incode psc

Časové razítko QTSP
Politika / prováděcí směrnice

Verze	Upraveno podle	Provedené změny	Datum úpravy
1.0	LV	Obsah	02/2025

OBSAH

1. Úvod

V dnešním digitálním prostředí vyžadují organizace, které se spoléhají na informační systémy, elektronické transakce nebo strukturované datové rámce, důvěryhodné a ověřitelné důkazy pro zajištění pravosti, integrity a přesného načasování svých dat. Vytvoření spolehlivého a právně uznávaného spojení mezi okamžikem vytvoření dat nebo uskutečnění transakce a jejich certifikovaným časovým razítkem je nezbytné pro dodržování právních předpisů, bezpečnost a nepopiratelnost v digitálním prostředí.

Tato Politika a prohlášení o kvalifikovaných časových razítkách v souladu s normou ETSI EN 319 421 definuje zásady, provozní rámec a bezpečnostní opatření, kterými se řídí vydávání, ověřování a správa kvalifikovaných časových razítek. Tato časová razítka slouží jako nezvratný důkaz, že konkrétní data nebo transakce existovaly k určitému datu a času, a zajišťují tak auditovatelnost, shodu s předpisy a dlouhodobou integritu dat.

Dodržováním této politiky společnost Incode zajišťuje, že její služby časových razítek poskytují vysoce spolehlivý, kryptograficky bezpečný a právně přípustný mechanismus ověřování času, který podporuje organizace při udržování důvěryhodnosti a dodržování předpisů v oblasti digitálních transakcí.

2. Oblast působnosti

Toto Prohlášení o zásadách a postupech pro kvalifikovaná časová razítka (QTPS) stanoví požadavky a provozní pokyny pro společnost Incode jako kvalifikovaného poskytovatele důvěryhodných služeb (QTSP), který je odpovědný za vydávání kvalifikovaných digitálních časových razítek v souladu s mezinárodními standardy a regulačními rámci.

Definuje technické a procesní mechanismy, které zajišťují, že časová razítka jsou:

- kryptograficky bezpečná a odolná proti manipulaci.
- vydávána s přesným a ověřitelným časovým údajem spojeným s oficiálním zdrojem času.
- V souladu s RFC 3161, ETSI EN 319 421 a nařízením eIDAS (EU 910/2014).

Autorita časových razítek (TSA) funguje v rámci modelu infrastruktury veřejného klíče (PKI), což zajišťuje, že všechna časová razítka jsou generována, spravována a ověřována prostřednictvím bezpečného, kontrolovaného a auditovatelného prostředí.

3. Definice pojmů a zkratek

3.1 Termíny

Termín	Definice
Koordinovaný světový čas (UTC)	Časová stupnice založená na sekundě, jak je definována v doporučení ITU-R TF.460-6.
Spoléhající se strana	Právnická nebo fyzická osoba, která se spoléhá na časové razítko poskytnuté Incode jako QTSP.
Odběratel	Právnická nebo fyzická osoba, které je časové razítko vydáno a která je odpovědná za splnění všech závazků odběratele.
Časové razítko	Časové razítko je kryptograficky zabezpečený záznam, který potvrzuje existenci konkrétních dat v určitém časovém okamžiku.
Politika časového razítka	Soubor pravidel, který označuje použitelnost časového razítka se společnými bezpečnostními požadavky.
Autorita časových razítek (TSA)	Důvěryhodná autorita, buď TSP, nebo QTSP, která poskytuje služby časových razítek pomocí jedné nebo více TSU.
Jednotka časových razítek (TSU)	Soubor hardwaru a softwaru, který je spravován jako jednotka a má v daném okamžiku aktivní jediný klíč pro podepisování časových razítek.
UTC(K)	Časová stupnice realizovaná laboratoří "k" a udržovaná v těsné shodě s UTC s cílem dosáhnout ±100 ns.

3.2 Zkratky

Zkratka	Definice
BIMP	Bureau International des Poids et Mesures
CA	Certifikační orgán
HSM	Hardwarový bezpečnostní modul
PKI	Infrastruktura veřejných klíčů
QTSP	Kvalifikovaný poskytovatel důvěryhodných služeb
TIS	Služby vydávání časových razítek
TSA	TimeStamping Authority
TSP	Poskytovatel důvěryhodných služeb
TSU	Jednotka časového razítkování
UTC	Koordinovaný světový čas
VPN	Virtuální privátní síť

4. Obecné pojmy

4.1Koncepty obecných požadavků na politiku

Incode TSA provozuje své služby časových razítek v plném souladu s normou ETSI EN 319 421 a veškerými dalšími platnými předpisy, mimo jiné včetně:

- nařízení eIDAS (EU) č. 910/2014
- ETSI EN 319 401 (Obecné požadavky na politiku pro poskytovatele služeb vytvářejících důvěru).
- Vnitrostátní právní předpisy a osvědčené postupy v odvětví, které se vztahují na služby časového razítkování.

Incode TSA zajišťuje, že všechna vydaná časová razítka jsou právně uznávána a přípustná jako důkaz v rámci příslušných jurisdikcí.

4.1.1 Důvěryhodnost služby časových razítek

Incode TSA zajišťuje, aby služba časových razítek fungovala bezpečně, spolehlivě a důvěryhodně a poskytovala časová razítka, která zaručují:

- pravost a integritu dat označených časovými razítky.
- Ochranu proti neoprávněné změně nebo zfalšování časových razítek.
- Sledovatelnost k bezpečnému a uznávanému zdroji času.

Musí být zavedeny vhodné bezpečnostní kontroly, které odhalí, zmírní a zabrání jakýmkoli hrozbám, které by mohly ohrozit důvěryhodnost služby.

4.2 Služby časových razítek

Za poskytování důvěryhodných služeb časových razítek v souladu s touto politikou je odpovědná autorita pro časová razítka (TSA). Tyto služby jsou rozděleny do dvou základních složek:

4.2.1 Služba generování časových razítek

Služba generování časových razítek odpovídá za vydávání tokenů časových razítek v reakci na platné požadavky. Každý vydaný token časového razítka váže kryptografický hash předložených dat na přesný zdroj času, čímž zajišťuje, že existenci dat v určitém časovém okamžiku lze kryptograficky prokázat.

Služba Incode musí:

- zajistit, aby všechna časová razítka byla generována v souladu s požadavky RFC 3161 (Internet X.509 PKI Time-Stamp Protocol) a ETSI EN 319 421.
- Zaručit, že čas obsažený v tokenu je synchronizován s koordinovaným světovým časem (UTC) pomocí důvěryhodného zdroje času.

- Zajistit integritu, pravost a nepopiratelnost každého vydaného tokenu časového razítka.

4.2.2 Služba správy časových razítek

Služba správy časových razítek dohlíží na správu, bezpečnost a provozní integritu infrastruktury pro vydávání časových razítek. Tato služba zahrnuje následující činnosti:

- Synchronizaci zdrojů času: Incode TSA zajišťuje, aby jeho hodiny zůstaly přesné a sledovatelné podle UTC, přičemž pravidelná synchronizace a monitorování udržují soulad s požadavky na přesnost.
- Správa klíčů: Incode TSA odpovídá za bezpečnou správu svých soukromých podpisových klíčů, včetně jejich generování, ukládání a pravidelné rotace podle bezpečnostních zásad.
- Protokolování a monitorování auditů: Veškeré požadavky na časová razítka, vydání a systémové události jsou bezpečně zaznamenávány a auditovány, aby byla zachována shoda s předpisy.
- Dostupnost a kontinuita systému: Společnost Incode TSA implementuje mechanismy redundance a obnovy po havárii, aby zajistila nepřetržitou dostupnost služby časových razítek.

4.2.3 Odpovědnost a dohled

Společnost Incode TSA si ponechává plnou odpovědnost za řádný provoz a soulad služeb časového razítkování, a to i v případech, kdy jsou některé provozní aspekty delegovány na třetí strany. Jakékoli delegování musí být prováděno na základě smluvních dohod, které zajišťují soulad s touto politikou a příslušnými předpisy.

4.3 Autorita časových razítek

Za poskytování služeb časových razítek účastníkům odpovídá Autorita časových razítek. TSA nese komplexní odpovědnost za poskytování a správu těchto služeb, zajišťuje jejich integritu, přesnost a soulad se stanovenými zásadami.

Incode TSA spravuje jednu nebo více TSU, což jsou systémy zahrnující hardware a software určené ke generování a podepisování časových razítek jménem TSA. Každá jednotka TSU pracuje pod jedinečným klíčem pro podepisování časových razítek, čímž zajišťuje pravost a sledovatelnost vydaných časových razítek.

Incode TSA musí být jasně identifikovatelný v každém časovém razítku, které vydává, což poskytuje spoléhajícím se stranám jistotu ohledně zdroje a důvěryhodnosti časového razítka.

4.4 Odběratelé

Za odběratele služby TSA se považují všichni jednotlivci nebo organizace, kteří mají oprávněný zájem požadovat digitální časová razítka a kteří dokončili proces smluvní dohody se společností Incode o opakovaném přístupu ke službě.

Předplatitelé služby TSA uznávají a přijímají odpovědnost a závazky TSA, jakož i odpovědnost a závazky, které na sebe berou jako uživatelé služby a používání tokenů časových razítek, které si vyžádali a které jim byly poskytnuty.

4.5 Spoléhající se strany

Jednotlivci, organizace nebo systémy, které důvěřují časovým razítkům vydaným QTSP a jsou na nich závislé při ověřování pravosti, integrity a existence dat v určitém časovém okamžiku. Tyto strany nepožadují časová razítka přímo, ale spoléhají na ně jako na důkaz platnosti dat opatřených časovým razítkem pro právní, regulační nebo provozní účely.

4.6 Prohlášení o politice a praxi v oblasti časových razítek

Toto Prohlášení o politice a praxi v oblasti časových razítek popisuje minimální provozní požadavky na generování digitálních časových razítek a zajišťuje soulad s nařízením eIDAS (EU č. 910/2014) a příslušnými normami, jako jsou ETSI EN 319 421 a RFC 3161. Jeho hlavním cílem je zajistit, aby data opatřená časovými razítky zůstala ověřitelná, právně uznávaná a odolná proti manipulaci v průběhu času.

Podle nařízení eIDAS kvalifikované časové razítko poskytuje právní jistotu tím, že prokazuje existenci elektronických údajů v konkrétním čase, čímž zajišťuje shodu s článkem 41 tohoto nařízení. Jednou z jeho klíčových vlastností je vysoká přesnost, která zaručuje, že vydání časového razítka probíhá s přesností na jednu sekundu nebo lepší.

Prohlášení o zásadách a postupech vydávání časových razítek je k dispozici jako veřejný dokument na internetových stránkách společnosti Incode: https://psc.incode.com/qtsp-legal-repository/.

4.7 Shoda

Incode TSA formálně deklaruje shodu s touto politikou/prováděcí směrnicí ve všech vydávaných tokenech časových razítek. Každý token časového razítka výslovně odkazuje na tento dokument prostřednictvím identifikátoru popsaného v části 5.2, čímž je zajištěna sledovatelnost, konzistence a soulad se zavedenými standardy.

Jako kvalifikovaná autorita časových razítek působí společnost Incode v regulovaném rámci a dodržuje osvědčené postupy v oboru a právní požadavky na služby vytvářející důvěru. Aby si společnost Incode udržela svůj kvalifikovaný status, podstupuje pravidelné audity a kontroly shody prováděné příslušnými certifikačními orgány

a regulačními úřady. Tato hodnocení ověřují, zda provoz, bezpečnostní kontroly a poskytování služeb společnosti Incode trvale splňují povinnosti, zásady a technické standardy uvedené v tomto dokumentu.

Prostřednictvím průběžného monitorování, bezpečnostních hodnocení a dodržování regulačních rámců (například eIDAS, ETSI EN 319 421 a RFC 3161) společnost Incode zajišťuje, aby její služby časových razítek zůstaly spolehlivé, bezpečné a právně uznávané.

5. Politika časových razítek

5.1 Obecné požadavky

Politika časových razítek stanovuje zásady, provozní rámec a bezpečnostní požadavky upravující vydávání, správu a ověřování časových razítek společností Incode jako poskytovatelem důvěryhodných služeb (TSA). Tato politika zajišťuje, že časová razítka poskytují nezpochybnitelný důkaz o existenci elektronických údajů v konkrétním okamžiku, čímž je zajištěna shoda s normou ETSI EN 319 421, RFC 3161 a dalšími platnými předpisy.

5.2 Název a identifikace dokumentu

Tento dokument je identifikován identifikátorem objektu (OID).

OID pro tuto politiku časových razítek je **1.3.6.1.4.1.22635891.1.3.1**, přidělený v souladu s předpisy Národního centra pro certifikaci digitálních podpisů a podle standardního formátu číslování IANA:

1.3.6.1.4.1.[EnterpriseNumber].[TypeCA].[codeTSA].[codeTSAPS].

Kde:

- Identifikátor EnterpriseNumber = 22635891.
- Identifikátor TypeCA = 1 (veřejný).
- Identifikátor QTSP codeTSA = 3.
- identifikátor codeTSAPS = 1.

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

Název dokumentu: Časové razítko QTSP, Politika / prováděcí směrnice.

5.3 Uživatelé a použitelnost

Komunita uživatelů služby časových razítek Incode zahrnuje fyzické i právnické osoby, kategorizované jako odběratelé a spoléhající se strany. Odběratelé podléhají

smluvnímu ujednání se společností Incode o přístupu ke službě časových razítek. Incode nenabízí veřejnou službu časových razítek.

Služba časových razítek poskytovaná společností Incode se vztahuje na všechny případy, kdy je nutné prokázat, že elektronická data existovala v určitém časovém okamžiku a od té doby se nezměnila.

6. Zásady a postupy

6.1 Posuzování rizik

Společnost Incode provádí hodnocení rizik pro svou službu TSA, aby identifikovala, vyhodnotila a zmírnila rizika, která by mohla ovlivnit bezpečnost, spolehlivost a integritu její služby časových razítek. Toto hodnocení zajišťuje soulad s normami ETSI EN 319 421, ETSI EN 319 401 a dalšími platnými regulačními požadavky při zachování důvěry v proces časového razítkování.

Hodnocení rizik společnosti Incode zahrnuje mimo jiné kryptografická rizika, integritu zdroje času, dostupnost systému a rizika výpadku. Kromě toho zahrnuje vypracování bezpečnostního plánu a strategie pro účinné řízení, kontrolu, zmírnění a odstranění rizik.

6.2 Prohlášení o praxi poskytovatele důvěryhodných služeb

Incode definuje politiku časových razítek, která stanovuje komplexní soubor politik a provozních postupů sladěných s normami ETSI EN 319 401, ETSI EN 319 421 a nařízením eIDAS. Tyto politiky jsou formálně schváleny vedením a jsou zveřejněny a sděleny příslušným zúčastněným stranám a spoléhajícím se stranám.

Řídicí a provozní postupy TSA jsou formálně popsány v oddíle 7 této politiky a zajišťují, aby TSA Incode fungovala strukturovaně, transparentně a v souladu s předpisy.

Politika TSA je zpřístupněna účastníkům a spoléhajícím se stranám prostřednictvím internetových stránek společnosti Incode na adrese https://psc.incode.com/qtsp-legal-repository/.

6.2.1 Platné hashovací algoritmy

Incode TSA používá kryptograficky bezpečné hashovací algoritmy, které jsou v souladu s normou ETSI EN 319 421 a dalšími platnými předpisy, aby byla zajištěna integrita a pravost dat s časovým razítkem. Vybrané hashovací algoritmy musí splňovat průmyslové normy pro odolnost proti kolizím, odolnost proti předobrazu a odolnost proti druhému předobrazu, aby se zabránilo manipulaci nebo padělání časových razítek.

Pro použití ve službě časových razítek jsou schváleny následující kryptografické hashovací funkce:

- SHA-256
- SHA-384
- SHA-512

6.2.2 Přesnost času

Incode zajišťuje, aby čas používaný pro generování časových razítek zachovával přesnost v rozmezí ±1 sekundy vzhledem k UTC. Časový signál je poskytován národní časovou autoritou Stratum-1.

Incode udržuje tuto přesnost za všech provozních podmínek, včetně scénářů špičkového zatížení, kolísání latence sítě a poruch systému.

6.2.3 Omezení používání služby

Nebyla deklarována žádná omezení.

6.2.4 Povinnosti účastníků

Odběratelé služby časových razítek poskytované společností Incode jsou povinni dodržovat povinnosti stanovené v těchto zásadách, aby bylo zajištěno bezpečné a správné používání časových razítek. Mezi tyto povinnosti patří např:

- Odběratel musí dodržovat požadavky uvedené v těchto zásadách pro časová razítka, jakož i veškeré další podmínky uvedené ve smluvním ujednání s TSA.
- Odběratel musí používat časová razítka pouze k zamýšleným a zákonem povoleným účelům.
- Odběratel odpovídá za to, že údaje předložené k časovému razítku jsou přesné, úplné a že s nimi nebylo před předložením manipulováno.
- Odběratel musí zajistit, aby údaje opatřené časovými razítky byly řádně uloženy a udržovány tak, aby se zabránilo jejich neoprávněným změnám po vydání.
- Odběratel odpovídá za ověřování vydaných časových razítek, aby byla zajištěna jejich pravost, integrita a soulad s příslušnými normami.
- Odběratel musí používat schválené ověřovací mechanismy k potvrzení platnosti časových razítek obdržených od TSA.
- Pokud jsou zjištěny jakékoli nesrovnalosti nebo nesoulad, musí je odběratel neprodleně nahlásit TSA.
- Pokud se odběratel dozví o jakémkoli narušení bezpečnosti, neoprávněném použití nebo potenciálním ohrožení souvisejícím se službou časových razítek, musí to neprodleně oznámit TSA.
- Předplatitel musí spolupracovat s TSA při vyšetřování a řešení incidentů souvisejících s bezpečností.
- Odběratel je odpovědný za to, že záznamy s časovými razítky budou uchovávány po požadovanou dobu v souladu s platnými předpisy a obchodními potřebami.

- TSA neodpovídá za uchovávání dat s časovým razítkem po skončení samotného vydaného záznamu s časovým razítkem.

6.2.5 Povinnosti spoléhajících se stran

Aby bylo zajištěno správné používání a důvěryhodnost časových razítek vydaných společností Incode, musí spoléhající se strany dodržovat následující povinnosti:

- Spoléhající se strany musí časová razítka před tím, než jim začnou důvěřovat, ověřit pomocí vhodných kryptografických ověřovacích mechanismů.
- Ověření by mělo potvrdit, že:
  - časové razítko bylo vydáno autoritou Incode pro časová razítka (TSA).
  - časové razítko je kryptograficky neporušené a nebylo změněno.
  - Digitální podpis TSA je platný a nebyl odvolán.
- Spoléhající se strany by měly používat důvěryhodné nástroje nebo služby pro ověřování časových razítek, aby zajistily soulad s průmyslovými normami a předpisy.
- Spoléhající se strany musí dodržovat podmínky uvedené v těchto zásadách časového razítka.

6.2.6 Ověřování časových razítek

Spoléhající se strany musí ověřit časové razítko potvrzením, že:

- bylo vydáno společností Incode TSA.
- Časové razítko je kryptograficky platné, což zajišťuje, že související údaje nebyly od doby razítkování změněny.
- Digitální podpis Incode TSA je platný, nevypršela jeho platnost a nebyl odvolán.
- Časové razítko odpovídá normě ETSI EN 319 421 a všem platným předpisům.

6.2.6.1 Ověření dlouhodobého časového razítka

Dlouhodobé ověřování časových razítek zajišťuje, že data s časovým razítkem zůstávají platná, důvěryhodná a právně přípustná po delší dobu, a podle přílohy D normy ETSI EN 319 421 lze ověřování časových razítek provádět i po skončení platnosti certifikátu TSA, přičemž se bere v úvahu:

1. soukromé klíče TSA nebo TSU nebyly kompromitovány.
2. Algoritmy hashovacích funkcí a digitálních podpisů se nestaly zranitelnými.
3. Velikost podpisového klíče je stále podporována touto politikou a CPS.

6.2.7 Rozhodné právo

Jakékoli nároky týkající se Incode TSA nebo jím vydaných časových razítek by měly být řešeny způsobem uvedeným v části 9.13 (Řešení sporů) CPS.

6.2.8 Dostupnost

Společnost Incode se zavazuje poskytovat vysoce dostupnou a spolehlivou službu časových razítek, aby zajistila nepřetržitý přístup pro účastníky a spoléhající se strany. Incode TSA implementuje robustní infrastrukturu, mechanismy redundance a strategie převzetí služeb při selhání, aby byla zachována kontinuita provozu a minimalizovány výpadky.

Incode TSA je nasazena tak, aby splňovala následující cíle dostupnosti:

- Míra dostupnosti nejméně 99,9 %, s výjimkou plánované údržby nebo nepředvídaných incidentů.
- Požadavky na časová razítka musí být zpracovány v rámci definovaných výkonnostních měřítek a musí být zajištěno minimální zpoždění.
- V případě selhání systému by měl být spuštěn mechanismus převzetí služeb při selhání.

6.3 Podmínky

Všeobecné obchodní podmínky popisují rozsah, omezení a povinnosti spojené se službou časových razítek poskytovanou společností Incode.

Tyto zásady definují omezení služby časového razítkování, jakož i odpovědnost a povinnosti:

- Incode TSA poskytující službu.
- Odběratelů, kteří požadují časová razítka.
- Spoléhajících se stran, které ověřují vydaná časová razítka a jsou na nich závislé.

Zatímco tato politika stanoví obecný provozní a právní rámec, další podmínky mohou být uvedeny ve smluvních ujednáních potřebných pro zřízení a průběžné poskytování služby.

6.4 Politika bezpečnosti informací

Jako součást svého systému řízení bezpečnosti informací (ISMS) společnost Incode vypracovala a zavedla komplexní politiku bezpečnosti informací. Tato politika integruje

všechny bezpečnostní zásady, postupy, standardy a pokyny, které společnost Incode uplatňuje pro zabezpečení svých důvěryhodných služeb.

Některé klíčové bezpečnostní kontroly použitelné pro TSA jsou popsány v oddílech CPS:

- Sekce 5 - Řídicí, provozní a fyzické kontroly
- Oddíl 6 - Technické bezpečnostní kontroly
- Oddíl 8 - Audity shody a další hodnocení

Politika bezpečnosti informací byla formálně schválena vedením společnosti Incode a byla vzata na vědomí a sdělena všem zaměstnancům.

6.5 Povinnosti TSA

6.5.1Obecně

Žádné ustanovení

6.5.2 Povinnosti TSA vůči účastníkům

Incode TSA je odpovědná za zajištění bezpečného, spolehlivého a vyhovujícího provozu své služby časových razítek. Následující povinnosti definují závazky TSA vůči odběratelům a zajišťují důvěryhodnost, integritu a právní spolehlivost vydávaných časových razítek.

- Vydávat časová razítka v souladu s touto politikou a normou ETSI EN 319 421 a platnými právními rámci.
- Zajistit, aby časová razítka byla digitálně podepsaná a odolná proti manipulaci, a to pomocí kryptografických mechanismů, které jsou v souladu s platnými bezpečnostními normami.
- synchronizovat časová razítka s důvěryhodným zdrojem koordinovaného světového času (UTC) s přesností ±1 sekunda.
- Zajistit vysokou dostupnost služby časových razítek, implementovat mechanismy převzetí služeb při selhání a plány obnovy po havárii, aby se minimalizovaly výpadky.
- S předstihem informovat o plánované údržbě nebo významných změnách služby, které mohou mít dopad na odběratele.
- Pravidelně podstupovat audity, které prokazují shodu s normami ETSI EN 319 421, ETSI EN 319 401, eIDAS a dalšími platnými normami.
- Zajistit, aby zásady, bezpečnostní kontroly a operace časových razítek byly transparentní a ověřitelné regulačními orgány.

6.6 Informace pro spoléhající se strany

Spoléhající se strany časových razítek vydaných Incode TSA jsou povinny časová razítka před tím, než se na ně spolehnou, řádně ověřit. To zahrnuje mimo jiné následující:

- Ověření, že časové razítko bylo správně podepsáno společností Incode TSA.
- Ujištění, že soukromý klíč použitý k podpisu časového razítka byl v době jeho vydání platný a nebyl kompromitován.

7. Správa a provoz TSA

7.1 Úvod

Společnost Incode zavádí systém řízení bezpečnosti informací (ISMS) v souladu s normou ISO 27001, který zajišťuje důvěrnost, integritu a dostupnost jejích služeb TSA. Systém ISMS zahrnuje komplexní soubor bezpečnostních zásad, postupů a kontrolních mechanismů, které upravují správu, řízení a provoz TSA. Tyto zásady definují přísné kontroly přístupu, opatření pro řízení rizik a rámce shody pro ochranu operací časového razítkování.

Pravidelné audity a hodnocení bezpečnosti jsou prováděny za účelem udržení shody s předpisy a provozní bezpečnosti. Prostřednictvím tohoto systému ISMS společnost Incode zajišťuje, aby její TSA fungovala bezpečně, transparentně a v plném souladu s normou ETSI EN 319 421 a platnými zákony.

7.2 Vnitřní organizace

Incode TSA je služba poskytovaná společností Incode Czech Republic, právně uznaným subjektem založeným v České republice, který funguje v souladu s nařízením eIDAS a českými zákony. Incode TSA implementuje ISMS, aby zajistila důvěrnost, integritu a dostupnost svých služeb časových razítek.

Incode TSA zaměstnává kvalifikovaný personál, který musí splňovat požadavky oddílu 7.3 této politiky a disponuje odbornými znalostmi v oblasti kryptografické bezpečnosti, dodržování právních předpisů a řízení rizik, čímž zajišťuje řádnou správu a provoz služby.

Společnost Incode TSA navíc podléhá pravidelným auditům a bezpečnostním hodnocením, aby zajistila neustálé dodržování platných zákonů a regulačních norem.

Tato opatření zajišťují, že Incode TSA poskytuje spolehlivé, bezpečné a právně platné časové značky pro digitální transakce a regulační použití.

7.3 Personální zabezpečení

Aby společnost Incode zajistila bezpečnost, integritu a důvěryhodnost svých TSA, zavádí přísné zásady personální bezpečnosti v souladu s normami ETSI EN 319 421, ETSI EN 319 401 a ISO/IEC 27001. Tato opatření zajišťují, že k operacím TSA a citlivým kryptografickým materiálům mají přístup pouze oprávnění, kvalifikovaní a důvěryhodní pracovníci.

Podrobnosti o kontrolách personální bezpečnosti zavedených společností Incode lze nalézt v oddíle 5.3 CPS, který mimo jiné popisuje:

1. postupy kontroly vstupních dokladů
2. Kompetence, zkušenosti a další požadavky na obsluhu CA a TSA.

Společnost Incode má přesně definované popisy pracovních míst pro důvěryhodné role odpovědné za správu, řízení a provoz CA a TSA. Tyto role jsou přidělovány na základě přísných bezpečnostních požadavků a požadavků na dodržování předpisů, což zajišťuje, že kritické úkoly vykonávají pouze oprávnění pracovníci. Rámec navíc prosazuje jasné oddělení povinností, čímž minimalizuje riziko střetu zájmů a zvyšuje celkovou integritu a bezpečnost důvěryhodných služeb.

7.4 Správa aktiv

Společnost Incode implementuje politiku správy aktiv jako komplexní rámec pro správu životního cyklu organizačních aktiv, zejména paměťových médií. Tato politika stanoví jasné pokyny, postupy a odpovědnosti za ochranu, kontrolu a likvidaci aktiv, aby byl zajištěn soulad se standardy bezpečnosti informací.

Politika správy aktiv definuje zásady, které je třeba dodržovat během celého životního cyklu aktiv – od vydání a přidělení při nástupu zaměstnance do společnosti až po vyřazení, když se aktivum stane nefunkčním, nebo při odchodu zaměstnance.

Jako kvalifikovaný poskytovatel služeb vytvářejících důvěru (QTSP) považuje společnost Incode tuto politiku za zásadní pro zachování důvěrnosti, integrity a dostupnosti dat. Zajišťuje také bezpečnou likvidaci paměťových médií, aby se zabránilo neoprávněnému přístupu nebo narušení dat.

7.5 Řízení přístupu

Společnost Incode omezuje neoprávněný přístup k systémům a informacím tím, že vytváří, spravuje, monitoruje a deaktivuje účty s odpovídajícími úrovněmi oprávnění a přístupových práv.

Společnost Incode identifikuje vlastníky systémů a přiřazuje administrátory systémů, kteří spravují uživatelské účty v systémech používaných v rámci obchodní činnosti společnosti. Incode:

- Identifikuje citlivé systémy;
- přiděluje vlastníky a správce systémů;
- Stanovuje podmínky pro členství ve skupinách a rolích (podle potřeby);
- Určuje oprávněné uživatele informačního systému, členství ve skupinách a rolích a přístupová oprávnění (tj. práva k účtům) a další atributy (podle potřeby) pro každý účet;
- Vyžaduje souhlas vlastníka systému s vytvořením účtů informačního systému, pokud je přístup mimo jeho standardní pracovní náplň;
- Vytváří, povoluje, upravuje, zakazuje a odstraňuje účty informačního systému v souladu s tímto postupem;
- sleduje používání účtů informačního systému;

7.6 Kryptografické kontroly

7.6.1 Obecně

Generování kryptografických klíčů v Incode TSA se řídí přísnými bezpečnostními protokoly, které zajišťují integritu a důvěrnost kryptografických operací. Všechny kryptografické klíče jsou generovány v rámci HSM s certifikací FIPS 140-2/3 Level 3 nebo Common Criteria EAL4+, čímž je zajištěn soulad s průmyslovými standardy pro bezpečnou správu klíčů. Proces generování klíčů je navržen tak, aby byla zachována vysoká entropie, což zabraňuje jakékoliv předvídatelnosti nebo slabinám, které by mohly vést ke kryptografické kompromitaci. Velikosti klíčů jsou pečlivě vybrány tak, aby odpovídaly doporučeným silným stránkám zabezpečení, a využívají 4096bitový klíč RSA pro dlouhodobé zabezpečení a ECC P-256/P-384 pro optimalizovaný výkon se silnou kryptografickou odolností. Zavedením těchto osvědčených postupů zajišťuje Incode TSA, že všechny kryptografické operace probíhají ve vysoce bezpečném a vyhovujícím prostředí.

7.6.2 Generování klíčů TSU

TSU v rámci Incode TSA dodržuje přísný a bezpečný proces generování klíčů, aby byla zajištěna integrita, autenticita a nepopiratelnost časových razítek. Podpisový klíč TSU je kritickým kryptografickým aktivem a musí být spravován v souladu se standardy ETSI EN 319 421, RFC 3161 a NIST SP 800-57.

Proces bezpečného generování Incode, zajišťuje:

- Podpisový klíč TSU je generován uvnitř HSM certifikovaného podle FIPS 140-2/3 úrovně 3 nebo vyšší, aby se zabránilo neoprávněnému přístupu.
- Proces generování klíče zajišťuje dostatečnou entropii, minimalizuje předvídatelnost a kryptografické zranitelnosti.
- Generování provádějí důvěryhodné role, aby byla zajištěna odpovědnost a bezpečnost.
- Klíčový pár TSU se řídí osvědčenými postupy a používá 4096bitový klíč RSA s kódem SHA-256/SHA-512 pro dlouhodobé zabezpečení.

7.6.3 Ochrana soukromého klíče TSU

Soukromý klíč TSU se generuje, ukládá a používá výhradně v rámci HSM certifikovaného podle FIPS 140-2/3 úrovně 3, čímž je zajištěna fyzická a logická izolace před neoprávněným přístupem. Klíč není nikdy exportován z HSM a vestavěné šifrovací mechanismy jej chrání před extrakcí, manipulací nebo zneužitím.

Přísné řízení přístupu založené na rolích (RBAC) a vícefaktorové ověřování (MFA) omezují operace správy klíčů na oprávněné pracovníky Crypto Officers a vynucují politiku oddělení povinností.

Soukromý klíč se používá výhradně pro operace podepisování časových razítek, čímž je zajištěna nepopiratelnost a soulad s RFC 3161, což posiluje důvěru v integritu vydaných časových razítek.

7.6.4 Certifikát veřejného klíče

Certifikát veřejného klíče TSU je veřejně přístupný prostřednictvím důvěryhodného certifikátu veřejného klíče, což umožňuje spoléhajícím se stranám ověřit podpisy časových razítek a zajistit jejich pravost. Je distribuován prostřednictvím úložiště certifikátů TSA, což zajišťuje, že externí systémy a auditoři mohou bezpečně načíst a ověřit vydaná časová razítka.

Certifikát je navíc vložen do odpovědí časových razítek (TSR) v souladu s RFC 3161, což usnadňuje bezproblémové a automatizované ověřování spoléhajícími se stranami, a tím posiluje důvěryhodnost a integritu procesu časových razítek.

7.6.5 Opakované klíčování TSU

Incode neimplementuje procesy opakovaného klíčování. Pokud jsou certifikáty, algoritmy nebo velikosti klíčů považovány za zranitelné, vygeneruje se nový pár klíčů a použije se k vydání nového certifikátu.

7.6.6 Správa životního cyklu podepisovacího kryptografického hardwaru

Při pořizování, nasazování a vyřazování zařízení CloudHSM používaných společností Incode se musí dodržovat přísné bezpečnostní protokoly, aby byl zajištěn soulad s průmyslovými standardy a chráněny kryptografické operace. Služby CloudHSM jsou poskytovány od důvěryhodných poskytovatelů cloudových služeb, kteří dodržují certifikaci FIPS 140-2/3 Level 3 a prosazují přísné kontroly přístupu.

Proces bezpečného nasazení zajišťuje, že inicializovat a konfigurovat HSM mohou pouze oprávnění pracovníci, přičemž přísnou správu zajišťuje vícefaktorová autentizace (MFA) a řízení přístupu na základě rolí (RBAC). Před aktivací musí být ověřeno, zda firmware a bezpečnostní konfigurace instance CloudHSM odpovídají bezpečnostním zásadám společnosti Incode, což zajišťuje bezpečné generování klíčů, jejich ukládání a správu přístupu.

Po celou dobu provozního cyklu je činnost systému CloudHSM nepřetržitě monitorována a jsou zavedeny mechanismy protokolování a auditu, které umožňují sledovat kryptografické operace. Po skončení životnosti zařízení CloudHSM musí být související podpisové klíče trvale odstraněny, čímž je zajištěno, že je nelze obnovit.

Instance CloudHSM je poté bezpečně vyřazena z provozu v rámci infrastruktury poskytovatele cloudu a je proveden závěrečný audit shody, který ověří správné zničení klíčů a ukončení služby.

7.6.7 Ukončení cyklu klíčů TSU

Životní cyklus klíče TSU se řídí strukturovaným procesem, který zajišťuje bezpečnost, shodu a kontinuitu operací časového razítkování. Podpisovým klíčům TSU je přiřazena doba platnosti na základě osvědčených kryptografických postupů a regulačních požadavků. Před vypršením platnosti je vygenerován nový pár klíčů a důvěryhodná certifikační autorita Incode vydá nový certifikát TSU, aby byl zajištěn plynulý přechod bez narušení ověřování časových razítek.

Pokud je klíč TSU kompromitován nebo dosáhne konce své životnosti, je okamžitě odvolán, aby se zabránilo jeho dalšímu používání, a je zveřejněna odpověď CRL nebo

OCSP, aby byly informovány spoléhající se strany. Odvolaný klíč je poté v rámci HSM deaktivován, čímž je zajištěno, že již nemůže být použit k podepisování.

Po vyřazení z provozu je soukromý klíč trvale vymazán pomocí kryptografických technik mazání, čímž je zajištěno, že jej nelze obnovit ani znovu použít.

7.7 Časové razítko

7.7.1 Vydání časového razítka

Proces vydávání časových razítek od společnosti Incode TSA je navržen v souladu s normou ETSI EN 319 422, což zajišťuje bezpečné, přesné a ověřitelné generování časových razítek. Všechna vydaná časová razítka odpovídají profilu časového razítka definovanému v normách ETSI a jsou generována prostřednictvím bezpečných procesů odolných proti neoprávněné manipulaci.

Aby byla zaručena přesnost času, obsahuje časové razítko správnou a sledovatelnou hodnotu času, synchronizovanou s UTC prostřednictvím uznávané laboratoře UTC(k). Tyto laboratoře, oficiálně uznané BIPM, zajišťují, že si časová razítka zachovávají vědecky ověřitelnou přesnost.

V případě, že se hodiny TSA vychýlí nad povolenou přesnost, časová razítka se nevydávají, dokud se neobnoví synchronizace, a každé časové razítko je digitálně podepsáno pomocí speciálního podpisového klíče TSU, který je generován výhradně pro tento účel, čímž je zajištěna kryptografická integrita a nepopiratelnost.

Systém generování časových razítek navíc odmítne jakýkoli pokus o vydání časového razítka, pokud vypršela platnost soukromého klíče TSU nebo pokud již není platný.

7.7.2 Synchronizace hodin s UTC

Zajištění přesné synchronizace hodin s UTC je pro Incode TSA zásadní pro generování důvěryhodných a ověřitelných časových razítek. Incode TSA se řídí normami ETSI EN 319 421, ETSI EN 319 422 a ITU-R TF.460-6, aby udržoval přesné časové reference pro všechna vydávaná časová razítka.

- Zdroj času Incode TSA je sledovatelný v uznávané laboratoři UTC(k), která je součástí celosvětové sítě Bureau International des Poids et Mesures.
- TSA zajišťuje, aby její interní hodiny zůstaly synchronizovány s UTC v rámci přesnosti definované politikou časových razítek.
- Incode zajišťuje, že čas používaný pro generování časových razítek si zachovává přesnost ±1 sekunda vzhledem k UTC.

- TSA nepřetržitě sleduje, zda se její hodiny neodchylují od UTC.
- Pokud systém zjistí, že se hodiny vychýlily mimo povolenou přesnost, vydávání časových razítek se okamžitě pozastaví, dokud se neobnoví synchronizace.

7.8 Fyzická bezpečnost a bezpečnost prostředí

Provoz Incode TSA probíhá v chráněném fyzickém prostředí, které je navrženo tak, aby se zabránilo neoprávněnému přístupu, použití nebo vyzrazení citlivých informací a aby se tyto informace odhalily. Toto prostředí odpovídá bezpečnostním požadavkům QTSP a standardům testování QTSP.

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

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

7.8.1 Fyzický přístup

Servery Incode TSA jsou umístěny v kontrolovaném prostředí s omezeným přístupem, který je vynucován prostřednictvím individuálních přístupových práv. Podpisový systém Incode TSA pracuje na vyhrazených serverech a soukromý klíč je v době, kdy se nepoužívá, bezpečně uložen, aby byla zajištěna jeho ochrana a integrita.

7.8.2 Klimatizace a napájení

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

7.8.3 Kontakt s vodou

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

7.8.4 Protipožární ochrana a prevence

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

7.8.5 Úložná média

Veškerá 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.

7.8.6 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 zacházení s médii, společnost Incode se řídí zásadami zacházení s médii, které definují postupy mazání požadované pro fyzická a elektronická média. Tyto postupy zajišťují bezpečné zničení médií a zabraňují jakémukoli vystavení nebo opětovnému použití uložených informací.

7.8.7 Vzdálené zálohování

Procesy a systémy Incode TSA 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.

7.9 Zabezpečení provozu

Incode TSA zajišťuje integritu, bezpečnost a spolehlivost svých služeb časových razítek prostřednictvím přísných provozních bezpečnostních kontrol. Zabezpečení je zakomponováno již od návrhu, s důslednou kontrolou změn, ochranou proti škodlivému softwaru a správou přístupu, která zabraňuje neoprávněným úpravám. Řízení přístupu na základě rolí a vícefaktorová autentizace (MFA) chrání administrativní funkce, zatímco včasné záplatování a průběžné monitorování zajišťují integritu systému.

Naše správa konfigurace prosazuje základní zásady zabezpečení pomocí automatických kontrol shody a detekce hrozeb v reálném čase.

Incode TSA nepřetržitě monitoruje požadavky na kapacitu, aby zajistila optimální výkon systému a zabránila nedostatku zdrojů. Projekce budoucích požadavků na kapacitu jsou prováděny na základě trendů využití a prognóz růstu. Škálování je řízeno prostřednictvím funkce automatického škálování cloudu, která umožňuje Incode TSA dynamicky přidělovat zdroje podle poptávky po službách. Tento přístup zajišťuje dostupnost, spolehlivost a efektivitu služeb a zároveň zmírňuje případné výpadky.

7.10 Řízení zabezpečení sítě

Incode TSA pracuje v rámci zabezpečené sítě, dodržuje bezpečnostní zásady a standardní dokumenty o shodě, aby se zabránilo neoprávněnému přístupu, manipulaci a útokům na službu.

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

Kromě toho jsou všechny ostatní systémy TSA 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.

7.11 Řízení incidentů

Společnost Incode zavedla postup pro řízení incidentů v oblasti bezpečnosti informací, který má usnadnit hlášení bezpečnostních incidentů, potenciálních zranitelností a chování, které mohou ohrozit informační systémy. Tento postup popisuje metody hlášení, monitorování a reakce na incidenty na adrese , aby byl zajištěn strukturovaný a efektivní proces řešení.

Postup zahrnuje povinná oznámení příslušným orgánům v případě bezpečnostních incidentů, které by mohly ovlivnit důvěryhodnost důvěryhodných služeb společnosti Incode. Kromě toho jsou v případě potřeby informováni účastníci a spoléhající se strany, aby byla zachována transparentnost a důvěryhodnost.

Zaměstnanci hrají v systému řízení bezpečnosti informací zásadní roli tím, že dodržují tuto politiku a aktivně hlásí incidenty. Všechny nahlášené případy jsou sledovány, analyzovány a řešeny prostřednictvím nápravných a preventivních opatření, čímž je zajištěno, že budou zavedena opatření, která zabrání opakování a posílí celkovou bezpečnost.

7.12 Shromažďování důkazů

V rámci této politiky společnost Incode zajišťuje, aby byly všechny operace s časovými razítky auditovatelné a ověřitelné, a to zavedením přísných postupů shromažďování důkazů. Tím je zajištěn soulad s právním a regulačním rámcem eIDAS při zachování integrity, autenticity a spolehlivosti vydaných časových razítek.

Na podporu platnosti každého vydaného časového razítka jsou systematicky zaznamenávány následující údaje:

- události související s klíči a certifikáty TSA a TSU.

7.13 Řízení kontinuity provozu

Společnost Incode zavedla postupy řízení kontinuity provozu pro scénáře zahrnující potenciální kompromitaci soukromého klíče TSA nebo ztrátu synchronizace času s referenčním zdrojem UTC.

7.13.1 Reakce na kompromitaci soukromého klíče TSA

V případě jakéhokoli podezření na kompromitaci nebo neoprávněný přístup k soukromému klíči TSA nebo jeho TSU společnost Incode přijme okamžitá opatření na ochranu bezpečnosti a důvěryhodnosti své služby časového razítkování. Reakce zahrnuje:

- Dodržování postupů uvedených v části 5.7 CPS za účelem posouzení, potvrzení a zmírnění případné kompromitace klíče.
- Přerušení vydávání časových razítek, dokud nebude vygenerován, bezpečně uložen a ověřen nový kryptografický klíč, aby byla zachována důvěra ve službu.
- Zrušení a nahrazení kompromitovaného certifikátu TSA a oznámení bezpečnostního incidentu odběratelům, spoléhajícím se stranám a příslušným orgánům.
- Provedení forenzní analýzy s cílem určit hlavní příčinu, rozsah a dopad kompromitace.

- Zavedení dalších bezpečnostních opatření, která zabrání budoucím incidentům, jako jsou přísnější kontroly správy klíčů, zvýšené monitorování a další vrstvy ověřování.

7.13.2 Automatické monitorování a reakce na synchronizaci času

Incode TSA se spoléhá na vysoce přesné zdroje času, aby bylo zajištěno, že časové značky splňují regulační požadavky, zejména udržování přesnosti ±1 sekunda s UTC. Aby byla tato přesnost zaručena:

- Automatizované monitorovací mechanismy průběžně ověřují synchronizaci s referenčními zdroji UTC.
- Pokud je zjištěna ztráta synchronizace nebo nelze dodržet práh přesnosti ±1 sekunda, TSA automaticky pozastaví vydávání časových razítek, dokud se synchronizace neobnoví.
- Výstražné mechanismy upozorní správce systému na jakoukoli odchylku, což umožní okamžité nápravné opatření k obnovení integrity služby.

7.13.3. Oznámení příslušným orgánům

V jakémkoli z výše uvedených scénářů společnost Incode neprodleně informuje příslušné regulační orgány v souladu se svou politikou řízení incidentů a platnými právními závazky. Proces oznámení zahrnuje následující činnosti:

- Poskytnutí podrobných zpráv o povaze incidentu, potenciálním dopadu a přijatých krocích ke zmírnění následků.
- Spolupráci s regulačními orgány, odběrateli a spoléhajícími se stranami s cílem zajistit transparentnost a udržet důvěru ve službu.
- Provedení řízeného plánu obnovy s cílem obnovit bezpečné vydávání časových razítek a zároveň zajistit soulad s příslušnými předpisy.

7.14 Ukončení činnosti TSA a plány ukončení činnosti

V případě ukončení služby Incode TSA společnost Incode zavede strukturovaný plán ukončení, aby zajistila řízené a bezpečné ukončení poskytování svých služeb vytvářejících důvěru, minimalizovala narušení pro spoléhající se strany a zajistila soulad s příslušnými právními a regulačními požadavky.

7.14.1 Odvolání certifikátů, kterým vypršela platnost

Při ukončení platnosti certifikátů společnost Incode:

- zruší všechny aktivní certifikáty TSA, aby zabránil neoprávněnému použití časových razítek po ukončení služby.
- S předstihem oznámí odběratelům a spoléhajícím se stranám harmonogram odvolání a zajistí, aby přijali nezbytná opatření k přechodu na alternativní služby.
- Zveřejní seznamy CRL nebo aktualizuje respondéry OCSP tak, aby odrážely stav odvolání.
- Zajistěte, aby záznamy o časových razítkách zůstaly přístupné po požadovanou dobu uchovávání pro potřeby právních důkazů a ověřování.

7.14.2 Dodržování standardů CPS a regulačních standardů

Ukončení činnosti Incode TSA se řídí postupy popsanými v části 5.8 Incode CPS, která popisuje požadované kroky pro řádné ukončení činnosti certifikační autority nebo RA. Mezi tyto kroky patří např:

- Regulační oznámení: Informování dozorových orgánů, akreditačních orgánů a příslušných regulačních subjektů o ukončení činnosti.
- Komunikace s uživateli a partnery: Informování všech zúčastněných stran, včetně odběratelů, spoléhajících se stran a integrátorů, o plánu přechodu a časovém harmonogramu.
- Bezpečná likvidace klíčů a dat: Zavedení bezpečných postupů vyřazování kryptografických klíčů, které zajistí, že všechny soukromé klíče TSA budou řádně zničeny v souladu s nejlepšími kryptografickými postupy, aby se zabránilo jejich zneužití.

7.14.3 Uchovávání údajů a právní povinnosti

I po ukončení poskytování služeb bude společnost Incode:

- Zajistí, aby záznamy s časovými razítky zůstaly přístupné pro účely ověření v rámci zákonem požadované doby uchovávání.
- Bezpečně uchovávat auditní protokoly a záznamy a zajistit, aby mohly být použity pro řešení sporů nebo audity dodržování předpisů.
- Poskytne oficiální prohlášení s podrobnými informacemi o ukončení a jeho dopadu, čímž zajistí transparentnost a jasnost pro dotčené strany.

8. Další požadavky na kvalifikovaná elektronická časová razítka podle nařízení (EU) č. 910/2014

Pokud časové razítko tvrdí, že je kvalifikovaným časovým razítkem, očekává se, že spoléhající se strany ověří, zda jsou časové razítko a jeho vydávající TSU kvalifikované, nahlédnutím do důvěryhodného seznamu. Pokud je veřejný klíč TSU uveden v důvěryhodném seznamu a je spojen se službou kvalifikovaného časového razítka, lze časová razítka, která vydává, považovat za kvalifikovaná.

V případech, kdy orgán pro vydávání časových razítek (TSA) provozuje více TSU, může být veřejný klíč TSA uveden v důvěryhodném seznamu podle ETSI TS 119 612. Pokud je TSA uznána za poskytovatele kvalifikovaných služeb časových razítek a TSU je v rámci svého certifikátu řádně identifikována, pak jsou kvalifikovaná i časová razítka vydaná touto TSU. Navíc přítomnost qcStatement "esi4-qtstStatement-1", jak je definováno v ETSI EN 319 422, bod 9.1, slouží jako indikace, že časové razítko je prohlašováno za kvalifikované elektronické časové razítko.

Incode PSC