SMLOUVA O POSKYTOVÁNÍ SLUŽEB PŘI VYDÁVÁNÍ KVALIFIKOVANÝCH ELEKTRONICKÝCH PEČETÍ NA DÁLKU

Smluvní strany:

Česká republika – Státní pozemkový úřad

se sídlem: Husinecká 1024/11a, 130 00 Praha 3 – Žižkov

IČ: 01312774, DIČ: CZ01312774

bankovní spojení: Česká národní banka, číslo účtu: 3723001/0710

zastoupený: Mgr. Pavlem Škeříkem, ředitelem Sekce provozních činností

(dále jen „**Objednatel**“)

číslo smlouvy Objednatele: SPU 120206/2025, UID: spuess97ffbecd

a

Název poskytovatele: Software602 a.s.

se sídlem: Hornokrčská 15, 140 00 Praha 4

IČ: 630 78 236, DIČ: CZ63078236

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 3044,

bankovní spojení: Česká spořitelna, a.s., číslo účtu: 976652/0800

zastoupená: xxxxx

(dále jen **„Poskytovatel“**)

číslo smlouvy Poskytovatele: 030206/2025

dnešního dne uzavřely tuto smlouvu v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

(dále jen „**Smlouva**“).

Smluvní strany, vědomy si svých závazků v této Smlouvě obsažených a s úmyslem být touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:

1. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

1.1.1 je správním úřadem s celostátní působností, organizační složkou státu a účetní jednotkou, přičemž byl zřízen zákonem č. 503/2012 Sb., o Státním pozemkovém úřadu a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a

1.1.2 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Poskytovatel prohlašuje, že:

1.2.1 je právnickou osobou řádně založenou a existující podle českého právního řádu, a

1.2.2 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené, a

1.2.3 prohlašuje, že je kvalifikovaným poskytovatelem služeb vytvářejících důvěru v souladu s nařízením 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, oprávněným vydávat kvalifikované certifikáty pro elektronické pečetě, má formální souhlas orgánu dohledu potřebný pro poskytování plnění dle této Smlouvy a je uveden na seznamu poskytovatelů služeb vytvářejících důvěru v ČR, a

1.2.4 ke dni uzavření této Smlouvy není v úpadku dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (dále jen „**Insolvenční zákon**“), a zavazuje se Objednatele bezodkladně informovat o všech skutečnostech, které nasvědčují hrozícímu úpadku, popř. o prohlášení úpadku jeho společnosti, a

1.2.5 má zájem splnit veřejnou zakázku „V*ydávání kvalifikovaných elektronických pečetí na dálku*“ (dále jen „**Veřejná zakázka**“) pro Objednatele řádně a včas, a to za úplatu sjednanou v této Smlouvě;

1.2.6 se detailně seznámil s rozsahem a povahou předmětu Veřejné zakázky, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k její realizaci, těmto podmínkám rozumí a je schopný je dodržet, a

1.2.7 disponuje veškerými profesními znalostmi a dovednostmi k řádnému splnění předmětu Veřejné zakázky.

2. ÚČEL SMLOUVY

2.1 Účelem této Smlouvy je naplnění potřeb Objednatele v oblasti poskytování služeb při vydávání kvalifikovaných elektronických pečetí na dálku dle požadavků uvedených v této Smlouvě a příslušných právních předpisech.

3. PŘEDMĚT SMLOUVY

3.1 Poskytovatel se touto Smlouvou zavazuje poskytovat Objednateli služby ve formě vydávání kvalifikovaných elektronických pečetí na dálku (dále též „**elektronické pečetě**“) pro potřeby Objednatele (dále jen „**Služby**“) v souladu s platnou Certifikační

3.2 politikou vydávání kvalifikovaných certifikátů pro elektronické pečetě (dále jen „**certifikační politika“)**, která je uvedena v příloze č. 4 této Smlouvy.

3.3 Poskytovatel poskytuje Objednateli službu vytváření kvalifikovaných elektronických pečetí na dálku v souladu s bodem 52 recitálu, články 29 a 39, Přílohou II body 3 a 4 a Přílohou III nařízení Evropského parlamentu a Rady č. 910/2014, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS) a dále v souladu s ustanovením § 8 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů. Popis služby je uveden v příloze č. 2 této Smlouvy.

3.4 Poskytovatel poskytuje službu vydávání elektronických pečetí v souladu s příslušnými ustanoveními této Smlouvy. Objednatel se zavazuje při využívání elektronických pečetí vydaných na základě této smlouvy zabezpečit dodržování certifikační politiky.

3.5 Objednatel se zavazuje zaplatit Poskytovateli za řádně a včas poskytnuté Služby cenu dohodnutou v této Smlouvě.

3.6 Poskytovatel se zavazuje poskytovat Objednateli komplexní službu vydávání kvalifikovaných elektronických pečetí, které jsou založené na kvalifikovaném certifikátu, přičemž data pro vytváření elektronických pečetí (soukromý klíč) spojený s tímto certifikátem jsou uložena na kvalifikovaném prostředku pro vytváření elektronických pečetí (HSM modul) po celou dobu trvání Smlouvy.

3.7 Poskytovatel se zavazuje poskytnout ode dne účinnosti této Smlouvy webovou on-line aplikaci dostupnou Objednateli k ověření stavu archivní elektronické pečetě po zadání SN pečetě či hash dokumentu.

3.8 Poskytovatel se taktéž zavazuje zajistit, aby elektronické pečetě obsahovaly všechny náležitosti stanovené příslušnými obecně závaznými právními předpisy.

3.9 Poskytovatel se zavazuje Poskytovat Objednateli podporu zaručenou platnou certifikační politikou

3.10 Poskytovatel se zavazuje poskytovat službu vydávání elektronických pečetí s dostupností 98% za běžný kalendářní rok v nepřetržitém režimu 24 hodin denně 7 dní v týdnu (365 x 24) po celou dobu trvání této Smlouvy.

3.11 Poskytovatel prohlašuje, že vydávání elektronických pečetí odpovídá všem požadavkům vyplývajícím z právních předpisů, které se na plnění vztahují.

3.12 Poskytovatel se zavazuje poskytovat službu vydávání elektronický pečetí s propustností 2 ks elektronických pečetí za sekundu.

3.13 Poskytovatel se zavazuje poskytovat technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem této smlouvy prostřednictvím e-mailové adresy hotline@602.cz a telefonní linky +420 xxxxx

3.14 Poskytovatel se zavazuje sledovat stav kryptografických algoritmů používaných pro zajištění služby elektronických pečetí a v případě jejich oslabení neprodleně informovat Objednatele a seznámit jej s riziky z toho vyplývajícími. Další postup v případě, že rizika budou ze strany Objednatele posouzena jako závažná, bude řešen dohodou obou smluvních stran. Současně se Poskytovatel zavazuje používat vždy kryptografické algoritmy v souladu s právními předpisy, mezinárodními normami a aktuálními bezpečnostními doporučeními

4. DOBA A MÍSTO PLNĚNÍ

4.1 Poskytovatel se zavazuje **zahájit poskytování Služeb ode dne nabytí účinnosti této Smlouvy** a tyto Služby dále řádně poskytovat **po dobu 48 měsíců, nebo do vyčerpání finančního limitu 1 000 000 Kč bez DPH,** podle toho, která skutečnost nastane dříve.

4.2 Místem plnění smlouvy je sídlo Objednatele.

4.3 Poskytovatel poskytuje Objednateli službu technické podpory uživatelů, řešení nestandardních situací a poradenství související s předmětem této Smlouvy prostřednictvím e-mailové adresy hotline@602.cz a telefonní linky +420 xxxxx. Cena poskytování technické podpory je součástí ceny elektronických pečetí.

5. ZPŮSOB POSKYTOVÁNÍ SLUŽEB

5.1 Zahájení poskytování Služeb

5.1.1 Řádné zahájení poskytování Služeb bude zástupci smluvních stran potvrzeno v rámci písemného protokolu.

5.2 Poskytovatel se zavazuje:

5.2.1 poskytovat Služby ve vysoké kvalitě s odbornou péčí odpovídající podmínkám sjednaným v této Smlouvě;

5.2.2 plnit tuto Smlouvu objektivním, nestranným a profesionálním způsobem, neovlivněným jakýmkoliv konkrétním jiným obchodním zájmem Poskytovatele či kohokoliv z jeho personálu, bez návaznosti na obdržení jakýchkoli odměn ve spojitosti s plněním této Smlouvy od jiné osoby než je Objednatel;

5.2.3 poskytovat Služby v kvalitě definované v přílohách této Smlouvy a/nebo v kvalitě odpovídající technickým normám a standardům upravujícím kvalitu jednotlivých Služeb;

5.2.4 upozorňovat Objednatele včas na všechny hrozící vady svého plnění či potenciální výpadky plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro plnění Smlouvy nezbytné;

5.2.5 upozornit Objednatele na potenciální rizika vzniku újmy či příležitosti realizace úspor nebo jiných zlepšení a včas a řádně dle svých možností provést bezodkladně taková opatření, která riziko vzniku újmy zcela vyloučí nebo sníží;

5.2.6 dodržovat bezpečnostní, hygienické, požární, organizační, ekologické předpisy, předpisy o bezpečnosti a ochraně zdraví při práci na pracovištích Objednatele a veškeré další platné právní předpisy

a zároveň interní předpisy Objednatele, se kterými byl seznámen, resp. mohl se s nimi seznámit, a za stejných podmínek zajistit, aby všechny osoby podílející se na plnění jeho závazků z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích Objednatele, dodržovaly zmíněné předpisy;

5.2.7 postupovat při poskytování plnění podle této Smlouvy s vysokou odbornou péčí a aplikovat postupy *„best practice“*;

5.2.8 chránit práva duševního vlastnictví Objednatele a třetích osob;

5.2.9 upozorňovat Objednatele na možné či vhodné rozšíření či změny Služeb za účelem jejich lepšího využívání v rozsahu této Smlouvy;

5.2.10 upozorňovat Objednatele na případnou nevhodnost pokynů Objednatele;

5.2.11 poskytovat Objednateli na vyžádání součinnost související s odbornými, zákonnými či jinými kontrolami a audity, které mohou být uplatňovány vůči Objednateli v souvislosti s poskytováním Služeb či provozem informačních systémů Objednatele, jichž se poskytování Služeb týká;

5.2.12 jakékoliv dokumenty zpracovávané dle této Smlouvy vést ve formě umožňující přezkoumatelnost a auditovatelnost ze strany kontrolních orgánů. Pokud by byl jakýkoliv dokument související s poskytováním Služeb zpochybněn kontrolním orgánem, je Poskytovatel povinen poskytnout Objednateli takové dokumenty či podklady, které budou kontrolním orgánem akceptovány. V případě, že Poskytovatel nebude schopen tyto dokumenty či podklady poskytnout nebo by tyto nebyly kontrolním orgánem akceptovány, a pokud absence těchto dokumentů bude důvodem k udělení jakékoliv sankce vůči Objednateli, zavazuje se Poskytovatel Objednateli uhradit takovouto sankci v plné výši, a to i po vypršení platnosti a účinnosti této Smlouvy, pokud se bude taková sankce týkat období platnosti dokumentu zpracovaného Poskytovatelem;

5.2.13 chránit data v systémech Objednatele před ztrátou nebo poškozením a přistupovat k nim a užívat je pouze v souladu s touto Smlouvou, obecně závaznými právními předpisy a zájmy Objednatele.

5.3 Pojištění

5.3.1 Poskytovatel se dále zavazuje udržovat v platnosti a účinnosti po celou dobu poskytování Služeb pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za újmu, zejména majetkovou újmu (škodu) způsobenou Poskytovatelem třetí osobě (Objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy nesmí být nižší než **1 000 000 Kč** za rok a pojistné plnění v uvedené výši se musí vztahovat na jakoukoliv újmu, kterou může způsobit Poskytovatel Objednateli při plnění této Smlouvy. Poskytovatel je kdykoliv v průběhu trvání této Smlouvy povinen na požádání Objednatele předložit pojistnou smlouvu dle tohoto odstavce, nebo její relevantní části, nebo pojistku ve smyslu § 2775 občanského zákoníku, a to nejpozději do 7 dnů ode dne doručení žádosti Objednatele.

5.4 Kybernetická bezpečnost

5.4.1 Poskytovatel se při plnění zavazuje dodržovat zásady bezpečnosti informací v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, (dále jen „**zákon o kybernetické bezpečnosti**“), a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „**vyhláška o kybernetické bezpečnosti**“). Bezpečností informací se v souladu se zákonem o kybernetické bezpečnosti rozumí zajištění důvěrnosti, integrity a dostupnosti informací, které budou uchovávány, vytvářeny nebo zpracovávány v rámci plnění Poskytovatele dle této Smlouvy nebo v systémech, které mají vazbu na plnění Poskytovatele dle této Smlouvy a v souvislosti s kterými Objednateli vznikají právní povinnosti na základě zákona o kybernetické bezpečnosti.

5.4.2 Jestliže vznikne v souvislosti se zavedením a prováděním bezpečnostních opatření podle právních předpisů uvedených v předchozím odstavci potřeba uzavřít dodatek k této Smlouvě nebo zvláštní smlouvu, zavazuje se Poskytovatel poskytnout veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy, a k uzavření takového dodatku, resp. smlouvy.

5.5 Odpovědné zadávání

5.5.1 Poskytovatel si je vědom skutečnosti, že Objednatel má zájem o plnění předmětu této Smlouvy dle zásad odpovědného zadávání veřejných zakázek. Poskytovatel se proto výslovně zavazuje k plnění veškerých povinností vyplývajících z právních předpisů České republiky, zejména pak z předpisů pracovněprávních, předpisů z oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, a to vůči všem osobám, které se na plnění Veřejné zakázky podílejí.

6. CENA A PLATEBNÍ PODMÍNKY

6.1 Maximální cena za Služby dle této Smlouvy je smluvními stranami dohodnuta ve výši **1 000 000 Kč bez DPH**, přičemž sazba DPH činí 21 %, výše DPH činí **210 000 Kč** a cena včetně DPH činí **1 210 000 Kč**, a to jako nejvýše přípustná celková cena za Služby za 48 měsíců. Cena za Služby je dále specifikována v Příloze č. 1 této Smlouvy. Pro vyloučení pochybností to znamená, že celková částka za poskytnutí Služeb uvedená v tomto odstavci je nejvýše přípustná celková částka za poskytnutí Služeb a všech zřizovacích či jiných poplatků a veškerých dalších nákladů s poskytnutím Služeb souvisejících.

6.2 Cena Služeb bude placena na základě faktur (daňových dokladů), které budou Poskytovatelem vystavovány v měsíčních intervalech podle skutečného rozsahu poskytnutých Služeb.

6.3 Lhůta splatnosti fakturované částky je stanovena na 30 dní od doručení faktury Objednateli. Poskytovatel se zavazuje odeslat daňový doklad Objednateli nejpozději následující pracovní den po jeho vystavení. V případě, že má lhůta

splatnosti faktury uplynout v období od 16. do 31. prosince, bude se za poslední den lhůty splatnosti takovéto faktury považovat třetí pracovní den po skončení uvedeného období.

6.4 Faktura musí splňovat náležitosti obchodní listiny ve smyslu § 435 občanského zákoníku a řádného daňového dokladu požadované zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Přílohu faktury bude tvořit report o rozsahu poskytnutí Služeb schválený Objednatelem.

6.5 Nebude-li faktura obsahovat stanovené náležitosti a přílohy, nebo v ní nebudou správně uvedené údaje dle této Smlouvy, je Objednatel oprávněn vrátit ji Poskytovateli. V takovém případě se přeruší běh lhůty splatnosti a nová lhůta splatnosti počne běžet doručením opravené faktury.

6.6 Platby peněžitých částek se provádí bankovním převodem na účet druhé smluvní strany uvedený ve faktuře. Peněžitá částka se považuje za zaplacenou okamžikem jejího odepsání z účtu odesílatele ve prospěch účtu příjemce.

6.7 Ceny Služeb dle této Smlouvy jsou neměnné a konečné s výhradou změny zákonné sazby daně z přidané hodnoty.

7. OCHRANA INFORMACÍ A OSOBNÍCH ÚDAJŮ

7.1 Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:

7.1.1 si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „**důvěrné informace**“),

7.1.2 mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé strany nebo i jejím opominutím přístup k důvěrným informacím druhé strany.

7.2 Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě důvěrné informace, které při plnění této Smlouvy získala od druhé smluvní strany a neužije důvěrné informace v rozporu s účelem této Smlouvy a pro svůj vlastní prospěch.

7.3 Za třetí osoby podle odst. 7.2 se nepovažují:

7.3.1 zaměstnanci smluvních stran a osoby v obdobném postavení,

7.3.2 orgány smluvních stran a jejich členové,

7.3.3 ve vztahu k důvěrným informacím Poskytovatele externí Poskytovatelé Objednatele, a to i potenciální,

za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeným s plněním dle této Smlouvy, důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této Smlouvě.

7.4 Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající strany a přijímající strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě strany zavazují neduplikovat žádným způsobem důvěrné informace druhé strany,

nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Obě strany se zároveň zavazují nepoužít důvěrné informace druhé strany jinak, než za účelem plnění této Smlouvy.

7.5 Nedohodnou-li se smluvní strany výslovně písemnou formou jinak, považují se za důvěrné implicitně všechny informace, které jsou anebo by mohly být součástí obchodního tajemství, tj. například, ale nejenom, popisy nebo části popisů technologických procesů a vzorců, technických vzorců a technického know-how, informace o provozních metodách, procedurách a pracovních postupech, obchodní nebo marketingové plány, koncepce a strategie nebo jejich části, nabídky, kontrakty, smlouvy, dohody nebo jiná ujednání s třetími stranami, informace o výsledcích hospodaření, o vztazích s obchodními partnery, o pracovněprávních otázkách a všechny další informace, jejichž zveřejnění přijímající stranou by předávající straně mohlo způsobit újmu.

7.6 Bez ohledu na výše uvedená ustanovení se veškeré informace vztahující se k předmětu této Smlouvy a příslušné dokumentaci považují s ohledem na potencionálně vysokou zneužitelnost informací Objednatele výlučně za důvěrné informace Objednatele a Poskytovatel je povinen tyto informace chránit v souladu s touto Smlouvou. Poskytovatel při tom bere na vědomí, že povinnost ochrany těchto informací podle tohoto článku 7 se vztahuje pouze na Poskytovatele.

7.7 Pokud jsou důvěrné informace poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je předávající strana povinna upozornit přijímající stranu na důvěrnost takového materiálu jejím vyznačením alespoň na titulní stránce nebo přední straně média. Absence takovéhoto upozornění však nezpůsobuje zánik povinnosti ochrany takto poskytnutých informací.

7.8 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

7.8.1 se staly veřejně známými, ani by jejich zveřejněním došlo k porušení závazků přijímací smluvní strany či právních předpisů,

7.8.2 měla přijímající strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy o ochraně informací,

7.8.3 jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy,

7.8.4 po podpisu této Smlouvy poskytne přijímající straně třetí osoba, jež není omezena v takovém nakládání s informacemi,

7.8.5 mají být zpřístupněny na základě zákona či jiného právního předpisu včetně práva EU nebo závazného rozhodnutí oprávněného orgánu veřejné moci jsou obsažené ve Smlouvě a jsou zveřejněné dle příslušných právních předpisů.

7.9 Poskytovatel se zavazuje v plném rozsahu zachovávat mlčenlivost o osobních údajích zpracovávaných v systémech Objednatele.

7.10 V případě, že by se Poskytovatel stal v souvislosti s plněním této Smlouvy zpracovatelem osobních údajů, které jsou pod správou Objednatele, se Poskytovatel zavazuje v plném rozsahu zachovávat povinnost mlčenlivosti a povinnosti chránit důvěrné informace i ve vztahu k osobním údajům podléhajícím zákonu č. 110/2019 Sb., o zpracování osobních údajů a nařízení 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 (dále je „**GDPR**“), zejména čl. 28.

7.11 Za porušení povinnosti mlčenlivosti smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v odst. 7.3, které daná smluvní strana poskytla důvěrné informace druhé smluvní strany.

7.12 Poruší-li Poskytovatel povinnosti vyplývající z této Smlouvy ohledně ochrany důvěrných informací, je Objednatel oprávněn po Poskytovateli požadovat smluvní pokutu ve výši 100 000 Kč za každé porušení takové povinnosti, aniž by bylo dotčeno oprávnění Objednatele zakotvené v odst. 10.3.2 Smlouvy. Zaplacení jakékoliv sjednané pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky, ani nahradit způsobenou škodu nebo nemajetkovou újmu.

7.13 Ukončení účinnosti této Smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto článku 7 Smlouvy a jejich účinnost přetrvá i po ukončení účinnosti této Smlouvy.

7.14 Poskytovatel souhlasí se zveřejněním této Smlouvy včetně všech jejích změn a dodatků.

7.15 Poskytovatel dále výslovně prohlašuje a bere na vědomí, že tato Smlouva nepředstavuje jeho obchodní tajemství ani neobsahuje jeho důvěrné informace a souhlasí s tím, aby tato Smlouva, včetně veškerých změn a dodatků, byla v plném rozsahu zveřejněna v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Uveřejnění Smlouvy v registru smluv provede Objednatel, nedohodnou-li se strany jinak.

8. SANKCE

8.1 V případě, že bude Poskytovatel v prodlení se zahájením poskytování Služeb dle této Smlouvy v termínu sjednaném v této Smlouvě, je Objednatel oprávněn po něm požadovat smluvní pokutu ve výši 10 000 Kč za každý i započatý den prodlení.

8.2 V případě, že by Poskytovatel na požádání Objednateli nepředložil pojistnou smlouvu dle odstavce 5.3.1 nebo její relevantní část, je Objednatel oprávněn po něm požadovat smluvní pokutu ve výši 10 000 Kč.

8.3 V případě zaviněného nedodržení parametru SLA dostupnosti služby uvedeného v článku III. odst. 3.9 této Smlouvy, tj. pokud dostupnost služby klesne pod 98 % za kalendářní den, je Poskytovatel povinen uhradit Objednateli smluvní pokutu ve výši 1.000 Kč bez DPH za každých započatých 0,1 %, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu.

8.4 Zaplacení jakékoliv sjednané pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky, ani nahradit způsobenou škodu nebo nemajetkovou újmu.

8.5 Každá ze stran nese odpovědnost za způsobenou majetkovou újmu (škodu) a nemajetkovou újmu v rámci platných právních předpisů a této Smlouvy. Obě smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

9. SOUČINNOST PŘI UKONČENÍ SMLOUVY

9.1 V případě, že dojde k uzavření nové smlouvy týkající se Služeb nebo jakékoli jejich části s novým poskytovatelem odlišným od Poskytovatele, zavazuje se Poskytovatel po skončení účinnosti této Smlouvy poskytovat Objednateli nebo jím určeným třetím stranám veškerou součinnost potřebnou pro účely plynulého a řádného poskytování služeb obdobných Službám či jejich příslušné části novým poskytovatelem, pokud bude naplnění tohoto cíle záviset na znalostech poskytovatele získaných na základě plnění této Smlouvy. Pro vyloučení pochybností se uvádí, že Poskytovatel je v rámci součinnosti dle tohoto odstavce Smlouvy povinen zabezpečit osobní účast příslušných členů realizačního týmu na jednáních s Objednatelem či jím určenými třetími stranami. Po uplynutí lhůty dle předchozí věty tohoto odstavce bude součinnosti zabezpečována formou emailové či telefonické konzultace. Poskytovatel se zavazuje tuto součinnost poskytovat s odbornou péčí, bez zbytečného odkladu a zodpovědně, a to minimálně po dobu tří měsíců ode dne, ve kterém tato Smlouva zanikla. Poskytovatel se zavazuje reagovat na požadavek Objednatele nebo jím určené třetí strany a zahájit poskytování součinnosti dle tohoto odstavce Smlouvy nejpozději do 3 pracovních dnů ode dne doručení takovéhoto požadavku. Smluvní strany se dohodly, že cena za plnění dle tohoto odstavce je součástí ceny za poskytování Služeb dle této Smlouvy.

10. PLATNOST A ÚČINNOST SMLOUVY

10.1 Tato Smlouva nabývá platnosti dnem jejího podpisu zástupci smluvních stran. Smlouva nabývá účinnosti dne jejího uveřejnění v registru smluv podle § 6 zákona č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů

10.2 Tato Smlouva se uzavírá na dobu určitou, která končí uplynutím **48 měsíců** ode dne nabytí účinnosti této Smlouvy, nebo vyčerpáním finančního **limitu 1 000 000 Kč bez DPH**, podle toho, která skutečnost nastane dříve.

10.3 Objednatel je bez jakýchkoliv sankcí vedle důvodů uvedených v právních předpisech oprávněn odstoupit od této Smlouvy v případě, že:

10.3.1 Poskytovatel je v prodlení s plněním déle než 10 dní a nezjedná nápravu ani do 10 dnů ode dne doručení písemného oznámení Objednatele o takovém prodlení; nebo

10.3.2 dojde k porušení povinnosti ochrany důvěrných informací dle této Smlouvy ze strany Poskytovatele;

10.3.3 bude vydáno rozhodnutí o úpadku Poskytovatele, Poskytovatel sám podá dlužnický návrh na zahájení insolvenčního řízení nebo insolvenční návrh ohledně Poskytovatele je zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení (ve znění insolvenčního zákona); nebo

10.3.4 Poskytovatel vstoupí do likvidace, nebo dojde k jinému byť jen faktickému podstatnému omezení rozsahu jeho činnosti, který by mohl mít negativní dopad na jeho způsobilost plnit závazky podle této Smlouvy;

10.3.5 Poskytovatel nebude schopen předložit pojistnou smlouvu, její relevantní části nebo pojistku dle odst. 5.3 této Smlouvy;

10.4 Poskytovatel je oprávněn odstoupit od této Smlouvy pouze v případě, že:

10.4.1 Objednatel je v prodlení se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než 60 dnů;

10.4.2 Objednatel je v prodlení s poskytováním nezbytné součinnosti dle této Smlouvy; nebo

10.4.3 Objednatel jiným způsobem podstatně poruší tuto Smlouvu, a Objednatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Poskytovatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než 60 dnů od doručení takovéto výzvy k nápravě a v této výzvě zároveň musí být uvedeno právo Poskytovatele od Smlouvy odstoupit.

10.5 Účinky odstoupení od Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.

10.6 S ohledem na ustanovení odst. 10.4 této Smlouvy je vyloučena aplikace ustanovení § 2591 občanského zákoníku, který mj. stanoví, že Poskytovatel má právo po předchozím upozornění Objednatele odstoupit od Smlouvy v případě, že marně uplyne Poskytovatelem stanovená dodatečná lhůta k poskytnutí součinnosti Objednatelem.

10.7 Objednatel je oprávněn tuto Smlouvu písemně vypovědět bez udání důvodů, a to s výpovědní dobou v délce trvání 3 měsíců, která začíná běžet prvního dne měsíce následujícího po měsíci, kdy došlo k doručení písemné výpovědi Poskytovateli, a to bez jakýchkoliv sankcí.

10.8 Ukončením účinnosti této Smlouvy, včetně zrušení závazku v důsledku odstoupení od této Smlouvy, nejsou dotčena ustanovení Smlouvy týkající se licencí, záruk, nároků z odpovědnosti za vady, nároky z odpovědnosti za újmu a nároky ze smluvních pokut, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy, a to zejména práva a povinnosti uvedená v čl. 9 Smlouvy.

11. ROZHODNÉ PRÁVO A ŘEŠENÍ SPORŮ

11.1 Práva a povinnosti smluvních stran touto Smlouvou výslovně neupravené se řídí právními předpisy České republiky, zejména občanským zákoníkem a příslušnými právními předpisy souvisejícími.

11.2 Případné spory smluvních stran budou řešeny příslušnými soudy České republiky.

12. ZÁVĚREČNÁ USTANOVENÍ

12.1 Tato Smlouva představuje úplnou dohodu smluvních stran o předmětu této Smlouvy. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků.

12.2 Pokud by se kterékoliv ustanovení této Smlouvy ukázalo být neplatným, zdánlivým nebo nevynutitelným nebo se jím stalo po uzavření této Smlouvy, pak tato skutečnost nepůsobí neplatnost, zdánlivost ani nevynutitelnost ostatních ustanovení této Smlouvy.

12.3 Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce smluvních stran.

12.4 Poskytovatel výslovně prohlašuje, že tato Smlouva nepředstavuje jeho obchodní tajemství ani neobsahuje jeho důvěrné informace a souhlasí s tím, aby tato Smlouva byla v plném rozsahu zveřejněna Objednatelem.

12.5 Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1:	Souhrnná cenová tabulka
Příloha č. 2:	Popis služby Poskytovatele
Příloha č. 3:	Způsob autentizace ke službě kvalifikovaných elektronických pečetí
Příloha č. 4:	Politika vydávání elektronických pečetí

Smluvní strany prohlašují, že si tuto Smlouvu přečetly, že s jejím obsahem souhlasí a na důkaz toho k ní připojují svoje podpisy.

Objednatel	**Poskytovatel**
V Praze dne 17. 6. 2025	V Praze dne 12.6.2025
.....	.....
Česká republika – Státní pozemkový úřad	**Software602 a.s.**
Mgr. Pavel Škeřík	xxxxx
ředitel Sekce provozních činností	

Za správnost: Ing. Katarína Víšková,

Příloha č. 1

Souhrnná cenová tabulka

Cena za elektronické pečetě je počítána jako počet skutečně odebraných elektronických pečetí. Cena za jednu elektronickou pečeť se odvíjí od počtu odebraných pečetí v daném měsíci a je stanovena následovně:

Počet odebraných pečetění od – do / za měsíc	Cena za 1 ks pečetění v Kč bez DPH
1 – 1 500	xxxxx
1 501 – 3 000	xxxxx
3 001 – 4 500	xxxxx
4 501 – 6 000	xxxxx
nad 6 000	xxxxx

Příloha č. 2

Popis služby Poskytovatele

Služba vytváření kvalifikovaných elektronických pečetí na dálku

Architektura poskytovaných služeb

Služba vzdáleného pečetění je realizována prostřednictvím SDK komponenty (SecuSign SDK), provozované na serveru zákazníka. Tato komponenta komunikuje s backendovými službami poskytovatele, zejména s HSM infrastrukturou a cloudovou aplikací SOFA. Komponenty zajišťují generování kvalifikovaných elektronických pečetí v souladu s nařízením eIDAS a zákonem č. 297/2016 Sb.

Obrázek architektury řešení: xxxxx

Neuveřejněno z důvodu výjimky dle §3 odst. 2 pism. b, Zákona o registru smluv.

Postup aktivace služby

Implementace SDK komponenty SecuSign na server dodaný zákazníkem.

Odsouhlasení umístění soukromého klíče do HSM zařízení za účelem poskytování služby

vzdáleného pečetění.

Výjezd pracovníka ERA za účelem vydání kvalifikovaných certifikátů pečetí a komerčních certifikátů pro autentizaci.

Konfigurace SDK komponenty na serveru (provádí poskytovatel).

Propojení komponenty s volající aplikací či spisovou službou zákazníka.

Ověření funkčnosti, testování a předání příkladových requestů odpovědným osobám.

Podrobná dokumentace: https://www.602.cz/dokumentace/uloziste/secusign/index.html

Proces pečetění dokumentu

Po úspěšné implementaci a konfiguraci SDK je zákazníkovi předána URL adresa endpointu služby. Současně jsou poskytnuty příkladové requesty pro volání služby (např. Seal/SealEx).

Volající aplikace odesílá požadavek na danou URL. Pokud má správnou strukturu, vrací odpověď BASE64 řetězec představující výsledný PDF dokument s aplikovanou pečetí. Aplikace zákazníka je odpovědná za převod tohoto řetězce na výstupní formát PDF a jeho zpřístupnění uživateli.

Podrobný popis:
- Pečetění – základ:
https://www.602.cz/dokumentace/uloziste/secusign/zakladni/peceteni.html
- Seal: https://www.602.cz/dokumentace/uloziste/secusign/technicka/seal.html
- SealEx: https://www.602.cz/dokumentace/uloziste/secusign/technicka/sealex.html

Obnova pečetícího certifikátu

Obnovu certifikátu je nutné provést v prostředí SOFA za přítomnosti pracovníka ERA. Certifikát je vydán a uložen na kvalifikovaném prostředku HSM.

Platnost certifikátu je omezena a před expirací je možné ji prodloužit (nejdříve 21 dní před uplynutím platnosti). O blížící se expiraci jsou informováni správci certifikátů i vlastník.

Standardní postup zahrnuje vydání nového kvalifikovaného certifikátu, opět za účasti pracovníka ERA. Certifikát může vydat i oprávněná osoba v roli KRA (Klientská registrační autorita).

Podrobnosti:
- Správa certifikátů: https://www.602.cz/dokumentace/uloziste/sofa/sprava_certifikatu.html
- Žádost o certifikát:
https://www.602.cz/dokumentace/uloziste/sofa/sprava_certifikatu/zadost_o_pecetici_certifikat.html

Technické požadavky (prerekvizity)

Windows Server 2022 nebo novější, 8 GB RAM, 4 jádrový CPU, 100 GB místa, .NET Framework 4.8+

Povolení komunikace mezi SDK a backendem poskytovatele (HSM, SOFA, QS)

Administrátorský přístup pro implementaci

SSL certifikát ve formátu .pfx/.p12 od důvěryhodné CA

Komunikace mezi SDK komponentou a volající aplikací/spisovou službou

Autentizační údaje a URL pro TSA, pokud se využívají vlastní časová razítka

Více informací:

https://www.602.cz/dokumentace/uloziste/secusign/konfigurace/casova_razitka.html

Bezpečnostní požadavky

Důvěrnost:

Ověřovaná data, která jsou podkladem pro vytváření kvalifikovaných elektronických pečetí na dálku, nejsou v systému Poskytovatele ukládána.

Důvěrnost dat je řešena:

– Při přenosu dat: prostřednictvím SSL protokolu.

– Při zpracování požadavku na ověření na serveru: s ověřovanými daty se pracuje pouze v paměti a nejsou v žádném kroku fyzicky uložena do souboru (ani dočasného) nebo databáze. Po procesu ověření jsou data z paměti vymazána.

– Celý proces ověření je logován.

Integrita:

Integrita vstupních dat při přenosu je řešena na úrovni datové struktury webové služby (vstupem je hash ověřovaných dat a hash z podpisu) a jejich kontrolou na serveru.

Příloha č. 3

Způsob autentizace ke službě kvalifikovaných elektronických pečetí

Proces přístupu ke službě kvalifikovaného elektronického pečetění vyžaduje autentizaci, jejíž způsob je nutné předem specifikovat Objednatelem a následně jej odpovídajícím způsobem implementovat a nakonfigurovat ze strany Poskytovatele.

V rámci implementace jsou možné následující způsoby autentizace:

1. **Autentizace pomocí autentizačního certifikátu**
   Autentizační certifikát může být vystaven pracovníkem ERA (zpravidla současně s vystavením pečetícího certifikátu v rámci jednoho výjezdu). Jedná se o komerční certifikát vydaný kvalifikovanou certifikační autoritou (typicky PostSignum). Pomocí konfiguračního klíče je možné omezit použití tohoto certifikátu výhradně pro účely autentizace při procesu pečetění, bez nutnosti jeho využití v jiných metodách služeb.

2. **Autentizace pomocí přístupových údajů (Basic Authentication) k uživatelskému účtu v systému SOFA**
   V tomto případě Poskytovatel předá přístupové údaje (uživatelské jméno a heslo) vlastníka pečeti, které budou využity jako součást autentizačních údajů při volání služby pečetění. I tento způsob lze prostřednictvím konfiguračního klíče a příslušné úpravy backendové části HSM omezit výhradně na autentizaci při pečetění.

3. **Kombinovaná autentizace (autentizační certifikát + Basic Authentication)**
   V tomto režimu se autentizace provádí souběžně pomocí autentizačního certifikátu i přístupových údajů (viz body 1 a 2 výše). Pomocí konfiguračního klíče lze rovněž vymezit použití pouze na proces pečetění.

Z pohledu bezpečnosti, technické proveditelnosti a zkušeností z předchozích implementací Poskytovatel výslovně doporučuje využít **autentizaci pomocí autentizačního certifikátu** (bod 1), která představuje bezpečnější a robustnější řešení oproti autentizaci prostřednictvím přístupových údajů.

Příloha č. 4

Certifikační politika vydávání kvalifikovaných certifikátů pro elektronické pečetě

Na následujících samostatně číslovaných stránkách předkládáme Certifikační politiky a Politika vzdáleného pečetění:

Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronickou pečeť

Verze 2.0.3

OBSAH

Evidence revizí a změn

Verze	Datum revize	Důvod a popis změny	Autor	Schválil
1.0	1. 7. 2016	První verze	PCA ČP	PAA ČP
1.1	2. 10. 2017	Změna v souvislosti s akreditací dle eIDAS	PCA ČP	PAA ČP
1.2	10. 9. 2018	Změny v souvislosti s QESCD prostředky a GDPR	PCA ČP	PAA ČP
2.0	20. 6. 2019	Změny v souvislosti s novou kořenovou CA	PCA ČP	PAA ČP
2.0	1. 9. 2020	Revize dokumentu - žádná změna	PCA ČP	
2.0	1. 9. 2021	Revize dokumentu - žádná změna	PCA ČP	
2.0.1	15. 8. 2022	Revize dokumentu bez větších změn, změna číslování verzí, úprava položky Country v profilu certifikátu	PCA ČP	PAA ČP
2.0.2	15. 8. 2023	Revize dokumentu - přidání popisu důvodů zneplatnění	PCA ČP	PAA ČP
2.0.3	15. 8. 2024	Revize dokumentu - žádná změna	PCA ČP	

1 ÚVOD

Tento dokument stanoví pravidla a postupy pro vydávání kvalifikovaných certifikátů pro elektronickou pečeť (dále také jen certifikát pro elektronickou pečeť nebo jen certifikát). Pověřená osoba organizace stanoví, které osoby mohou o vydání certifikátu žádat.

1.1 Přehled

Česká pošta, s.p. (dále i Česká pošta či ČP) provozuje certifikační autoritu s názvem PostSignum QCA.

Při vydávání certifikátů koncovým uživatelům uplatňuje model tzv. pre-registrace zákazníka, jehož cílem je minimalizovat účast statutárního zástupce organizace v celém procesu a vyžadovat minimální množství dokladů od osob, jež si budou žádat o certifikát.

Zákazník, který má zájem o služby PostSignum QCA, uzavře s Českou poštou smlouvu o poskytování certifikačních služeb. Ve smlouvě jsou stanoveny tzv. pověřené osoby, které jménem zákazníka stanovují, kterým žadatelům budou moci být vydány certifikáty podle jednotlivých certifikačních politik. Tito žadatelé jsou zavedeni do systému certifikační autority a následně požádají o certifikát na registrační autoritě České pošty.

Česká pošta může dohodnout se zákazníkem zvláštní podmínky procesu registrace, případně vznik nové certifikační politiky.

Certifikáty vydané podle této certifikační politiky jsou určeny pro zákazníky České pošty, kteří s Českou poštou uzavřeli smlouvu o poskytování certifikačních služeb. Tyto zákazníky budeme v souladu s platnými právními předpisy nazývat pečetícími osobami. Pečetící osoba bude též držitelem certifikátu vydaného PostSignum Qualified CA podle této certifikační politiky.

Certifikát dle této certifikační politiky lze vydat pouze právnické osobě, nikoliv potom nepodnikající nebo podnikající fyzické osobě.

Zákazník odpovídá za vazbu mezi údaji o sobě a údaji, které jsou uvedeny v certifikátu vydaném podle této certifikační politiky. Poskytovatel certifikačních služeb ověřuje vazbu mezi zákazníkem a veřejným klíčem v certifikátu.

Certifikáty vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronické pečetě pečetící osoby v souladu s platnými právními předpisy.

Odpovídající soukromý klíč k vydanému certifikátu dle této certifikační politiky může být uložen na QESCD, ale není to vyžadováno.

Plnění zásad této politiky rozpracovává a zajišťuje aktuální Certifikační prováděcí směrnice PostSignum QCA.

1.2 Název a jednoznačné určení dokumentu

Tab. 1 Identifikace politiky

Název dokumentu	Certifikační politika PostSignum Qualified CA pro kvalifikované certifikáty pro elektronickou pečeť
Verze dokumentu	2.0.3
Stav	finální
OID poskytovatele certifikačních služeb	2.23.134
OID PostSignum Root QCA	2.23.134.1.4.2.1
OID PostSignum Qualified CA	2.23.134.1.4.2.2
OID této politiky	2.23.134.1.4.1.18.200
Datum vydání	20. 5. 2019
Datum účinnosti	20. 6. 2019
Datum revize	15. 8. 2024
Doba platnosti	Do odvolání nebo do dne ukončení služeb autorit PostSignum QCA.

1.3 Participující subjekty

Podřízené certifikační autority mohou být řízeny a provozovány pouze Českou poštou (s výjimkou registračních autorit - viz dále).

Identifikační a kontaktní údaje poskytovatele certifikačních služeb jsou:

Česká pošta, s.p.

IČ 47114983, DIČ CZ47114983

Politických vězňů 909/4, 225 99 Praha 1

tel.: 954 301 111

e-mail: info@cpost.cz

Česká pošta je akreditovaným poskytovatelem certifikačních služeb na základě akreditace udělené Ministerstvem informatiky ČR dne 3.8.2005.

Česká pošta se dne 1. 7. 2016 stala kvalifikovaným poskytovatelem služeb vytvářejících důvěru v souladu s [eIDAS].

1.3.1 Certifikační autority (dále „CA“)

Úkolem CA PostSignum QCA je především vydávat a spravovat certifikáty certifikačních autorit PostSignum Root QCA, PostSignum Qualified CA a zákazníků České pošty v souladu s definovanými certifikačními politikami.

1.3.2 Registrační autority (dále „RA“)

Služby registračních autorit jsou zajišťovány poskytovatelem certifikačních služeb nebo externím subjektem na základě smlouvy s Českou poštou jako poskytovatelem certifikačních služeb.

Registrační autority zajišťují zejména tyto služby:

- přijímají (registrují) žádosti o certifikát, schvalují je nebo zamítají v souladu s platnými certifikačními politikami,
- ověřují totožnost žadatelů o certifikát,
- zajišťují předání vydaného certifikátu žadateli,
- zneplatňují certifikáty podle platných certifikačních politik,
- spravují a provozují kvalifikované prostředky pro vytváření elektronických pečetí (pouze vybrané externí subjekty).

Kontaktní údaje registračních autorit České pošty jsou uvedeny na webových stránkách poskytovatele.

Registrační autority zajišťované externím subjektem mohou poskytovat jen vybrané služby z výše uvedeného seznamu, což je stanoveno ve smlouvě mezi externím subjektem a Českou poštou.

1.3.3 Držitelé certifikátů, kteří požádali o vydání certifikátu pro elektronickou pečeť a kterým byl certifikát vydán.

1.3.4 Spoléhající se strany

Spoléhající se stranou je libovolný subjekt spoléhající se na certifikát vydaný PostSignum QCA. Spoléhající se strany nevstupují do smluvního vztahu s poskytovatelem certifikačních služeb.

1.3.5 Jiné participující subjekty

Certifikační autorita PostSignum QCA může využívat pro zajištění poskytování služeb externí subjekty.

1.4 Použití certifikátu

1.4.1 Přípustné použití certifikátu

Kvalifikované certifikáty pro elektronickou pečeť vydané podle této certifikační politiky mohou být použity pouze pro ověření elektronické pečetě pečetící osoby v souladu s platnými právními předpisy.

1.4.2 Omezení použití certifikátu

Certifikáty vydávané podle této certifikační politiky nejsou primárně určené pro komunikace nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod. nebo v souvislosti s bezpečností a obranyschopností státu. Česká pošta je připravena diskutovat se zákazníkem zvláštní podmínky poskytování certifikačních služeb ve výše uvedených sektorech.

Certifikáty vydávané podle této certifikační politiky je možné využívat pouze v souvislosti s řádnými a legálními účely a v souladu s platnými právními předpisy.

1.5 Správa politiky

1.5.1 Organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Za správu této certifikační politiky je odpovědný poskytovatel certifikačních služeb, tedy Česká pošta, konkrétně Manažer CA.

1.5.2 Kontaktní osoba organizace spravující certifikační politiku nebo certifikační prováděcí směrnici

Kontaktní osobou ve věci správy této certifikační politiky je Manažer CA. Další informace je možné získat na emailové adrese

manager.postsignum@cpost.cz

nebo na webových stránkách poskytovatele.

1.5.3 Subjekt odpovědný za rozhodování o souladu postupů poskytovatele s postupy jiných poskytovatelů certifikačních služeb

Za správu této certifikační politiky odpovídá Manažer CA, který rovněž rozhoduje o souladu postupů s postupy jiných poskytovatelů certifikačních služeb.

1.5.4 Postupy při schvalování souladu podle 1.5.3

Tento dokument je vytvářen týmem pro tvorbu certifikačních politik ČP, který je dle potřeby ustavován Komisí pro certifikační politiky ČP, je jí řízen a kontrolován.

Vypracovanou politiku předloží Manažer CA ke schválení Komisi pro certifikační politiky, která potvrdí OID politiky a přidělí číslo verze.

1.6 Přehled použitých pojmů a zkratek

Akreditace - Pod pojmem akreditace je myšleno získání statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle [eIDAS].

CDP (CRL Distribution Point) – URL adresa uvedená v certifikátu, ze které lze stáhnout aktuální CRL.

Coordinated Universal Time (UTC) – Koordinovaný světový čas, časový standard založený na Mezinárodním atomovém čase (TAI).

CRL (Certificate Revocation List) – seznam zneplatněných certifikátů. Obsahuje certifikáty, které nadále nelze pokládat za platné například z důvodu prozrazení odpovídajícího soukromého klíče subjektu. CRL je digitálně podepsán vystavitelem certifikátů – certifikační autoritou.

DMZ – demilitarizovaná zóna

Držitel certifikátu – zákazník od okamžiku vydání certifikátu.

Komise pro certifikační politiky ČP (Policy Approval Authority – PAA) – orgán, v jehož pravomoci je schvalovat, sledovat a udržovat certifikační politiky a certifikační prováděcí směrnice, jimiž se řídí činnost certifikační autority.

Kontaktní místo veřejné správy – pracoviště České pošty určené pro nabídku vybraných služeb klientům.

Kvalifikovaný certifikát pro elektronickou pečeť – kvalifikovaný certifikát pro právnické osoby ve smyslu [eIDAS].

Kvalifikovaný certifikát pro elektronický podpis – kvalifikovaný certifikát ve smyslu [eIDAS].

Kvalifikované elektronické časové razítko – kvalifikované elektronické časové razítko ve smyslu [eIDAS], v textu může být nazváno také jako kvalifikované časové razítko nebo jen časové razítko.

Manažer CA – osoba v řídící roli zodpovědná za provoz PostSignum QCA a PostSignum VCA.

Mobilní registrační autorita – mobilní pracoviště České pošty, jehož základním úkolem je přebírat žádosti o vydání certifikátu nebo jeho zneplatnění, kontrolovat identitu žadatelů, poté přijmout nebo zamítnout žádost a předat vydaný certifikát žadateli nebo tento certifikát zneplatnit.

Následný certifikát – certifikát vydaný na základě uzavřené smlouvy jako náhrada za již vydaný certifikát PostSignum; příslušná certifikační politika stanovuje, které údaje původního certifikátu mohou být v následném certifikátu změněny. Pro vydání následného certifikátu není vyžadovaná fyzická návštěva registrační autority.

Obchodní místo – centrální regionální pracoviště poskytující certifikační služby a zajišťující evidenci smluv.

Online Certificate Status Protocol (OCSP) – protokol pro on-line zjištění stavu (zneplatnění) certifikátu.

Orgán dohledu – Dohledový orgán nad kvalifikovanými poskytovateli služeb vytvářejících důvěru dle [eIDAS], který je stanoven na základě platných právních předpisů.

Otisk – unikátní datový řetězec o neměnné délce, který je vypočítán z libovolných vstupních dat; jednoznačně reprezentuje vstupní data, tj. neexistuje stejný otisk pro dvě různé zprávy.

Párová data (klíčový pár) – Jsou základním primitivem asymetrické kryptografie. Tvoří je soukromý a veřejný klíč. Z hlediska důvěrnosti je potřebné chránit především jejich generování a soukromý klíč.

Pečetící osoba – osoba definovaná v [eIDAS].

PKI – Public Key Infrastructure – Infrastruktura veřejných klíčů

Platné právní předpisy – Jsou jimi myšleny právní předpisy upravující oblast elektronického podpisu, zejména potom Zákon o službách vytvářejících důvěru pro elektronické transakce 297/2016 Sb. a NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES včetně navazujících právních předpisů.

Podepisující osoba – osoba definovaná v [eIDAS].

PostSignum – hierarchie certifikačních autorit a autority časového razítka tvořená kořenovou certifikační autoritou PostSignum Root QCA, všemi podřízenými certifikačními autoritami, pro něž PostSignum Root QCA vydala certifikát, a autoritami časového razítka, pro které některá z certifikačních autorit PostSignum vydala certifikát pro elektronickou pečeť.

PostSignum QCA – hierarchie certifikačních autorit, vydávajících kvalifikované certifikáty ve smyslu [eIDAS].

PostSignum VCA – hierarchie certifikačních autorit, vydávajících komerční certifikáty.

PostSignum Root QCA – kořenová certifikační autorita, která má samopodepsaný certifikát pro elektronickou pečeť. Vydává certifikáty pro elektronickou pečeť pro podřízené certifikační autority a CRL. V hierarchii PostSignum mohou existovat další kořenové certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Root QCA 2.

PostSignum Qualified CA – certifikační autorita, která má certifikát pro elektronickou pečeť podepsaný kořenovou certifikační autoritou PostSignum Root QCA. Vydává kvalifikované certifikáty pro subjekty,

které nejsou certifikačními autoritami. V hierarchii PostSignum QCA mohou existovat další podřízené certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Qualified CA 2.

PostSignum Public CA – certifikační autorita, která má certifikát pro elektronickou pečeť podepsaný kořenovou certifikační autoritou PostSignum Root QCA. Vydává komerční certifikáty pro subjekty, které nejsou certifikačními autoritami. V hierarchii PostSignum VCA mohou existovat další podřízené certifikační autority, které jsou navíc označeny pořadovým číslem, např. PostSignum Public CA 2.

PostSignum TSA – autorita vydávající kvalifikovaná elektronická časová razítka ve smyslu [eIDAS]. Autoritu tvoří více jednotek (TSU). Každá jednotka má vlastní klíč a kvalifikovaný certifikát pro elektronickou pečeť.

Pověřená osoba – ten, kdo vůči certifikační autoritě vystupuje jako zástupce zákazníka. Pověřené osoby musí být vyjmenovány ve smlouvě mezi zákazníkem a Českou poštou, případně smlouva stanovuje, že se jedná o samotného zákazníka.

QCA ČP – viz PostSignum QCA.

QESCD – (Qualified Electronic Seal Creation Device) kvalifikovaný prostředek pro vytváření elektronických pečetí v souladu s [eIDAS]

Registrační autorita – pracoviště, jehož základním úkolem je přebírat žádosti o certifikát nebo jeho zneplatnění, kontrolovat identitu žadatelů, poté přijmout nebo zamítnout žádost a předat vydaný certifikát žadateli nebo tento certifikát zneplatnit.

Rozlišovací jméno – jednoznačně identifikuje podepisující osobu dle pravidel definovaných příslušnou certifikační politikou.

Soukromý klíč – souhrnné označení dat pro vytváření elektronického podpisu, dat pro vytváření elektronických pečetí, dat pro šifrování a dešifrování a dat pro autentizaci.

Správa žadatelů – aplikace zajišťující informační podporu procesu registrace a evidence (dále také SŽ).

Tým pro tvorbu certifikačních politik (Policy Creation Authority – PCA) – tým, který vytváří politiky, jež předkládá ke schválení Komisi pro certifikační politiky. PCA je ustaven Komisí pro certifikační politiky, která řídí a kontroluje jeho činnost.

Uživatel certifikátu (relying party) – osoba, která užívá certifikát vydaný PostSignum například pro ověření elektronického podpisu či pečetě nebo pro zajištění jiných bezpečnostních služeb. Jinak též označována jako Osoba spoléhající se na certifikát.

VCA ČP – viz PostSignum VCA.

Veřejný klíč – souhrnné označení dat pro ověřování elektronického podpisu, dat pro ověřování elektronických pečetí a dat pro šifrování.

Webové stránky poskytovatele – https://www.postsignum.cz – webové stránky poskytovatele služby PostSignum.

Zákazník – právnická osoba, státní orgán nebo orgán místní samosprávy. Uzavírá s Českou poštou smlouvu o poskytování certifikačních služeb.

Zaměstnanec – osoba v zaměstnaneckém nebo jiném poměru k zákazníkovi, pro kterou zákazník schválil vydání certifikátu podle této certifikační politiky.

Žadatel – osoba, která má právo žádat u PostSignum o certifikát podle některé z platných certifikačních politik a je zástupcem pečetící osoby.

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

Jednotlivá úložiště informací a dokumentace provozuje a za jejich provoz odpovídá Česká pošta jako poskytovatel certifikačních služeb.

Za zveřejňování informací odpovídá Česká pošta jako poskytovatel certifikačních služeb.

2.2 Zveřejňování informací a dokumentace

Vydané certifikáty jsou uloženy v databázi certifikační autority.

Informace o vydaných certifikátech, o provozu PostSignum QCA a dokumentace PostSignum QCA jsou zveřejňovány v níže uvedeném rozsahu.

2.2.1 Zveřejňování certifikátů a CRL

Certifikáty certifikačních autorit jsou zveřejňovány

- na webových stránkách poskytovatele

  www.postsignum.cz,

  www.postsignum.eu, nebo

- na obchodních místech České pošty, kde je možné požádat o jejich zkopírování na přinesené médium.

Vydané certifikáty koncových uživatelů (a s nimi spojené informace), u nichž zákazník (držitel certifikátu) souhlasil se zveřejněním, jsou zveřejňovány

- na webových stránkách poskytovatele

Informace o zneplatněných certifikátech jsou zveřejňovány ve formě seznamu zneplatněných certifikátů (CRL)

- na webových stránkách poskytovatele, nebo
- na distribučních bodech seznamu zneplatněných certifikátů uvedených ve vydaném certifikátu (CDP).

2.2.2 Zveřejňování informací o certifikační autoritě

Certifikační politiky, zpráva pro uživatele a případně i další dokumenty jsou zveřejňovány na

- webových stránkách poskytovatele, nebo
- obchodních místech (pouze k nahlédnutí).

Další důležité informace, zejména informace požadované platnými právními předpisy (např. odnětí akreditace, zneplatnění certifikátu pro elektronickou pečeť certifikační autority) nebo informace o mimořádné události jsou zveřejňovány

- na webových stránkách poskytovatele,
- na obchodních místech a registračních autoritách ve formě vyvěšeného textového oznámení,

- v celostátně distribuovaném deníku.

2.3 Periodicita zveřejňování informací

Informace jsou zveřejňovány v následujících intervalech:

- certifikační politiky, certifikační prováděcí směrnice a zpráva pro uživatele jsou zveřejňovány po schválení a vydání nové verze.

- certifikáty, pokud byly označeny pro zveřejnění, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od přijetí certifikátu;

- informace o zneplatněných certifikátech ve formě seznamu zneplatněných certifikátů (CRL) jsou zveřejňovány neprodleně po jejich vydání, nejpozději však před koncem platnosti posledního zveřejněného seznamu zneplatněných certifikátů.

- důležité informace, zejména informace požadované platnými právními předpisy jsou zveřejňovány neprodleně.

2.4 Řízení přístupu k jednotlivým typům úložišť

Certifikační politiky (pokud jsou určeny ke zveřejnění), certifikáty certifikačních autorit a seznamy zneplatněných certifikátů a další důležité informace jsou přístupné pro čtení bez jakéhokoliv omezení.

Poskytovatel certifikačních služeb neumožňuje neautorizovaný přístup k vydaným certifikátům, u kterých nebyl držitelem vysloven souhlas se zveřejněním.

3 IDENTIFIKACE A AUTENTIZACE

3.1 Pojmenování

3.1.1 Typy jmen

Jméno subjektu je konstruováno podle standardu X.501 resp. návazného standardu X.520.

E-mailová adresa uvedená v rozšíření Subject Alternative Name certifikátu odpovídá standardu RFC-822.

3.1.2 Požadavek na významovost jmen

Význam údajů použitých v atributech subjektu certifikátu a v rozšířeních certifikátu je popsán v kapitole 7.

3.1.3 Anonymita a používání pseudonymu

PostSignum Qualified CA nepodporuje pseudonym žadatele o certifikát ani zákazníka v položce Subject certifikátu.

3.1.4 Pravidla pro interpretaci různých forem jmen

V certifikátech vydávaných PostSignum Qualified CA jsou podporovány pouze následující znakové sady:

- UTF8, znaky středoevropské znakové sady,
- US ASCII.

Veškeré údaje dokladované pověřenou osobou nebo samotným zákazníkem při pre-registraci žádosti o certifikát se do certifikátů vydávaných PostSignum Qualified CA a do žádostí o certifikáty přenášejí ve tvaru, ve kterém jsou uvedeny v předkládaných dokladech. Transkripce, jako například odstranění diakritiky, není možná.

E-mailová adresa uvedená v rozšíření Subject Alternative Name certifikátu může být kódována pouze znakovou sadou US ASCII.

3.1.5 Jedinečnost jmen

Každý zákazník v systému certifikační autority má přiřazen jedinečný identifikátor, který je uložen v údaji „serialNumber“ v Subjectu certifikátu. Zákazník je dále zodpovědný za zaručení jednoznačnosti rozlišovacího jména v subjectu certifikátu vydaného podle této certifikační politiky.

V položce Subject certifikátu je uvedena kombinace jednoznačných údajů o zákazníkovi (IČ zákazníka a jméno zákazníka) a jednoznačného rozlišovacího jména.

3.1.6 Obchodní značky

Všechna pole certifikátu, která PostSignum QCA ověřuje, mají předepsanou strukturu a musí být doložena jejich správnost a úplnost (viz ustanovení kapitoly 3.2.3).

Odpovědnost za použití obchodních značek nebo registrovaných ochranných známek v polích certifikátu, které nejsou PostSignum QCA ověřovány (viz kapitola 3.2.4), má zákazník.

3.2 Počáteční ověření identity

3.2.1 Ověřování souladu dat, tj. postup při ověřování, zda má osoba data pro vytváření elektronických pečetí odpovídající datům pro ověřování elektronických pečetí

Žadatel o certifikát předkládá registrační autoritě elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč, která je podepsána soukromým klíčem odpovídajícím veřejnému klíči uvedenému v žádosti. Tím je prokázáno, že žadatel o certifikát v době vytváření žádosti vlastnil soukromý klíč odpovídající veřejnému klíči uvedenému v žádosti.

3.2.2 Ověřování identity právnické osoby nebo organizační složky státu

Zákazník uzavírající smlouvu o poskytování certifikačních služeb prokazuje svou totožnost tak, jak je v obchodním styku obvyklé. Zákazník odpovídajícím způsobem prokazuje oprávněnost použití názvu organizace, který bude uveden v certifikátech pečetící osoby.

3.2.3 Ověřování identity fyzické osoby

Identita fyzické osoby (žadatele) při vydání prvotního certifikátu je prokázána na základě elektronického podpisu založeného na kvalifikovaném osobním nebo komerčním osobním certifikátu PostSignum vydaného žadateli o prvotní certifikát.

Při osobním podání žádosti o zneplatnění certifikátu na pobočce registrační autority předkládá jeden platný, nepoškozený osobní doklad.

Předložený osobní doklad z níže uvedeného seznamu je akceptován za předpokladu, že z něj lze zjistit údaje o státním občanství, o totožnosti, fotografii držitele, rodné číslo (resp. datum narození u cizinců) a údaj o době platnosti dokladu.

- Občané České republiky předkládají občanský průkaz nebo cestovní pas.

- Cizinci předkládají cestovní, diplomatický, služební nebo jinak nazývaný pas vydaný cizím státem nebo samostatný průkaz o povolení k pobytu vydávaný orgány ČR.
  Občané členských států Evropské unie a dále občané Islandu, Lichtenštejnska, Norska a Švýcarska mohou předložit také osobní doklad, který jim byl vydán k prokazování totožnosti na území příslušného státu.

3.2.4 Neověřené informace vztahující se k držiteli certifikátu

E-mailová adresa žadatele o certifikát nebo zákazníka může být umístěna v nepovinném rozšíření certifikátu Subject Alternative Name. Česká pošta, jakožto poskytovatel certifikačních služeb, neověřuje existenci e-mailové adresy ani její vztah k žadateli o certifikát nebo zákazníkovi. Tuto položku proto nelze použít pro identifikaci držitele certifikátu.

Česká pošta, jakožto poskytovatel certifikačních služeb, dále neověřuje správnost údaje organizační jednotka, uvedeného v seznamu žadatelů, který předává poskytovateli certifikačních služeb pověřená osoba zákazníka.

3.2.5 Ověřování specifických práv

Žádná ustanovení v této kapitole.

3.2.6 Kritéria pro interoperabilitu

Případná spolupráce s jinými poskytovateli certifikačních služeb je možná až po schválení Komisí pro certifikační politiky ČP, na základě uzavřené smlouvy a za podmínek definovaných touto komisí.

3.3 Identifikace a autentizace při zpracování požadavků na výměnu dat pro ověřování elektronických pečetí v certifikátu

3.3.1 Identifikace a autentizace při rutinní výměně dat pro vytváření elektronických pečetí a jim odpovídajících dat ověřování elektronických pečetí (dále „párová data“)

Identita žadatele o vydání následného certifikátu je ověřena při ověřování elektronického podpisu na žádosti o vydání následného certifikátu. Pro podpis příslušné žádosti musí být použit platný kvalifikovaný osobní nebo komerční osobní certifikát PostSignum (certifikát nebyl zneplatněn a ani neskončila jeho platnost) náležející žadateli.

3.3.2 Identifikace a autentizace při výměně párových dat po zneplatnění certifikátu

V případě zneplatnění certifikátu je nutné při identifikaci a autentizaci spojené s vydáním nového certifikátu postupovat stejně jako v případě počátečního ověření identity při vydání prvního certifikátu (viz kapitola 3.2.3).

3.4 Identifikace a autentizace při zpracování požadavků na zneplatnění certifikátu

O zneplatnění certifikátu může žádat žadatel nebo pověřená osoba. Žadatel prokáže svou totožnost:

- znalostí hesla pro zneplatnění, které zadal při registraci žádosti o certifikát, nebo
- jedním osobním dokladem v případě zaměstnance organizace.

Pověřená osoba prokáže svou totožnost:

- podpisem písemné žádosti o zneplatnění certifikátu, nebo
- elektronickým podpisem, založeným na certifikátu vydaném podřízenou certifikační autoritou z hierarchie PostSignum, na elektronicky zaslané žádosti o zneplatnění certifikátu, nebo
- osobním dokladem při podání žádosti o zneplatnění certifikátu osobně na registrační autoritě České pošty; pracovník registrační autority dále ověřuje, zda se pověřená osoba nachází na aktuálním seznamu pověřených osob.

Ke zneplatnění certifikátu může dojít i z vůle poskytovatele certifikačních služeb. V tomto případě je oprávněným žadatelem o zneplatnění certifikátu Manažer CA.

O zneplatnění kvalifikovaného certifikátu může požádat orgán dohledu. Oprávněným žadatelem o zneplatnění kvalifikovaného certifikátu je v tomto případě zástupce orgánu dohledu.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS CERTIFIKÁTU

4.1 Žádost o vydání certifikátu

4.1.1 Subjekty oprávněné podat žádost o vydání certifikátu

Žádost o vydání certifikátu podle této certifikační politiky mohou podat:

- osoby určené pověřenou osobou zákazníka – organizace.

4.1.2 Registrační proces a odpovědnosti poskytovatele a žadatele

4.1.2.1 Uzavření smlouvy

Zákazník získá přístup ke službě poskytování certifikačních služeb uzavřením písemné smlouvy o poskytování certifikačních služeb. Tato smlouva se uzavírá následujícím způsobem:

Zákazník předá České poště vyplněný formulář smlouvy, který je k dispozici na webové stránce poskytovatele, a zástupce ČP svým podpisem uzavře se zákazníkem smlouvu o poskytování certifikačních služeb.

Formuláře smlouvy obsahují odkazy na webové stránky poskytovatele, na nichž je možno získat Certifikační politiky a aktuální ceník.

Certifikační politika a aktuální ceník se stávají součástí smlouvy o poskytování služeb spolu s [VOP] ke dni uzavření smlouvy o poskytování služeb.

Smlouva o poskytování certifikačních služeb obsahuje mimo jiné:

- identifikační údaje zákazníka (je-li to relevantní, včetně IČ),
- rozsah poskytovaných certifikačních služeb,
- seznam pověřených osob, které budou s poskytovatelem certifikačních služeb komunikovat ohledně vydávání certifikátů.

Smlouva je se zákazníkem uzavřena tak, jak je v obchodním styku obvyklé (statutární zástupce organizace apod.). Smlouva musí být uzavřena v písemné formě.

Česká pošta si vyhrazuje právo nepřistoupit k uzavření smlouvy o poskytování certifikačních služeb.

4.1.2.2 Pre-registrace žadatelů o certifikát

Pre-registrací se rozumí postup, kdy pověřená osoba v případě zákazníka schvaluje seznam žadatelů, kteří mohou žádat o certifikát podle této certifikační politiky, a tento seznam předává poskytovateli certifikačních služeb.

Seznam žadatelů obsahuje povinné a nepovinné údaje certifikátu, jež jsou uvedeny v kapitole 7.1. Rodné číslo resp. datum narození žadatele není ve vydaném certifikátu uvedeno.

Dále pověřená osoba určuje, zdali může být vydaný certifikát zveřejněn široké veřejnosti bez omezení.

Registrační autorita ověřuje totožnost žadatele o certifikát na základě elektronického podpisu založeného na kvalifikovaném osobním nebo komerčním osobním certifikátu PostSignum. Vazbu mezi žadatelem a

zákazníkem (organizací) uvedeným v certifikátu garantuje pověřená osoba zákazníka (organizace), která spravuje seznam žadatelů předávaný poskytovateli certifikačních služeb.

4.1.2.3 Odpovědnost zákazníka

Zákazník je povinen zejména:

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování certifikačních služeb,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které jsou ve smlouvě uvedeny, zejména o změnách údajů o pověřených osobách,
- neprodleně informovat poskytovatele certifikačních služeb o změnách údajů zákazníka, které jsou uvedeny v certifikátu. Podle charakteru změny poskytovatel certifikačních služeb rozhodne, zda je třeba zneplatnit platné certifikáty, které byly pro zákazníka vydány.

4.1.2.4 Odpovědnost pověřených osob

Pověřená osoba je povinna zejména:

- poskytovat pravdivé a úplné informace o žadatelích oprávněných žádat o certifikát podle této politiky,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které udržuje v seznamech žadatelů o certifikát.

Pověřená osoba dále definuje, které certifikáty zákazníka budou zveřejněny prostřednictvím informačních služeb poskytovatele certifikačních služeb. Tyto služby jsou přístupné široké veřejnosti bez omezení.

4.1.2.5 Odpovědnost žadatele

Žadatel je povinen zejména:

- poskytovat pravdivé a úplné informace při pre-registraci žádosti o certifikát a při registraci žádosti o vydání následného certifikátu,
- zkontrolovat, zda údaje uvedené v certifikátu jsou správné a odpovídají požadovaným údajům,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,
- užívat soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice,
- neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, požádat o zneplatnění certifikátu a ukončit používání příslušného soukromého klíče,
- seznámit se s certifikační politikou, podle které mu byl vydán certifikát,
- po vygenerování párových dat (soukromý a veřejný klíč) provést neprodleně jejich zálohu, pokud je to technicky možné,
- umožnit poskytovateli certifikačních služeb přístup k QESCD, pokud je QESCD pod správou poskytovatele certifikačních služeb a je na něm uložený soukromý klíč a odpovídající certifikát vydaný dle této certifikační politiky.

4.1.2.6 Odpovědnost poskytovatele

Poskytovatel certifikačních služeb je zejména povinen:

- v procesu registrace zákazníka a žadatele o certifikát ověřit všechny údaje podle dostupných informací,
- v nejkratším možném termínu od podání žádosti posoudit žádost o certifikát resp. žádost o následný certifikát, vydat rozhodnutí, zda bude certifikát vydán, v případě zamítnutí žádosti o tomto rozhodnutí informovat žadatele nebo zákazníka,
- vydat certifikát obsahující věcně správné údaje na základě informací, které jsou certifikační autoritě k dispozici v době vydávání certifikátu,
- v případě žádosti o certifikát, jehož soukromý klíč byl vygenerován na QESCD, se prokazatelně o této skutečnosti přesvědčit a vložit do certifikátu příslušný příznak, že soukromý klíč je uložen na QESCD,
- spravovat a provozovat QESCD, u kterého je stanoveno, že je možné ho spravovat a provozovat pouze kvalifikovaným poskytovatelem služeb vytvářejících důvěru a zároveň obsahuje soukromý klíč a odpovídající certifikát vydaný dle této certifikační politiky (správa a provoz QESCD probíhá na základě dohodnutých podmínek mezi zákazníkem a poskytovatelem),
- zveřejňovat certifikační politiky, podle kterých vydává certifikáty, na webových stránkách poskytovatele, případně jinými vhodnými způsoby (viz kapitola 2.2),
- zveřejnit certifikát pro elektronickou pečeť poskytovatele certifikačních služeb tak, aby se každý mohl ujistit o jeho identitě,
- věnovat náležitou péči všem činnostem spojeným s poskytováním certifikačních služeb; náležitá péče zahrnuje provoz v souladu
    - s platnými právními předpisy,
    - s touto certifikační politikou,
    - s certifikační prováděcí směrnicí,
    - se systémovou bezpečnostní politikou,
    - s provozní dokumentací.

4.2 Zpracování žádosti o certifikát

4.2.1 Identifikace a autentizace

Žadatel o certifikát požádá o vydání certifikátu elektronicky způsobem upřesněným na webových stránkách poskytovatele nebo podmínek dohodnutých se zákazníkem. Žádost musí být opatřena elektronickým podpisem založeným na osobním kvalifikovaném nebo osobním komerčním certifikátu PostSignum, který byl vydán žadateli.

Žadatel o certifikát má možnost sdělit heslo pro případné zneplatnění certifikátu, pokud to systém registrační autority umožňuje. Heslo pro zneplatnění musí být zasláno v šifrované formě. Heslo musí splňovat požadavky (min. 8 znaků, z toho min. jedno malé písmeno, min. jedno velké písmeno, min. jednu číslici a min. jeden neabecední znak). Pokud žadatel heslo nesdělí nebo nebude splňovat uvedené

požadavky, bude vygenerováno automaticky systémem. Heslo pro zneplatnění certifikátu je vždy uvedeno v protokolu o vydání certifikátu.

Pracovník registrační autority ověří elektronický podpis na žádosti, zejména platnost certifikátu použitého pro ověření podpisu v době doručení žádosti na Českou poštu (musí být platný), jeho vydávající certifikační autoritu (PostSignum QCA). Oproti seznamu žadatelů ověří, zda daná osoba skutečně smí žádat o certifikát dle dané certifikační politiky.

4.2.2 Přijetí nebo zamítnutí žádosti o certifikát

4.2.2.1 Přijetí nebo zamítnutí žádosti o první certifikát

Žadatel poskytne registrační autoritě elektronickou žádost ve formátu PKCS#10 obsahující veřejný klíč elektronicky způsobem upřesněným na webových stránkách poskytovatele.

Do certifikátu budou vloženy údaje dle platného seznamu žadatelů.

Registrační autorita ověří elektronický podpis na žádosti, zejména platnost certifikátu použitého pro ověření podpisu v době doručení žádosti na Českou poštu (musí být platný), jeho vydávající certifikační autoritu (PostSignum Qualified CA nebo PostSignum Public CA) a zkontroluje ostatní náležitosti žádosti.

Pokud se nepodaří ověřit elektronický podpis na žádosti o vydání certifikátu nebo nebudou splněny všechny podmínky pro vydání certifikátu, odmítne registrační autorita certifikát vydat a o tomto informuje žadatele.
Česká pošta si vyhrazuje právo odmítnout vydat certifikát žadateli podle této certifikační politiky.

Pokud má pracovník registrační autority pochybnosti o předložené žádosti nebo pokud se vyskytnou jiné nesrovnalosti, odmítne vydat certifikát a o této skutečnosti informuje žadatele o certifikát.

4.2.2.2 Přijetí nebo zamítnutí žádosti o následný certifikát

Platí ustanovení v kapitole 4.2.2.1.

4.2.3 Doba zpracování žádosti o certifikát

Poskytovatel certifikačních služeb je povinen v nejkratším možném termínu od podání žádosti posoudit žádost o certifikát, vydat rozhodnutí, zda bude certifikát vydán, a v případě zamítnutí žádosti o tomto rozhodnutí informovat žadatele o certifikát. Od okamžiku kladného rozhodnutí je poskytovatel povinen neprodleně vydat certifikát.

4.3 Vydání certifikátu

Po kontrole a schválení žádosti o certifikát vloží registrační autorita tuto žádost do systému certifikační autority ke zpracování. Systém certifikační autority na základě této žádosti vydá certifikát a předá ho zpět registrační autoritě a publikačním službám.

Certifikát se stává platným okamžikem vydání.

4.3.1 Úkony CA v průběhu vydávání certifikátu

Certifikát je vydán systémem certifikační autority automaticky po přijetí žádosti od registrační autority.

4.3.2 Oznámení o vydání certifikátu držiteli certifikátu

Na e-mailovou adresu žadatele je odeslána informace o umístění vydaného certifikátu (URL), kde je možné vydaný certifikát po omezenou dobu uvedenou v e-mailové zprávě akceptovat (potvrdit převzetí certifikátu) a certifikát včetně protokolu o vydání certifikátu stáhnout.

4.4 Převzetí vydaného certifikátu

4.4.1 Úkony spojené s převzetím certifikátu

Poté, co je certifikát vydán, žadatel o certifikát zkontroluje správnost údajů uvedených v certifikátu a potvrdí převzetí certifikátu.

Převzetím certifikátu žadatel o certifikát za zákazníka stvrzuje:

- že na sebe bere závazky vyplývající z certifikační politiky, podle které byl certifikát vydán,
- že mu nejsou známy žádné skutečnosti, které by svědčily o tom, že soukromý klíč odpovídající veřejnému klíči v certifikátu vlastní jiná osoba, než je povoleno v příslušné certifikační politice,
- že údaje ve vydaném certifikátu jsou správné a úplné (zejména, že veřejný klíč v certifikátu odpovídá veřejnému klíči uvedenému v poskytnuté PKCS#10 žádosti).

Převzetím certifikátu se zákazník stává držitelem certifikátu.

Vydaný certifikát je pečetící osobě předán ve formátu DER.

4.4.2 Zveřejňování vydaných certifikátů poskytovatelem

Certifikáty vydané PostSignum Qualified CA, u nichž byl vysloven souhlas se zveřejněním, jsou zveřejňovány elektronickou cestou nejpozději do 24 hodin od převzetí certifikátu žadatelem.

4.4.3 Oznámení o vydání certifikátu jiným subjektům

Kromě zveřejnění vydaného certifikátu, u kterého byl držitelem vysloven souhlas se zveřejněním, a zaslání oznámení žadateli a volitelně pověřené osobě zákazníka neoznamuje poskytovatel certifikačních služeb vydání certifikátu žádné třetí straně.

Toto ustanovení se netýká předávání seznamu všech vydaných kvalifikovaných certifikátů na základě žádosti orgánu dohledu.

4.5 Použití párových dat a certifikátu

Páry klíčů svázané s certifikáty mají stejnou dobu platnosti jako certifikáty. Klíčové páry, na základě kterých již byl vydán certifikát certifikační autoritou PostSignum Qualified CA, nemohou být v prostředí PostSignum Qualified CA znovu použity.

4.5.1 Použití dat pro vytváření elektronických pečetí a certifikátu držitelem certifikátu nebo pečetící osobou

Pečetící osoba:

- nakládá se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle této certifikační politiky, s náležitou péčí, a to tak, aby nemohlo dojít k jeho neoprávněnému použití,

- v případě ztráty, odcizení nebo podezření na kompromitaci soukromého klíče neprodleně informuje poskytovatele certifikačních služeb a zároveň ukončí používání uvedeného soukromého klíče,

- užívá soukromý klíč a odpovídající certifikát vydaný podle této certifikační politiky pouze pro účely stanovené v této certifikační politice, uvedené v kapitole 1.4.1, tj. pro vytváření elektronické pečetě a v souladu s platnými právními předpisy,

- v případě, že soukromý klíč je uložen na QESCD, pečetící osoba:

    - musí mít generování a používání soukromého klíče pod svou výhradní kontrolou, pouze v případě, že správu a provoz QESCD zajišťuje poskytovatel, je generování a používání klíče pod kontrolou poskytovatele,

    - musí soukromý klíč používat pouze pro vytváření elektronických pečetí a v souladu s platnými právními předpisy.

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

Uživatel certifikátu (spoléhající se strana) vydaného PostSignum Qualified CA:

- získá certifikáty PostSignum Qualified CA a PostSignum Root QCA z bezpečného zdroje (webové stránky poskytovatele, webové stránky orgánu dohledu, EU Trusted Lists, na pracovišti registrační autority) a ověří otisk ("fingerprint") těchto certifikátů.

- před použitím certifikátu vydaného PostSignum Qualified CA ověří platnost certifikátu PostSignum Qualified CA a následně i platnost vydaného koncového certifikátu; kontrola se provádí na správnost podpisu vydávající autority a vůči příslušnému aktuálnímu CRL a aktuálnímu času, případně pomocí služby OCSP (tuto činnost obvykle vykonává aplikace uživatele certifikátu).

- dostatečně zváží, zda je certifikát vydaný podřízenou certifikační autoritou podle této politiky vhodný pro účel, ke kterému jej chce použít.

4.6 Obnovení certifikátu

Pod službou obnovení certifikátu je myšleno vydání nového certifikátu se stejným veřejným klíčem a novou dobou platnosti. PostSignum QCA tuto službu neposkytuje.

4.6.1 Podmínky pro obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.2 Subjekty oprávněné požadovat obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.3 Zpracování požadavku na obnovení certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.4 Oznámení o vydání obnoveného certifikátu držiteli certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.5 Úkony spojené s převzetím obnoveného certifikátu

PostSignum QCA tuto službu neposkytuje.

4.6.6 Zveřejňování vydaných obnovených certifikátů poskytovatelem

PostSignum QCA tuto službu neposkytuje.

4.6.7 Oznámení o vydání obnoveného certifikátu jiným subjektům

PostSignum QCA tuto službu neposkytuje.

4.7 Výměna dat pro ověřování elektronických pečetí v certifikátu

Služba výměny dat pro ověřování elektronických pečetí v certifikátu je označována jako vydání následného certifikátu. Toto označení bude dále používáno i dále v textu.

4.7.1 Podmínky pro výměnu dat pro ověřování elektronických pečetí v certifikátu

Vydání následného certifikátu se řídí ustanoveními v kapitole 3.3.1.

Pokud nejsou splněny všechny tyto podmínky, není vydání následného certifikátu možné, a je nutné použít postup popsaný v kapitole 4.2.

4.7.2 Subjekty oprávněné požadovat výměnu dat pro ověřování elektronických pečetí v certifikátu

Žádost o vydání následného certifikátu podle této certifikační politiky mohou podat osoby, jimž byl vydán certifikát, o jehož následný certifikát je žádáno.

4.7.3 Zpracování požadavku na výměnu dat pro ověřování elektronických pečetí

Žadatel o následný certifikát požádá o vydání následného certifikátu dle postupů uvedených na webových stránkách poskytovatele.

Zpracování žádosti o následný certifikát se řídí ustanoveními v kapitolách 4.2.1 a 4.2.2.2.

4.7.4 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických pečetí pečetící osobě

Pro oznámení o vydání následného certifikátu řídí příslušnými ustanoveními kapitoly 4.3.2.

4.7.5 Úkony spojené s převzetím certifikátu s vyměněnými daty pro ověřování elektronických pečetí

Převzetí následného certifikátu se řídí příslušnými ustanoveními kapitoly 4.4.1.

4.7.6 Zveřejňování vydaných certifikátů s vyměněnými daty pro ověřování elektronických pečetí

Zveřejňování následného certifikátu se řídí příslušnými ustanoveními kapitoly 4.4.2.

4.7.7 Oznámení o vydání certifikátu s vyměněnými daty pro ověřování elektronických pečetí jiným subjektům

Oznámení o vydání následného certifikátu se řídí příslušnými ustanoveními kapitoly 4.4.3.

4.8 Změna údajů v certifikátu

Certifikát se změněnými údaji lze vydat pouze

- jako nový certifikát podle postupů uvedených v kapitolách 4.1 - 4.4, nebo

- jako následný certifikát podle postupů uvedených v kapitole 4.7, pokud byly změněny pouze údaje, které dovoluje tato certifikační politika změnit v následných certifikátech.

Změna údajů musí být zákazníkem oznámena poskytovateli odpovídajícím způsobem ještě před podáním žádosti o nový nebo následný certifikát.

Pokud pozbyl pravdivosti některý z údajů uvedených v aktuálním certifikátu, je nutné rovněž odpovídajícím způsobem požádat o zneplatnění aktuálního certifikátu.

4.8.1 Podmínky pro změnu údajů v certifikátu

Veškeré změny údajů v certifikátu musí být poskytovateli certifikačních služeb hlášeny změnovým seznamem žadatelů.

V případě, že poskytovatel certifikačních služeb zjistí, že údaje o zákazníkovi nebo žadateli v certifikátu nebo v systému certifikační autority neodpovídají skutečnosti, je oprávněn tyto údaje změnit.

4.8.2 Subjekty oprávněné požadovat změnu údajů v certifikátu

Změnový seznam žadatelů podává pověřená osoba zákazníka.

4.8.3 Zpracování požadavku na změnu údajů v certifikátu

Pracovník, případně systém registrační autority ověří:

- v případě pověřené osoby, zda je tato uvedena na aktuálním seznamu pověřených osob zákazníka, v případě osobní návštěvy její identitu prostřednictvím osobního dokladu,

- v případě samotného zákazníka, zda má uzavřenou platnou smlouvu o poskytování certifikačních služeb, a jeho identitu prostřednictvím osobního dokladu.

Pracovník, případně systém registrační autority poté aktualizuje údaje o žadateli a certifikátu v systému certifikační autority.

4.8.4 Oznámení o vydání certifikátu se změněnými údaji pečetící osobě

Totožné s vydáním prvního certifikátu. Viz ustanovení kapitoly 4.3.2.

4.8.5 Úkony spojené s převzetím certifikátu se změněnými údaji

Totožné s převzetím prvního certifikátu. Viz ustanovení kapitoly 4.4.1.

4.8.6 Zveřejňování vydaných certifikátů se změněnými údaji

Totožné se zveřejněním prvního certifikátu. Viz ustanovení kapitoly 4.4.2.

4.8.7 Oznámení o vydání certifikátu se změněnými údaji jiným subjektům

Totožné s oznámením o vydání prvního certifikátu. Viz ustanovení kapitoly 4.4.3.

4.9 Zneplatnění a pozastavení platnosti certifikátu

Žádost o zneplatnění certifikátu lze podat níže uvedenými způsoby:

- osobní návštěva registrační autority (pouze v provozní době kontaktního místa)

Seznam kontaktních míst registrační autority je uveden na webových stránkách poskytovatele.

- telefonicky

Telefon: 954 303 303

- e-mailem (nonstop)

E-mail: postsignum@cpost.cz

- webovou aplikací (nonstop)

Webová stránka: www.postsignum.cz/zneplatneni_certifikatu.html

Platnost certifikátu je ukončena v okamžiku jeho zneplatnění a zveřejněním na seznamu zneplatněných certifikátů.

Pokud není certifikát po dobu jeho platnosti nutné zneplatnit, skončí jeho platnost v časovém okamžiku uvedeném v certifikátu. Každý vydaný certifikát zůstává po ukončení své platnosti nadále uložen v databázi vydávající certifikační autority a archivován v souladu s platnou legislativou a archivačními předpisy České pošty.

4.9.1 Podmínky pro zneplatnění certifikátu

Důvody pro zneplatnění certifikátu koncového uživatele jsou především následující:

- jakékoliv podezření na kompromitaci odpovídajícího soukromého klíče,
- ukončení certifikace QESCD v případě, že odpovídající soukromý klíč je na tomto QESCD uložen,
- neplnění podmínek smlouvy o poskytování certifikačních služeb ze strany zákazníka,
- příkaz orgánu dohledu,
- příslušná žádost držitele nebo pečetící osoby,
- další důvody (úmrtí, zánik, zbavení nebo omezení právní způsobilosti pečetící osoby; pozbytí pravdivosti údajů, na jejichž základě byl certifikát vydán).

Certifikační autorita umožňuje zvolit jeden z následujících důvodů zneplatnění:

Kompromitace klíče (Key Compromise) – existuje podezření nebo je známo, že soukromý klíč žadatele byl ohrožen.

Změna vlastníka (Affiliation Changed) – označuje, že jméno subjektu nebo jiné identifikační údaje subjektu v certifikátu se změnily.

Nahrazení certifikátu (Superseded) – certifikát je nahrazen, protože žadatel požádal o nový certifikát.

Skončení operace (Cessation Of Operation) – žadatel již nevlastní nebo neovládá certifikát před vypršením jeho platnosti.

Neznámý (Unspecified) – důvod zneplatnění certifikátu není žádný z výše uvedených. Tento důvod zneplatnění není uveden u příslušného certifikátu v seznamu zneplatněných certifikátů.

Odejmuto oprávnění (Privilege withdrawn) – tento důvod může být nastaven v případě zneplatnění z vůle certifikační autority v případě, kdy žadatel podstatným způsobem porušil ustanovení smlouvy nebo certifikační politiky.

4.9.2 Subjekty oprávněné žádat o zneplatnění certifikátu

O zneplatnění certifikátu může požádat:

- zákazník (držitel certifikátu) prostřednictvím pověřené osoby nebo statutárního zástupce,
- žadatel o certifikát,
- Manažer CA,
- zástupce orgánu dohledu.

4.9.3 Požadavek na zneplatnění certifikátu

4.9.3.1 Žádost o zneplatnění certifikátu podaná osobně žadatelem o certifikát na registrační autoritě

Žadatel o certifikát požádá o zneplatnění certifikátu osobně na pracovišti registrační autority, kde prokáže svou totožnost (viz kapitola 3.2.3). Podepíše písemnou žádost o zneplatnění certifikátu, kterou vytiskne pracovník registrační autority. Žádost obsahuje sériové číslo certifikátu, jméno vydávající certifikační autority a volitelně i důvod zneplatnění.

Pracovník registrační autority vyhledá certifikát a zahájí proces zneplatnění. Ověří, zda žadatel má právo žádat o zneplatnění certifikátu. Pokud ověření proběhne úspěšně, odešle pracovník registrační autority žádost o zneplatnění do systému certifikační autority ke zpracování. Po zpracování žádosti systémem certifikační autority ověří pracovník stav certifikátu a zajistí předání protokolu o zneplatnění certifikátu žadateli.

4.9.3.2 Žádost o zneplatnění certifikátu podaná telefonicky nebo jiným vzdáleným způsobem

Žadatel o zneplatnění certifikátu podává žádost o zneplatnění certifikátu telefonicky na telefonní číslo uvedené v kapitole 4.9, nebo jiným vzdáleným způsobem specifikovaným na webových stránkách poskytovatele. Služba pro telefonické zneplatnění je dostupná 24 hodin denně. Každá takto podaná žádost musí obsahovat sériové číslo certifikátu, jméno vydávající certifikační autority, heslo pro zneplatnění certifikátu a volitelně důvod zneplatnění.

Pracovník oprávněný provádět zneplatnění zkontroluje heslo pro zneplatnění v žádosti oproti heslu zadanému při registraci žádosti o certifikát. V případě, že údaje souhlasí, certifikát zneplatní. V opačném případě pracovník zneplatnění neprovede a informuje žadatele.

Pokud bylo zneplatnění úspěšné, je vytvořen protokol o zneplatnění, který je prostřednictvím elektronické pošty zaslán žadateli na adresu uvedenou ve zneplatněném certifikátu. (pokud certifikát adresu elektronické pošty obsahuje) a na kontaktní adresu žadatele uvedenou v systému certifikační autority.

4.9.3.3 Žádost o zneplatnění certifikátu podaná pověřenou osobou

V případě, že o zneplatnění žádá zákazník, učiní tak písemnou formou. Pověřená osoba se dostaví osobně na registrační autoritu České pošty, kde s ní bude sepsána žádost o zneplatnění certifikátu.

Pokud pověřená osoba vlastní certifikát určený k podpisu, vydaný podřízenou certifikační autoritou v hierarchii PostSignum, může zaslat žádost o zneplatnění certifikátu v e-mailové zprávě opatřené elektronickým podpisem na adresu uvedenou v kapitole 4.9.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je prostřednictvím elektronické pošty zaslán pověřené osobě. Žadatel je o zneplatnění certifikátu informován prostřednictvím elektronické pošty na adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje) a na kontaktní adresu žadatele uvedenou v systému certifikační autority.

4.9.3.4 Zneplatnění certifikátu z vůle certifikační autority

O zneplatnění certifikátu může rozhodnout rovněž poskytovatel certifikačních služeb, pokud pečetící osoba porušuje pravidla certifikační politiky nebo dohodnuté smluvní podmínky. PostSignum QCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát zneplatněn. Manažer CA podává elektronicky podepsanou žádost o zneplatnění certifikátu, kterou předá některému z pracovníků oprávněných provádět zneplatnění certifikátu.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je prostřednictvím elektronické pošty neprodleně zaslán žadateli společně s důvodem zneplatnění certifikátu na adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje) a na kontaktní adresu žadatele uvedenou v systému certifikační autority.

4.9.3.5 Zneplatnění certifikátu z vůle orgánu dohledu

O zneplatnění kvalifikovaného certifikátu může rozhodnout rovněž orgán dohledu. PostSignum QCA v takovém případě informuje zákazníka o zneplatnění certifikátu s udáním důvodu, proč byl certifikát zneplatněn. Zástupce orgánu dohledu podává písemnou žádost o zneplatnění certifikátu Manažerovi CA, v žádosti musí být uveden důvod zneplatnění certifikátu.

Po úspěšném zneplatnění je vytvořen protokol o zneplatnění certifikátu, který je prostřednictvím elektronické pošty neprodleně zaslán žadateli společně s důvodem zneplatnění certifikátu na adresu uvedenou ve zneplatněném certifikátu (pokud certifikát adresu elektronické pošty obsahuje) a na kontaktní adresu žadatele uvedenou v systému certifikační autority.

4.9.4 Doba odkladu požadavku na zneplatnění certifikátu

V okamžiku, kdy se osoba oprávněná žádat o zneplatnění certifikátu dozví skutečnost, která je důvodem pro zneplatnění certifikátu, musí neprodleně požádat o zneplatnění certifikátu.

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

Doba od přijetí žádosti o zneplatnění certifikátu do zveřejnění CRL obsahujícího i zneplatněný certifikát nepřesáhne 24 hodin.

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

Uživatel certifikátu vydaného PostSignum Qualified CA (spoléhající se strana) je povinen postupovat v souladu s ustanoveními kapitoly 4.5.2.

4.9.7 Periodicita vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů (CRL) je vydáván vždy vzápětí po zpracování žádosti o zneplatnění certifikátu. Nedojde-li ke zneplatnění certifikátu, je nový CRL vydáván alespoň každých 24 hodin. Seznam zneplatněných certifikátů je zveřejňován na těchto místech:

- distribučních bodech CRL (CDP) uvedených v certifikátu
- na webových stránkách poskytovatele,
- u nezávislého poskytovatele webových služeb.

Primárním zdrojem aktuálního CRL jsou distribuční body CRL.

4.9.8 Maximální zpoždění při vydávání seznamu zneplatněných certifikátů

Seznam zneplatněných certifikátů je zveřejněn co nejdříve po vydání; vždy je dodrženo ustanovení kapitoly 4.9.5.

4.9.9 Možnost ověřování statutu certifikátu on-line (dále „OCSP“)

Pro ověření certifikátu vydaného dle této certifikační politiky je možné využít veřejně dostupnou bezplatnou službu OCSP, která je poskytována dle standardu RFC 6960.

Odkaz na OCSP responder je uveden přímo v certifikátu vydaném dle této certifikační politiky, viz profil certifikátu uvedený v kapitole 7.

Profil certifikátu OCSP responderu je uveden v certifikační politice pro vydání certifikátu OCSP, která je dostupná na webových stránkách poskytovatele.

Profil žádosti a odpovědi OCSP responderu je uveden v certifikační prováděcí směrnici.

4.9.10 Požadavky při ověřování statutu certifikátu on-line

Viz ustanovení v kapitole 4.9.9.

4.9.11 Jiné způsoby oznamování zneplatnění certifikátu

Poskytovatel certifikačních služeb neposkytuje žádné další možnosti, kromě výše uvedených, pro ověření stavu certifikátu.

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

Postup pro zneplatnění certifikátu v případě kompromitace dat pro vytváření elektronických pečetí je shodný s obecným postupem pro zneplatnění certifikátu.

4.9.13 Podmínky pro pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.9.14 Subjekty oprávněné požadovat pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.9.15 Zpracování požadavku na pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.9.16 Omezení doby pozastavení platnosti certifikátu

PostSignum QCA tuto službu neposkytuje.

4.10 Služby související s ověřováním statutu certifikátu

Status certifikátu je možné ověřit

- na seznamu zneplatněných certifikátů (CRL) v rámci služby umožňující přístup k veřejným informacím PostSignum QCA protokolem HTTP, nebo
- v rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách poskytovatele, nebo
- pomocí služby OCSP.

4.10.1 Funkční charakteristiky

Seznam zneplatněných certifikátů a informace o stavu certifikátu jsou považovány za veřejně přístupné informace. Seznam zneplatněných certifikátů (CRL) je zveřejňován na místech uvedených v kapitole 4.9.7.

V rámci služby vyhledávání vydaných certifikátů přístupné na webových stránkách poskytovatele je zveřejňována rovněž informace o stavu vyhledávaného certifikátu. Tato informace o stavu certifikátu je pouze informativní, jedná se pouze o doplňkovou informaci k aktuálnímu CRL, které je vždy závazným zdrojem informací o stavu certifikátu.

Služba OCSP vrací stav certifikátu v reálném čase (on-line) na základě zaslané žádosti. Informace o stavu certifikátu získané pomocí služby OCSP jsou závazným zdrojem informací o stavu certifikátu.

4.10.2 Dostupnost služeb

Seznam zneplatněných certifikátů je prostřednictvím služby umožňující přístup k veřejným informacím dostupný 7 dní v týdnu 24 hodin denně. Architektura řešení a havarijní plány jsou navrženy tak, aby vždy existovalo alespoň jedno místo, kde je možné získat aktuální Seznam zneplatněných certifikátů.

Služba pro vyhledávání certifikátů je dostupná 7 dní v týdnu 24 hodin denně.

Služba OCSP je dostupná 7 dní v týdnu 24 hodin denně.

4.10.3 Další charakteristiky služeb statutu certifikátu

Další charakteristiky služeb statutu certifikátu nejsou stanoveny.

4.11 Ukončení poskytování služeb pro držitele certifikátu

Poskytování služeb pro držitele certifikátu končí ukončením smlouvy mezi zákazníkem a poskytovatelem certifikačních služeb. Toto se netýká služeb zneplatnění certifikátu, které jsou poskytovány po celou dobu platnosti certifikátu.

Ukončení smlouvy o poskytování certifikačních služeb nebo odstoupení od této smlouvy se řídí [VOP].

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

PostSignum QCA tuto službu neposkytuje.

4.12.1 Politika a postupy při úschově a obnovování dat pro vytváření elektronických pečetí

PostSignum QCA tuto službu neposkytuje.

4.12.2 Politika a postupy při zapouzdřování a obnovování šifrovacího klíče pro relaci

PostSignum QCA tuto službu neposkytuje.

5 MANAGEMENT, PROVOZNÍ A FYZICKÁ BEZPEČNOST

Pro PostSignum QCA byly zpracovány dokumenty:

- Systémová bezpečnostní politika, popisující zásady bezpečnosti v oblasti fyzické, procedurální a personální;
- Plán pro zvládání krizových situací a plán obnovy, popisující postupy pro zachování garantované úrovně služeb v případě výskytu mimořádné situace,
- Provozní a bezpečnostní procedury, popisující na logické úrovni postupy dodržované v PostSignum QCA, a
- Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, která mj. upravuje oblast obsazování rolí PostSignum QCA.

Zmíněné dokumenty byly vypracovány na základě výsledků provedené analýzy rizik.

Tyto dokumenty jsou mj. přístupné osobám, které provádějí kontrolu bezpečnostní shody PostSignum QCA. Tato kapitola vychází z výše uvedených dokumentů a poskytuje stručný přehled základních bezpečnostních zásad uplatňovaných v PostSignum QCA.

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

V PostSignum QCA existují následující typy stabilních pracovišť umístěných v prostorách České pošty nebo jejích smluvních partnerů:

- centrální pracoviště (hlavní a záložní lokalita),
- operátorská pracoviště centra (zejména pro správu podpůrného informačního systému),
- pracoviště registrační autority a
- obchodní místa.

Použitá konstrukce vyplývá z bezpečnostních požadavků uvedených v dokumentu Systémová bezpečnostní politika; obecně platí, že všechny výše uvedené typy pracovišť mají jasně definovaný perimetr a jsou proti neoprávněnému vniknutí chráněny mechanickými prostředky. Centrální pracoviště jsou zabezpečena obdobně jako zabezpečené oblasti kategorie „Důvěrné“.

Kromě toho existuje pracoviště mobilní registrační autority, kde je neexistence opatření z oblasti fyzické bezpečnosti kompenzována opatřeními z oblasti organizační bezpečnosti.

5.1.2 Fyzický přístup

Pro každý typ pracoviště je v jeho provozním řádu definováno, kteří pracovníci mají na pracoviště fyzický přístup. Prostory jsou chráněny proti neoprávněnému vniknutí mechanickými prostředky (bezpečnostní zámky a mříže), na centrálním pracovišti též samostatnou smyčkou elektronického zabezpečovacího zařízení. Na pracoviště mobilní registrační autority se vztahují režimová opatření definovaná v Systémové bezpečnostní politice.

5.1.3 Elektřina a klimatizace

Centrální pracoviště jsou připojena na nepřerušitelný zdroj napájení (UPS) a mají nainstalovánu klimatizaci, která udržuje teplotu a vlhkost optimální pro provozovaná zařízení.

5.1.4 Vlivy vody

Centrální pracoviště jsou umístěna mimo zátopové oblasti.

Prostory centrálních pracovišť jsou vybaveny signalizací zatopení vodou.

5.1.5 Protipožární opatření a ochrana

Prostory centrálních pracovišť jsou vybaveny elektronickou požární signalizací (EPS).

5.1.6 Ukládání médií

Pro účely uskladnění dat PostSignum QCA jsou k dispozici trezory.

5.1.7 Nakládání s odpady

Papírové dokumenty a média, která jsou používána v PostSignum QCA, jsou poté, co nejsou zapotřebí, likvidována bezpečným způsobem:

- média jsou fyzicky zlikvidována nebo je použit vhodný program zajišťující úplné smazání média,
- papírové dokumenty jsou zlikvidovány v zařízení k tomu určeném.

5.1.8 Zálohy mimo budovu

Pro PostSignum QCA byla vybudována záložní lokalita, kam provoz přechází v mimořádných situacích, kdy není možné zabezpečit řádný provoz QCA v hlavní lokalitě, a kam jsou také pravidelně zasílány zálohy systémů PostSignum QCA.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

V PostSignum QCA byly definovány role, které zastává obsluha PostSignum QCA. Jsou stanovena pravidla, podle kterých jsou role obsazovány, tedy kdo pracovníka v dané roli jmenuje a odvolává, které role nesmí zastávat současně jedna osoba. Veškerá přístupová práva (na úrovni fyzického přístupu, na úrovni přístupu k operačnímu systému, na úrovni přístupu k aplikaci) jsou vázána na tyto role.

Zvláštní pozornost je zejména věnována při obsazování rolí s možností přístupu k centrálním systémům PostSignum QCA.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

V PostSignum QCA jsou definovány činnosti vyžadující přítomnost více než jedné osoby. Jedná se zejména o činnosti, při kterých se manipuluje se soukromým klíčem certifikační autority a s kryptografickým modulem použitým pro generování a úschovu soukromého klíče (bezpečným kryptografickým modulem) certifikační autority.

5.2.3 Identifikace a autentizace pro každou roli

Představitel každé role se musí při přístupu k prostředkům PostSignum QCA identifikovat a autentizovat. Každý uživatel má přidělenou jednoznačnou identifikaci ve všech systémech, ke kterým má přístup. V systémech PostSignum QCA je používaná identifikace jménem resp. certifikátem a autentizace heslem resp. soukromým klíčem.

5.2.4 Role vyžadující rozdělení povinností

V PostSignum QCA jsou stanovena pravidla, podle kterých jsou obsazovány jednotlivé role, a rovněž byla stanovena pravidla pro separaci rolí. Tato pravidla jsou uvedena v dokumentu Organizační zajištění úlohy Kvalifikovaná certifikační autorita České pošty, s.p

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Role, zajišťující provoz, správu, údržbu a rozvoj systémů PostSignum QCA jsou obsazovány na základě procedur (např. vyžadování referencí, zkušební období apod.), které zajišťují, aby tyto funkce byly obsazovány důvěryhodnými a kvalifikovanými pracovníky. Obdobné procedury platí pro uzavírání smluv s externími spolupracovníky nebo smluvními partnery.

V případě, že daná osoba není zaměstnancem České pošty, ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

5.3.2 Posouzení spolehlivosti osob

Do rolí obsluhy PostSignum QCA jsou jmenovány výhradně osoby, které jsou delší dobu zaměstnány v České poště a mají dobré pracovní a osobní reference.

V případě, že daná osoba není zaměstnancem České pošty, ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

5.3.3 Požadavky na přípravu pro výkon role, vstupní školení

Všichni pracovníci, podílející se na provozu, správě, údržbě a rozvoji systémů PostSignum QCA, jsou vyškoleni. Součástí školení je i školení o bezpečnosti systému a o chování v havarijních situacích.

O provedení školení musí být proveden písemný zápis obsahující mj. datum školení, obsah školení, jméno školitele a seznam účastníků. Tento zápis musí být podepsán všemi účastníky i školitelem.

U rolí určených Manažerem CA může být školení nahrazeno prokazatelným seznámením pracovníka se všemi dokumenty upravujícími provoz QCA se vztahem k příslušné roli.

V případě, že daná osoba není zaměstnancem České pošty, ale jejího smluvního partnera, uplatní se uvedené požadavky v příslušném rozsahu u daného partnera.

5.3.4 Požadavky a periodicita školení

V PostSignum QCA existuje program vytváření, udržování a prohlubování bezpečnostního vědomí, diferencovaný podle rolí.

Manažer CA v pravidelných intervalech (zejména při změnách v postupech PostSignum QCA) organizuje školení obsluhy.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Požadavky na rotaci pracovníků a její frekvenci nejsou definovány.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Postihy za porušení pracovní kázně se řídí organizačními předpisy České pošty nebo ustanoveními smlouvy mezi Českou poštou a smluvním partnerem.

5.3.7 Požadavky na nezávislé zhotovitele (dodavatele)

Na smluvní (externí) pracovníky jsou uplatňována obdobná kritéria jako na zaměstnance České pošty.

5.3.8 Dokumentace poskytovaná zaměstnancům

Personál PostSignum QCA má k dispozici dokumentaci odpovídající jím obsazené roli, zejména

- bezpečnostní politiky,
- certifikační politiky,
- certifikační prováděcí směrnici,
- provozní dokumentaci – příručky a pracovní postupy pro obsluhu.

5.4 Auditní záznamy (logy)

Pro PostSignum QCA byl zpracován dokument Auditní a archivační politika (je přílohou dokumentu Systémová bezpečnostní politika), který popisuje zásady kontroly, auditu a archivace PostSignum QCA. Tento dokument je přístupný osobám, které provádějí kontrolu bezpečnostní shody PostSignum QCA. Tato kapitola vychází z dokumentu Auditní a archivační politika a poskytuje stručný přehled základních zásad uplatňovaných při kontrole PostSignum QCA.

5.4.1 Typy zaznamenávaných událostí

Pro potřeby kontroly a případné analýzy a vyšetření mimořádných událostí (obecně pro zajištění možnosti prokázat sled operací PostSignum QCA a jejich přiřazení osobě, která je vyvolala) jsou vedeny záznamy o událostech při vydání certifikátů, ukončení platnosti certifikátů, nakládání s klíči a certifikáty PostSignum QCA a dalších významných událostech (např. ukončení činnosti certifikační autority).

Auditní záznamy v písemné podobě musí být podepsány a musí uvádět jméno pracovníka, který záznam pořídil.

5.4.2 Periodicita zpracování záznamů

Auditní záznamy jsou kontrolovány osobami v odpovídající roli pověřené tímto úkolem v intervalech definovaných Systémovou bezpečnostní politikou. Dále podléhají interní a externí kontrole.

5.4.3 Doba uchování auditních záznamů

Auditní záznamy jsou uchovávány po dobu deseti let, pokud jiný předpis nestanoví dobu delší.

5.4.4 Ochrana auditních záznamů

Auditní záznamy jsou uloženy tak, aby byly ochráněny proti krádeži, modifikaci a zničení úmyslnému i neúmyslnému (ohněm, vodou).

Auditní záznamy v podobě datových souborů jsou archivovány na nepřepisovatelných médiích.

5.4.5 Postupy pro zálohování auditních záznamů

Auditní záznamy (kromě auditních záznamů o činnosti centrálních komponent certifikační autority v elektronické podobě) nejsou obecně zálohovány; jsou pouze archivovány. Důležité auditní záznamy spojené s vydáním certifikátů jsou uchovávány ve dvou kopiích, které jsou uložené v různých lokalitách.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

V prostředí PostSignum QCA není nasazen systém na centrální shromažďování auditních záznamů. Auditní záznamy jsou shromažďovány v rámci jednotlivých systémů PostSignum QCA.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjektu, který způsobil událost zaznamenanou v auditním logu, není tato skutečnost nijak oznamována.

5.4.8 Hodnocení zranitelnosti

Auditní záznamy jsou v pravidelných intervalech procházeny, kontrolovány a analyzovány na výskyt záznamů o nestandardních událostech, které mohou znamenat pokus o narušení bezpečnosti. Dále jsou definovány postupy, jak v těchto případech dále postupovat.

Zprávy o nestandardních událostech jsou mj. předávány i Auditorovi CA.

5.5 Uchovávání informací a dokumentace

Pro PostSignum QCA byl zpracován dokument Auditní a archivační politika, který popisuje zásady kontroly, auditu a archivace v PostSignum QCA. Tento dokument je mj. přístupný osobám, které provádějí kontrolu PostSignum QCA.

5.5.1 Typy informací a dokumentace, které se uchovávají

V PostSignum QCA se archivují tyto záznamy:

- programové vybavení a data, včetně vydaných certifikátů a CRL,
- veškerá dokumentace související s registrací žádosti o certifikát, včetně smluv,
- záznamy o obsazování rolí PostSignum QCA a záznamy o školení obsluhy,
- logy automaticky vytvářené komponentami informačního systému PostSignum QCA.

5.5.2 Doba uchování uchovávaných informací a dokumentace

Programové vybavení, data a auditní záznamy se archivují po dobu deseti let.

5.5.3 Ochrana úložiště uchovávaných informací a dokumentace

Archiv je zabezpečen pomocí opatření technické a objektové bezpečnosti. Je rovněž chráněn proti vlivům prostředí, jako jsou teplota, vlhkost atd.

5.5.4 Postupy při zálohování uchovávaných informací a dokumentace

Zálohovací procedury archivu jsou upraveny samostatným dokumentem Auditní a archivační politika, který je mj. přístupný osobám provádějícím kontrolu PostSignum QCA.

5.5.5 Požadavky na používání časových razítek při uchovávání informací a dokumentace

Pokud jsou v PostSignum QCA využívána časová razítka, jedná se o kvalifikovaná elektronická časová razítka PostSignum QCA.

5.5.6 Systém shromažďování uchovávaných informací a dokumentace (interní nebo externí)

V prostředí PostSignum QCA jsou auditní záznamy shromažďovány a přesouvány do Archivu CA v souladu s postupy uvedenými v dokumentu Auditní a archivační politika.

5.5.7 Postupy pro získání a ověření uchovávaných informací a dokumentace

Archivy dat a programového vybavení jsou umístěny v k tomu určených trezorech.

V každé lokalitě, kde je umístěn trezor, musí být veden protokol o uložených archivních médiích, do kterého jsou zaznamenávány veškeré manipulace s uloženými médii.

Přístup k archivům je omezen na osoby v odpovídajících rolích.

5.6 Výměna dat pro ověřování elektronických pečetí v nadřízeném certifikátu pro elektronickou pečeť poskytovatele

Platnost klíčů certifikačních autorit v hierarchii PostSignum QCA je omezena.

S dostatečným předstihem, avšak nejméně 1 rok před vypršením platnosti certifikátu PostSignum Root QCA se musí uskutečnit ceremoniál vydání nového certifikátu. Výsledkem ceremoniálu bude vytvořený nový samopodepsaný certifikát kořenové certifikační autority, který bude zveřejněn způsobem popsaným v kapitole 2.

Nejméně 1 rok před vypršením platnosti certifikátu je provozovatel certifikační autority PostSignum Qualified CA povinen požádat o vydání dalšího certifikátu u PostSignum Root QCA.

Plánovaná výměna klíčů certifikační autority musí být oznámena zákazníkům nejpozději 6 měsíců před aktivním používáním nového certifikátu PostSignum Root QCA resp. 3 měsíce před aktivním používáním certifikátu autority PostSignum Qualified CA. Toto oznámení bude (včetně důvodu ukončení platnosti certifikátu) zveřejněno na webových stránkách poskytovatele a na všech pracovištích registrační autority PostSignum QCA.

Po ukončení potřeby používání původních dat pro vytváření elektronických pečetí Česká pošta prokazatelně tato data, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, zničí a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy bude nutné provést výměnu dat z důvodu nedostatečnosti záruk poskytovaných použitým algoritmem nebo jeho parametry (např. velikostí modulu).

5.7 Obnova po havárii nebo kompromitaci

Pro PostSignum QCA byly vypracovány dokumenty popisující zvládání krizových situací a postupy pro následnou obnovu.

Tato dokumentace je mj. přístupná pro osoby provádějící kontrolu PostSignum QCA.

Personál PostSignum QCA je řádně vyškolen, jak postupovat v případě havárie. Test havarijního plánu se provádí minimálně jedenkrát ročně.

5.7.1 Postup v případě incidentu a kompromitace

Zabezpečení prostředků certifikační autority po živelné katastrofě nebo jiné mimořádné události je rozpracováno v dokumentech Krizový plán ochrany objektu a Plán zvládání krizových situací a plán obnovy.

5.7.2 Poškození výpočetních prostředků, softwaru nebo dat

Zabezpečení prostředků certifikační autority po živelné katastrofě nebo jiné mimořádné události je rozpracováno v dokumentech Krizový plán ochrany objektu a Plán zvládání krizových situací a plán obnovy.

5.7.3 Postup při kompromitaci dat pro vytváření elektronických pečetí poskytovatele

5.7.3.1 Kompromitace soukromého klíče podřízené certifikační autority

V případě podezření na kompromitaci soukromého klíče PostSignum Qualified CA budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán dohledu a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb o mimořádném ukončení činnosti této autority; oznámení bude rovněž zveřejněno na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

PostSignum Root QCA okamžitě zneplatní certifikát PostSignum Qualified CA a tato zneplatní všechny platné certifikáty vydané koncovým zákazníkům; zneplatněné certifikáty budou neprodleně zveřejněny na příslušném CRL.

Po zveřejnění informace o mimořádném ukončení činnosti končí platnost všech certifikátů vydaných PostSignum Qualified CA.

Česká pošta prokazatelně zničí data pro vytváření elektronických pečetí PostSignum Qualified CA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, u nichž existuje podezření na kompromitaci, a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických pečetí, které nepopiratelně zpochybní důvěryhodnost vydávaných certifikátů a seznamů vydávaných certifikátů.

5.7.3.2 Kompromitace soukromého klíče PostSignum Root QCA

V případě podezření na kompromitaci soukromého klíče PostSignum Root QCA provede poskytovatel certifikačních služeb zneplatnění certifikátu PostSignum Root QCA, platných certifikátů všech podřízených certifikačních autorit a všech jimi vydaných platných certifikátů; zneplatněné certifikáty budou neprodleně zveřejněny na příslušném CRL. O zneplatnění certifikátů (případně o mimořádném

ukončení činnosti autority) budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán dohledu a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb; oznámení bude rovněž zveřejněno na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA a v jednom celostátně vydávaném deníku. Součástí oznámení bude i důvod ukončení platnosti certifikátu certifikační autority.

Po zveřejnění informace o mimořádném ukončení činnosti končí platnost všech certifikátů vydaných PostSignum Root QCA i podřízenými certifikačními autoritami.

Česká pošta prokazatelně zničí data pro vytváření elektronických pečetí PostSignum Root QCA, která sloužila pro podepisování kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, u nichž existuje podezření na kompromitaci, a o tomto zničení provede záznam.

Tento postup bude také použit v případě, kdy dojde k náhlému oslabení algoritmu použitého pro vytváření elektronických pečetí, které nepopiratelně zpochybní důvěryhodnost vydávaných certifikátů a seznamů vydávaných certifikátů.

5.7.4 Schopnost obnovit činnost po havárii

Obnova činnosti po havárii se řídí platným interním dokumentem Plán zvládání krizových situací a plán obnovy.

5.8 Ukončení činnosti CA nebo RA

5.8.1 Ukončení činnosti kořenové certifikační autority

Ukončení činnosti PostSignum Root QCA musí být písemně oznámeno všem držitelům platných certifikátů, orgánu dohledu a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a rovněž zveřejněno na webových stránkách poskytovatele a na všech pracovištích registrační autority PostSignum QCA. V případě, že součástí ukončení činnosti autority je i ukončení platnosti jejího certifikátu, musí být součástí oznámení i tato informace včetně příslušného důvodu ukončení platnosti. Dokud je platný alespoň jeden certifikát vydaný PostSignum Root QCA, musí PostSignum Root QCA zajišťovat alespoň funkci zneplatnění certifikátu a vydání CRL.

Pokud PostSignum Root QCA tuto funkci není schopna zajistit po celou dobu platnosti vydaných certifikátů, musí o této skutečnosti informovat držitele platných certifikátů spolu s uvedením data, do kdy bude funkce poskytována. Toto datum může být nejdříve 6 měsíců ode dne zaslání oznámení. K tomuto datu PostSignum Root QCA zneplatní všechny dosud platné vydané certifikáty a vydá poslední CRL. Teprve poté může být činnost PostSignum Root QCA ukončena.

V tomto případě budou smlouvy o poskytování certifikačních služeb ukončeny ze strany ČP dohodou nebo výpovědí.

Následně ČP prokazatelně zničí data pro vytváření elektronických pečetí PostSignum Root QCA, která sloužila pro pečetění kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole 5.4.

5.8.2 Ukončení činnosti podřízené certifikační autority

Ukončení činnosti PostSignum Qualified CA musí být písemně oznámeno všem držitelům platných certifikátů, orgánu dohledu a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a rovněž zveřejněno na webových stránkách poskytovatele a na všech pracovištích registrační autority PostSignum QCA. Součástí oznámení musí být i informace o ukončení platnosti

certifikátu autority včetně příslušného důvodu ukončení. Dokud je platný alespoň jeden certifikát vydaný PostSignum Qualified CA, musí tato autorita zajišťovat alespoň funkci zneplatnění certifikátu a vydání CRL.

Pokud PostSignum Qualified CA tuto funkci není schopna zajistit po celou dobu platnosti vydaných certifikátů, musí o této skutečnosti informovat držitele platných certifikátů spolu s uvedením data, do kdy bude funkce poskytována. Toto datum může být nejdříve 3 měsíce ode dne zaslání oznámení. K tomuto datu PostSignum Qualified CA zneplatní všechny dosud platné vydané certifikáty a vydá poslední CRL. Teprve poté může být činnost této autority ukončena.

Zneplatněný certifikát pro elektronickou pečeť PostSignum Qualified CA bude zveřejněn na CRL PostSignum Root QCA v čase uvedeném v certifikační politice PostSignum Root QCA.

Smlouvy o poskytování certifikačních služeb budou v tomto případě ukončeny ze strany ČP dohodou nebo výpovědí.

Následně ČP prokazatelně zničí data pro vytváření elektronických pečetí PostSignum Qualified CA, která sloužila pro pečetění kvalifikovaných certifikátů a seznamů zneplatněných certifikátů, a o tomto zničení provede záznam. Záznamy budou uchovávány v souladu s ustanoveními této certifikační politiky uvedenými v kapitole 5.4.

5.8.3 Ukončení činnosti registrační autority

Ukončení činnosti pracoviště registrační autority je zákazníkům oznámeno vývěskami na příslušném pracovišti nebo na budově a na webových stránkách poskytovatele. Spolu s oznámením o ukončení činnosti pracoviště je uvedena i adresa a kontakty pracoviště náhradního.

5.8.4 Ukončení činnosti poskytovatele certifikačních služeb

Činnost poskytovatele certifikačních služeb bude ukončena v souladu s platnými právními předpisy. Pokud po ukončení činnosti poskytovatele certifikačních služeb nebude nadále možné zajistit přístup k údajům, které byly evidovány z důvodu poskytování certifikačních služeb a které by mohly sloužit pro účely poskytnutí důkazů v soudním a správním řízení a pro účely zajištění kontinuity služby, tak tyto údaje předá Manažer CA orgánu dohledu.

5.8.5 Odnětí akreditace

V případě odnětí akreditace musí být informace o odnětí akreditace písemně nebo elektronicky oznámena všem držitelům platných certifikátů a subjektům, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb a zveřejněna na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA a dalšími způsoby uvedenými v platných právních předpisech. Součástí informace bude i sdělení, že kvalifikované certifikáty vydané tímto poskytovatelem nelze nadále používat podle platných právních předpisů.

O dalším postupu v tomto případě rozhodne management ČP na základě příslušného rozhodnutí orgánu dohledu.

6 TECHNICKÁ BEZPEČNOST

6.1 Generování a instalace párových dat

6.1.1 Generování párových dat

Klíčové páry certifikačních autorit v hierarchii PostSignum QCA jsou generovány a uloženy v hardwarovém kryptografickém modulu. Generování těchto klíčových párů probíhá kontrolovaným procesem, na jehož průběh dohlíží Manažer CA a Auditor CA.

Klíčové páry jednotlivých komponent nebo systémů PostSignum QCA (infrastrukturní klíče) jsou generovány v kontrolovaném prostředí systémů PostSignum QCA. Tyto klíčové páry jsou uloženy v kryptografickém modulu; pro přístup k těmto klíčovým párům je nutné vložit čipovou kartu obsluhy a zadat PIN.

Klíčové páry operátorů PostSignum QCA (včetně operátorů RA; kontrolní klíče) jsou generovány ve vyhrazených hardwarových prostředcích, které svou konstrukcí neumožňují export soukromých klíčů. Pro použití soukromých klíčů je vždy nutné zadat PIN.

Soukromé klíče žadatelů jsou generovány a uschovávány žadatelem o certifikát. Klíče mohou být generovány a následně i uloženy jak v softwarovém, tak i hardwarovém úložišti. PostSignum QCA nepředepisuje konkrétní požadavky na příslušné úložiště.
Pokud žadatel požaduje vydání certifikátu s příznakem, že soukromý klíč je uložený na QESCD, musí být soukromý klíč vygenerován přímo na QESCD.

6.1.2 Předání dat pro vytváření elektronických pečetí pečetící osobě

PostSignum QCA neposkytuje službu generování klíčových párů pro žadatele o certifikát a se soukromými klíči žadatelů nepřichází do styku a není zodpovědná za jejich ochranu ani zálohování.

V případě, že poskytovatel spravuje a provozuje QESCD pro účely uložení dat pro vytváření elektronických pečetí zákazníkem, generování soukromého klíče provádí poskytovatel přímo v QESCD dle podmínek dohodnutých se zákazníkem.

6.1.3 Předání dat pro ověřování elektronických pečetí poskytovateli certifikačních služeb

Veřejný klíč žadatele je poskytovateli certifikačních služeb doručen v elektronické podobě, v žádosti o certifikát ve formátu PKCS#10.

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

Certifikáty certifikačních autorit a dále certifikáty podepisujících nebo pečetících osob, pro které byl vysloven souhlas se zveřejněním, jsou zveřejněny způsobem popsaným v kapitole 2.

6.1.5 Délky párových dat

Klíče certifikačních autorit v hierarchii PostSignum mají pro algoritmus RSA délku modulu minimálně 2048 bitů.

Klíče držitelů certifikátů mají pro algoritmus RSA délku modulu 2048 nebo 4096 bitů. Jiný algoritmus než RSA není pro držitele certifikátů povolen.

6.1.6 Generování parametrů dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí a kontrola jejich kvality

Parametry používané při vytváření veřejných klíčů komponent PostSignum QCA jsou generovány odpovídajícím softwarovým a hardwarovým vybavením. Použité algoritmy a jejich parametry odpovídají požadavkům platných právních předpisů nebo technických norem, které upravují činnost poskytovatelů certifikačních služeb.

Parametry používané při vytváření veřejných klíčů žadatelů o certifikát jsou generovány softwarovým nebo hardwarovým vybavením žadatele a poskytovatel certifikačních služeb za ně nenese odpovědnost.

Kontrola kvality dat pro ověřování elektronických podpisů nebo dat pro ověřování elektronických pečetí je nastavena na úrovni certifikační autority, která kontroluje jedinečnost a povolenou délku veřejného klíče.

6.1.7 Omezení pro použití dat pro ověřování elektronických pečetí

Veřejné klíče koncových uživatelů mohou být použity pouze v souladu s pravidly popsanými v kapitole 1.4

6.2 Ochrana dat pro vytváření elektronických podpisů nebo dat pro ověřování elektronických pečetí a bezpečnost kryptografických modulů

6.2.1 Standardy a podmínky používání kryptografických modulů

Kryptografický modul použitý pro generování a úschovu soukromého klíče certifikačních autorit (nástroj pro vytváření elektronického podpisu nebo elektronické pečetě) působících v hierarchii PostSignum QCA splňuje požadavky standardu FIPS 140-2 Level 3 a byla mu orgánem dohledu vyslovena shoda.

6.2.2 Sdílení tajemství

Soukromý klíč certifikační autority je během provozu uložen v aktivovaném a konfigurovaném kryptografickém modulu (bezpečném kryptografickém modulu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (bezpečného kryptografického modulu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však tří osob.

6.2.3 Úschova dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Službu, která by vyžadovala uschování soukromých klíčů, PostSignum QCA neposkytuje.

6.2.4 Zálohování dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Soukromý klíč certifikační autority je zálohován v zašifrované formě. Při obnově zálohovaných klíčů do nového nebo inicializovaného modulu je zapotřebí součinnosti minimálně tří osob.

6.2.5 Uchovávání dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Soukromé klíče certifikačních autorit v hierarchii PostSignum QCA nejsou archivovány. Po ukončení provozu certifikační autority jsou klíče včetně záloh zničeny, o čemž je vyhotoven záznam.

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

Soukromý klíč certifikační autority je generován v kryptografickém modulu (bezpečném kryptografickém modulu) a veškeré operace s nezašifrovaným klíčem se provádějí pouze v tomto modulu. Klíč opouští kryptografický modul pouze v zašifrované podobě na zálohách vytvářených a chráněných v souladu s ustanoveními interních dokumentů Systémová bezpečnostní politika, Provozní a bezpečnostní procedury a Auditní a archivační politika (součást [SBP]).

Klíč je do původního kryptografického modulu vkládán ze záloh po autentizaci jednoho pracovníka s přístupem k zálohám klíčů a ke kryptografickému modulu.

Klíč je do nového nebo inicializovaného kryptografického modulu vkládán ze záloh po autentizaci dvou pracovníků, kteří nemají přístup k záloze soukromého klíče a kteří nemají právo na aktivaci soukromého klíče (spuštění procesu certifikační autority).

6.2.7 Uložení dat pro vytváření elektronických pečetí v kryptografickém modulu

Soukromý klíč certifikační autority je během provozu uložen v nezašifrovaném tvaru v aktivovaném a konfigurovaném kryptografickém modulu (bezpečném kryptografickém modulu), k jehož zapnutí a vypnutí postačuje jedna osoba.

K aktivování kryptografického modulu (bezpečného kryptografického modulu) a k obnově soukromého klíče po havárii (případně v jiném kryptografickém modulu) je zapotřebí součinnosti několika, minimálně však tří osob.

6.2.8 Postup při aktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Soukromý klíč certifikační autority je aktivován autorizovanou obsluhou v souladu s interními dokumenty Systémovou bezpečnostní politikou a Provozními a bezpečnostními procedurami.

6.2.9 Postup při deaktivaci dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Soukromý klíč certifikační autority je deaktivován autorizovanou obsluhou v souladu s interními dokumenty Systémovou bezpečnostní politikou a Provozními a bezpečnostními procedurami.

6.2.10 Postup při zničení dat pro vytváření elektronických podpisů nebo dat pro vytváření elektronických pečetí

Soukromý klíč certifikační autority uložený v kryptografickém modulu je zničen prostředky poskytovanými kryptografickým modulem v případě, že kryptografický modul má být dočasně použit k jiným účelům, v případě ukončení činnosti kryptografického modulu nebo v případě ukončení činnosti certifikační autority, jejíž klíče jsou v kryptografickém modulu uloženy. Toto zničení soukromého klíče se provádí autorizovanou obsluhou v souladu s ustanoveními interních dokumentů Systémová bezpečnostní politika a Provozní a bezpečnostní procedury nebo na základě požadavku Manažera CA.

Zničení soukromého klíče je provedeno uvedením kryptografického modulu do inicializovaného stavu, kdy je pomocí mechanismů kryptografického modulu bezpečně vymazán veškerý kryptografický materiál (včetně soukromého klíče CA). Zničení soukromého klíče zahrnuje i smazání všech zálohovaných kopií klíčů a deaktivaci karet použitých pro přístup ke klíčům

6.2.11 Hodnocení kryptografických modulů

Vzhledem ke skutečnosti, že kryptografický modul užívaný k úschově soukromého klíče certifikační autority úspěšně prošel hodnocením podle standardu FIPS 140–2 na úroveň 3, nepředpokládá se, že by obsahoval závažné chyby na úrovni konstrukce zařízení. Přesto se průběžně sleduje, zda nebyl objeven útok na toto zařízení, aby bylo možné včas na takové ohrožení reagovat.

6.3 Další aspekty správy párových dat

6.3.1 Uchovávání dat pro ověřování elektronických pečetí

Veřejné klíče ve formě certifikátů koncových uživatelů jsou archivovány v souladu s interním dokumentem Auditní a archivační politika.

6.3.2 Maximální doba platnosti certifikátu vydaného pečetící osobě a párových dat

Délka platnosti certifikátu je 385 dní nebo 1115 dní dle objednávky zákazníka. Při vydání nového certifikátu v rámci reklamačního řízení nebo na žádost zákazníka při změně údajů, může být doba platnosti certifikátu zkrácena.

Doba platnosti certifikátu vydaného podle této certifikační politiky je vždy uvedena v certifikátu.

6.4 Aktivační data

V systému PostSignum QCA jsou používána aktivační data různého charakteru, například přístupová hesla, PIN a jiné. Všechny aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v interních dokumentech Systémové bezpečnostní politika, Provozní a bezpečnostní procedury a v interní provozní dokumentaci.

6.4.1 Generování a instalace aktivačních dat

Aktivační data jsou většinou vytvářena nebo zadávána pracovníkem, který je bude dále používat. V opačném případě, kdy je generuje jiný subjekt, jsou použita náhodná data splňující obecné požadavky na tato data a je definována povinnost tato náhodně generovaná data neprodleně změnit.

Všechna vytvářená aktivační data musí splňovat požadavky kladené na jejich délku nebo složení.

6.4.2 Ochrana aktivačních dat

Všechna aktivační data musí být chráněna před prozrazením neoprávněné osobě. Příslušné povinnosti v tomto smyslu mají všichni pracovníci PostSignum QCA a jsou uvedeny v interním dokumentu Systémová bezpečnostní politika.

6.4.3 Ostatní aspekty aktivačních dat

Ostatní aspekty týkající se aktivačních dat, jejich generování, instalace a používání, jsou popsány v interních dokumentech Systémové bezpečnostní politika, Provozní a bezpečnostní procedury a v interní provozní dokumentaci.

6.5 Počítačová bezpečnost

6.5.1 Specifické technické požadavky na počítačovou bezpečnost

Pro každou komponentu v hierarchii PostSignum QCA jsou definována nastavení zajišťující bezpečnost dané komponenty na technologické úrovni, které vycházejí z požadavků platných právních předpisů a návazných dokumentů, a to zejména ze standardů [ETSI EN 319 401] a [ETSI EN 319 411].

6.5.2 Hodnocení počítačové bezpečnosti

Systém PostSignum QCA prošel po vybudování externí kontrolou bezpečnostní shody zaměřenou na splnění požadavků kladených legislativou na kvalifikovaného poskytovatele služeb vytvářejících důvěru, a to zejména požadavků uvedených v [eIDAS].

6.6 Bezpečnost životního cyklu

6.6.1 Řízení vývoje systému

Implementace systému probíhala podle metodologie KeyStep, která byla vytvořena speciálně pro návrh a implementaci rozsáhlých PKI projektů. Vývoj dílčích aplikací probíhal v souladu s interní metodikou vývoje České pošty.

Následné změny jsou realizovány v souladu s definovaným změnovým řízením.

6.6.2 Kontroly řízení bezpečnosti

Bezpečnost systémů PostSignum QCA je ověřována provozními kontrolami zavedenými v rámci zavedeného systému řízení informační bezpečnosti podle [ISO 27001], kontrolami bezpečnostní shody prováděnými pracovníky kontroly ČP a externími audity, které provádí externí subjekt.

6.6.3 Řízení bezpečnosti životního cyklu

Součástí změnového řízení je i hodnocení dopadu změn na bezpečnost řešení. V případě velkých změn nebo po sérii menších změn je provedena rozdílová nebo opakovaná analýza rizik.

6.7 Síťová bezpečnost

Lokální sítě centrálních pracovišť (hlavní a záložní lokalita) obsahující centrální systémy PostSignum QCA jsou od interní sítě ČP odděleny firewallem. Tento firewall neumožňuje žádnou komunikaci směrem z interní sítě ČP přímo do lokální sítě obsahující systémy PostSignum QCA. Veškerá komunikace směrem do lokální sítě centrálního pracoviště je ukončena na vyhrazené DMZ.

Interní síť ČP je mimo to od všech externích sítí včetně Internetu oddělena vlastním firewallem.

Veškerá komunikace mimo vyhrazené lokální sítě centrálních pracovišť je šifrovaná.

6.8 Časová razítka

Viz kapitola 5.5.5.

7 PROFILY CERTIFIKÁTU, SEZNAMU ZNEPLATNĚNÝCH CERTIFIKÁTŮ A OCSP

7.1 Profil certifikátu

PostSignum QCA vydává certifikáty odpovídající standardu X.509. Profil kvalifikovaného certifikátu pro elektronickou pečeť je uveden v následující tabulce. Certifikační autorita si vyhrazuje právo vložit do certifikátu další položky, pokud si to vyžádá změna právních předpisů nebo technických norem, které upravují činnost poskytovatelů certifikačních služeb.

Tab. 2 Profil kvalifikovaného certifikátu pro elektronickou pečeť

Položka	Hodnota	Pov.	Změna	ORG	
Version	3 (0x2)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.			
Serial number	sériové číslo certifikátu přidělené certifikační autoritou				
SignatureAlgorithm	sha256WithRSAEncryption				
Issuer					
C countryName	CZ	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit. *(X je číslo označující konkrétní podřízenou certifikační autoritu)*			
OID 2.5.4.97 organizationIdentifier	NTRCZ-47114983				
O organisationName	Česká pošta, s.p.				
CN commonName	PostSignum Qualified CA X				
Validity					
Not Before	Počátek platnosti vydaného certifikátu (UTCTime)	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.			
Not After	Konec platnosti vydaného certifikátu (UTCTime)				
Subject					
C countryName	kód státu, kde má zákazník (právnická osoba) sídlo	**ano**	ne	X	
OID 2.5.4.97 organizationIdentifier	obsahuje identifikátor organizace dle mezinárodních standardů ve tvaru: NTR*YY-IČO organizace* nebo VAT*YY-DIČ organizace* *YY je kód státu, kde má zákazník sídlo*	**ano**	**ano**	X	
O organisationName	jméno právnické osoby	**ano**	**ano**	X	
OU organizationalUnitName	rozlišující organizační jednotka právnické osoby	ne	**ano**	X	
OU organizationalUnitName	organizační jednotka	ne	**ano**	X	
CN commonName	název certifikátu zvolený pečetící osobou	**ano**	**ano**	X	
serialNumber	jednoznačný identifikátor zákazníka, přidělovaný poskytovatelem certifikačních služeb ve tvaru: S*číslo*	**ano**	ne	X	
Subject Public Key Info					
Algorithm	rsaEncryption	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.			
SubjectPublicKey	veřejný klíč pečetící osoby o velikosti 2048 nebo 4096 bitů				

Extensions	rozšíření certifikátu podle tabulky 3	
Signature	elektronická pečeť poskytovatele certifikačních služeb	

Vysvětlivky:
Pov povinná položka certifikátu
Změna položku je možné změnit v následném certifikátu
ORG položka je obsažena v certifikátech vydávaných zaměstnancům organizací

7.1.1 Číslo verze

PostSignum Qualified CA vydává certifikáty vyhovující standardu X.509 verze 3.

7.1.2 Rozšiřující položky v certifikátu

Rozšiřující položky použité v kvalifikovaném certifikátu pro elektronickou pečeť jsou uvedeny v následující tabulce.

Tab. 3 Rozšíření v certifikátu

Položka	**Hodnota**	**Pov.**	**Změna**	**ORG**		
Authority Key Identifier						
Key Identifier		Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Subject Key Identifier						
Subject Alternative Name						
rfc822Name emailAddress	e-mailová adresa	ne	**ano**	X		
rfc822Name emailAddress	e-mailová adresa	ne	**ano**	X		
rfc822Name emailAddress	e-mailová adresa	ne	**ano**	X		
otherName	vlastní obsah určený zákazníkem obsah je kódován pomocí ASCII v hexadecimálním zápisu položka „Description“ s OID: 2.5.4.13	ne	**ano**	X		
Key Usage ***(kritické rozšíření)***						
DigitalSignature	ano/ne*	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit. * Pokud je odpovídající soukromý klíč uložený na QESCD, nejsou položky označené * uvedené v Key Usage.				
NonRepudiation	ano					
KeyEncipherment	ano/ne*					
DataEncipherment	ne					
KeyAgreement	ne					
KeyCertSign	ne					
CRLSign	ne					
Extended Key usage						
Secure E-mail	id-kp-emailProtection OID 1.3.6.1.5.5.7.3.4	Rozšířené použití klíče je uvedeno ve všech vydávaných certifikátech a nelze je změnit.				
Document Signing	id-ms-kp-document-signing OID 1.3.6.1.4.1.311.10.3.12					
Certificate Policies						
Policy Information [1]						
Policy Identifier	OID této certifikační politiky	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit.				
Policy Qualifier id	CPS					
CPS URI	http://www.postsignum.cz					

User Notice	Tento kvalifikovany certifikat pro elektronickou pecet byl vydan v souladu s narizenim EU c. 910/2014.This is a qualified certificate for electronic seal according to Regulation (EU) No 910/2014.	
Policy Information [2]		
Policy Identifier	OID pro QCP-l: 0.4.0.194112.1.1 nebo OID pro QCP-l-qscd: 0.4.0.194112.1.3	Povinně je uvedeno vždy jedno z OID. OID 0.4.0.194112.1.3 je uvedeno pouze, pokud je odpovídající soukromý klíč uložený na QESCD.
Qualified certificate statement		
OID	0.4.0.1862.1.1 *esi4-QCStatement-1*	Položka je obsažena povinně ve všech vydávaných certifikátech a nelze ji změnit.
OID	0.4.0.1862.1.4 *esi4-QCStatement-4*	Je uvedeno pouze, pokud je odpovídající soukromý klíč uložený na QESCD.
OID	0.4.0.1862.1.5 *esi4-QCStatement-5*	Položka je obsažena povinně ve všech vydávaných certifikátech a nelze ji změnit. Hodnotou položky je odkaz na zprávu pro uživatele v anglické a české verzi.
OID	0.4.0.1862.1.6.2 *esi4-QCStatement-6* *(id-etsi-qct-eseal)*	Položka je obsažena povinně ve všech vydávaných certifikátech a nelze ji změnit. Položka značí, že certifikát byl vydán jako certifikát pro elektronickou pečeť dle [eIDAS].
CRL Distribution Points		
URI	http://crl.postsignum.cz/crl/psqualifiedcaX.crl	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit *(X je číslo označující konkrétní podřízenou certifikační autoritu)*.
URI	http://crl2.postsignum.cz/crl/psqualifiedcaX.crl	
URI	http://crl.postsignum.eu/crl/psqualifiedcaX.crl	
AuthorityInfoAccess		
accessMethod URI	id-ad-caIssuers (1.3.6.1.5.5.7.48.2) http://crt.postsignum.cz/crt/psqualifiedcaX.crt	Položky jsou obsaženy povinně ve všech vydávaných certifikátech a nelze je změnit. *(X je číslo označující konkrétní podřízenou certifikační autoritu)*
accessMethod URI	id-ad-ocsp (1.3.6.1.5.5.7.48.1) http://ocsp.postsignum.cz/OCSP/QCAX/	

Vysvětlivky:
Pov povinná položka certifikátu
Změna položku je možné změnit v následném certifikátu
ORG položka je obsažena v certifikátech vydávaných zaměstnancům organizací

Poznámka: Některé položky certifikátu neobsahují diakritiku z důvodu lepší čitelnosti údajů v certifikátu v různých systémech.

Poznámka: Tato certifikační politika umožňuje vložit do certifikátu až 3 e-mailové adresy. Žadatel by si však měl předem ověřit, zda certifikát s více e-mailovými adresami podporují aplikace, ve kterých hodlá certifikát používat.

7.1.3 Objektové identifikátory (dále „OID“) algoritmů

Algoritmům používaným v PostSignum QCA nejsou přiřazeny OID. V hierarchii PostSignum QCA se nepoužívají specifické algoritmy, které by vyvíjel provozovatel PostSignum QCA nebo jeho dodavatel, ale pouze algoritmy odpovídající požadavkům platných právních předpisů a technických norem, které upravují činnost poskytovatelů certifikačních služeb.

7.1.4 Způsoby zápisu jmen a názvů

Pravidla pro zápis jmen a názvů jsou uvedena v kapitolách 3.1.1 až 3.1.4.

7.1.5 Omezení jmen a názvů

Název certifikátu (položka CN) nesmí obsahovat doménové jméno (např. example.com) nebo IP adresu (X.X.X.X).

7.1.6 OID certifikační politiky

V každém certifikátu koncového uživatele je uveden odkaz na politiku, podle které byl certifikát vydán (OID politiky). OID této politiky je uvedeno v kapitole 1.2.

7.1.7 Rozšiřující položka „Policy Constraints“

Rozšiřující položka „Policy Constraints“ se v PostSignum QCA nepoužívá.

7.1.8 Syntaxe a sémantika rozšiřující položky kvalifikátorů politiky „Policy Qualifiers“

Rozšiřující položka „Policy Qualifier“ obsahuje odkaz na webové stránky poskytovatele, kde lze získat certifikační politiku, podle které byl certifikát vydán, textovou informaci o skutečnosti, že certifikát byl vydán jako certifikát pro elektronickou pečeť podle [eIDAS] a další položky odpovídající technickým standardům pro kvalifikované certifikáty, které jsou v souladu s [eIDAS].

7.1.9 Způsob zápisu kritické rozšiřující položky „Certificate Policies“

Způsob zápisu rozšiřující položky „Certificate Policies“ je uveden v Tab. 3. Tato položka není označena jako kritická.

7.2 Profil seznamu zneplatněných certifikátů

Tab. 4 Profil CRL

Název položky	**Hodnota/příznak použití**
Version	2 (0x1)
Issuer Distinguished Name	
C countryName	CZ
OID 2.5.4.97 organizationIdentifier	NTRCZ-47114983
O organisationName	Česká pošta, s.p.
CN commonName	PostSignum Qualified CA X *(X je číslo označující konkrétní podřízenou certifikační autoritu)*
Validity	
This Update	Počátek platnosti vydaného CRL (UTCTime)
Next Update	Konec platnosti vydaného CRL (UTCTime)

RevokedCertificates	opakující se položka pro každý zneplatněný certifikát
UserCertificate	sériové číslo zneplatněného certifikátu
RevocationDate	datum a čas zneplatnění
CrlEntryExtensions	rozšíření položky CRL podle tabulky 5
CrlExtensions	rozšíření CRL podle tabulky 5
SignatureAlgorithm	sha256WithRSAEncryption
Signature	elektronická pečeť poskytovatele certifikačních služeb

7.2.1 Číslo verze

PostSignum Qualified CA vydává seznamy zneplatněných certifikátů podle standardu X.509 verze 2.

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

Tab. 5 Rozšíření v CRL

Název rozšiřující položky	**Hodnota/příznak použití**	**Kritická ano/ne**
Rozšíření položky CrlEntryExtensions		
InvalidityDate	datum a čas vzniku události vedoucí ke zneplatnění certifikátu; volitelné rozšíření	ne
ReasonCode	důvod zneplatnění certifikátu	ne
Rozšíření CRL (CrlExtensions)		
Authority Key Identifier		ne
Key Identifier	používá se	
AuthorityCertIssuer	používá se	
AuthorityCertSerialNumber	používá se	
CRL Number	sériové číslo CRL přiřazené certifikační autoritou	ne

7.3 Profil OCSP

Viz ustanovení v kapitole 4.9.9.

7.3.1 Číslo verze

Viz ustanovení v kapitole 4.9.9.

7.3.2 Rozšiřující položky OCSP

Viz ustanovení v kapitole 4.9.9.

8 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

8.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

V prostředí PostSignum QCA jsou pravidelně prováděny interní kontroly (jednou za 12 měsíců). Kromě těchto interních kontrol jsou prováděny externí kontroly dle platných právních předpisů. Tyto pravidelné kontroly mohou být podle potřeby doplněny další kontrolou, mimo jiné na základě rozhodnutí Manažera CA, managementu České pošty nebo interního auditu České pošty.

8.2 Identita a kvalifikace hodnotitele

Interní kontrolu provádějí pracovníci znalí problematiky PKI a proškolení pro daný úkol. Pracovníci provádějící kontrolu jsou v dokumentaci QCA označováni jako Auditoři CA.

Externím auditorem smí být pouze osoba nebo společnost znalá problematiky implementace PKI s dostatečnou zkušeností v této oblasti.

8.3 Vztah hodnotitele k hodnocenému subjektu

Interní kontrolu provádí zaměstnanci České pošty, kteří se nepodílejí na provozu certifikační autority PostSignum QCA.

Externí kontrolu smí provádět pouze osoba nebo společnost nezávislá na České poště.

8.4 Hodnocené oblasti

Oblasti hodnocené v rámci pravidelných kontrol jsou specifikovány v platných právních předpisech a příslušnými standardy.

8.5 Postup v případě zjištění nedostatků

Výsledky kontrol jsou předávány Manažerovi CA, který zajistí nápravu zjištěných nedostatků.

V případě zjištění nedostatků, které závažně ovlivní schopnost PostSignum QCA dostát svým závazkům a požadavkům uvedeným v platných právních předpisech, přeruší PostSignum QCA vydávání certifikátů do doby, než budou nedostatky odstraněny.

8.6 Sdělování výsledků hodnocení

O provedení každé kontroly je vypracována podepsaná písemná zpráva, která je předána Manažerovi CA. Ten zajistí její distribuci a projednání. Pokud je to nutné, zajistí Manažer CA předání zprávy orgánu dohledu do termínu, která je stanoven platným právním předpisem.

V případě, kdy je součástí zprávy samostatný výrok auditora, může Manažer CA rozhodnout o jeho zveřejnění.

9 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

9.1 Poplatky

9.1.1 Poplatky za vydání nebo obnovení certifikátu

Cena za poskytnuté certifikační služby je stanovena ve smlouvě mezi zákazníkem a poskytovatelem certifikačních služeb a běžně se řídí aktuálně platným ceníkem. Cena za vydané certifikáty může být i zahrnuta v ceně jiné služby poskytované Českou poštou.

9.1.2 Poplatky za přístup k certifikátu na seznamu vydaných certifikátů

Služba přístupu k certifikátu na seznamu vydaných certifikátů je poskytována bezplatně.

9.1.3 Poplatky za informace o statutu certifikátu nebo o zneplatnění certifikátu

Služba zneplatnění certifikátu a informace o stavu certifikátu jsou poskytovány bezplatně.

9.1.4 Poplatky za další služby

Cena za další služby PostSignum QCA je stanovena v ceníku služeb České pošty.

9.1.5 Jiná ustanovení týkající se poplatků (vč. refundací)

Žádná ustanovení v této kapitole.

9.2 Finanční odpovědnost

9.2.1 Krytí pojištěním

Česká pošta má sjednané pojištění odpovědnosti za škodu takovým způsobem, aby byly pokryty případné škody.

9.2.2 Další aktiva a záruky

Aktiva České pošty jsou uvedena ve Výroční zprávě. Výroční zpráva je uložena v obchodním rejstříku u Městského soudu v Praze pod spisovou značkou A7565.

Výroční zpráva je k nahlédnutí též na webových stránkách České pošty (www.ceskaposta.cz).

9.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

PostSignum QCA tuto službu neposkytuje.

9.3 Citlivost obchodních informací

V maximálním rozsahu podle ustanovení platných právních předpisů se každá ze zúčastněných stran zavazuje uchovat v tajnosti veškeré důvěrné informace, okolnosti a údaje, které se dozvěděla v souvislosti s plněním smlouvy o poskytování certifikačních služeb a o kterých nebylo písemně dohodnuto mezi smluvními stranami, že mohou být zveřejněny.

9.3.1 Výčet citlivých informací

Za důvěrné jsou považovány všechny informace s výjimkou informací uvedených v dokumentech s označením „Veřejné“.

9.3.2 Informace mimo rámec citlivých informací

Za důvěrné se nepovažují informace, které:

- se staly veřejně známými, aniž by to zavinila záměrně či opomenutím přijímající strana,
- měla přijímající strana legálně k dispozici před uzavřením smlouvy o poskytování certifikačních služeb, pokud takové informace nebyly předmětem jiné, dříve mezi zúčastněnými stranami uzavřené smlouvy o ochraně informací, nebo pokud takové informace nemají samy o sobě charakter obchodního tajemství,
- jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je schopna to doložit svými záznamy nebo důvěrnými informacemi třetí strany,
- po uzavření smlouvy o poskytování certifikačních služeb poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem, nebo je nezíská nezákonným způsobem, o čemž by přijímající strana věděla nebo vědět musela,
- jsou uvedené v certifikátu pro elektronickou pečeť, pokud k jeho zveřejnění dal držitel souhlas.

9.3.3 Odpovědnost za ochranu citlivých informací

Odpovědnost za zpracování důvěrných informací v PostSignum QCA nese Česká pošta, jakožto poskytovatel certifikačních služeb, všichni její zaměstnanci a smluvní partneři.

9.3.4 Poskytnutí citlivých informací pro soudní či správní účely

Veškeré informace zpracovávané v PostSignum QCA jsou zpřístupněny orgánům zmocněným ze zákona v případech, kdy to zákon vyžaduje, a do té míry, do jaké to zákon vyžaduje. Zpřístupnění informací zajistí Manažer CA poté, co orgány zmocněné ze zákona prokáží své zmocnění způsobem obvyklým v těchto případech.

9.4 Ochrana osobních údajů

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy ve Všeobecných obchodních podmínkách certifikačních služeb a vycházejí z [GDPR].

9.4.1 Osobní údaje

Za osobní údaje jsou považovány veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat.

9.4.2 Odpovědnost za ochranu osobních údajů

Odpovědnost za ochranu osobních údajů zpracovávaných v systémech PostSignum QCA nese Česká pošta, jakožto poskytovatel certifikačních služeb, všichni její zaměstnanci a smluvní partneři v rozsahu stanoveném [GDPR].

9.4.3 Poskytnutí osobních údajů

V této oblasti je postupováno podle příslušných ustavení [GDPR], obecně závazných právních přepisů a interních předpisů České pošty upravujících problematiku ochrany osobních údajů.

9.5 Práva duševního vlastnictví

Tato certifikační politika a veškeré související dokumenty jsou chráněny autorskými právy České pošty a představují významné know-how České pošty. Česká pošta je rovněž nositelem výlučných práv k informačnímu systému pro provoz PostSignum QCA a ke struktuře, organizaci, vzhledům obrazovek a obsahu webových stránek poskytovatele.

9.6 Zastupování a záruky

Česká pošta zaručuje, že splní veškeré povinnosti uložené touto certifikační politikou a ustanoveními příslušných právních předpisů.

Česká pošta poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb.

9.6.1 Zastupování a záruky CA

Viz ustanovení kapitoly 9.6.

9.6.2 Zastupování a záruky RA

V poskytování služeb registrační autority může být Česká pošta jako poskytovatel certifikačních služeb zastupována třetím subjektem na základě uzavřeného smluvního vztahu; uvedená úroveň záruk není tímto dotčena.

Jinak viz ustanovení kapitoly 9.6.

9.6.3 Zastupování a záruky držitele certifikátu

Zákazník ručí za naplnění všech povinnosti zákazníků a žadatelů o certifikát uvedených v této certifikační politice a povinností uvedených v platných právních předpisech.

9.6.4 Zastupování a záruky spoléhajících se stran

Spoléhající se strana ručí za naplnění všech povinností, které jsou na spoléhající se stranu kladeny před použitím kvalifikovaného certifikátu. Tyto povinnosti jsou uvedeny v této certifikační politice, především v kapitole 4.5.2.

9.6.5 Zastupování a záruky ostatních zúčastněných subjektů

Subjekty, které se přímo podílí na provozu PostSignum QCA na základě smluvního vztahu s poskytovatelem certifikačních služeb, mají povinnost dodržovat ustanovení certifikační politiky, certifikační prováděcí směrnice, systémové bezpečnostní politiky a dalších interních dokumentů.

Záruky, které v těchto případech poskytuje poskytovatel certifikačních služeb, jsou definovány příslušnými ustanoveními v platných právních předpisech.

9.7 Zřeknutí se záruk

Záruky uvedené v kapitole 9.6 výše jsou výlučnými zárukami České pošty a Česká pošta jiné záruky neposkytuje.

Česká pošta neodpovídá za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb držitelem,

zejména za provozování v rozporu s podmínkami uvedenými v této certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj.

9.8 Omezení odpovědnosti

Česká pošta neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu pro el. pečeť, pokud došlo ze strany držitele nebo spoléhající se osoby k nedodržení omezení pro jeho použití, uvedených v této certifikační politice a zveřejněných na webové stránce poskytovatele.

Česká pošta neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu pro el. pečeť v období po přijetí žádosti o jeho zneplatnění, pokud Česká pošta dodrží lhůtu pro zveřejnění zneplatněného kvalifikovaného certifikátu pro el. pečeť na seznamu zneplatněných certifikátů (CRL), uvedenou v kapitole 2 této certifikační politiky.

Česká pošta bude průběžně s rostoucími provozními zkušenostmi s poskytováním certifikačních služeb ověřovat, zda podmínky omezení odpovědnosti České pošty uvedené v tomto ustanovení odpovídají obvyklým podmínkám na trhu a přiměřenému obchodnímu riziku České pošty.

Ustanovení tohoto článku zůstávají v platnosti i po ukončení platnosti této certifikační politiky.

9.9 Odpovědnost za škodu, náhrada škody

Pokud nevyplývá z ustanovení platných právních předpisů jinak, odpovídá Česká pošta držiteli certifikátu za škodu způsobenou porušením povinností České pošty v souvislosti s plněním smlouvy o poskytování certifikačních služeb.

9.10 Doba platnosti, ukončení platnosti

9.10.1 Doba platnosti

Doba platnosti této certifikační politiky je od data vydání uvedeného v kapitole 1.2 do odvolání.

9.10.2 Ukončení platnosti

Platnost dokumentu je ukončena v případě

- jeho nahrazení novější verzí, nebo
- ukončení poskytování služeb Českou poštou jako poskytovatelem certifikačních služeb.

9.10.3 Důsledky ukončení a přetrvání závazků

V případě ukončení platnosti tohoto dokumentu v důsledku ukončení poskytování služeb zůstávají v platnosti omezení a ustanovení uvedená v kapitole 9, která se týkají obchodních a právních záležitostí.

9.11 Komunikace mezi zúčastněnými subjekty

9.11.1 Komunikace s poskytovatelem certifikačních služeb

Veškeré informace, které chce poskytovatel certifikačních služeb sdělit zákazníkům, zveřejní na svých webových stránkách a na vývěskách na pracovištích registračních autorit. Závažné informace, jako například podezření na kompromitaci klíče některé z certifikačních autorit hierarchie PostSignum, sděluje poskytovatel certifikačních služeb opět na webových stránkách a současně písemným nebo elektronickým upozorněním směrovaným na zákazníky.

Zákazník komunikuje s poskytovatelem certifikačních služeb prostřednictvím pověřené osoby. Pověřená osoba se obrací na pracoviště registrační autority nebo na obchodní místa CA.

Komunikace zákazníka s poskytovatelem certifikačních služeb může probíhat rovněž elektronicky. V případě požadavku na právní prokazatelnost elektronické komunikace musí být tato založena na certifikátech vydaných PostSignum QCA nebo jinou autoritou, kterou Česká pošta označí za důvěryhodnou, a o akceptaci jejíhož certifikátu se se zákazníkem předem písemně dohodne.

9.11.2 Komunikace v rámci systému PostSignum QCA

Komunikace v systému PostSignum QCA se řídí platnými předpisy České pošty a interními dokumenty úlohy PostSignum QCA.

9.11.3 Komunikační jazyk

Veškerá komunikace v systému PostSignum QCA musí probíhat v českém jazyce, pokud se obě strany nedohodnou jinak.

9.12 Změny

9.12.1 Postup při změnách

Postupy pro zapracování změn jsou uvedeny v kapitole. 1.5.

9.12.2 Postup při oznamování změn

Vydání nové certifikační politiky se změněným OID (viz následující kapitola) bude oznámeno v aktualitách na webových stránkách poskytovatele.

V případě identifikace oslabení záruk poskytovaných používanými kryptografickými algoritmy vyžadující neodkladný zásah budou písemně nebo elektronicky informováni všichni držitelé certifikátů, orgán dohledu a subjekty, které mají uzavřenou smlouvu přímo se vztahující k poskytování certifikačních služeb. Oznámení bude rovněž zveřejněno na webových stránkách poskytovatele, na všech pracovištích registrační autority PostSignum QCA. Na toto oznámení mohou navazovat další akce, které jsou popsány v této certifikační politice.

V případě, že nebude hrozit nebezpečí z prodlení, bude toto oznámení provedeno min. 10 pracovních dní před začátkem platnosti nové verze certifikační politiky.

9.12.3 Okolnosti, při kterých musí být změněn OID

Česká pošta přiřadila dle svých interních pravidel identifikátory objektů (OID) užívané v prostředí PostSignum QCA.

OID jsou přiřazeny:

- PostSignum Root QCA,
- každé certifikační autoritě, které PostSignum Root QCA vydala certifikát, zejména certifikační autoritě PostSignum Qualified CA,
- každé certifikační politice, podle které jsou vydávány certifikáty v rámci PostSignum QCA.

OID nejsou přiřazeny registračním autoritám ani certifikační prováděcí směrnici.

Pouze větší změna v certifikační politice vyvolá změnu verze dokumentu na úrovni x.**X** a také změnu OID. Menší změny, příp. revize beze změn vyvolají změnu verze dokumentu na úrovni x.x.**X**, přičemž OID se nemění.

9.13 Řešení sporů

V případě vzniku sporu mezi zákazníkem a PostSignum QCA se zákazník obrátí na

- Manažera CA, nebo
- registrační autoritu (formou žádosti o reklamaci).

Pokud ani jedna z výše uvedených instancí nesjedná ukončení sporu, bude se spor mezi zákazníkem a PostSignum QCA řešit u místně a věcně příslušného soudu.

9.14 Rozhodné právo

Činnost PostSignum QCA se řídí právním řádem České republiky.

9.15 Shoda s právními předpisy

Činnost PostSignum QCA je v souladu s platnými právními předpisy České republiky.

Vztah mezi Českou poštou a zákazníkem je upraven písemnou smlouvou o poskytování certifikačních služeb.

Struktura této certifikační politiky je v souladu se strukturou uvedenou v RFC 3647.

9.16 Další ustanovení

9.16.1 Rámcová dohoda

Žádná ustanovení v této kapitole.

9.16.2 Postoupení práv

Česká pošta může přenést část nebo všechny povinnosti poskytovatele certifikačních služeb na jiný právní subjekt, u kterého je zajištěna stejná úroveň bezpečnosti i poskytovaných služeb. Vztahy mezi Českou poštou a tímto subjektem budou upraveny zvláštní smlouvou. Povinnosti a odpovědnost České pošty, jakožto poskytovatele certifikačních služeb, zůstávají tímto nedotčeny.

V případě ukončení činnosti kvalifikovaného poskytovatele certifikačních služeb vyvine Česká pošta v souladu s platnými právními předpisy přiměřené úsilí pro převzetí správy platných kvalifikovaných certifikátů a související agendy jiným kvalifikovaným poskytovatelem certifikačních služeb. V tomto případě budou vztahy mezi tímto kvalifikovaným poskytovatelem certifikačních služeb a Českou poštou rovněž upraveny zvláštní smlouvou.

Převzetí části nebo všech povinností poskytovatele certifikačních služeb třetí stranou neomezuje služby ani záruky poskytované Českou poštou vzhledem k zákazníkům a spoléhajícím se stranám.

9.16.3 Oddělitelnost ustanovení

Smlouva o poskytování certifikačních služeb uzavřená mezi zákazníkem a Českou poštou zůstává platná i v případě, že jakákoliv její dílčí část pozbude platnost, pokud se obě strany nedohodnou jinak.

9.16.4 Zřeknutí se práv

Žádná ustanovení v této kapitole.

9.16.5 Vyšší moc

Česká pošta nenese odpovědnost za porušení svých povinností způsobené zásahy vyšší moci, jako jsou například přírodní katastrofy velkého rozsahu, stávky, občanské nepokoje nebo válečný stav.

9.16.6 Přístupnost pro osoby se zdravotním postižením

Poskytované služby vytvářející důvěru a konečné uživatelské produkty používané při poskytování těchto služeb jsou dostupné osobám se zdravotním postižením. Bližší informace ohledně poskytování služeb těmto osobám poskytnou registrační autority nebo Zákaznická podpora. Kontaktní údaje jsou uvedené na webových stránkách poskytovatele www.postsignum.cz.

9.17 Další opatření

9.17.1 Řídící dokumenty

Při tvorbě certifikačních politik a certifikační prováděcí směrnice bylo zejména přihlíženo k následujícím dokumentům:

[eIDAS]	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
[ETSI EN 319 401]	Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 411]	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 – 3
[ETSI EN 319 412]	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5
[ETSI EN 119 312]	Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[GDPR]	NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 2016/679 ze dne 27. dubna 2016 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)
[ISO 27001]	ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky
[RFC 6960]	Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[RFC 5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC 3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[ZoEP] Zákon č. 227/2000 Sb. o elektronickém podpisu (zrušen zákonem 297/2016 Sb.)

[ZoSVD] Zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce v platném znění

9.17.2 Odkazy a literatura

[VOP] Všeobecné obchodní podmínky certifikačních služeb.

Politika služby vzdáleného pečetění elektronických dokumentů a dat

SecuSeal

Historie změn

Datum	vydání	Status	autor
02. 08. 2019	V 0.1	Internal Draft	Martin Vondrouš
18. 09. 2019	V 0.2	Release Candidate	Martin Vondrouš
27.10.2019	V 1.0	Release	Martin Vondrouš
15.4.2021	V 1.1	Doplnění odstavce 3.1 – Souhlas s umístěním klíče do HSM	Martin Vondrouš
30.5.2021	V 1.2	Změna loga	Martin Vondrouš

.

Obsah

1. Úvod

1.1. Přehled

Služba vzdáleného pečetění elektronických dokumentů a dat s využitím kvalifikovaných certifikátů pro elektronickou pečeť vytvořených a umístěných na serverovém kvalifikovaném prostředku pro vytváření kvalifikovaných elektronických pečetí (dále jen „Služba“, nebo „Pečetění“) je služba vytvořená a provozovaná obchodní společností Software602 a.s. (dále též jako „Software602“) pro zajištění opatření podporovaného typu dokumentu kvalifikovanou elektronickou pečetí dle specifikací ETSI. Službu provozuje Software602 a.s. jako kvalifikovaný poskytovatel služeb vytvářecích důvěru (dále jen „QTSP“) jako službu vytvářející důvěru.

Volitelnou nikoliv nedílnou součástí služby mohou být nástroje pro správu kvalifikovaného elektronického pečetícího certifikátu a aplikace pro vytváření kvalifikované pečeti.

Předmětem tohoto dokumentu je definovat politiku (dále „PP“) k poskytování Služby. PP popisuje podmínky a nezbytné postupy, které je zapotřebí uplatňovat v zájmu dodržení přijatých bezpečnostních standardů QTSP. Součástí dokumentu je také vymezení rozsahu odpovědnosti zúčastněných stran.

Dodržení postupů a podmínek uvedených v této PP zajišťuje, správné a bezpečné nakládání s kvalifikovaným certifikátem elektronické pečeti a jeho použití pro vzdálené pečetění dokumentů a dat s kvalifikovaným časovým razítkem. Používání kvalifikovaného časového razítka není podmiňující pro poskytování služby vzdáleného pečetění.

Důležité upozornění pro uživatele Služby: Před prvním použitím Služby je uživatel povinen se prokazatelně seznámit s touto PP v plném rozsahu.

1.2. Název a jednoznačné určení dokumentu

Název dokumentu: Politika služby vzdáleného pečetění elektronických dokumentů a dat.

PP je v souladu s dokumenty uvedenými v kapitole 8.14.

1.3. Participující subjekty

1.3.1. PostSignum

PostSignum je poskytovatel služby vytvářející důvěru, který poskytuje kvalifikovaná časová razítka v souladu s požadavky legislativního rámce daného českým právním prostředím a požadavky EU. Politika vydávání kvalifikovaných časových razítek od tohoto poskytovatele je vystavena na jeho stránkách www.postsignum.cz.

Dále je PostSignum poskytovatel kvalifikovaných certifikačních služeb pro kvalifikované certifikáty pro pečeť a Software602 je oprávněna tyto certifikáty vytvářet a spravovat na kvalifikovaných prostředcích pro vytváření elektronických pečetí (dále jen „QSealCD“) s odpovídající certifikací na základě smlouvy.

1.3.2. Azure

Microsoft Azure je poskytovatel infrastruktury pro běhové prostředí služby pro správu identit a kontrolu přístupu a autentizace uživatelů a poskytuje záruku pro bezpečné prostředí pro zpracování dat a jejich ukládání v souladu s požadavky kladenými na ochranu osobních údajů a lokalitu, kde jsou data uložena. Toto prostředí není podmiňující pro využívání služby, v případě že správce identit je zajištěn jiným poskytovatel na základě smluvního vztahu.

1.3.3. O2

Telefónica O2 a.s. je poskytovatel prostředí chráněného proti neoprávněnému zásahu s úrovní bezpečnosti TIER III pro bezpečný provoz a umístění HSM modulů ve funkci QSealCD, serverové podepisující aplikace a aktivačního modulu pro pečetění.

1.4. Použití Služby

1.4.1. Přípustné použití Služby

Službu smí používat pouze uživatelé, kteří se seznámili s touto PP. Uživatel Služby akceptuje její použití dle podmínek této PP a v souladu s garantovaným použitím Služby.

Službu je možné čerpat výhradně prostřednictvím definovaných rozhraní a aplikací, které jsou dodané a poskytnuté poskytovatelem služby vzdáleného pečetění.

1.4.1.1. Rozhraní

Uživatel Služby je povinen chránit rozhraní pro použití Služby proti neoprávněnému použití a zajistit odpovídající bezpečnost při používání Služeb. Toto platí pro jakékoliv rozhraní, prostřednictvím kterého je Služba čerpána (dále jen „Rozhraní“).

Tímto Rozhraním je myšleno zejména webová aplikace pro autentizaci, pro správu a nastavení Služby, webové služby pro integraci, jakákoliv aplikační či integrační rozhraní dodané výhradně provozovatelem Služby nebo jím určeným integrátorem.

1.4.2. Omezení použití Služby

Za nepovolené je považováno takové využití Služby, které není definováno a povoleno v rámci této PP. Za nepovolené využití Služby nenese její poskytovatel žádnou odpovědnost. V případě porušení bezpečnosti či integrity Rozhraní nenese poskytovatel Služby jakoukoliv odpovědnost za škody jakéhokoliv druhu způsobené použitím tohoto nezabezpečené, podvrženého či jakkoliv porušeného Rozhraní.

1.5. Správa politiky

1.5.1. Organizace spravující službu

Software602, a.s., technické oddělení, Hornokrčská 15, Praha 4

1.5.2. Kontakt na Správce Služby

ID datové schránky: 7dcsfzg

Ředitel technického oddělení
Software602 a.s., Hornokrčská 15, Praha 4

1.6. Přehled použitých pojmů a zkratek

Akronym	Plný význam	Vysvětlení
602ID	Identifikátor uživatele	Jedná se o unikátní identifikátor uživatele služeb poskytovaných QTSP Software602. 602 ID se skládá z emailové adresy a hesla. Údaje jsou uloženy v databázi spravované výlučně QTSP Software602 a je zajištěna ochrana osobních dat uživatelů. Pro některé služby je k unikátnímu 602 ID uživatele připojena další sada dat určená pro fakturaci a obchodní styk s uživatelem.
AEC	Advanced Electronic Certificate	Zaručený elektronický certifikát, obsahuje soubor údajů fyzické osoby umožňující její identifikaci.
AES	Advanced Electronic Signature	Zaručený elektronický pečeť.
CA	Certifikační autorita / Certification Authority	Certifikační autorita, poskytovatel služeb elektronických certifikátů pro elektronický pečeť/pečeť/razítka/certifikáty webových stránek
Certifikát		Datová struktura obsahující veřejný klíč spolu s údaji o držiteli klíče, vydavateli klíče, dovoleném způsobu užití a další relevantní informace definované příslušející PP.
CP	Certifikační politika	Dokument, který definuje parametry certifikátu vydávaného CA, vymezuje způsob užití certifikátu a definuje životní cyklus certifikátu. Jedná se také o certifikační politiku pro vydávání certifikátů pro pečeť, pečeť či razítko od QTSP..
CRL	Certification Revocation List	Seznam zneplatněných nebo pozastavených certifikátů, jejichž doba platnosti ještě nevypršela.
Držitel certifikátu	Držitel certifikátu	Fyzická nebo právnická osoba, jež má výhradní právo nakládat se soukromým klíčem, který souvisí s předmětným certifikátem.
DTBS	Data To Be Sealed	Data určená k pečetění
Důvěryhodná		Důvěryhodné role, na kterých je závislá bezpečnost provozu.
eIDAS		Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
Elektronický pečeť		V rámci použití v tomto dokumentu, pokud není definováno jinak, se jedná o kvalifikovaný elektronický pečeť
EP	Elektronický pečeť	Údaje v elektronické podobě připojené k datové zprávě (dokumentu či datům) sloužící k ověření původnosti integrity této datové zprávy a podepisující osoby na základě certifikátu pro elektronický pečeť.
ID datové schránky		Jednoznačný identifikátor datové schránky uživatele Informačního systému datových schránek

Akronym	Plný význam	Vysvětlení
ISDS	Informační systém datových schránek	Informační systém datových schránek je informační systém veřejné správy, který obsahuje údaje o datových schránkách, jejich uživatelích, přístupech do schránky a dalších událostech spojených s jejich provozem atd.
Klient Služby	Klient Služby	Právnická osoba využívající službu vzdáleného pečetění elektronických dokumentů a dat. Má platnou smlouvu o poskytování certifikačních služeb PostSignum a platnou smlouvu o čerpání Služby.
LoTL	List of Trusted Lists	EU:Seznam zveřejněný podle čl. 2 odst. 4 rozhodnutí Komise 2009/767/ES ze dne 16. října 2009, kterým se stanovují opatření pro usnadnění užití postupů s využitím elektronických prostředků prostřednictvím „jednotných kontaktních míst“ podle směrnice Evropského parlamentu a Rady 2006/123/ES o službách na vnitřním trhu, ve znění rozhodnutí Komise 2010/425/EU a prováděcího rozhodnutí Komise 2013/662/EU, který obsahuje informace oznámené členskými státy v souladu s čl. 2 odst. 3 rozhodnutí Komise 2009/767/ES.
LT	Long-Term	
LTA	Long-Term Archivation	Dlouhodobá ověřitelnost platnosti elektronických pečeťových certifikátů
OCSP	Online Certificate Status Protocol	Protokol pro online ověření platnosti certifikátu dle RFC 2560.
OID	Object Identifier	Číselná identifikace objektu v rámci jednotné klasifikace objektů podle ISO/ITU
PKI	Public Key Infrastructure	Infrastruktury správy a distribuce veřejných klíčů asymetrické kryptografie
Podepisování	Služby pečetění	Služby podepsání zajišťující připojení elektronického pečeti s časovým razítkem k vloženému dokumentu / datům
Pečeť		Elektronický pečeť dokumentu či dat vytvořený dle platných technických norem na základě certifikátu pro elektronický pečeť
POE	Proof Of Existence	Jednoznačný časový údaj poskytující důkaz existence ověřovaných dat v čase, ke kterému je prováděna validace
PP	Politika pečetění	Politika služby vzdáleného pečetění elektronických dokumentů a dat kvalifikovaným elektronickým pečeťem s kvalifikovaným elektronickým časovým razítkem. Jedná se o tento dokument.
Privátní klíč		Datová struktura pro vytváření elektronického pečeti nebo šifrování datových zpráv.
QSealCD	Qualified Signature Creation Device	Kvalifikovaný prostředek pro vytváření elektronických pečeťů. V rámci tohoto dokumentu se jedná o HSM moduly s odpovídající certifikací.

Akronym	Plný význam	Vysvětlení
QTS	Qualified Trusted Service	Kvalifikovaná služby vytvářející důvěru
QTSP	Qualified Trust Service Provider	Kvalifikovaný poskytovatel služby vytvářející důvěru
RA	Registrační autorita	Subjekt definovaný QTSP PostSignum s odpovídající smlouvu. Registrační autorita ověřuje identitu Uživatelů Služby.
Rozhraní	Integrační rozhraní pro čerpání Služby	Jakékoliv rozhraní určené poskytovatelem Služby pro její čerpání, zejména webová aplikace pro čerpání Služby, webové služby pro integraci, jakákoliv aplikační či integrační rozhraní dodané výhradně provozovatelem Služby nebo jím určeným poskytovatelem.
SAM	Signature Activation Module	Modul pro aktivaci použití elektronického certifikátu pro vytvoření pečeti
SCD	Signature Creation Device	Zařízení pro vytváření elektronického pečeti
Služba	Služba vzdáleného pečetění elektronických dokumentů a dat	Služby provozovaná QTSP Software602. Vytváří kvalifikované elektronické pečeťy.
Správce Služby	Správce Služby	Osoba určená Klientem Služby, oprávněná k administraci služby a zejména nastavení oprávnění čerpání pro Uživatele Služby.
TIER III	Klasifikace datacentra dle organizace Uptime Isntitute	S tímto nastavením je možné provádět údržbu bez ovlivnění dostupnosti a chodu služeb na serveru. Tato datacentra neochrání před vážnými incidenty, které se mohou odehrát na různých komponentách infrastruktury.
TIER IV	Klasifikace datacentra dle organizace Uptime Isntitute	Nejvyšší úroveň záruk. Tato datacentrová kategorie je plně redundantní co se týče elektrických okruhů, chlazení a sítě. Tato architektura odolá i nejvážnějším technickým incidentům, aniž by byla jakkoli ovlivněna dostupnost serveru.
TPE	Tamper Protected Enviroment	Prostředí chráněné proti neoprávněnému zásahu.
TS	Trusted Service	Služba vytvářející důvěru
TSA	Time-Stamping Authority	Poskytovatel služeb elektronických časových razítek

Akronym	Plný význam	Vysvětlení
TSP	Trust Service Provider	Poskytovatel služby vytvářející důvěru
UP	User Policy	Definuje povinnosti a zodpovědnosti uživatelů certifikátů.
Uživatel Služby	Uživatel Služby	Uživatel Služby je fyzická osoba. Uživatel Služby je zaměstnancem Klienta Služby. Jedná se o podepisující osobu
WS	Web Services	Technologie vzdáleného volání funkcí v distribuovaných systémech založená na protokolu pro vzdálená volání SOAP a jazyku pro popis poskytovaných služeb WSDL.

2. Odpovědnost za zveřejňování a úložiště informací a dokumentace

2.1. Úložiště informací a dokumentace

Software602 zřizuje a udržuje interní úložiště informací a dokumentace formou interního portálu.

2.2. Zveřejňování informací a dokumentace

Služba pečetění je poskytována jako komerční veřejná TS, která je součástí ostatních nabízených služeb. Poskytovatelem TS je QTSP Software602.

Základní politika poskytování Služby je popsána v tomto dokumentu a je umístěna na této adrese:

https://602.cz/links/RSealpolicy

Základní adresa, kde jsou dostupné ostatní veřejné dokumenty v tištěné podobě:

Technické oddělení Software602 a.s.
Hornokrčská 15
140 00 Praha 4

Základní adresy, kde jsou k dispozici veřejné informace v elektronické podobě:

https://602.cz, https://602.cz/secusign

2.3. Periodicita zveřejňování informací

Software602 zveřejňuje aktualizované dokumenty a aktuální informace týkající se změn v poskytování Služby prostřednictvím webových stránek společnosti.

Jakékoliv změny v používání Služby oznámí klientům prostřednictvím kontaktních údajů klientem uvedených.

Pokud je Služba součástí QTS, jsou jakékoliv změny v poskytování Služby, včetně záměru o ukončení činnosti oznámeny poskytovatelem Služby orgánu dohledu v souladu s eIDAS, článkem 24, odstavec 2, paragraf a).

2.4. Řízení přístupu k jednotlivým typům úložišť

Přístup ke konkrétním typům úložišť je definován interními směrnicemi Software602. Přístup s právem zápisu mají přidělen správci odpovídajících dat. Veřejné údaje jsou přístupné pro čtení bez omezení. Pro dokumenty s omezeným přístupem je implementováno řízení přístupu.

3. Identifikace a autentizace

Tato kapitola specifikuje požadavky na verifikaci identity uživatele Služby.

3.1. Ověření identity Klienta Služby

Klientem služby může být právnická osoba, která má s Poskytovatelem uzavřenou platnou smlouvu. Před uzavřením smlouvy je ověřena identita právnické osoby Klienta služby. Součástí smlouvy či dohody o čerpání Služby je podepsaný Souhlas s umístěním soukromého klíče do HSM pro poskytování služby vzdáleného pečetění.

Identita Klienta služby je ověřena na základě výpisu z odpovídajícího registru (obchodní rejstřík, živnostenský list a podobně)

Klient musí mít dále uzavřenou smlouvu s poskytovatelem certifikačních služeb PostSignum. V rámci této smlouvy je Klient identifikován dle odpovídající politiky QTSP PostSignum - http://www.postsignum.cz/certifikacni_politiky_qca.html.

3.1.1. Registrace Správce Služby

Správce Služby se registruje na portálech Software602 pro získání 602 ID. Základní údaje nezbytné pro prvotní registraci jsou emailová adresa a uživatelem zvolené heslo. Po zadání požadavku na registraci je na uvedený email odeslán potvrzovací email pro ověření držitele emailové schránky. Další čerpání služeb je umožněno po sepsání smlouvy, ověření identity Správce Služby a aktivaci Služby Poskytovatelem.

3.1.2. Ověření identity Správce Služby

Správce Služby je pověřená osoba Klienta Služby, který je oprávněn k administraci služby a zejména nastavení oprávnění čerpání pro Uživatele Služby. Ověření identity Správce Služby zajišťuje Klient Služby.

3.2. Aplikace pro čerpání služby

Služba vzdáleného pečetění je určena pro čerpání z aplikací třetích stran, které jsou důvěryhodné a vytváří požadavek na pečetění elektronických dokumentů a dat.

Aplikace se vůči aplikačnímu rozhraní Poskytovatele autentizuje prostřednictvím certifikátu.

3.3. Ukončení čerpání služby

Pokud Klient nedodržuje podmínky čerpání Služeb plynoucí z této PP a Smlouvy, stanovuje si QTSP Software602 výhradní právo ukončit poskytování Služeb v plném rozsahu. Ukončení poskytování Služby ze strany Klienta je možné na základě písemné žádosti podepsané zaručenou elektronickou pečetí Klienta založenou na kvalifikovaném certifikátu, nebo kvalifikovaným elektronickým podpisem s kvalifikovaným elektronickým časovým razítkem statutárního zástupce Klienta. V případě listinného dokumentu je akceptován dokument, který je podepsán vlastnoručním a ověřeným podpisem statutárního zástupce Klienta.

3.4. Zrušení uživatelského účtu

Uživatelský účet včetně 602 ID je zrušen na základě písemné žádosti podepsané zaručenou elektronickou pečetí Klienta založenou na kvalifikovaném certifikátu, nebo kvalifikovaným elektronickým podpisem s kvalifikovaným elektronickým časovým razítkem statutárního zástupce Klienta. V případě listinného dokumentu je akceptován dokument podepsaný vlastnoručním a ověřeným podpisem statutárního zástupce Klienta.

4. Služba pečetění

Služba zpracovává na vstupu definovaného Rozhraní data určená k pečetění. Akceptuje formáty dat určených k pečetění, které je možné opatřit kvalifikovanou elektronickou pečetí dle specifikací definovaných ETSI na něž je odkazováno z Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES prostřednictvím Prováděcího rozhodnutí komise (EU) 2015/1506 ze dne 8. září 2015, kterým se stanoví specifikace pro formáty zaručených elektronických podpisů a zaručených pečetí uznávaných subjekty veřejného sektoru podle čl. 27 odst. 5 a čl. 37 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu.

Rozhraním Služby je pouze Rozhraní dodané a poskytnuté poskytovatelem. Tímto rozhraním může být například webová aplikace, webové služby nebo jiné aplikační rozhraní. Konzumováním Služby jiným způsobem, než je definováno Poskytovatelem, není povoleno a je vnímáno jako porušení podmínek poskytování Služby.

4.1. Certifikát pro pečeť

4.1.1. Akceptované formáty certifikátu

Služba je připravena zajistit pečetění dat určených k pečetění na základě certifikátu pro kvalifikovanou elektronickou pečeť. Kvalifikovaný elektronický certifikát pro elektronickou pečeť je vydáván QTSP PostSignum a je vytvářen a spravován v QSealCD s odpovídající certifikací.

4.1.2. Vytvoření certifikátu

V rámci Služby jsou používány kvalifikované certifikáty pro elektronickou pečeť od QTSP PostSignum jehož externí RA s pověřením vytváření tohoto certifikátu je Poskytovatel Služby. Certifikát je vytvořen přímo v certifikovaném QSealCD. Proces vytvoření a vydání certifikátu splňuje požadavky definované politikou vydávání certifikátů pro kvalifikovanou pečeť od QTSP PostSignum http://www.postsignum.cz/certifikacni_politiky_qca.html.

4.1.3. Použití certifikátu

Použití certifikátu pro kvalifikovanou elektronickou pečeť za účelem pečetění dat určených k pečetění a opatření kvalifikovaným časovým razítkem je vždy iniciováno Aplikací pro čerpání Služby. Použití je dostupné pouze přes definované Rozhraní TSP a po odpovídající autentizaci uživatele Služby. Veškerá komunikace probíhá po šifrovaném spojení a provozovatel Služby nemá přístup k obsahu podepisovaného dokumentu ani přímý přístup k certifikátu pro pečetění bez vědomí pečetícího subjektu.

4.2. Formát podpisu pro kvalifikovanou elektronickou pečeť

4.2.1. PAdES

Jde o podpis využívaný pro pečetění PDF a PDF/A dokumentů. Jeho technická specifikace ETSI TS 103172 v.2.2.2 je uvedena zde:
http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Současně také jako evropský standard ETSI EN 319 142
https://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf

4.2.2. XAdES

Jde o podpis využívaný pro pečetění strukturovaných dokumentů s datovou XML strukturou. Jeho technická specifikace ETSI TS 103171 v.2.1.1 je uvedena zde:
http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103172v020101p.pdf

Současně také jako evropský standard ETSI EN 319 132
https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf

4.2.3. CAdES

Jde o podpis využívaný pro pečetění obecných binárních dat a dokumentů, u kterých není možné použít vložený pečeť. Jeho technická specifikace ETSI TS 103173 v.2.2.1 je uvedena zde:
http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103172v020201p.pdf

Současně také jako evropský standard ETSI EN 319 122
https://www.etsi.org/deliver/etsi_en/319100_319199/31912201/01.01.01_60/en_31912201v010101p.pdf

4.2.4. ASiC

Jedná se o druh podpisu využívaný pro možnost pečetění více dokumentů najednou v rámci jednoho kontejneru. Jeho technická specifikace ETSI TS 103 174 v2.2.1. je uvedena zde:

http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Současně také jako evropský standard ETSI EN 319 162

http://www.etsi.org/deliver/etsi_en/319100_319199/31916201/01.01.01_60/en_31916201v010101p.pdf

4.3. Dostupnost Služby

4.3.1. Služba pečetění

Dostupnost služby vzdáleného pečetění je garantována na základě definovaných záruk poskytování Služby a dle požadavků konkrétního Klienta. Služba je poskytována QTSP Software602 v režimu vysoké dostupnosti. QTSP Software602 poskytuje garantovanou dostupnost ukotvenou ve smlouvě o poskytování Služby s koncovým klientem.

5. Management, provozní a fyzická bezpečnost

5.1. Fyzická bezpečnost

5.1.1. Umístění a konstrukce

Umístění je voleno tak, aby bylo možno zajistit ochranu před přístupem nepovolaných osob, ochranu před živelnými pohromami a nehodami v inženýrských sítích.

Technologie Služby a QSealCD jsou umístěna v infrastruktuře společnosti Telefonica O2, která poskytuje vysokou úroveň bezpečnosti a komplexní zajištění dodržování předpisů.

Certifikace prostředí O2 je k dispozici zde:

https://www.o2.cz/spolecnost/certifikaty/

https://602.cz/links/O2_Tier3

Certifikace prostředí Azure jsou k dispozici zde:

https://www.microsoft.com/en-us/TrustCenter/Compliance?service=Azure

Reálně jsou datová centra společnosti provozována mezi klasifikací Tier III a Tier IV, tak jak je definováno ve standardu TIA 942. Nicméně nespoléhají se jen na HW nástroje pro zajištění dostupnosti, tak jak to předpokládali Uptime Institute v době housingu a webového hostingu.

5.1.2. Fyzický přístup

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.3. Elektřina a klimatizace

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.4. Vliv vody

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.5. Protipožární opatření a ochrana

Technologie Služby je umístěna v centrech splňujících TIER III.

5.1.6. Ukládání médií

Všechna datová media jsou uložena v prostorách prostředí chráněného proti neoprávněnému zásahu. Prostory jsou vybaveny zařízením pro zajištění stálé teploty a vlhkosti a poskytují ochranu proti magnetickému rušení a jsou pod neustálým kamerovým dohledem.

5.1.7. Zálohy

Zálohy technologie Služby jsou zajišťovány v rámci TIER III v prostředí chráněném proti neoprávněnému zásahu.

5.2. Procesní bezpečnost

5.2.1. Důvěryhodné role

Všichni zaměstnanci, kteří mají přístup nebo kontrolu nad kryptografickými a operacemi pro vytváření pečeti prováděnými v rámci Služby, jsou zařazeni do důvěryhodných rolí odpovídajících prováděným činnostem. V rámci správy systému Služby je důsledně využíváno principu oddělení zodpovědnosti (separation of duties). Zařazování pracovníků do důvěryhodných rolí se řídí interními předpisy Software602.

5.2.2. Počet osob požadovaných na zajištění jednotlivých činností

Počty zaměstnanců na jednotlivých pozicích odpovídají potřebné míře oddělení odpovědností a jsou detailně specifikovány v související dokumentaci.

5.2.3. Identifikace a autentizace pro každou roli

Pracovníkům jsou přiděleny prostředky pro řádnou autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné. Tyto prostředky jsou při ukončení role, nebo pracovního poměru skartovány a odvolány dle interních směrnic Software602.

5.2.4. Role vyžadující rozdělení povinností

V systému nelze slučovat následující činnosti:

- Bezpečnostní dohled systému Služby s žádnou další výkonnou rolí v systému.
- Nasazení jakýchkoliv změn bez potvrzení nadřízených pracovníků
- Nasazení jakýchkoliv změn do produkčního prostředí bez řádného otestování a potvrzení nadřízených pracovníků

Detailně jsou role a rozdělení pravomocí popsány v interní dokumentaci poskytovatele Služby.

5.3. Personální bezpečnost

Důvěryhodnost a spolehlivost Služby a celé infrastruktury je mimo jiné závislá i na kvalitě jejího personálu. Kvalita personálu je dále vnímána jako souhrn důvěryhodnosti a kompetentnosti. Software602 se řídí takovými pravidly pro řízení zaměstnanců, jejichž dodržování zajistí potřebnou míru důvěryhodnosti.

5.3.1. Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Kandidát musí splňovat podmínky stanovené v rámci interních předpisů Software602 a podmínek definovaných Personálním odborem a úsekem bezpečnosti pro danou pozici.

Především pak:

- Občanská bezúhonnost
- Odpovídající vzdělání
- Potvrzená praxe v oblasti informačních a komunikačních technologií alespoň 3 roky

Povolení přístupu k systémům a aplikacím důvěryhodných služeb je definováno interními předpisy Software602 a povinnosti a odpovědnosti pracovníka jsou uvedeny v pracovní smlouvě.

5.3.2. Posouzení spolehlivosti osob

Personální odbor a úsek bezpečnosti Software602 provádějí počáteční prověření všech kandidátů ucházejících se o práci v citlivých pozicích. Toto prověření pokrývá osobní a kvalifikační oblast.

Zaměstnanci personálního odboru podle možností ověří předané reference u předchozího zaměstnavatele, nejlépe s využitím jiných zdrojů než těch, které předložil kandidát.

Personální odbor a úsek bezpečnosti Software602 provádějí periodické prověření všech zaměstnanců již činných v citlivých pozicích.

5.3.3. Požadavky na přípravu pro výkon role, vstupní školení

Personální odbor a úsek lidské zdroje Software602 zajišťuje pro všechny zaměstnance potřebnou úroveň počátečních školení, aby tito byli schopni správně a efektivně zastávat své pozice. Požadavky pro každou roli jsou stanoveny v interních směrnicích pro provoz Služby.

5.3.4. Požadavky a periodicita školení

Personální odbor a úsek lidské zdroje Software602 zajišťuje pro všechny zaměstnance potřebnou úroveň pokračovacích periodických školení, aby tito byli schopni správně a efektivně zastávat své pozice. Intenzita školení je minimálně jednou za dvanáct měsíců.

5.3.5. Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Nepředepisuje se.

5.3.6. Postihy za neoprávněné činnosti zaměstnanců

Všichni zaměstnanci podepisují Prohlášení o mlčenlivosti a jednají podle něj a podle dalších interních předpisů.

5.3.7. Požadavky na nezávislé zhotovitele (dodavatele)

Služba a technologie Služby nevyužívá nezávislé zhotovitele (dodavatele).

5.3.8. Dokumentace poskytovaná zaměstnancům

Všichni zaměstnanci obdrží informaci o existenci a závaznosti bezpečnostní dokumentace. Všichni zaměstnanci mají přístup k bezpečnostní politice Software602.

5.4. Auditní záznamy (logy)

5.4.1. Typy zaznamenávaných událostí

Do elektronického auditního logu jsou zaznamenávány následující typy událostí:

- ***systémové události***. Záznam je vytvořený operačním systémem k zaznamenávání každého úkonu uskutečněného na počítačích, kde jsou nainstalovány procesy *Služby*:
    - Instalaci nového software;
    - Zapnutí, vypnutí;
    - Úkony vykonávané jakoukoliv aplikací;
    - Úkony vykonávané jakýmkoliv uživatelem.
- **události pečetění**.
    - Datum a čas
    - Hash vstupních dat
    - Hash souboru s pečetí
    - Výsledek operace
    - Doba provedení operace
- **autentizační události**
    - Identifikátor Uživatele
    - Identifikátor Klienta
    - Datum a čas požadavku na autentizaci
    - IP adresa, ze které požadavek vznikl
    - Identifikátor o provedené autentizaci

Všechny auditní záznamy jsou v nutné míře pořizovány, uchovávány a zpracovávány se zachováním prokazatelnosti původu, integrity, dostupnosti, důvěrnosti a časové autentičnosti.

Auditní systém je navržen a provozován způsobem, který zaručuje udržování auditních dat, rezervování dostatečného prostoru pro auditní data, automatické nepřepisování auditního souboru, prezentaci auditních záznamů pro uživatele vhodným způsobem a omezení přístupu k auditnímu souboru pouze pro definované uživatele.

5.4.2. Periodicita zpracování záznamů

Informace jsou zaznamenávány on-line a záznamy jsou pravidelně analyzovány Správcem bezpečnosti tak, aby byly detekovány jakékoliv případné odchylky od běžných činností nebo úmyslné poškozování. Dále jsou záznamy vyhodnocovány skupinou Dohledu.

5.4.3. Doba uchování auditních záznamů

Lhůta uchovávání záznamů pro audit je v souladu s kapitolou 5.5.2. Doba uložení dat pro data publikovaná v rejstříku a data z provozních systémů Služby činí 10 let.

5.4.4. Ochrana auditních záznamů

Elektronické záznamy pro potřeby auditu vytvářené systémy Infrastruktury veřejných klíčů Software602 obsahují časový údaj o vzniku záznamu a mohou být zabezpečeny před změnou digitální pečetí.

Soubory obsahující údaje pro audit jsou fyzicky zabezpečeny, stejně jako ostatní části PKI. Přístup k těmto souborům má Správce PKI.

5.4.5. Postupy pro zálohování auditních záznamů

Existují dvě hlavní zálohovací procedury:

- každodenní zálohování pomocí zálohovacího robota;
- kontinuální replikační systém do záložního pracoviště (užívající vysoce zabezpečenou síť) umístěném v bezpečném prostoru se stejnou úrovní zabezpečení jako hlavní místo.

Archivace je popsána v kapitole 5.5..

5.4.6. Systém shromažďování auditních záznamů

Veškeré citlivé auditní záznamy jsou zálohovány do databáze a v pravidelných intervalech zálohované. Ostatní bezpečnostní logy jsou kontrolovány v režimu 7 x 24 oddělením dohledu.

5.4.7. Postup při oznamování události subjektu, který ji způsobil

Subjekt není standardně informován, v rámci šetření incidentu ale může být vyzván oprávněnou osobou k podání vysvětlení.

5.5. Uchovávání informací a dokumentace

5.5.1. Typy informací a dokumentace, které se uchovávají

Správce Služby v Software602 zajišťuje vhodným způsobem archivaci zejména:

- informace pro účely auditu (popsané v předešlé kapitole);
- výsledky auditu;
- výsledky certifikací;
- písemné a elektronické dokumenty používané v rámci Služby:
    - smluvní dokumenty;
    - písemné žádosti o čerpání/zrušení čerpání Služby;
    - dokumenty vzniklé při nastavení služby

5.5.2. Doba uchování informací a dokumentace

Všechny dokumenty v archivech budou uchovávány po dobu nejméně 10 let od vypršení jednotlivých certifikátů nebo ukončení platnosti dokumentů.

5.5.3. Ochrana úložiště informací a dokumentace

Ochrana je zajištěna následujícím souborem opatření:

- Archivy v elektronické formě jsou uloženy v databázi / souborovém úložišti na infrastruktuře poskytovatele Cloudové služby Azure s dlouhou životností. Všechna data vytvářená systémy Služby jsou zabezpečena před změnou elektronickou pečetí.
- Záznamové soubory jsou fyzicky zabezpečeny.
- Přístup k těmto souborům mají pouze určení členové *Správy Služby* a členové nezávislého týmu auditorů Software602, nebo členové externího auditu pověření Správci Služby.
- Bezpečný transport písemných dokumentů zajišťuje *Správce PKI*.

5.5.4. Postupy při zálohování uchovávaných informací a dokumentace

Zálohovací postupy jsou upraveny interní směrnicí a další relevantní interní dokumentací Software602.

5.5.5. Požadavky na používání časových razítek při pečetění a uchovávání informací a dokumentace

Elektronická kvalifikovaná časová razítka používaná při

- poskytování Služby,
- uchovávání elektronické dokumentace a
- souvisejících informací

jsou zajištěna na základě spolupráce s QTSP PostSignum a jejich používání se řídí politikou QTSP PostSignum.

5.5.6. Systém shromažďování uchovávaných informací a dokumentace

Správce Služby ověřuje neporušenost a celistvost archivu v rámci pravidelného interního auditu. Přístup k archivu má pouze Správce Služby a členové nezávislého týmu auditorů určeného Software602 podle procedur popsaných v interní dokumentaci.

Správce Služby může určit pověřeného pracovníka Dohledu, aby průběžně prováděl kontrolu archivu.

5.5.7. Postupy pro získání a ověření uchovávaných informací a dokumentace

Archivované informace jsou dostupné na základě oprávněné žádosti. Informace může zpřístupnit Správce Služby interním pracovníkům poskytovatele, pokud je to nezbytné pro vykonávání jejich činnosti, nebo oprávněným kontrolním subjektům a o tomto poskytnutí informací je vytvořen záznam. Informace je možno ověřit.

5.6. Obnova po havárii

5.6.1. Postup v případě incidentu

Konkrétní postup je stanoven příslušnou interní prováděcí směrnicí Software602.

5.6.2. Poškození výpočetních prostředků, softwaru nebo dat

Je ošetřeno opatřeními dle kapitol 5.1, 5.5 a konkrétní postup je stanoven příslušnou interní prováděcí směrnicí Software602.

5.6.3. Schopnost obnovit činnost po havárii

V případě havárie postupuje Software602 v souladu s interními havarijními směrnicemi, provoz Služby se může přerušit jen na dobu nezbytně nutnou k migraci postižených subsystémů do záložní lokality. Pro rychlou obnovu je možné v rámci Azure obnovit celou infrastrukturu Služby z prováděných záloh.

5.7. Ukončení činnosti Služby

Ukončení činnosti Služby musí být písemně oznámeno všem uživatelům Služby a subjektům, které mají uzavřenou smlouvu týkající se provozu a čerpání Služby. Zároveň musí být tato skutečnost oznámena na webových stránkách poskytovatele.

V případě ukončení činnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru je postupováno následujícím způsobem:

Ukončení činnosti Služby musí být oznámeno všem uživatelům Služby, orgánu dohledu a subjektům, které mají uzavřenou smlouvu týkající se provozu a čerpání Služby. Zároveň musí být tato skutečnost oznámena na webových stránkách QTSP.

Poskytovatel se zavazuje poskytovat Službu 6 měsíců ode dne oznámení o ukončení činnosti.

Správa Služby přijme opatření pro zajištění archivovaných záznamů po dobu předepsanou v kapitole 5.5.2.

6. Technická bezpečnost

6.1. Počítačová bezpečnost

6.1.1. Specifické technické požadavky na počítačovou bezpečnost Poskytovatele

Jsou definovány v rámci interních směrnic pro provoz PKI Software602 a řídí se těmito principy:

- Kritické systémy Software602 jsou umístěny ve fyzicky chráněném prostředí s řízeným přístupem.
- Kritické systémy Software602 jsou umístěny v Cloudovém prostředí s vysokou mírou zabezpečení s řízeným přístupem a odpovídající certifikací (Tier III minimálně)
- Na těchto počítačích jsou spuštěny nebo instalovány pouze programy související s provozem kritického systému Software602.
- Provoz systémů je monitorován a pravidelně auditován.
- Používané jsou jen HSM moduly schválené a uvedené na seznamu EU s odpovídající certifikací pro QSealCD
- HSM moduly jsou umístěné v bezpečné infrastruktuře s bezpečnostní TIER III v dedikovaném prostředí jen pro potřeby Poskytovatele
- Testovací a vývojové systémy jsou důsledně odděleny od produkčních systémů.

6.1.2. Specifické technické požadavky na počítačovou bezpečnost Klienta

Jsou specifikovány v konkrétní smlouvě SLA, obecně je třeba dodržet následující požadavky na umístění integračního serveru v infrastruktuře klienta.

- Integrační server pro zajištění práce s dokumenty určenými k podepsání je umístěn na dedikovaném virtuálním či fyzickém serveru s operačním systémem MS Windows Server v podporované verzi
- Dedikovaný virtuální či fyzický stroj je umístěn v místnosti / serverovně s kontrolovaným přístupem a je pro něj zajištěna odpovídající fyzická bezpečnost.
- Poskytovatel služby má možnost kdykoliv zkontrolovat bezpečnostní požadavky

6.1.3. Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti je založeno na mezinárodních a národních standardech a je prováděno pracovníky Software602.

6.2. Bezpečnost životního cyklu

6.2.1. Řízení vývoje systému

Při vývoji systému je postupováno v souladu s interní dokumentací a best practice postupy pro vývoj software. Důsledně jsou dodržovány principy:

- Oddělení vývojového, testovacího a produkčního prostředí.

- Implementace principu PDCA (Plan – Do – Check – Act).
    - Plánování – analytická příprava, plánování zamýšleného řešení, zlepšení či změny
    - Realizace – implementace navrženého řešení
    - Ověření a testování – průběžné monitorování a hodnocení vybraných ukazatelů kvality a funkčnosti.
    - Provoz – probíhá provozní sledování a vyhodnocování bezpečnosti a kvality, provádění navržených opatření ke zlepšení, změně či nápravě

6.2.2. Kontroly řízení bezpečnosti

Soulad se standardy je ověřován pravidelnými audity a kontrolami bezpečnostní shody.

6.2.3. Řízení bezpečnosti životního cyklu

Změnové řízení probíhá ve smyslu interního předpisu Software602 v souladu s principy PDCA.

6.3. Síťová bezpečnost

Zabezpečení sítí je popsáno v interních směrnicích pro provoz Software602. Je kladen maximální důraz na důkladné zabezpečení všech komponent, síťová bezpečnost integračního serveru musí být řízena těmito směrnicemi také.

- Testovací a vývojové systémy jsou důsledně odděleny od produkčních systémů.
- Počítačové sítě kritických systémů Software602 jsou odděleny od běžné podnikové sítě pomocí interního firewallu.
- Provoz systémů je monitorován a pravidelně auditován.
- Kontroly a ověřování průchodnosti sítě jsou pravidelně prováděny prostřednictvím technických správců v rámci struktury Software602.

6.4. Časová razítka

V rámci poskytované Služby jsou využívána kvalifikovaná elektronická časová razítka od QTSP.

Vydávání kvalifikovaných časových razítek se řídí Politikou vydávání kvalifikovaných časových razítek příslušného QTSP.

7. Hodnocení shody a jiná hodnocení

7.1. Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Správce Služby je oprávněn vyžádat si pravidelné i nepravidelné inspekce a audity kterékoliv lokality a infrastrukturní části či komponenty Služby. Tyto audity budou provedeny za účelem ověření, zda provoz Služby je v souladu s bezpečnostními postupy a procedurami, tak jak jsou definovány v této politice a interních předpisech.

Z důvodu kontroly souladu praxe s ustanoveními současné PP a příslušných směrnic projde Služby v pravidelných intervalech interním auditem.

7.2. Identita a kvalifikace hodnotitele

Odpovědný hodnotitel musí být kvalifikovaný auditor a musí znát principy TSP a související informace a odpovídající předpisy definované dle eIDAS.

7.3. Vztah hodnotitele k hodnocenému subjektu

Hodnotitel musí být od hodnocené Služby a TSP dostatečně organizačně oddělen, aby jeho hodnocení mohlo být skutečně nezávislé a nepředpojaté.

7.4. Postup v případě zjištění nedostatků

Jakékoliv nesrovnalosti mezi činností Služby a ustanoveními jejích PP a/nebo interních směrnic TSP musí být zaznamenány a bezodkladně nebo ve stanovené lhůtě řešeny.

Jakákoliv náprava může obsahovat pokyny k trvalému či dočasnému pozastavení činnosti části Služby, přičemž je nutno – ještě před přijetím takového rozhodnutí – přihlédnout k několika faktorům, mezi něž se též řadí závažnost nesrovnalostí, vzniklých rizik a újmy, které takové narušení způsobí subjektům využívajících Službu.

Rozhodnutí o tom, jaké kroky budou podniknuty, se bude též odvíjet od způsobu předchozích reakcí na vzniklé problémy, od závažnosti odchylek a od doporučení auditora.

7.5. Sdělování výsledků hodnocení

Závěrečné výsledky auditu budou předány vedení Software602. Závěrečným výsledkem se zde rozumí informace o veškerých odchylkách, jež by mohly mít vliv na důvěru závislé strany v kvalitu a bezpečnost poskytované Služby, včetně adekvátního ohodnocení závažnosti, nikoliv však podrobné informace, které by šlo použít k napadení systému.

Shodně s ustanoveními odstavce 7.4, jakákoliv součást Služby, u níž se prokáže, že nepracuje v souladu s touto PP, musí být ihned, jakmile je audit hotov, zhodnocena a zajištěna její náprava. Kvůli maximálnímu snížení rizik, je nutno, aby byly pokyny k požadované nápravě určeny i oznámeny co

možná nejdříve. O realizaci pokynů k dosažení nápravy je pak nutno zpravit přímo správce Služby. Je možné, že pro potvrzení sjednané nápravy a její efektivnosti bude vyžádán zvláštní audit.

8. Ostatní obchodní a právní záležitosti

8.1. Poplatky

Poskytování Služby je zpoplatněno dle ceníku TSP a QTSP. Konkrétní zpoplatnění poskytované Služby je zakotveno ve smlouvě mezi uživatelem Služby a Poskytovatelem Služby

8.2. Finanční odpovědnost

8.2.1. Krytí pojištěním

Poskytovatel Služby, společnost Software602 a.s. prohlašuje, že má smluvně uzavřené dostatečné pojištění rizik tak, aby bylo možné krýt případná rizika a finanční škody. Toto pojištění je mandatorní pro kvalifikovaného poskytovatele služeb vytvářejících důvěru.

8.2.2. Další aktiva a záruky

Informace o aktivách poskytovatele Služby je možné získat z výroční zprávy, která je uveřejněna na webových stránkách poskytovatele – Software602 a.s.

8.2.3. Pojištění nebo krytí zárukou pro koncové uživatele

Není v rámci tohoto dokumentu definováno a není předmětem této politiky.

8.3. Důvěrnost obchodních informací

8.3.1. Výčet důvěrných informací

Důvěrnými informacemi TSP jsou:

- Veškeré informace týkající se procesu pečetění a uložené v rámci Služby v záznamech.
- Ostatní kryptograficky podstatné informace sloužící k provozu Služby.
- Vybrané obchodní informace.
- Veškeré informace a dokumentace s ohledem na poskytování služeb vytvářejících důvěru.
- Veškeré osobní údaje.

Za chráněné informace se rovněž považují veškeré další informace označené některým ze subjektů jako zvláště důvěrné. S chráněnými informacemi, bez ohledu na typ nosiče, je zacházeno tak, aby byla zajištěna jejich důvěrnost a integrita.

8.3.2. Informace mimo rámec důvěrných informací

Za důvěrné nejsou považovány:

- Veřejné části certifikátů,
- Hashe podepsaných dokumentů,

8.3.3. Odpovědnost za ochranu důvěrných informací

Za ochranu důvěrných informací odpovídá organizační složka nebo osoba, která tyto informace spravuje. Každý pracovník, který přijde do styku s informacemi, které jsou předmětem utajení podle kapitoly 8.2.1, je nesmí poskytnout třetí osobě.

Zaměstnanci Software602, spolupracující osoby nebo společnosti, které přicházejí do styku s citlivými informacemi, jsou povinni zachovávat mlčenlivost o těchto informacích. Tato povinnost trvá i po skončení pracovního nebo jiného obdobného poměru nebo po provedení kontrahovaných prací.

Jako organizačně právní opatření vedoucí k naplnění výše uvedených podmínek je se všemi subjekty podepisováno smluvní ujednání (formou dodatku k pracovní smlouvě, dohoda o zachování mlčenlivosti apod.).

8.4. Ochrana osobních údajů

Ochrana osobních údajů se řídí nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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 - GDPR), směrnicí Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV, dále adaptačním zákonem č. 110/2019 Sb. (ze dne 12. března 2019 o zpracování osobních údajů) a zákonem č. 89/2012 Sb. (občanský zákoník).

8.5. Práva duševního vlastnictví

Tato PP, veškeré související dokumenty, obsah webových stránek, aplikační rozhraní, procedury a směrnice, jimiž je zajišťován provoz Služby, jsou chráněny právy Software602 a představují její významné know-how a práva duševního vlastnictví.

8.6. Zřeknutí se záruk

QTSP a TSP Software602 odmítá jakékoliv záruky na provoz Služby a výsledky poskytnuté Službou, pokud byla Služba a/nebo Rozhraní Služby použito v rozporu s podmínkami použití Služby a touto politikou.

8.7. Omezení odpovědnosti

Za žádných okolností neponese Software602, jeho představitelé, ředitelé, zaměstnanci, partneři, poskytovatelé licence nebo dodavatelé vůči uživateli nebo jiné osobě odpovědnost za jakékoli zvláštní, náhodné, nepřímé, vedlejší nebo trestněprávní škody, včetně škod plynoucích ze ztráty či zničení dat nebo ztráty zisků, ať již jsou předvídatelné nebo bylo na možnost takových škod poskytovatele Služby upozorněno, nebo na základě jakékoli teorie odpovědnosti, včetně porušení smlouvy nebo záruky, nedbalosti nebo jiného protiprávního jednání, nebo jakéhokoli jiného nároku plynoucího z použití nebo přístupu ke stránkám, službám nebo materiálům, nebo s takovým použitím souvisejícího. Žádné ustanovení v podmínkách nesmí omezit ani vyloučit odpovědnost poskytovatele Služby za hrubou

nedbalost nebo úmyslné způsobení škody či újmy poskytovatelem Služby nebo jeho zaměstnanci nebo za smrt nebo zranění osob.

8.8. Odpovědnost za škodu, náhrada škody

Povinnost Software602 k náhradě škody či nemajetkové újmy touto obchodní společností způsobené nikoliv úmyslně, z hrubé nedbalosti či na přirozených právech člověka porušením jakýchkoliv jejích závazků a/nebo povinností v souvislosti s poskytování Služby pečetění je omezena částkou 100 000,- Kč (slovy: jedno sto tisíc korun českých), kterážto částka představuje ve smyslu ust. § 2898 zákona č. 89/2012 Sb., občanský zákoník, v platném znění maximální částku náhrady škody či nemajetkové újmy, za kterou odpovídá Software602 a kterou bude případně povinna uhradit.

Při poskytování Služby pečetění, je důkazní břemeno, pokud jde úmysl nebo nedbalost TSP, na fyzické či právnické osobě uplatňující nárok na náhradu škody.

8.9. Doba platnosti, ukončení platnosti

8.9.1. Doba platnosti

Tento dokument zůstává v platnosti do skončení poskytování Služby dle této PP .

8.9.2. Ukončení platnosti

Ukončení platnosti této PP musí schválit vedení Software602 písemnou a nezpochybnitelnou formou. Tato skutečnost musí být zveřejněna na místech definovaných v kapitole 2.2.

8.10. Komunikace mezi zúčastněnými subjekty

Individuální komunikace může využívat všechny typy kontaktů, které si zúčastněné subjekty v rámci vzájemné autentizace vyměnili.

Veřejná komunikace probíhá kanály specifikovanými v kapitole 2.2. této PP.

8.10.1. Incidenty

Poskytovatel Služby identifikuje jednotné komunikační místo pro zadávání požadavků, incidentů a podnětů. Tímto jednotným kontaktním místem je emailová adresa hotline@602.cz. Toto rozhraní je napojeno na automatický systém pro sledování požadavků, který každému požadavků přiřadí unikátní číslo a zajistí včasné vyřízení požadavku s možností jeho zpětného sledování.

8.11. Změny

8.11.1. Postup při změnách

Software602 je oprávněna v budoucnosti doplnit tuto PP o ustanovení, jejichž nutnost bude teprve zjištěna. Takové změny budou zveřejněny na místech definovaných v kapitole 2.2 této PP. Případné změny nebudou mít zpětnou platnost.

Změny nemající materiální povahu vstoupí v platnost okamžikem řádného zveřejnění podle tohoto odstavce.

Změny mající materiální povahu vstoupí v platnost 15 dní po svém řádném zveřejnění, neoznámí-li Software602 před ukončením 15 denní lhůty jejich stažení.

8.11.2. Postup při oznamování změn

Řídí se pravidly a postupy uvedenými v kapitole 2.

8.11.3. Změny infrastruktury

Infrastruktura má vliv na bezpečnost a důvěryhodnost poskytované Služby. Pokud by se při průběžných interních auditech zjistila nedostatečnost poskytované kvality infrastruktury, bude v souladu s interními předpisy Software602 zajištěn přesun Služby na jinou infrastrukturu. Tato změna bude provedena tak, aby neovlivnila kontinuitu služby. Změny budou oznámeny v souladu s odstavcem 2.2. této PP.

8.12. Řešení sporů

Uživatel souhlasí s tím, že jakýkoli požadavek nebo nárok vznesený vůči Poskytovateli musí být řešen příslušným soudem soustavy obecných soudů České republiky v České republice, pokud si strany neujednají výslovně písemně jinak. Uživatel se zavazuje se, že se pro účely projednání takových nároků nebo sporů podvolí jurisdikci soudů v České republice. Jednacím jazykem bude český jazyk a místem konání soudního řízení bude sídlo příslušného soudu určené podle místa sídla Software602.

8.13. Rozhodné právo

Rozhodným právem je právo České republiky.

8.14. Shoda s právními předpisy

Tento dokument splňuje požadavky stanovené Nařízením eIDAS, legislativou České republiky a doporučeních orgánů EU, jmenovitě se jedná o dokumenty:

[1] ETSI TS 119 431-1 – Electronic Signatures and Infrastructures (ESI);Policy and security requirements for trust service providers; Part 1
[2] ETSI TS 119 431-2 - Electronic Signatures and Infrastructures (ESI);Policy and security requirements for trust service providers; Part 2
[3] ETSI TS 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Provider
[4] ETSI EN 319 142-1 - Electronic Signatures and Infrastructures (ESI); PAdES Digital Signatures
[5] ETSI EN 319 132 - Electronic Signatures and Infrastructures (ESI); XAdES Digital Signatures
[6] ETSI EN 319 122 - Electronic Signatures and Infrastructures (ESI); CAdES Digital Signatures
[7] ETSI EN 319 122 - Electronic Signatures and Infrastructures (ESI); Associated Signature Containers ASiC
[8] RFC3647 – Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework
[9] ETI EN 419 241-1 - Trustworthy Systems Supporting Server Signing

TSP je dále certifikován dle:

[10] ISO 27001 – Systém managementu bezpečnosti informací
[11] ISO 9001 – Systém managementu kvality
[12] ISO 10006 – Systém managementu poskytování ICT služeb organizace
[13] ISO 20000 – Systém managementu poskytování ICT služeb organizace