli jiný systém, jehož selhání by mohlo vést ke zranění, ztrátě života nebo poškození životního prostředí.

3. Tam, kde je to zakázáno zákonem

Certifikáty nesmí být použity v žádném scénáři, kde je jejich použití výslovně zakázáno platnými zákony nebo předpisy.

Kromě toho musí být certifikáty používány pouze k účelům k nim určeným. Mezi běžná omezení patří např:

- Certifikáty TLS se nesmí používat k podepisování dokumentů.
- Certifikáty pro podepisování kódu se nesmí používat pro šifrování e-mailů.
- Certifikáty koncových subjektů se nesmí používat k vydávání jiných certifikátů (vyhrazeno pouze pro certifikáty certifikačních autorit).

Tím je zajištěn soulad s bezpečnostními zásadami a zabráněno nesprávnému nebo neoprávněnému použití certifikátů.

1.5 Správa politiky

1.5.1 Oddělení Incode Odpovědné za politiku

Společnost Incode Czech Republic, s.r.o. spravuje, podporuje a dohlíží na CPS spolu s dokumenty souvisejícími s provozem Incode jako QTSP a jeho registračních autorit (RA).

Ředitel CA je jedinou osobou odpovědnou za rozhodování o dodržování postupů společnosti Incode Czech Republic, s.r.o. stanovených tímto dokumentem.

Přezkum postupů stanovených v tomto CPS 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 CPS a souvisejících zásad.

1.5.2 Kontaktní osoba

- Incode Czech Republic, s.r.o.
- Ředitel CA
- Pujmanové 1753/10a, Nusle, 140 00 Praha 4
- psc@incode.com, tsp@incode.com

1.5.3 Kontaktní osoba pro odvolání

- Incode Czech Republic, s.r.o.
- Zprostředkovatel odvolání
- Pujmanové 1753/10a, Nusle, 140 00 Praha 4
- revocations@incode.com, tsp@incode.com

Incode schválí CPS. Každá instance CPS má jedinečný identifikátor objektu (OID). Změny, aktualizace CPS jsou zaznamenány v dokumentu obsahujícím změny CPS nebo informace o procesu aktualizace a jsou zveřejněny na adrese https://psc.incode.com/qtsp-legal-repository/.

1.6 Definice a zkratky

1.6.1 Definice

Termíny	Vysvětlení
Číslo certifikátu QTSP	Je forma elektronického certifikátu vydaného společností QTSP.
Platný digitální certifikát	Je digitální certifikát, jehož platnost nevypršela, není pozastaven ani odvolán.
Digitální podpisy	Forma elektronického podpisu vytvořená transformací datové zprávy pomocí asymetrického kryptografického systému, kdy osoba vlastnící původní datovou zprávu a veřejný klíč podepisující osoby může určit, zda je přesná: - Výše uvedená transformace je generována pomocí správného soukromého klíče odpovídajícího veřejnému klíči ve stejném páru klíčů; - Integrita obsahu datové zprávy, protože je provedena výše uvedená transformace.
Služba ověřování digitálního podpisu	Je typ služby ověřování elektronického podpisu, kterou poskytuje poskytovatel certifikačních služeb digitálního podpisu. Certifikační služby digitálního podpisu zahrnují: - Generování klíčového páru včetně veřejného a soukromého klíče pro odběratele; - Vydávání, prodlužování, pozastavování, obnovování a rušení digitálních certifikátů odběratelů; - vedení online databáze digitálních certifikátů; - další související služby podle stanovených pravidel.
Asymetrický kryptosystém	Kryptografický systém schopný generovat klíčový pár sestávající ze soukromého a veřejného klíče.
Zámek	Posloupnost binárních čísel (0 a 1) používaná v kryptografických systémech.
Soukromý klíč	Klíč v klíčovém páru asymetrického kryptosystému používaný k vytváření digitálních podpisů.

Termíny	Vysvětlení
Veřejný klíč	Klíč v páru klíčů asymetrického kryptosystému, který se používá k ověření digitálního podpisu vytvořeného odpovídajícím soukromým klíčem v páru klíčů.
Digitální podpis	Zavedení soukromého klíče do softwarového programu, který automaticky generuje a připojuje digitální podpis k datové zprávě.
Podepisující	Účastník, který používá svůj vlastní soukromý klíč k digitálnímu podpisu datové zprávy pod svým jménem.
Příjemce	Organizace nebo jednotlivec, který obdrží datovou zprávu digitálně podepsanou podepisující osobou, použije digitální certifikát této osoby ke kontrole digitálního podpisu v přijaté datové zprávě a provádí činnosti a transakce. related.
Odběratelé	Organizace nebo jednotlivec, kterému je vydán digitální certifikát, přijímá digitální certifikát a uchovává soukromý klíč odpovídající veřejnému klíči zaznamenanému v tomto vydaném digitálním certifikátu.
Pozastavení digitálního certifikátu	Je dočasné zneplatnění digitálního certifikátu od stanoveného okamžiku.
Zrušení platnosti digitálního certifikátu	Je trvalé zneplatnění digitálního certifikátu od stanoveného okamžiku.

1.6.2 Zkratky

Symbol	Úplný název
SHIFT	Certifikační autorita / Certifikační autorita
AC	Řízení přístupu - Správa přístupu
Správce	Superadministrátorská práva pro Signer SAM
AES	Advanced Encryption Standard - Standard pokročilého šifrování
APNs	Služba Apple push notification - Služba zasílání zpráv společnosti Apple.
CC	Common Criteria
CGA	Certificate Generation Application – služba, která umožňuje podepisujícím osobám vydávat digitální certifikáty.
CM	Cryptographic Module (kryptografický modul) - zabudovaný v zařízení HSM.
CMS	Syntaxe kryptografické zprávy
CP	Certificate Policy / Politika certifikátu
CPS	Certification Practice Statement / certifikační prováděcí směrnice
CRLs	Seznamy odvolaných certifikátů / osvědčení o odvolaných certifikátech
CSP	Poskytovatel certifikačních služeb – služba, která umožňuje koncovému uživateli přiřadit veřejný klíč a identifikátor podepisující osoby.
CSR	Žádost o podepsání certifikátu – žádost o vydání digitálního certifikátu
DES	Standard šifrování dat / Standard šifrování dat
DNS	Systém doménových jmen
DTBS	Data To Be Signed – podepsaná data/dokumenty

Symbol	Úplný název
DTBS/CHEAP	Data To Be Signed Representation - DTBS/R je generován z DTBS pomocí hashovacího algoritmu.
EAL	Evaluation Assurance Level (úroveň zabezpečení hodnocení)
FCM	Firebase Cloud Messaging
HMAC	Hash-based Message Authentication Code (kód pro ověřování zpráv založený na hash)
HSM	Hardwarový bezpečnostní modul - hardware, který digitálně podepisuje a uchovává soukromý klíč.
Hlavní klíč HSM	Hlavní klíč hardwarového bezpečnostního modulu – hlavní klíč HSM se používá k šifrování dalších klíčů pro šifrování dat, která chce systém chránit. Tento hlavní klíč může dešifrovat ostatní klíče a také nepřímo dešifrovat data
HTTPS	Standard zabezpečených hypertextových transakcí
ICT	Informační a komunikační technologie
iDP	Identity Provider – poskytovatel autentizačních služeb
keyUUID	Univerzálně jedinečný identifikátor klíče – D.Signing_Key_ID je odkazován jako UUID klíče s jedinečným identifikátorem pro podpisový klíč koncového uživatele.
KTK	Key Transfer Key – klíč používaný k zašifrování jiných klíčů pro přenos při přenosu z komponent systému RSSP.
NTR	Národní obchodní rejstřík
DPH	Daň z přidané hodnoty

2 Odpovědnost za zveřejnění a uložení

2.1 Úložiště

Společnost Incode je odpovědná za udržování online vydávání a správování digitálních certifikátů. Úložiště certifikátů zajišťuje, že uživatelé mají v případě potřeby přístup k digitálním certifikátům vydaným QTSP a seznamům CRL. Kromě toho jsou dokumenty související se službou, včetně CPS, k dispozici na webových stránkách Incode nebo prostřednictvím kontaktní osoby definované v části Správa politik.

1. Nepřetržitá dostupnost a infrastruktura systému

Společnost Incode zajišťuje nepřetržitou dostupnost platných digitálních certifikátů a digitálních certifikátů s prošlou platností prostřednictvím správy vyhrazených funkčních serverů, které podporují:

- Seznamy odvolaných certifikátů (CRL)
- Odpovědi protokolu OCSP (Online Certificate Status Protocol)

Tyto servery jsou:

- umístěny ve veřejném síťovém oddílu s vysokorychlostním širokopásmovým připojením.
- jsou umístěny v datovém centru společnosti QTSP, které je vybaveno:
    - stabilním připojením k internetu
    - vysokorychlostní infrastrukturou
    - kontrolovanými podmínkami prostředí
    - stabilním napájením
    - specializovaným technickým týmem, který udržuje nepřetržitou dostupnost služeb a systému 24 hodin denně, 7 dní v týdnu.

2. Seznamy odvolaných certifikátů (CRL) a odpovědnost spoléhající se strany

CRL je seznam sériových čísel odpovídajících odvolaným digitálním certifikátům, který zveřejňuje poskytovatel služby QTSP. Spoléhající se strany zapojené do transakcí musí:

- Kontrolovat seznam CRL, aby si ověřily platnost certifikátu.
- Odmítnout všechny certifikáty uvedené v seznamu CRL.

Seznam CRL je uložen ve veřejném adresáři poskytovatele služeb a je generován:

- pravidelně v definovaném časovém rámci.
- ihned po odvolání nebo pozastavení platnosti certifikátu.

Systém Incode automaticky a pravidelně aktualizuje informace o platných a zněplatněných digitálních certifikátech. Seznam CRL je uložen ve vyhrazeném úložišti CRL, což zajišťuje nepřetržitý online přístup prostřednictvím protokolů, jako je HTTPS.

3. Uchovávání údajů o odvolání a odběratelích

Veškeré informace týkající se zneplatnění certifikátů, databází účastníků a digitálních certifikátů musí být uchovávány po dobu alespoň deseti (10) let od data pozastavení nebo zneplatnění certifikátu.

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.

Na webových stránkách Incode jsou k dispozici informace o:

1. Certifikátech certifikačních autorit a autoritách časových razítek.
2. Veřejné certifikáty.
3. Seznam zneplatněných certifikátů – odkaz na místo, kde lze získat seznam zneplatněných certifikátů.
4. Online Certificate Status Service – adresa URL, na které lze zadat dotaz OCSP.
5. Certifikáty a CPS QTSP včetně dřívějších verzí.
6. Další důležité informace.

Zrušení certifikátu CA z důvodu podezření na kompromitaci nebo skutečné kompromitace daného soukromého klíče oznámí společnost Incode na svých webových stránkách.

2.3 Četnost zveřejňování informací

Společnost Incode zveřejňuje informace následujícím způsobem:

- Digitální certifikát QTSP bude zveřejněn ihned po jeho přijetí odběratelem v souladu s postupy požadovanými QTSP.
- CRL je aktualizován nejméně každých 24 hodin a je automaticky generován systémem QTSP.
- Frekvence zveřejňování CPS: Nová verze CPS bude zveřejněna okamžitě po schválení, zatímco předchozí verze bude bezpečně archivována.
- Systém automaticky a průběžně aktualizuje seznam platných a zneplatněných digitálních certifikátů v rámci databáze a adresářového systému.
- Platnost certifikátů lze ověřovat online 24 hodin denně, 7 dní v týdnu prostřednictvím služeb OCSP a CRL, což zajišťuje nepřetržitý a spolehlivý přístup.

2.4 Řízení přístupu k úložišti

Incode nevyžaduje autentizaci pro přístup třetích stran k CRL, digitálním certifikátům QTSP a CPS prostřednictvím určené adresy pro zpřístupnění online.

Jakékoli úpravy CPS nebo digitálních certifikátů poskytovatelů služeb QTSP mohou provádět pouze autorizované orgány Incode.

3 Identifikace a ověřování

3.1 Pojmenování

3.2 Typy názvů

Veškeré identifikátory a konvence pojmenování používané pro držitele certifikátu jsou interpretovány a udržovány v souladu s platnými technickými specifikacemi a uznávanými průmyslovými normami, které jsou v současné době v platnosti. To mimo jiné zahrnuje standardizované formáty digitálních identit a komunikačních protokolů.

Konkrétně mohou typy názvů přiřazené subjektu zahrnovat rozlišené názvy X.500, identifikátory ve stylu e-mailu RFC-822 a názvy X.400, z nichž každý musí být používán

a chápán v souladu s příslušnými řídicími normami, aby byla zajištěna konzistence, interoperabilita a shoda v rámci příslušných systémů a rámců.

3.3 Potřeba smysluplných názvů

V rámci této CPS Incode stanovuje, že atribut Common Name držitele certifikátu musí být reprezentativní. To znamená, že musí spoléhajícím se stranám umožnit jednoznačnou identifikaci držitele certifikátu v transakcích, kde se certifikát používá k ověření.

Podporované atributy tohoto pole jsou uvedeny v oddíle 7.

3.4 Anonymita nebo pseudonymita odběratelů

Incode se snaží zajistit, aby digitální certifikáty, které vydává, umožňovaly identifikaci osob a organizací v elektronických transakcích a procesech. Proto **není povoleno používat** při žádosti o certifikát **pseudonymy**.

Kromě toho budou žádosti o anonymní certifikát automaticky zamítnuty certifikační autoritou Incode, protože nesplňují požadavky uvedené v předchozí části této CPS.

3.5 Pravidla pro interpretaci různých forem jmen

Různé formáty názvů, jako jsou rozlišené názvy X.500 a identifikátory ve stylu e-mailu RFC-822, jsou interpretovány podle zavedených mezinárodních standardů, aby byla zajištěna konzistence a interoperabilita. Názvy X.500 se řídí hierarchickou strukturou používanou v adresářových systémech a systémech PKI, zatímco názvy RFC-822 dodržují pravidla syntaxe pro adresování elektronické pošty. Tato pravidla interpretace umožňují spolehlivou identifikaci a komunikaci mezi různými systémy a platformami.

3.6 Jedinečnost názvů

Pole subjekt uvedené v digitálním certifikátu musí být jasné a jedinečné pro všechny digitální certifikáty vydané vydávající certifikační autoritou a musí odpovídat standardu X.500 pro jedinečnost jmen.

3.7 Rozpoznávání, ověřování a úloha ochranných známek

Kapitola Potřeba smysluplných názvů v této CPS definuje požadavky na názvy pro fyzické a právnické osoby, které žádají o digitální certifikát od certifikační autority vydavatele.

V důsledku toho bude každá žádost o certifikát podaná se jménem, které se liší od právně uznaného jména fyzické nebo právnické osoby, jak je uvedeno v jejich oficiálních podkladech, zamítnuta.

Kromě toho vydávající certifikační autorita v rámci svých postupů neověřuje vlastnictví obchodních názvů nebo registrovaných ochranných známek ani je neuvádí v digitálních certifikátech, protože jejich použití je podle této politiky výslovně omezeno.

3.7.1 Práva vydávající certifikační autority v případě sporů

Vydávající certifikační autority mají právo zamítnout nebo zrušit jakoukoli žádost o certifikát v případě sporu o název, aniž by jí tím vznikla jakákoli odpovědnost vůči žadateli.

3.8 Počáteční ověření totožnosti

3.8.1 Jak prokázat vlastnictví soukromého klíče

Všechny soukromé klíče jsou generovány interně v rámci procesu podepisování certifikačními autoritami 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.

3.8.2 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) převede 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, skenování MRZ), 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 vůči:
    - vládním databázím (pokud je to relevantní).
    - Seznamům sankcí a sledovaných seznamů (za účelem dodržování pravidel AML/KYC).
    - Předchozím pokusům o ověření s cílem odhalit anomálie nebo nesrovnalosti.
- Systém označuje potenciální podvody s identitou, duplicitní identity nebo podezřelé chování.

5. Vydávání a používání certifikátů

- Pokud je ověření úspěšné a je požadován jednorázový nebo krátkodobý certifikát, je vydán se specifickým:
    - Omezením platnosti (např. několik minut až několik dní).
    - Omezeným rozsahem použití (např. jedna transakce, jedna relace, podepisování dokumentů, ověřování).
- Pokud je ověření úspěšné a je požadován dlouhodobý certifikát:
    - Certifikát je vydán s dlouhodobým ověřením (např. měsíce až roky).
    - Certifikát je žadateli doručen prostřednictvím:
        - zabezpečeného stažení
        - mobilního nebo webového úložiště
        - integrace do kryptografického modulu nebo úložiště klíčů

6. Vypršení platnosti a automatické odvolání

- Krátkodobý certifikát 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).

3.9 Služby pro osoby se zdravotním postižením

- Incode poskytuje služby pro osoby se zdravotním postižením v souladu s platnými zákony České republiky.
- Incode usiluje o zajištění rovného přístupu ke službám poskytovaným společností na nejvyšší možné úrovni. Za účelem vytvoření rovných příležitostí ke službám Incode podniká veškeré možné a přiměřené kroky k tomu, aby poskytovala své služby bez překážek pro osoby se zdravotním postižením. Zvláště důležité je zajistit, aby klienti se zdravotním postižením dostávali služby přizpůsobené jejich speciálním potřebám, a to ve stejné kvalitě jako služby pro ostatní zákazníky.
- Incode spolupracuje s klienty na dosažení souladu s regulačními požadavky v CPS, které nejlépe vyhovují jejich individuálním potřebám.

3.10 Identifikace a autentizace pro žádosti o opětovné zadání klíčů

3.10.1 Identifikace a autentizace pro běžné žádosti o opakované zadání klíčů

Během doby platnosti digitálních certifikátů QTSP mohou odběratelé Incode požádat o vydání nového digitálního certifikátu s novým párem klíčů.

Opětovné vydání klíče před vypršením platnosti certifikátu se provádí podáním žádosti o opětovné vydání klíče u registrační autority QTSP (RA), která obsahuje nový veřejný klíč a je digitálně podepsána starým soukromým klíčem. RA zajistí, že osoba nebo organizace, která žádá o opětovné vydání klíče, je oprávněným odběratelem původního digitálního certifikátu.

Aby RA mohla schválit žádost odběratele o opětovné vydání klíče, musí ověřit, že totožnost a informace o odběrateli zůstávají nezměněné a přesné. Po opětovném vydání klíče certifikační autorita QTSP nebo RA znovu potvrdí a ověří odběratele podle stejných požadavků na ověření jako u původní žádosti o certifikát.

Pokud účastník ztratí soukromý klíč, musí požádat o zrušení certifikátu a postupovat podle příslušného postupu popsaného v následující části.

3.10.2 Identifikace a ověření pro opětovné vydání klíče po odvolání certifikátu

Digitální certifikáty, které byly odvolány nebo jejichž platnost vypršela, jsou trvale neplatné a nelze je za žádných okolností opětovně zadat, obnovit nebo aktualizovat. Každá nová žádost o certifikát po jeho zrušení nebo vypršení platnosti musí bez výjimky projít celým procesem prvotní registrace.

3.11 Identifikace a ověření pro žádost o odvolání certifikátu

Odběratelé mohou kdykoli a z jakéhokoli důvodu požádat o zrušení svých digitálních certifikátů. Aby se však předešlo neoprávněným žádostem o odvolání, Incode implementuje mechanismus ověřování, který ověřuje oprávněnost takových žádostí, zejména pokud jsou podávány elektronicky.

- Je-li žádost o zrušení certifikátu zaslána elektronicky, musí být totožnost odběratele ověřena pomocí digitálního podpisu.
- Pokud je žádost podepsána soukromým klíčem odpovídajícím veřejnému klíči žadatele, bude přijata a považována za platnou.

Podávání a zpracování žádostí o odvolání

- Všechny žádosti o zrušení digitálního certifikátu musí být podány buď QTSP, nebo jeho registrační autoritě (RA):
  - prostřednictvím schváleného online procesu, nebo
  - písemně podle předepsaného postupu odvolání.
- Certifikační autorita zaznamená a uchová všechny ověřené žádosti o odvolání a všechny odpovídající kroky v souladu s regulačními požadavky.
- Pokud je digitální certifikát odvolán, bude v systému uložen záznam o zneplatnění pro účely auditu a bezpečnosti.
- Po odvolání bude stav certifikátu aktualizován a zveřejněn v seznamu CRL a službě OCSP společnosti Incode.

Nouzové odvolání v případě bezpečnostních rizik

Pokud účastník zjistí nebo má podezření, že jeho soukromý klíč, kód PIN nebo mobilní aplikace byly odhaleny, ohroženy, zkopírovány nebo zneužity, musí to neprodleně

oznámit vydávající certifikační autoritě nebo RA pomocí komunikačních metod uvedených jako kontakt pro odvolání v části Správa politik této CPS.

Po obdržení takového oznámení musí vydávající certifikační autorita nebo RA znovu ověřit vlastnictví dotčeného digitálního certifikátu. Teprve po úspěšném ověření bude žádost o odvolání certifikátu zpracována a schválena.

4 Provozní požadavky na životní cyklus certifikátu

4.1 Žádost o certifikát

4.1.1 Kdo může podat žádost o certifikát?

O digitální certifikáty mohou žádat následující subjekty:

- jednotlivci nebo organizace, které splňují zákonné požadavky a podmínky stanovené v tomto dokumentu Certifikační politika a prováděcí směrnice (CPS) a mají oprávněnou potřebu používat digitální certifikát.
- Zákonný zástupce organizace, pokud je k tomu oprávněn a splňuje podmínky uvedené v příslušných zákonech a CPS.

Všechny žádosti o vydání certifikátu podléhají kontrole, ověření a autorizaci ze strany RA, který musí ověřit soulad s postupy a předpisy stanovenými v tomto CPS.

4.2 Registrace

Společnost Incode je prostřednictvím svých vydávajících CA a RA odpovědná za provedení procesu ověření totožnosti, jehož cílem je zabránit podvodům s identitou a vydávání se za někoho jiného, u každého žadatele o digitální certifikát v souladu s touto CPS, a to před vydáním příslušného certifikátu.

1. Odpovědnosti odběratele

Odběratelé musí v rámci procesu podávání žádostí:

- Dokončit proces registrace a ověření totožnosti.
- Poskytnout úplné a pravdivé informace ve všech požadovaných oblastech.
- Potvrdit odpovědnost za správnost předložených údajů a dodržování platných zásad.

2. Přezkoumání a ověření registračním orgánem (RA)

Vydávající certifikační autorita nebo RA jsou odpovědné za:

- Ověření platnosti registračních údajů odběratele a ověření jeho totožnosti.
- Rozhodování o přijetí nebo zamítnutí žádosti o digitální certifikát na základě výsledků ověření.

3. Proces vydávání po schválení

Pokud je žádost přijata, RA musí:

1. zaregistrovat informace o odběrateli v systému vydávání digitálních certifikátů QTSP.
2. Předložit žádost o vydání QTSP, který přistoupí ke generování a vydání digitálního certifikátu.
3. Vydat certifikát a provést proces vzdáleného digitálního podpisu.

4.3 Zpracování žádosti o certifikát

4.3.1 Proces identifikace a ověřování

Identifikace a ověřování se provádí podle popisu v kapitole 3.2.

4.3.2 Přijetí nebo odmítnutí vydání digitálního certifikátu

4.3.2.1 Podmínky pro vydání certifikátu

Společnost Incode schválí žádost o digitální certifikát pouze v případě, že jsou splněny všechny následující podmínky:

- Úspěšné ověření všech údajů o identitě a informacích týkajících se žadatele o digitální certifikát.
- Úplné zaplacení všech příslušných poplatků za vydání certifikátu, služby digitálního podpisu a ověřování digitálního podpisu podle modelu vzdáleného digitálního podpisu.

4.3.2.2 Podmínky pro zamítnutí žádosti o certifikát

Společnost Incode zamítne žádost o digitální certifikát za následujících podmínek:

- Selhání ověření totožnosti u všech požadovaných údajů o žadateli.
- Neúplné předložení nezbytných dokumentů požadovaných pro vydání certifikátu.
- Absence odpovědi žadatele na kontaktní žádost ve stanovené lhůtě.
- Nezaplacení požadovaných poplatků za vydání digitálního certifikátu.
- Důvodné obavy týkající se důvěryhodnosti nebo pověsti, kdy by vydání digitálního certifikátu žadateli mohlo negativně ovlivnit důvěryhodnost nebo spolehlivost společnosti Incode.

Tento proces zajišťuje, že digitální certifikáty obdrží pouze ověření a legitimní žadatelé, čímž je zachována integrita, důvěryhodnost a bezpečnost certifikačních služeb společnosti Incode.

4.3.3 Doba zpracování žádosti o certifikát

Společnost Incode odpovídá za včasné zpracování žádostí o digitální certifikát.

Pro dokončení zpracování žádosti o certifikát však není stanovena žádná pevná lhůta, ledaže:

- Ve smlouvě s účastníkem je stanoven konkrétní časový rámec.
- Vzájemná dohoda mezi stranami zapojenými do služby QTSP stanoví časový rámec.
- Certifikát je vydáván pro vzdálený podpis, kdy musí být doručen právě včas, aby byl proces dokončen.

Tím je zajištěna flexibilita při zpracování a zároveň je umožněno dodržet případné smluvní závazky.

4.4 Vydávání certifikátů

4.4.1 Činnosti prováděné certifikační autoritou při vydávání certifikátu

Jakmile je totožnost žadatele úspěšně ověřena a schválena, certifikační autorita pokračuje v procesu vydávání certifikátu. Ten zahrnuje vygenerování a podepsání certifikátu a zároveň zajištění toho, aby splňoval požadavky bezpečnosti, shody a politiky.

Ačkoli žádost o certifikát obsahuje informace poskytnuté žadatelem, Incode může některé údaje upravit na základě předem nakonfigurovaných profilů certifikátu. Tyto předem definované profily zajišťují:

- certifikáty dodržují konzistentní formáty a bezpečnostní parametry.
- Certifikáty jsou v souladu s pokyny CPS.
- Úpravy prosazují požadavky na délku klíče, kryptografické standardy a rozšíření certifikátu.

Mezi běžné předdefinované úpravy profilů certifikátů patří:

1. Informace o vydavateli. Certifikační autorita Incode nastaví DN vystavitele tak, aby odráželo její vlastní identitu.
2. Použití klíče a rozšířené použití klíče (EKU). Zajišťuje omezení certifikátu na autorizované funkce (např. digitální podpisy, ověřování serveru).
3. Doba platnosti certifikátu. Může být přepsán, aby odpovídal regulačním omezením nebo zásadám.
4. Přiřazení sériového čísla. Incode přiděluje jedinečné sériové číslo pro účely sledování a ověřování.
5. Distribuční místa CRL a OCSP. Incode vkládá odkazy na CRL a respondéry OCSP.

4.4.2 Oznámení odběrateli nebo žadateli o certifikát.

Incode informuje odběratele, jakmile byl jeho digitální certifikát úspěšně vytvořen, a poskytuje odběrateli přístup k ověření jeho dostupnosti. Platný certifikát bude odběrateli zpřístupněn nebo přístupný ke stažení po dokončení procesu vystavení.

V případě jednorázových nebo krátkodobých certifikátů používaných pro vzdálené digitální podpisy nebudou zasílána žádná oznámení.

4.5 Přijetí certifikátu

4.5.1 Úkony představující přijetí certifikátu

Odběratel potvrdí přijetí certifikátu tím, že:

- výslovným přijetím prostřednictvím e-mailového potvrzení nebo mechanismu digitálního přijetí.
- Implicitním přijetím, ke kterému může dojít, pokud odběratel použije certifikát k zamýšlenému účelu (např. podepsání dokumentu, provedení ověření).
- Od vydání certifikátu uplynulo patnáct kalendářních dnů.
- U procesů vzdáleného digitálního podpisu je přijetí potvrzeno před procesem podepisování, takže není třeba provádět žádné další kroky.

Pokud odběratel zjistí ve vydaném certifikátu chyby nebo nesrovnalosti, musí:

- Odmítnout certifikát a požádat společnost Incode o opravu.
- Požádat o odvolání, pokud je chyba zjištěna po vydání.

- Incode pak musí ověřit platnost vydání a v případě potřeby přistoupit k odvolání a novému vydání.

4.5.2 Zveřejnění certifikátu QTSP

Jakmile QTSP obdrží akceptaci vydaného digitálního certifikátu, Incode zveřejní platný certifikát ve svém online úložišti. Všechny platné certifikáty jsou uloženy a přístupné prostřednictvím:

- webového archivu, kde si odběratelé mohou ověřit vydané certifikáty.

4.6 Použití klíčového páru a certifikátu

4.6.1 Použití certifikátu a soukromého klíče odběratele

1. Aktivace soukromého klíče po přijetí certifikátu
   - Použití soukromého klíče odpovídajícího veřejnému klíči v digitálním certifikátu je povoleno až po přijetí certifikátu odběratelem.
   - Do přijetí nelze soukromý klíč legálně ani provozně používat.
2. Dodržování právních a smluvních předpisů

Digitální certifikát musí být používán striktně v souladu s:

- Podmínkami smlouvy o poskytování služeb.
- Zásadami uvedenými v této CPS.
- Platnými právními a regulačními ustanoveními upravujícími používání certifikátu.

3. Omezení používání klíčů
   - Použití digitálního certifikátu musí být v souladu s polem KeyUsage uvedeným v certifikátu.
   - Pokud určitá hodnota KeyUsage chybí, nelze certifikát pro daný účel použít.
     - Příklad: Pokud hodnota Digitální podpis není uvedena, nelze certifikát použít pro digitální podepisování.
4. Povinnosti odběratele
   - Odběratel je odpovědný za ochranu soukromého klíče před neoprávněným přístupem, ztrátou nebo zneužitím.
   - Soukromý klíč nesmí být použit, pokud:
     - Digitální certifikát vypršel nebo byl odvolán.
     - Vypršela platnost balíčku služeb digitálního podpisu a ověřování, jak je definováno ve smlouvě o poskytování služeb.
5. Soulad s certifikátem X.509
   - Certifikáty X.509 verze 3 jsou generovány v plném souladu s RFC 5280.
   - Rozšíření Key Usage v certifikátech X.509 v3 je nakonfigurováno následovně:
     - Kritická pole klíče jsou pro základní funkce certifikátu nastavena na hodnotu TRUE.
     - U certifikátů registrátorů koncových uživatelů mohou být některá pole klíčů povolena (TRUE) nebo zakázána (FALSE) na základě požadavků zásad.

		Certifikační autority	Digitální certifikáty pro jednotlivce a organizace
Kritičnost		TRUE	FALSE
0	digitalSingnature	Clear	Set
1	nonRepudiation	Clear	Set
2	keyEncipherment	Clear	Clear
3	dataEncipherment	Clear	Clear
4	keyAgreement	Clear	Clear
5	keyCertSign	Set	Clear
6	CRLSign	Set	Clear
7	encipherOnly	Clear	Clear
8	decipherOnly	Clear	Clear

Odběratel má plnou kontrolu nad všemi činnostmi souvisejícími se soukromým klíčem, včetně: generování soukromého klíče, generování žádosti o digitální certifikát, digitálního podpisu.

4.6.2 Použití veřejného klíče a certifikátu spoléhající se strany

Spoléhající se strany musí před použitím digitálních certifikátů vydaných společností Incode nezávisle posoudit jejich platnost a spolehlivost. Toto hodnocení zahrnuje následující kroky ověření:

1. Ověření vydání certifikátu společností Incode
   - Ověřením, že digitální certifikát byl vydán důvěryhodným certifikačním řetězcem společnosti Incode.
2. Ověření stavu odvolání certifikátu
   - Zkontrolováním nejnovějšího seznamu CRL nebo dotazem na službu OCSP se ujistěte, že digitální certifikát nebyl odvolán.
3. Potvrzení souladu použití klíče
   - Ověřte, zda je certifikát používán v souladu s rozšířením pole KeyUsage definovaným v certifikátu.

- Příklad: Pokud pole KeyUsage neumožňuje digitální podpisy, nesmí být certifikát používán k podepisování dokumentů.

4. Ujistěte se, že je certifikát používán k určenému účelu
   - Spoléhající se strana musí potvrdit, že:
     - Certifikát je používán pouze ke schváleným a zamýšleným účelům.
     - Použití certifikátu není zakázáno nebo omezeno podle CPS.
5. Ověřte stav celého řetězce certifikátů
   - Spoléhající se strana musí zkontrolovat stav digitálního certifikátu a všech certifikačních autorit, které se podílejí na jeho vydání.
   - Pokud je některý certifikát v řetězci certifikátů odvolán, spoléhající se strana musí:
     - posoudit důvěryhodnost všech digitálních podpisů vytvořených před odvoláním.
     - Uvědomit si, že další důvěřování odvolanému certifikátu představuje riziko.

4.7 Obnovení certifikátu

Obnovení certifikátu umožňuje odběrateli prodloužit platnost jeho digitálního certifikátu před vypršením jeho platnosti, čímž je zajištěno nepřetržité používání kryptografických funkcí, jako je ověřování, šifrování a digitální podpisy.

Při obnovení digitálního certifikátu je vygenerován nový pár klíčů, který zvyšuje bezpečnost a kryptografickou integritu.

Společnost Incode dává přednost obnově klíče před prostým obnovením, což znamená, že místo obnovení certifikátu pomocí stávajícího páru klíčů je pro obnovený certifikát vytvořen nový pár klíčů.

4.7.1 Oprávněnost a podmínky obnovení

Digitální certifikát je způsobilý k obnově, pokud:

- Stávající certifikát je stále platný (nevypršela jeho platnost ani nebyl odvolán).
- Nezměnily se identifikační údaje odběratele.
- Žádost o obnovu **je podána v rámci povoleného okna pro obnovu** (90 dní před vypršením platnosti certifikátu).

Digitální certifikát nelze obnovit, pokud:

- platnost certifikátu již vypršela nebo byl certifikát zrušen, místo obnovy je třeba podat novou žádost o certifikát.
- Pokud byl certifikát vydán jako jednorázový nebo krátkodobý certifikát.

4.7.2 Zpracování žádostí o obnovení digitálních certifikátů

Všechny žádosti o obnovení certifikátu se zpracovávají jako nové klíče certifikátu podle postupů uvedených v části 4.7. To znamená, že místo prostého prodloužení platnosti stávajícího certifikátu se stejným párem klíčů se vygeneruje nový pár klíčů a vydá se nový certifikát s aktualizovanou dobou platnosti.

4.7.3 Upozornění pro odběratele na vydávání nových digitálních certifikátů

Oznámení odběratelům o prodloužení platnosti je dokončeno v souladu s procesem obnovy klíče popsaným v části 4.4.

4.7.4 Podmínky přijetí obnovy digitálních certifikátů

Podmínky, kterými se řídí obnovení digitálních certifikátů, jsou popsány v oddíle 4.4 a musí být dodrženy v rámci procesu obnovení.

4.7.5 Oznámení o prodloužení platnosti digitálních certifikátů

Vydávající certifikační autorita nebo RA odpovídá za zveřejnění obnoveného digitálního certifikátu na veřejném úložišti.

4.8 Obnovení klíče certifikátu

Ve shodě s požadavky kapitoly 3.10.

4.8.1 Kdo může požádat o obnovení klíče certifikátu?

O obnovení klíče certifikátu je oprávněn požádat pouze odběratel certifikátu. Žádost musí být podána stejným postupem jako původní žádost o certifikát.

4.8.2 Zpracování žádostí o nový klíč pro certifikáty

Vydávající certifikační autorita, RA a certifikační autorita budou s žádostí o nový klíč certifikátu nakládat jako s původní žádostí o certifikát.

4.8.3 Oznámení o vydání nových certifikátů odběratelům

Ve shodě s požadavky kapitoly 4.4.2.

4.8.4 Oznámení o přijetí nového vydání klíčů certifikátů

Ve shodě s požadavky kapitoly 4.5.1

4.8.5 Vydání certifikátu, který byl vydán s novým klíčem QTSP

Ve shodě s požadavky kapitoly 4.5.2

4.8.6 Oznámení o vydání certifikátů QTSP jiným subjektům

Ve shodě s požadavky kapitoly 4.5.3

4.9 Změna certifikátu

Žádosti o modifikaci certifikátu jsou zpracovávány jako žádosti o prvotní certifikát.

4.9.1 Případy modifikace certifikátů

Digitální certifikát nelze modifikovat. Místo toho musí být starý certifikát odvolán a musí být vygenerován nový klíčový pár. Žádost o aktualizaci obsahu certifikátu musí být zpracována jako nové vydání certifikátu s nově vygenerovaným párem klíčů.

Zrušení stávajícího certifikátu je podmíněno vydáním a přijetím nového certifikátu. Starý certifikát proto zůstává v platnosti, dokud není úspěšně vydán a přijat nový certifikát. Teprve po přijetí nového certifikátu bude předchozí certifikát odvolán, aby byla zajištěna nepřetržitá dostupnost a bezpečnost.

4.9.2 Předmět žádosti o změnu certifikátu

Není specifikováno

4.9.3 Zpracování žádosti o změnu certifikátu

Není specifikováno

4.9.4 Oznámení o vydání nových certifikátů odběratelům

Není specifikováno

4.9.5 Podmínky pro přijímání změn předplatného

Není specifikováno

4.9.6 Vydávání upravených certifikátů z QTSP

Není specifikováno

4.9.7 Oznámení o vydání certifikátů QTSP jiným subjektům

Není specifikováno

4.10 Zrušení platnosti a pozastavení platnosti certifikátu

4.10.1 Zrušení platnosti certifikátu

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

Digitální certifikát může být odvolán z různých důvodů bezpečnosti, shody 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 zranitelnostech.
4. Dobrovolné odvolání certifikátu – Odběratel požádá o odvolání, protože již certifikát nepotřebuje.
5. Ztráta nebo zneužití soukromého klíče odběratele – Odběratel 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 zásady používání certifikátů (CP), Certifikační prováděcí směrnice (CPS) nebo smlouvy 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 služeb vytvářejících důvěru (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.

4.10.1.1 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.

4.10.1.2 Postup pro podání žádosti o zrušení certifikátu

Standardní žádost o zrušení certifikátu

- Odběratel musí zaslat e-mailovou žádost o odvolání certifikátu.
- E-mail musí být digitálně podepsán pomocí soukromého klíče certifikátu (pokud je certifikát stále platný a nevypršela jeho platnost).
- Tím je zajištěna pravost a zabráněno neoprávněným žádostem o odvolání.

Nouzová žádost o odvolání

- Pokud účastník 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.

4.10.1.3 Odkladná lhůta pro podání žádosti o zrušení

Pokud existuje podezření na kompromitaci klíče nebo jiný důvod pro odvolání uvedený v oddíle 4.10.1, musí odběratel 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.

Odběratel je výhradně odpovědný za ochranu svého soukromého klíče a za neprodlené ohlášení jakéhokoli podezření na kompromitaci.

Po zpracování žádosti o zrušení certifikátu je certifikační autorita odpovědná za okamžitou aktualizaci stavu certifikátu ve službách CRL a OCSP.

Certifikační autorita se řídí zásadami definovanými v tomto dokumentu Certifikační prováděcí směrnice (CPS), aby zajistila, že odvolaný certifikát bude řádně oznámen a zpřístupněn spoléhajícím se stranám.

4.10.1.4 Doba, ve které musí certifikační autorita zpracovat žádost o odvolání certifikátu

- Incode zpracovává žádosti o odvolání v přiměřené lhůtě, čímž zajišťuje včasnou aktualizaci stavu certifikátu.
- Neexistují žádné konkrétní časové požadavky na zpracování žádostí o odvolání, pokud nejsou výslovně dohodnuty s odběratelem ve smlouvě o poskytování služeb.
- Po zpracování je odvolaný certifikát aktualizován ve službách CRL a OCSP.

4.10.1.5 Mechanismy kontroly stavu certifikátu spoléhajícími se stranami

Před použitím digitálního certifikátu musí přijímající strana (spoléhající se strana) ověřit jeho stav pomocí nejnovějšího seznamu odvolaných certifikátů (CRL) nebo rovnocenného mechanismu ověření.

Incode poskytuje potřebné informace k ověření stavu certifikátu prostřednictvím služeb CRL a OCSP.

Odpovědnosti spoléhajících se stran

- Spoléhající se strany musí použít jeden z těchto mechanismů k ověření stavu certifikátu před tím, než mu začnou důvěřovat.
- OCSP je upřednostňovanou metodou pro ověřování v reálném čase, která zajišťuje okamžitou aktualizaci stavu odvolání.
- CRL slouží jako alternativa, pokud není vyžadováno ověření v reálném čase, a nabízí dávkové informace o odvolání.
- Neověřování stavu certifikátu může vést k bezpečnostním rizikům, například k důvěře v odvolaný nebo kompromitovaný certifikát, což může spoléhající se stranu vystavit podvodu, narušení dat nebo porušení předpisů.

4.10.1.6 Přidělení frekvence CRL

Seznam odvolaných certifikátů (CRL) je vydáván a aktualizován v pravidelných intervalech, aby bylo zajištěno včasné a spolehlivé ověření stavu certifikátu. Společnost Incode vydává aktualizované seznamy CRL nejméně jednou denně.

4.10.1.7 Maximální prodleva mezi generováním CRL

- Nový seznam CRL se u certifikátů koncových entit generuje nejméně jednou za 24 hodin.
- Seznamy CRL pro certifikáty vydávajících certifikačních autorit se vydávají nejméně každých 12 měsíců nebo při odvolání certifikátu.
- V případě mimořádného zrušení certifikátu se aktualizovaný seznam CRL zveřejní okamžitě.

4.10.1.8 Dostupnost protokolu OCSP

Server Incode OCSP je v provozu 24 hodin denně, 7 dní v týdnu, aby poskytoval nepřetržitý přístup k informacím o stavu certifikátu. Odpovědi OCSP jsou digitálně podepsány, aby byla zajištěna integrita a pravost.

4.10.1.9 Požadavky na online kontrolu stavu odvolání

Spoléhající se strany musí před použitím certifikátu ověřit jeho stav odvolání, aby byla zajištěna důvěryhodnost, bezpečnost a shoda.

4.10.1.10 Další formy oznámení o odvolání

Není specifikováno

4.10.2 Pozastavení platnosti certifikátu

Společnost Incode nenabízí pozastavení certifikátu. Pokud certifikát již není potřeba, je ohrožen nebo vyžaduje výměnu, musí být spíše odvolán než pozastaven. Jakmile je certifikát jednou odvolán, nelze jej obnovit a v případě potřeby musí být vydán nový certifikát.

4.11 Služba stavu certifikátu

4.11.1 Provozní charakteristiky

Stav certifikátu je zveřejňován ve veřejném úložišti Incode a je zpřístupňován prostřednictvím adresářů CRL a OCSP.

4.11.2 Dostupnost služby

Služba ověřování stavu certifikátu (distribuce OCSP a CRL) je k dispozici 24 hodin denně, 7 dní v týdnu, aby byl zajištěn nepřetržitý přístup pro spoléhající se strany.

Dostupnost služby však může být ovlivněna:

- plánovanými údržbovými činnostmi, které jsou předem oznámeny, aby se minimalizovalo narušení.
- nepředvídané výpadky sítě způsobené faktory, které společnost Incode nemůže ovlivnit, například přerušení provozu poskytovatele cloudových služeb.

Pokud je služba stavu certifikátu dočasně nedostupná, spoléhající se strany by měly:

- Po krátkém intervalu zopakovat žádost.
- Použít alternativní ověřovací mechanismus, je-li k dispozici.
- Před provedením transakcí založených na certifikátu vyhodnotit riziko.

QTSP se zavazuje minimalizovat výpadky a zajistit vysokou dostupnost služeb stavu certifikátu.

4.11.3 Volitelné funkce

Není specifikováno.

4.12 Ukončení předplatného

Předplatitelé mohou ukončit smlouvu o využívání certifikačních služeb Incode za následujících podmínek:

- Vypršení platnosti certifikátu bez obnovení
  - Pokud odběratel nechá svůj certifikát vypršet, aniž by požádal o jeho obnovení, smlouva o certifikační službě se automaticky ukončí na konci doby platnosti certifikátu.
- Dobrovolné vypovězení certifikátu bez náhrady
  - Pokud odběratel požádá o zrušení nebo stažení svého certifikátu před vypršením jeho platnosti a nepožádá o jeho nahrazení, smlouva se považuje za ukončenou okamžikem zrušení.

4.13 Prohledání a obnovení klíče

Společnost Incode neposkytuje služby key escrow a obnovy.

5 Řídicí, provozní a fyzická opatření

5.1 Opatření fyzické bezpečnosti

Operace QTSP a RA jsou prováděny v chráněném fyzickém prostředí, které má zabránit neoprávněnému přístupu, použití nebo vyzrazení citlivých informací a odhalit je. 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, zamčené 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 mazání 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.

Pověřenými 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 auditních záznamů 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 záznamů.

5.4.3 Doba uchovávání záznamů auditu

Minimální doba uchovávání záznamů z auditu je alespoň 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 alespoň 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 Změna klíče

Změna klíče certifikační autority Incode musí být provedena, když se blíží datum vypršení platnosti stávajících klíčů certifikační autority.

Provozovatelé certifikačních autorit musí zajistit, aby nebyl vydán žádný certifikát s datem platnosti, které přesahuje datum platnosti vydávající certifikační autority.

V tomto ohledu, jakmile je zbývající doba platnosti klíčů CA dva roky nebo méně, musí být zahájeny nezbytné postupy pro vygenerování nového páru klíčů. Stávající certifikační autorita a certifikáty, které vydala, zůstanou platné a účinné až do data vypršení platnosti certifikační autority.

5.7 Kompromitace a zotavení po havárii

5.7.1 Postupy pro řešení úniku 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.

5.7.2 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.

5.7.3 Schopnost zachovat kontinuitu provozu po havárii

Společnost Incode zajišťuje bezpečnostní opatření pro vývoj, testování a údržbu certifikačních autorit (CA) a registračních autorit (RA). 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 stanoví priority obnovy 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 umožnilo obnovu dat do 24 hodin od vzniku havárie.
- Systém obnovy po havárii bude podporovat alespoň následující základní funkce PKI:
    - vydávání digitálních certifikátů
    - odvolání certifikátu
    - zveřejňování informací o odvolání certifikátů
    - Podpora obnovy klíčů pro podnikové zákazníky využívající infrastrukturu správy PKI

- Databáze pro obnovu po havárii je pravidelně synchronizována s produkční databází, aby byla zajištěna konzistence dat.

5.8 Ukončení činnosti certifikační autority nebo RA

Ukončení činnosti certifikační autority nebo RA vyžaduje formální proces vyřazení z provozu, který zajistí bezpečný přechod, odvolání a archivaci 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
   - Informovat národní dozorový orgán o zahájení a dokončení oficiálních postupů ukončení služby..
   - Informování odběratelů a RA co nejdříve, aby měli dostatek času na přechod k alternativnímu poskytovateli.
   - Prostřednictvím veřejného oznámení ve velkém rozsahu transparentně sdělit ukončení provozu.
2. Ukončení vydávání certifikátů a pokračování podpůrných služeb
   - Po potvrzení ukončení provozu okamžitě ukončit vydávání nových digitálních certifikátů.
   - Pokračovat 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 odběratele, 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 kapitoly 5.5.2 CPS.
  - Provedení strukturovaného předání služby CA jiným CA, které fungují na základě stávající dohody, pokud je to relevantní.

6 Technická bezpečnostní opatření

6.1 Generování páru klíčů a nastavení

6.1.1 Vygenerování páru klíčů

1. Generování páru klíčů QTSP
   - Klíčový pár QTSP generuje ověřující autorita na počítačích s uzavřeným přístupem (nepřipojených k žádné síti), aby byla zajištěna maximální bezpečnost a izolace.
   - Kořenové a vydávající certifikační autority (Root CA a Issuer CA) generují své klíče v hardwarovém bezpečnostním modulu (HSM) splňujícím standard FIPS 140-2 úrovně 3.
2. Generování páru klíčů poskytovatele digitálního podpisu
   - V rámci modelu vzdáleného digitálního podepisování poskytovatel služby digitálního podpisu:
     - Generuje svůj vlastní pár klíčů, který tvoří self-signed certifikát.
     - Generuje pár klíčů odběratele, který zahrnuje veřejný a soukromý klíč.
3. Zabezpečení 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.

6.1.2 Předání soukromého klíče odběrateli

Při vydávání jednorázových nebo krátkodobých certifikátů certifikační autorita Incode nepředává ani neposkytuje soukromé klíče odběratelům. Tyto certifikáty jsou určeny pro jednorázové nebo časově omezené digitální podepisování a soukromý klíč zůstává bezpečně spravován v rámci důvěryhodné infrastruktury QTSP.

V případě dlouhodobých certifikátů bude dvojice klíčů zpřístupněna ke stažení na konci procesu ověřování totožnosti, jakmile bude úspěšně ověřena totožnost odběratele.

6.1.3 Předání veřejného klíče certifikační autoritě

Incode může zpracovávat žádosti o vydání certifikátu na základě žádosti o podepsání certifikátu (CSR) ve formátu PKCS#10 nebo paketů certifikátů přenášených v rámci relace zabezpečené protokolem SSL.

6.1.4 Přenos veřejného klíče certifikační autority důvěryhodným partnerům

Digitální certifikáty kořenové certifikační autority a certifikační autority vydavatele (obsahující veřejný klíč) jsou odběrateli doručeny prostřednictvím online transakce přes webový server certifikační autority. Tyto certifikáty je navíc možné stáhnout z důvěryhodného úložiště pro účely ověření a použití.

6.1.5 Velikost klíče

Páry klíčů musí mít dostatečnou kryptografickou sílu, aby se zabránilo kompromitaci soukromého klíče během používání. Systém Incode podporuje délku klíče až 8192 bitů pro RSA.

Současný standard QTSP vyžaduje pro klíče RSA minimální délku klíče 2048 bitů. Certifikáty s délkou klíče 1024 bitů nebo nižší nejsou kvůli bezpečnostním zranitelnostem akceptovány.

Pro svůj provoz musí certifikační autorita Incode vydávat certifikáty s použitím následujících velikostí klíčů, podpisových algoritmů a algoritmů hash.

	Velikost klíče (Nejméně)	Podpisový algoritmus	Algoritmus hašování (Nejméně)
Kořenová certifikační autorita	4096	RSA	SHA- 256
Vydávající certifikační autorita	4096	RSA	SHA-256
Autorita časového razítka	4096	RSA	SHA-256
OCSP Signer	4096	RSA	SHA-256
Certifikát koncového uživatele	2048	RSA	SHA-256

6.1.6 Generování parametrů veřejného klíče a kontrola kvality

Není specifikováno.

6.1.7 Účel použití klíče (jako v poli použití klíče X.509 v3)

Rozšíření Key Usage (Použití klíče) v certifikátech X.509 v3 definuje zamýšlené účely kryptografického páru klíčů a zajišťuje, aby byl certifikát používán pouze pro určené funkce.

6.1.7.1 Kořenová certifikační autorita - certifikát s vlastním podpisem

Kořenové certifikáty mají nejvyšší úroveň důvěryhodnosti v PKI a musí být chráněny před zbytečným používáním. V zájmu zachování bezpečnosti, integrity a shody je použití těchto soukromých klíčů přísně omezeno na následující scénáře:

- Kořenová certifikační autorita musí podepsat svůj vlastní certifikát, aby vytvořila důvěru v hierarchii PKI.
- Kořenová certifikační autorita může podepisovat certifikáty pro podřízené certifikační autority, což jim umožňuje vydávat certifikáty koncových entit.
- Kořenová certifikační autorita může vydávat certifikáty pro zabezpečení interních administrativních operací, včetně:
    - Provozní role CA (např. administrátoři, kryptografičtí pracovníci).
    - Interní zařízení systému CA používaná pro klíčové funkce PKI.
- Kořenová certifikační autorita může vydávat certifikáty pro respondéry OCSP, což umožňuje ověřování stavu certifikátu v reálném čase.

6.1.7.2 Certifikáty podezřelých osob

Rozšíření Key Usage v certifikátech odběratele definuje zamýšlené kryptografické funkce, které může soukromý klíč spojený s certifikátem vykonávat. Tím je zajištěno, že certifikát je používán pouze k určeným účelům, a pomáhá udržovat shodu a bezpečnost v rámci infrastruktury veřejného klíče (PKI).

Následující atributy použití klíče se běžně přiřazují certifikátům odběratele v závislosti na jejich účelu:

1. Digitální podpis
2. Potvrzení obsahu (nepopiratelnost)
3. Šifrování klíče (Key Encipherment)
4. Šifrování dat (Data Encipherment)
5. Dohoda o klíči (Key Agreement)

6.2 Ochrana soukromého klíče a kontrola metody šifrování

6.2.1 Standardy kryptografických modulů

Systém Incode CA využívá specializované HSM moduly s certifikací FIPS 140-2 úrovně 3, které jsou v souladu s platnými normami a jsou provozovány podle pokynů výrobce.

Tyto moduly HSM zajišťují všechny operace správy klíčů, včetně:

- generování klíčů
- správu klíčů certifikační autority
- podepisování digitálních certifikátů
- ověřování
- bezpečné ukládání a zálohování klíčů

Všechny operace související s klíči se provádějí výhradně v rámci HSM, což zajišťuje, že soukromé klíče nejsou nikdy vystaveny a nemohou k nim mít přístup neoprávněné osoby.

6.2.2 Řízení více soukromých klíčů

Incode implementuje pravidlo vícenásobné kontroly pro ochranu aktivačních údajů soukromého klíče certifikační autority. Tím je zajištěno, že citlivé kryptografické operace vyžadují účast více důvěryhodných osob.

Účast v tomto procesu je ověřována prostřednictvím autentizačního mechanismu založeného na kvóru, kde je pro schválení operací aktivace klíče, podepisování nebo obnovy nutné předložit práh počtu kvórum tokenů (n) z celkového počtu (m).

Žádný jednotlivec nemá plnou kontrolu nad přístupem ke klíčům nebo kryptografickým funkcím, což zajišťuje shodu s bezpečnostními standardy FIPS 140-2/140-3 úrovně 3 a zvyšuje bezpečnost, integritu a shodu s předpisy.

6.2.3 Soukromý klíč escrow

Incode neprovádí escrow soukromých klíčů.

6.2.4 Zálohování soukromých klíčů

HSM implementované certifikační autoritou společnosti Incode jako součást její infrastruktury PKI mají automatizované postupy zálohování, které se provádí každých 24 hodin nebo při každé změně clusteru HSM.

Všechny zálohy jsou šifrovány a lze je obnovit pouze v případě, že požadavek pochází od bezpečnostní skupiny, pod kterou byly vytvořeny, což zajišťuje kontrolované a autorizované obnovení.

Zálohy soukromých klíčů jsou chráněny stejnými bezpečnostními opatřeními jako aktivní klíče, což zaručuje důvěrnost, integritu a soulad s průmyslovými standardy.

Incode provádí zálohování soukromých klíčů CA za účelem obnovy dat po havárii, čímž garantuje nepřetržitý provoz a vysokou odolnost systému.

Soukromé klíče odběratelů se nezálohují.

6.2.5 Archivace soukromých klíčů

Po vypršení platnosti certifikátu kvalifikovaného poskytovatele služeb vytvářejících důvěru (QTSP) jsou s certifikátem spojené páry klíčů certifikační autority bezpečně uchovávány po minimální dobu deseti (10) let v hardwarových modulech vybavených silnými šifrovacími mechanismy, čímž je zajištěn soulad s požadavky této CPS.

Tyto páry klíčů certifikačních autorit nebudou po vypršení platnosti použity k žádným podpisovým operacím, pokud nebudou certifikáty certifikačních autorit oficiálně obnoveny podle ustanovení uvedených v CPS.

6.2.6 Ukládání soukromých klíčů v kryptografických modulech

Certifikáty kořenové certifikační autority Incode a certifikační autority vydavatele jsou uloženy v HSM, který je certifikován alespoň na úrovni FIPS 140-2 level 3.

6.2.7 Aktivace soukromého klíče

Postup aktivace soukromého klíče je popsán v oddíle 6.1.1. Jakmile je aktivace klíče dokončena, zůstává klíč aktivní po neomezenou dobu, pokud není výslovně deaktivován nebo odvolán v souladu s bezpečnostními zásadami.

6.2.8 Deaktivace soukromého klíče

Není specifikováno.

6.2.9 Zničení soukromého klíče

Odběratelé, kterým byl certifikát vydán, jsou plně odpovědní za zničení svého soukromého klíče.

U jednorázových nebo krátkodobých certifikátů určených k podepisování dokumentů se soukromý klíč zničí ihned po dokončení procesu podepisování. Tyto certifikáty se nikdy neukládají do žádného zařízení.

Soukromé klíče kořenové CA a vydávajících CA jsou bezpečně zničeny přímo v HSM pomocí procesu zeroizace, což zajišťuje, že nezůstávají žádná zbytková data a klíče nelze obnovit.

6.3 Další aspekty správy klíčových párů

6.3.1 Archivace veřejných klíčů

Společnost Incode uchovává a udržuje všechny veřejné klíče vydané svými kořenovými certifikačními autoritami a certifikačními autoritami vydavatele.

6.3.2 Provozní období certifikátů a období používání klíčových párů

Typ certifikátu	Maximální doba platnosti
Kořenová certifikační autorita	25 let
Vydávající certifikační autorita	15 let
OCSP Responder	2 roky

Autorita časových razítek	5 let
Kvalifikované certifikáty	Až 4 roky
Kvalifikované jednorázové nebo krátkodobé certifikáty	Doba trvání podpisové transakce

6.4 Kontrola počítačové bezpečnosti

6.4.1 Specifické technické požadavky na počítačovou bezpečnost

Incode zajišťuje, aby systémy obsahující software certifikační autority a datové soubory byly bezpečné a odolné proti neoprávněnému přístupu. Kromě toho prosazuje přísné řízení přístupu na hlavní server, 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.

6.4.2 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 správy systému je odpovědný za zpracování zpráv z kontrolních inspekcí a za navržení a realizaci opatření a plánů k odstranění zjištěných nedostatků.

6.5 Kontroly bezpečnosti v průběhu životního cyklu

6.5.1 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.

6.5.2 Řízení správy zabezpečení

Společnost Incode zavádí mechanismy a zásady pro kontrolu, monitorování a údržbu konfigurace své infrastruktury PKI.

6.5.3 Kontrola zabezpečení v průběhu životního cyklu

Není specifikováno.

6.6 Řízení bezpečnosti sítě

Funkce certifikační autority (CA) a registrační autority (RA) fungují v rámci zabezpečené sítě, 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 z bodu do bodu 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.

6.7 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.

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 jakékoliv změny v provozních procesech časového serveru.

Dále, pro zachování kryptografické integrity musí být algoritmus hašování (digest algorithm), který se používá k podepisování tokenů časových razítek, shodný s algoritmem používaným k podepisování certifikátu časového razítka. Toto zajišťuje konzistenci, bezpečnost a důvěryhodnost procesu časového razítkování.

7 Formát certifikátů, CRL a OCSP

7.1 Profil certifikátu

Profil certifikátu definuje strukturu, atributy a rozšíření digitálního certifikátu a určuje, jak by měl být používán v rámci Incode PKI. Zajišťuje shodu se standardy, jako je X.509 v3, a definuje potřebná pole a omezení na základě účelu certifikátu.

7.1.1 Základní pole certifikátu

Pole	Obsah
verze	v3
serialNumber	Jedinečné sériové číslo certifikátu
signatureAlgorithm	sha256withRSAEncryption (s parametry = NULL) minimálně
issuer	Rozlišující jméno vydávající certifikační autority

Pole	Obsah
platnost	
notBefore	Začátek doby platnosti certifikátu (UTC)
notAfter	notBefore + maximálně 90 minut
předmět	Viz oddíl 7.1.2
subjectPublicKeyInfo	
algoritmus	rsaEncryption
subjectPublicKey	Minimálně 2048 bitů
rozšíření	Viz oddíl 7.1.3
podpis	Zaručená elektronická pečeť certifikační autority vydavatele

7.1.2 Atributy pole Subject

Pole	Povinné	Poznámky
countryName	Ano	Kód země (ISO 3166), jediný výskyt
givenName	Ano	Jak bylo získáno z dokladu totožnosti poskytnutého při prvotním ověření totožnosti; jediný výskyt
surName	Ano	Získáno z dokladu totožnosti poskytnutého při prvotním ověření totožnosti; jediný výskyt

Pole	Povinné	Poznámky
Pseudonym	-	Tento atribut nesmí být v certifikátu uveden
serialNumber (1)	Ano	Jedinečná identifikace držitele certifikátu v systému certifikační autority, přímo spojená s procesem ověřování totožnosti.
serialNumber (2)	Ne	nepovinné; jedna z následujících možností: • IDCss-nnnnnnnn; • PASss-nnnnnnnn; kde ss je kód země (ISO 3166) vystavitele dokladu a nnnnnnn je číslo dokladu.
commonName	Ano	givenName + surName spojení řetězců; jediný výskyt
iniciály	Ne	Jediný výskyt
emailAddress	-	Tento atribut nesmí být uveden v primárním certifikátu
name	-	Tento atribut nesmí být obsažen v primárním certifikátu
generationQualifier	Ne	Jediný výskyt
organizationName	Ne	Povinné, pokud je zaměstnanec organizace; jediný výskyt

Pole	Povinné	Poznámky
		Pro jakoukoli jinou fyzickou osobu nesmí být tento atribut uveden.
organizationIdentifier	Ne	Povinný pouze v případě, že je uveden organizationName. Jedna z následujících možností: • NTRss-id, • VATss-id, • XX:ss-id; kde: ss je kód země (ISO 3166) státu, ve kterém je zaměstnavatel registrován (nemusí být shodný s názvem země); id je identifikační číslo organizace v příslušném registru, XX jsou dva znaky definované orgánem dané země, za nimiž následuje ":" (dvojtečka) - typ národního registru jiný než DPH a NTR
organizationalUnit	Ne	Povoleno více výskytů
title	Ne	Vícenásobný výskyt povolen
State	Ne	Jednorázový výskyt
localityName	Ne	Jeden výskyt

Pole	Povinné	Poznámky
		Pokud je uvedeno, musí být uvedeny také streetAddress a postalCode
streetAddress	Ne	Jediný výskyt Je-li zadáno, musí být uvedeny také localityName a postalCode
postalCode	Ne	Jediný výskyt Pokud je zadáno, musí být uvedeny také localityName a streetAddress
uniqueIdentifier	Ano	Jediný výskyt

7.1.3 Version

Kvalifikované certifikáty vydávané společností Incode jsou certifikáty verze 3 dle standardu X.509.

7.1.4 Rozšíření certifikátu

Rozšíření	Obsah	Komentáře
certificatePolicies		nekritické
.policyInformation (1)		
policyIdentifier	Viz oddíl 1.2	
policyQualifiers		
CPSUri	https://psc.incode.com/qtsp-legal-repository/	
userNotice	Jedná se o kvalifikovaný certifikát pro elektronický podpis v souladu s nařízením (EU) č. 910/2014.	
.policyInformation (2)		
policyIdentifier	• OID (QCP-n-qscd): 0.4.0.194112.1.2 (soukromý klíč je generován a uložen na QSCD).	
QCStatements		Nekritické
	0.4.0.1862.1.1	Id-etsi-qcs-QcCompliance
	0.4.0.1862.1.4	Id-etsi-qcs-QcSSCD; specifikováno, pokud je soukromý klíč generován a uložen na QSCD
	0.4.0.1862.1.5	id-etsi-qcs-QcPDS; odkaz (URI, https) na oznámení uživatele (PDS)
	0.4.0.1862.1.6	id-etsi-qcs-QcType
	0.4.0.1862.1.6.1	id-etsi-qct-esign
CRLDistributionPoints*	https://crl.tsp.incode.com/crls/qtsp/IncodeTechnologiesIssuerCAXYY.crl	Nekritické
authorityInformationAccess		Nekritické
Id-ad-ocsp*	https://ocsp.tsp.incode.com/ejbca/publicweb/status/ocsp	

Rozšíření	Obsah	Komentáře
Id-ad-calssuers*	https://crt.psc.incode.com/crts/qtsp/IncodeTechnologiesIssuerCAXYY.crt	
basicConstraints		Nekritické
CA	False	
keyUsage	digitalSignature, nonRepudiation	Kritické a povinné. Obě použití klíče musí být přítomna
extendedKeyUsage	ms-Document_Signing	Nekritické, povinné
subjectKeyIdentifier	Hash veřejného klíče (subjectPublicKey) v certifikátu.	Nekritické
authorityKeyIdentifier	Hash veřejného klíče certifikační autority vydavatele	
subjectAlternativeName		
rfc822Name	e-mailová adresa	Nepovinné; povoleno více výskytů

** XYY - X interní odkaz Incode Czech Republic s.r.o., který může nabývat hodnot F nebo M
YY představují poslední dvě číslice roku vydání certifikátu certifikační autority.

7.1.5 Číslo algoritmu

Algoritmy certifikátů jsou identifikovány pomocí identifikátorů objektů (OID), které specifikují kryptografické algoritmy pro digitální podpisy, hashování a správu klíčů v certifikátech X.509. Tyto identifikátory OID zajišťují standardizaci a interoperabilitu mezi různými implementacemi PKI.

Mezi algoritmy používané společností Incode patří:

Algoritmy RSA:

Algoritmus	OID
sha256withRSAEncryption	{iso(1) member- body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }

Algoritmy ECSDA

Algoritmus	OID
ecdsa-with-SHA224	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA224(3) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA256(3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA384(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA512(3) 4}

7.1.6 Název Formulář

Viz kapitola 3.1

7.1.7 Omezení jména

Neexistují žádná jiná omezení, než je uvedeno.

7.1.8 OID politiky certifikátu

Společnost Incode Czech Republic s.r.o. uvádí ve vydávaných certifikátech následující OID:

1. OID z CPS, jak je popsáno v kapitole 1.2.
2. OID příslušné certifikační politiky definované normou ETSI EN 319 411-2 pro certifikát vydaný fyzické osobě s ohledem na uložení soukromého klíče a deklarující, že certifikát je v souladu s eIDAS.

7.1.9 Použití rozšíření závazné politiky

Není specifikováno.

7.1.10 Sémantické zpracování pro rozšíření důležitých certifikátů

Není specifikováno

7.2 Profil CRL

Incode vytvoří a zveřejní CRL X.509 verze 2, který je v souladu s RFC 5280.

Verze	V2
signatureAlgorithm	sha256 minimálně sRSAEncryption
Vydavatel	Vydavatel CRL
thisUpdate	Uveďte datum a čas zveřejnění CRL.
nextUpdate	Uveďte datum a čas, kdy bude zveřejněno další CRL. (V případě kořenové CA maximálně 365 dní, v případě podřízené CA maximálně 24 hodin)
Odvolané certifikáty	Seznam odvolaných certifikátů
userCertificate	Sériové číslo zrušeného certifikátu
revocationDate	Datum a čas odvolání certifikátu
crlEntryExtensions	Viz oddíl 7.2.2
crlExtensions	Viz oddíl 7.2.2

podpis	Pokročilá elektronická pečeť vydavatele CRL

7.2.1 Verze

Incode vytvoří a zveřejní seznam odvolaných certifikátů CRL X.509 verze 2.

7.2.2 Rozšíření seznamu CRL a záznamů CRL

Rozšíření	Obsah	Komentáře
crlEntryExtensions		
CRLReason	Důvod odvolání certifikátu • Protože certifikační autorita nenabízí pozastavení platnosti certifikátu, nelze použít reasonCode certificateHold (6). • Jiný důvod než nespecifikovaný (0) se uvádí, pokud je certifikát zneplatněn.	Nekritický; nepovinný
crlExtensions		
authorityKeyIdentifier		
keyIdentifier	Hash veřejného klíče vydavatele CRL	Nekritické
CRLNumber	Jedinečné číslo CRL, které má být vydáno	Nekritické

7.3 Profil OCSP

Protokol OCSP se řídí datovou strukturou popsanou ve standardu IETF RFC 6960.

Verze	V1
ID respondenta	Název žadatele o OCSP
Vyrobeno v	Datum vydání
Odpovědi	Kód stavu (dobrý, odvolaný, neznámý) žádosti

7.3.1 Verze

Profil OCSP používá v požadavcích a odpovědích verzi 1, jak je popsáno v RFC 6960.

7.3.2 Rozšíření OCSP

Zatím neurčeno.

8 Audity shody a další posouzení

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.

8.1 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.

8.2 Totožnost a schopnosti auditora

Auditorská společnost slouží jako externí subjekt odpovědný za provádění auditů dodržování procesů společnosti Incode.

Počáteční posouzení a audit budou dále přezkoumány a potvrzeny buď:

1. certifikovanou účetní firmou, která se specializuje na audity počítačové bezpečnosti, nebo
2. Renomovanými odborníky na počítačovou bezpečnost jmenovanými příslušnou bezpečnostní poradní radou.

Navíc musí společnost podstupovat pravidelné audity zaměřené na IT bezpečnost a implementaci PKI, aby byla zajištěna trvalá shoda s průmyslovými standardy a regulatorními požadavky.

8.3 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.

8.4 Subjekty v procesu hodnocení

Rozsah auditu a požadavky na něj se liší v závislosti na auditovaném subjektu. Každý subjekt musí procházet pravidelnými audity výkonnosti v rámci každoročního přezkumu svých informačních systémů a dodržování zásad QTSP.

Audity RA (registrační autority):

- Odběratelé, kteří jsou podniky s prokázaným souladem s předpisy, se musí podrobit každoročnímu auditu.
- RA je auditována na základě požadavků QTSP s cílem zjistit výjimky nebo nedodržení zásad QTSP.

- Pokud je zjištěn nesoulad, musí RA provést nápravná opatření k zajištění souladu.

Inspekce Incode a inspekce spřízněných stran:

- Audit QTSP musí provádět nezávislý subjekt, který splňuje následující kvalifikační požadavky:
- Odborné znalosti v oblasti technologie infrastruktury veřejných klíčů (PKI).
- Znalost nástrojů a technik zabezpečení informací.
- Certifikace národní kořenové certifikační autority k ověření její autority.

8.5 Opatření přijatá v důsledku nedostatků

Incode musí přijmout okamžitá opatření, pokud posouzení odhalí porušení požadavků uvedených v dokumentu Certifikační prováděcí směrnice (CPS).

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

8.6 Oznámení o výsledku

Správa certifikační autority zveřejní výsledky na webových stránkách Incode s podrobnými informacemi o výsledku auditu, včetně případného porušení CPS.

9 Další obchodní a právní záležitosti

9.1 Poplatky

9.1.1 Poplatek za vydání certifikátu nebo obnovu certifikátu

Náklady na vydání nebo obnovu digitálního certifikátu vydaného certifikační autoritou Incode musí hradit odběratelé na základě poplatků definovaných v obchodních smlouvách uzavřených s jednotlivými odběrateli.

9.1.2 Poplatky za používání certifikátů

Odběratelé QTSP a RA nemusí platit za uložení certifikátů v archivu ani za službu, která poskytuje důvěryhodným partnerům informace o certifikátech online.

9.1.3 Poplatky za přístup k informacím o stavu certifikátů a jejich zneplatnění

Účastníkům služby Incode QTSP nejsou účtovány poplatky za vydávání seznamů CRL ani za přístup k informacím o stavu zneplatnění certifikátů vydaných certifikační autoritou Incode.

Zatímco základní kontroly stavu odvolání certifikátů jsou poskytovány bezplatně, Incode může účtovat poplatek za poskytování služeb OCSP nebo jiných informací o stavu certifikátů, zejména pokud využití přesáhne 1 000 dotazů denně.

9.1.4 Poplatky za použití dalších služeb

Předplatitelé mají k tomuto CPS přístup zdarma prostřednictvím:

- https://psc.incode.com/qtsp-legal-repository/.

Účastníci služby QTSP rovněž nemusí za přístup k CPS platit poplatek.

Použití tohoto dokumentu pro účely, jako je kopírování, další šíření, úpravy nebo vytváření odvozených děl, však podléhá právní dohodě s držitelem práv. Navíc, pokud jsou poskytovány jakékoli služby nad rámec uvedených služeb, budou náklady specifikovány v obchodní smlouvě uzavřené s odběratelem.

9.1.5 Pravidla pro vracení poplatků

Vrácení poplatku bude odběrateli poskytnuto pouze v případě, že je to výslovně uvedeno v obchodní smlouvě mezi společností Incode a odběratelem týkající se služby kvalifikovaného elektronického podpisu (QES) vydaného certifikační autoritou společnosti Incode.

Pokud nejsou ve smlouvě uvedeny žádné podmínky pro vrácení peněz, společnost Incode není povinna za službu vrátit peníze.

9.2 Finanční odpovědnost

9.2.1 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.

9.2.2 Případy, kdy QTSP provádí pojistné plnění

Společnost QTSP poskytuje pojistné plnění v následujících případech:

- Chyby způsobené certifikační autoritou, včetně technických závad, ke kterým došlo během procesu vydávání certifikátů, kdy je za ně odpovědná přímo certifikační autorita.
- Odškodnění bude poskytnuto v souladu s podmínkami uvedenými ve smlouvě s účastníkem.

9.2.3 Případy, na které se pojištění nevztahuje

Incode nenese odpovědnost v následujících případech:

- Použití certifikátů v rozporu s ustanoveními uvedenými v těchto CPS.
- Padělání dokumentů nebo podvodné činnosti související s používáním certifikátů.
- Nesprávná konfigurace zařízení nebo zneužití certifikátů, které nespadá do odpovědnosti certifikační autority.
- Ztráta, neoprávněná manipulace nebo zničení soukromého klíče odběratelem.
- Ztráta nebo vyzrazení kódu PIN chránícího soukromý klíč odběratelem.
- Chyby RA, včetně:
    - selhání ověřování
    - Nesprávná identifikace dat
    - Neshody v čísle certifikátu
    - Nesprávné hodnoty veřejného klíče
    - Neodeslání správné žádosti o certifikát

V případech, kdy dojde k chybám RA, přebírá RA plnou odpovědnost za odběratele a náhrada škody bude řešena podle podmínek smlouvy s odběratelem.

9.2.4 Další vlastnosti

Incode je finančně nezávislý, aby mohl udržovat svůj provoz a plnit své závazky. Kromě toho nese právní odpovědnost za řízení rizik spojených s odběrateli a důvěryhodnými partnery.

9.3 Důvěrnost obchodních informací

9.3.1 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, jak to vyžadují bezpečnostní politiky a normy pro dodržování předpisů.

9.3.2 Informace nespadají do procesu utajení

Informace vydané v digitálním certifikátu, seznamu CRL a protokolu OCSP nejsou považovány za důvěrné.

9.3.3 Odpovědnost za ochranu důvěrných informací

Společnost Incode zajišťuje bezpečnost soukromých informací, které nebudou vystaveny nebo zpřístupněny třetí straně, s výjimkou případů, kdy si to vyžádají bezpečnostní agentury, orgány státní správy na úseku autentizačních služeb.

9.4 Důvěrné osobní údaje

9.4.1 Zásady ochrany osobních údajů

Společnost Incode bude prosazovat přísnou politiku ochrany osobních údajů s cílem chránit informace o odběratelích. 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.

9.4.2 Informace, které jsou považovány za soukromé

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

9.4.3 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.

9.4.4 Odpovědnost za ochranu soukromí

Společnost Incode a její akreditované RA jsou odpovědné za ochranu soukromí svých odběratelů a musí dodržovat zákony na ochranu soukromí platné ve své jurisdikci.

9.4.5 Upozornění a povolení k použití důvěrných informací

V případě, že si společnost Incode nebo některý z jejích RA přeje použít soukromé informace, musí získat povolení od vlastníka těchto informací.

9.4.6 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 to vyžaduje příslušný státní orgán 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.

9.5 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.

9.6 Prohlášení a záruky

9.6.1 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 těchto CPS nebo v právně závazné smlouvě s odběrateli. Jakékoli popisy, prohlášení nebo implicitní závazky, které nejsou výslovně uvedeny v této CPS 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 ve smlouvách a zásadách.

Prohlášení společnosti Incode (jak je uvedeno v této CPS):

- CA funguje v plném souladu se svými CPS.
- CA se řídí průmyslovými standardy, včetně RFC 5280 a ETSI EN 319 411-2.
- Certifikační autorita udržuje a zveřejňuje službu CRL a OCSP, která poskytuje informace o stavu certifikátu v reálném čase.

- Certifikační autorita zpracovává žádosti o odvolání certifikátů neprodleně a zajišťuje, aby byly odvolané certifikáty zahrnuty do příští aktualizace CRL nebo odpovědi OCSP.
- Certifikační autorita zajišťuje, aby byli účastníci řádně informováni o svých právech, povinnostech a odpovědnosti při používání vydaných certifikátů.
- Certifikační autorita neodpovídá za zneužití certifikátů odběrateli nebo spoléhajícími se stranami nad rámec CPS.

Omezení odpovědnosti:
Incode nemůže zaručit, že její služby budou vhodné pro konkrétní účel odběratele nebo že služba bude bezchybná.

9.6.2 Prohlášení a záruky společnosti RA

RA jsou odpovědné za provádění identifikace a ověřování žadatelů o certifikát v přísném souladu s postupy uvedenými v této CPS.

Od RA se očekává, že bude:

- provádět ověřování totožnosti s náležitou pečlivostí a zajistí soulad s osvědčenými postupy v oboru a regulačními požadavky.
- Uplatňovat vhodné bezpečnostní kontroly, aby se zabránilo podvodům, krádežím identity nebo nesprávnému vydávání certifikátů.
- vést přesné záznamy o všech procesech ověřování pro účely auditu a dodržování předpisů.
- Jednat v souladu s právními a regulačními povinnostmi, které upravují ověřování totožnosti v prostředí PKI.

Neposkytuje však žádné další záruky nebo garance nad rámec toho, co je výslovně uvedeno v této CPS.

9.6.3 Prohlášení a záruky odběratele

Pokud odběratel požádá společnost Incode o vydání digitálního certifikátu, zavazuje se, že certifikát a s ním spojený soukromý klíč přijme, bude používat a chránit v přísném souladu s ustanoveními CPS platnými v době vydání.

Prohlášení odběratele jsou následující:

- Odběratel odpovídá za to, že soukromý klíč je bezpečně uložen a chráněn proti neoprávněnému přístupu, ztrátě nebo zneužití.
- Certifikát a soukromý klíč musí být používány pouze pro účely uvedené v CPS a nesmí být sdíleny nebo zneužity.
- Pokud odběratel ztratí soukromý klíč nebo má podezření, že byl jeho soukromý klíč kompromitován, musí to neprodleně oznámit společnosti Incode, aby iniciovala zrušení platnosti certifikátu.
- Tím je zajištěno, že certifikační autorita může včas přijmout opatření ke zrušení certifikátu, zabránit jeho dalšímu používání a informovat spoléhající se strany o jeho odmítnutí.
- Žádostí o certifikát se odběratel zavazuje dodržovat všechna ustanovení CPS, včetně jeho bezpečnostních politik, pravidel správy klíčů a postupů pro odvolání certifikátu.
- Nedodržení CPS může mít za následek povinné odvolání certifikátu společností Incode, aby byla zachována bezpečnost a důvěra v ekosystém PKI.

Od odběratele nejsou vyžadovány žádné další záruky:

- Pokud odběratel poruší požadavky CPS, společnost QTSP si vyhrazuje právo certifikát zrušit, aniž by vyžadovala další souhlas od odběratele.
- Odběratel nemůže od QTSP požadovat další záruky týkající se platnosti certifikátu, jakmile bylo požadováno nebo vynuceno jeho odvolání.

9.6.4 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 zodpovědný za rozhodnutí, zda informacím obsaženým v listině důvěřovat, či nikoli. Důvěryhodní partneři nesou odpovědnost za porušení ustanovení o povinnostech důvěryhodného partnera obsažených v CPS.

9.6.5 Zastupování ostatních zúčastněných stran a záležitosti týkající se ručení

Není specifikováno.

9.7 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.

9.8 Omezení odpovědnosti

- Tento dokument CPS podléhá systému místních a národních zákonů, pravidel, úprav, předpisů, nařízení a opatření, přičemž není omezen pouze na oblast exportu 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.

9.9 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.

9.10 Doba platnosti a Ukončení platnosti

9.10.1 Termín

Tento dokument nabývá účinnosti okamžikem zveřejnění v úložišti služby QTSP. Zveřejněním z úložišti nabývají účinnosti také další změny tohoto CPS.

9.10.2 Ukončení

Tento dokument je platný, dokud není nahrazen novější verzí.

9.10.3 Účinek ukončení a újma

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

9.11 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.

9.12 Změna

9.12.1 Postupy pro změny

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

1. samostatný dokument s podrobným popisem všech změn CPS, nebo
2. Aktualizovaná verze CPS, která zahrnuje změny.

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

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

Změnou položky v CPS dojde ke změně OID. Toto rozhodnutí provádí správce CPS Incode.

9.12.3 Jak a kdy oznámit

QTSP si vyhrazuje právo rozhodnout, zda je změna CPS nutná.

- QTSP shromažďuje a vyhodnocuje žádosti o změnu CPS od odběratelů služby QTSP.
- Pokud společnost QTSP zjistí, že je změna nutná, navrhne a provede změnu a předem ji oznámí v souladu s tímto oddílem.

Naléhavé bezpečnostní změny

Pokud QTSP zjistí bezpečnostní riziko, které by mohlo ohrozit službu QTSP, má právo okamžitě změnit CPS bez předchozího oznámení.

- Takové změny nabývají účinnosti okamžitě po zveřejnění.
- Společnost QTSP oznámí tuto změnu všem příslušným stranám co nejdříve po jejím provedení.

Období změn a zpětná vazba
Na změny CPS, které nejsou naléhavé, se vztahuje 15denní lhůta pro přezkum od data zveřejnění v úložišti služby QTSP.

Během této lhůty mohou účastníci služby QTSP předložit připomínky nebo námitky před uplynutím lhůty pro změnu.

9.13 Řešení sporů

V rozsahu povoleném platnými právními předpisy musí všechny účastnické smlouvy a smlouvy se spoléhajícími se stranami obsahovat ustanovení o řešení sporů.

Pokud společnost Incode neschválí jinak, musí se spory týkající se společnosti Incode řídit strukturovaným procesem 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 dokumentu 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.

9.14 Rozhodné právo

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

- příslušnými vnitrostátními právními předpisy upravujícími činnost Incode
- zákony České republiky v oblasti e-commerce

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.

9.15 Dodržování platných právních předpisů

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

9.16 Smíšené podmínky

Neuplatňují se.

9.17 Ostatní ustanovení

Neuplatňují se.