


Smlouva o dílo č. 20/600/0174

Níže uvedeného dne, měsíce a roku byla mezi smluvními stranami uzavřena podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ“), smlouva níže uvedeného znění na akci

„Zajištění služby kvalifikovaných pečeti na dálku pro systém AISG“

Smluvní strany

Název firmy: První certifikační autorita, a.s.
Se sídlem: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
Zapsaná: v obchodním rejstříku Městského soudu v Praze, oddíl B, vložka 7136
Zastoupená: Ing. Petrem Budišem, Ph.D., předsedou představenstva
Ing. Romanem Kučerou, členem představenstva

Spojení: 

IČ: 26439395
DIČ: CZ26439395
Bankovní spojení: Československá obchodní banka, a.s.
Číslo účtu: 168457418/0300
Adresa pro doručování korespondence: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00

dále jen „zhotovitel“

a

Česká republika – Generální ředitelství cel
Se sídlem: Budějovická 7, 140 96 Praha 4
Jednající: 

Spojení: 

IČ: 71214011
DIČ: CZ71214011
Bankovní spojení: ČNB Praha 1
Číslo účtu: 1020011/0710
Adresa pro doručování korespondence: Budějovická 7, 140 96 Praha 4

dále jen „objednatel“

Objednatel a zhotovitel (dále také jako „smluvní strany“) prohlašují, že údaje uvedené v tomto odstavci jsou v souladu s platnými zápisy v obchodním popř. jiném rejstříku.

Smluvní strany se zavazují, že změny ve výše uvedených údajích oznámí bez prodlení druhé straně (případně upozorní na důsledky z toho vyplývající). Pokud tak včas neučiní, uhradí druhé straně veškerou škodu, která jí tímto opomenutím vznikla.

Smluvní strany uzavírají tuto smlouvu s názvem „Zajištění služby kvalifikovaných pečeti na dálku pro systém AISG“ (dále jen „smlouva“).



Smluvní strany se dohodly, že se jejich závazkový vztah řídí OZ a zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“).

I. Předmět smlouvy

Předmětem smlouvy je závazek:

- 1.1. Zhotovitele v zajištění provozu služby vytváření kvalifikovaných elektronických pečeti na dálku v souladu s platnou Politikou služby vytváření kvalifikovaných elektronických pečeti na dálku (dále jen „Politika“) uvedenou v **Příloze č. 2** „Politika_PecetNaDalku_1v00“, která je nedílnou součástí této smlouvy. Obchodní označení zajišťové služby, která je předmětem této smlouvy, je I.CA RemoteSeal. Rozsah služby I.CA RemoteSeal je specifikován v **Příloze č. 1** „I.CA RemoteSeal - Služba vytváření kvalifikovaných elektronických pečeti na dálku, která je nedílnou součástí této smlouvy“. Závazek zhotovitele je dále označován souhrnně jako „dílo“.
- 1.2. Objednatele uhradit zhotoviteli za bezvadné dílo dohodnutou cenu dle článku VI. této smlouvy.

II. Povinnosti smluvních stran

2.1. Povinnosti zhotovitele:

- a) Zhotovitel je povinen dodat řádně a včas dílo dle této smlouvy bez faktických a právních vad.
- b) Zhotovitel je povinen zajistit ochranu dokumentů a dokumentace, v datové anebo listinné podobě, které od objednatele obdržel pro potřebu plnění předmětu díla nebo které vytvořil v rámci plnění předmětu díla. Zhotovitel je povinen takové dokumenty a dokumentaci po předání díla objednateli prokazatelně předat, nebo je se souhlasem objednatele prokazatelně zlikvidovat či je vést a prokazatelně evidovat. Zhotovitel je povinen zajistit, že takové dokumenty a dokumentace nebudou poskytnuty třetí straně nebo užity ve prospěch třetí strany.
- c) Veškeré podklady, které byly objednavatelem zhotoviteli předány, zůstávají v jeho vlastnictví a zhotovitel za ně odpovídá od okamžiku jejich převzetí jako skladovatel a je povinen je vrátit objednavateli po splnění svého závazku (předání díla), pokud není ujednáno jinak.
- d) Zhotovitel je povinen bez zbytečného odkladu oznámit objednateli všechny okolnosti, které zjistil při zařizování záležitostí, a které mohou mít vliv na změnu pokynů nebo zájmů objednatele, dále je povinen upozornit objednatele na nevhodnost předaných dokumentací, případně nevhodnost pokynů objednatele.
- e) Zhotovitel je povinen zachovávat mlčenlivost o všech záležitostech, o nichž se dozvěděl v souvislosti s prováděním předmětných činností.
- f) V případě, že v souvislosti s plněním závazků podle této smlouvy získá zhotovitel přístup k informacím obsahujícím osobní nebo citlivé údaje klientů či zaměstnanců objednatele, se zavazuje dodržovat mlčenlivost o všech těchto údajích vůči třetím osobám, zároveň se zavazuje učinit veškerá technická i organizační opatření, aby nedošlo k porušení povinností plynoucích objednateli z obecně závazných právních předpisů.

2.2. Zaměstnanci zhotovitele podílející se na plnění předmětu díla jsou povinni:

- a) zachovávat mlčenlivost ve vztahu k informacím, se kterými jakýmkoliv způsobem přijdou do styku při plnění předmětu díla,
- b) zdržet se pokusů o neoprávněný fyzický přístup do objektů anebo prostor objektů

objednatele, které nesouvisejí s plněním předmětu díla,

- c) zdržet se pokusů o neoprávněný logický přístup k objektům Informačního systému Celní správy ČR (dále jen „ISCS“), které nesouvisejí s plněním předmětu díla,
- d) zdržet se jakýchkoliv aktivit v objektech objednatele, které nesouvisejí s plněním předmětu díla,

2.3. Zhotovitel díla může pověřit jeho provedením jinou osobu (subdodavatele) jen s předchozím písemným souhlasem objednatele. I v takovém případě má však zhotovitel odpovědnost, jako by dílo prováděl sám. Zhotovitel má povinnost neprodleně informovat objednatele o tom, že pověřil provedením díla nebo jeho části subdodavatele.

2.4. Pracovníci zhotovitele nebudou kromě odpovědné osoby objednatele navazovat žádné další pracovní kontakty s jinými pracovníky objednatele pro řešení předmětu této smlouvy ani tyto jiné pracovníky seznamovat se stavem řešení projektu bez předchozího rozhodnutí oprávněné osoby na straně objednatele.

2.5. Zhotovitel prohlašuje ve smyslu ust. § 5 OZ, že je odborně způsobilý k zajištění předmětu této smlouvy a po celou dobu trvání závazku bude jednat se znalostí a pečlivostí, která je s touto odborností spojena. Zhotovitel výslovně prohlašuje, že je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady 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 („eIDAS“) a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, pro oblast vydávání kvalifikovaných certifikátů pro elektronické podpisy, kvalifikovaných elektronických časových razítek, kvalifikovaných certifikátů pro elektronické pečeti, kvalifikovaných certifikátů pro autentizaci internetových stránek a kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečeti. Služba I.CA RemoteSeal, vzhledem k tomu, že není přímo v nařízení eIDAS definována, nemůže být auditována jako kvalifikovaná služba. Nicméně byla posouzena orgánem dohledu, ministerstvem vnitra, a jeho rozhodnutím čj. MV-68158-6/EG-2018 ze dne 21. června 2018 bylo I.CA povoleno poskytovat službu vytváření kvalifikovaných elektronických pečeti na dálku I.CA RemoteSeal v souladu s politikou této služby a v souladu s technickou a uživatelskou dokumentací zařízení ARX CoSign v8.2 a DocuSign Signature Appliance v8.4. Dále bylo stejným Rozhodnutím povoleno I.CA vydávat kvalifikované certifikáty pro elektronické pečeti podle certifikační politiky vydávání kvalifikovaných certifikátů pro elektronické pečeti na dálku (algoritmus RSA), verze 1.00 (identifikátor 1.3.6.1.4.1.23624.10.1.38.1.0). Identifikátor této služby byl uveřejněn v důvěryhodném seznamu České republiky u služby „(78) I.CA – vydávání kvalifikovaných certifikátů“ společně s identifikátorem „QCQSCDManagedOnBehalf“ podle kap. 5.5.9.2.3 technických specifikací ETSI TS 119 612 v2.1.1. Důvěryhodný seznam je veden na https://tsl.gov.cz/publ/TSL_CZ.xtsl.

2.6. Povinnosti objednatele:

- a) umožnit přístup pracovníků zhotovitele do prostor objednatele v rozsahu, který je nezbytný pro provedení potřebných činností, které vyplývají z plnění předmětu díla a umožnit přístup k dalším souvisejícím prostředkům,
- b) poskytovat v dohodnutých termínech zhotoviteli informace a podklady, které potřebuje k řádné realizaci plnění díla podle této smlouvy, zejména pak poskytnout zhotoviteli technologickou infrastrukturu a součinnost v míře, kvalitě a termínech, které budou stanoveny a odsouhlaseny oběma stranami

pro příslušná plnění,

- c) zabezpečit dodržování platné **Politiky** služby vytváření kvalifikovaných elektronických pečetí na dálku. Veškeré změny a doplňky této **Politiky** jsou vůči objednateli účinné po podpisu dodatku k této **Smlouvě** podepsaného zástupci obou smluvních stran,
 - d) převzít bezvadné dílo ve smyslu této smlouvy a podepsat příslušné dokumenty v souladu s ustanoveními této smlouvy,
 - e) dodržovat provozní podmínky užívání prokazatelně dodané zhotovitelem a písemná doporučení zhotovitele,
 - f) realizovat příslušnou součinnost v rozsahu této smlouvy,
 - g) realizovat případnou další součinnost odsouhlasenou zástupci smluvních stran.
- 2.7. Pokud objednatel neposkytne zhotoviteli řádně a včas veškerou součinnost vyplývající z této smlouvy, má zhotovitel v takovém případě právo posunout termín předání dílčích prací, a to o dobu trvající maximálně počet dní, po které zhotovitel nemohl řádně smlouvu plnit.
- 2.8. Vyžaduje-li plnění závazků zhotovitele dle této smlouvy uskutečnění právních či jiných úkonů jménem objednatele, je objednatel povinen vystavit včas zhotoviteli písemně potřebnou plnou moc.
- 2.9. Objednatel je oprávněn schvalovat změny zaměstnanců zhotovitele podílejících se na díle, a to formou číslovaného dodatku smlouvy, prvotní seznam takových zaměstnanců je uveden ve čl. X. této smlouvy. Pro doplňování dodatků platí pravidla uvedená v čl. XIV. – Závěrečná ustanovení.
- 2.10. Objednatel je oprávněn při porušení nebo nedodržení bezpečnostních podmínek uvedených v odst. 1 až 4 tohoto článku uplatnit vůči zhotoviteli sankce podle čl. VIII – Smluvní sankce podle této smlouvy.
- 2.11. Zaměstnanci objednatele určení podle odst. 11 a 12 tohoto článku jsou uvedeni v čl. X. této smlouvy.
- 2.12. Zaměstnancem zhotovitele odpovědným za plnění bezpečnostních podmínek specifikovaných objednatelem je [REDACTED]
- 2.13. Zaměstnancem objednatele odpovědným za dohled plnění bezpečnostních podmínek uvedených v odst. 1 až 4 tohoto článku specifikovaných objednatelem a plněných zhotovitelem je [REDACTED]

III. Způsob plnění díla

- 3.1. Zhotovitel se zavazuje poskytovat službu I.CA RemoteSeal v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA (dostupností) 99,5 % za každý den a kapacitou až 30 vytvořených pečetí za každou minutu.
- 3.2. Zhotovitel poskytuje technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem této smlouvy prostřednictvím e-mailové adresy [REDACTED]
- 3.3. Zhotovitel zajišťuje provoz Hotline v rozsahu Po – Pá 8:00 – 17:00 hod. na kontaktech z odstavce 3.2. Provozní pohotovost služby v režimu 24/7 na telefonním čísle [REDACTED]

- 3.4. Zhotovitel se zavazuje zajišťovat právní a technickou aktuálnost komponenty pro zajištění komunikace se zhotovitelem, jakož i celou službu I.CA RemoteSeal, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
- 3.5. Zhotovitel se zavazuje poskytovat za účelem otestování nových verzí služby I.CA RemoteSeal před nasazením do ostrého provozu službu I.CA RemoteSeal v testovacím prostředí s funkcionalitou obdobnou službě I.CA RemoteSeal v ostrém prostředí, pro testovací prostředí platí SLA 95% a kapacita 5 vytvořených pečetí za minutu.

IV. Převzetí díla

- 4.1. Zhotovitel bude dílo předávat postupně, a to měsíčně na základě počtu vytvořených kvalifikovaných pečetí. Akceptace bude objednatelem potvrzena akceptačním protokolem dle vzoru v **Příloze č. 3**.

V. Místo a termín plnění díla

- 5.1. Místem plnění je sídlo objednatele, tj. Budějovická 7, 140 96 Praha 4, respektive sídlo podniku Státní pokladna Centrum sdílených služeb, s. p. (dále jen „SPCSS“) Na Vápence 915/14, 130 00 Praha 3, kde je umístěno záložní datové centrum objednatele.
- 5.2. Dílo bude plněno průběžně po celou dobu účinnosti smlouvy formou dílčích plnění. Parametry díla jsou stanoveny v čl. III.

VI. Cena díla

- 6.1. Smluvní strany se dohodly, že výše plnění za zhotovitelem dodané a objednatelem převzaté dílo za celou dobu trvání této smlouvy, resp. dobu platnosti této smlouvy, nepřekročí celkovou částku bez DPH 300.000,-Kč (slovy: tři sta tisíc korun českých), což je s 21% DPH celkem 363.000,-Kč (slovy: tři sta šedesát tři tisíc korun českých).
- 6.2. Cena za poskytování služby I.CA RemoteSeal, tj. za vytvoření kvalifikované elektronické pečeti, bude stanovena podle počtu vytvořených kvalifikovaných elektronických pečetí v daném kalendářním měsíci podle příslušného množstevního pásma následující tabulky, a to jako součin „Ceny v Kč za 1 ks pečetění bez DPH“ a počtu skutečně vytvořených kvalifikovaných elektronických pečetí v příslušném pásmu dle přiloženého rozpisu za kalendářní měsíc. K této ceně bude připočten paušální poplatek ve výši pro dané množstevní pásmo. K celkové ceně bude připočteno DPH podle aktuálně platných předpisů.

množstevní pásmo tj. počet pečetění od - do za měsíc	paušální poplatek Kč/měsíc bez DPH	Cena v Kč za 1 ks pečetění bez DPH
1 - 100	1 000	4,00
101 - 300	2 000	3,50
301 - 500	3 000	3,00
501 - 1.000	5 000	2,50
1.001 - 3.000	7 000	2,10
3.001 - 5.000	9 000	1,70
5.001 - 10.000	11 000	1,40
10.001 - 30.000	14 000	1,10
30.001 - 50.000	17 000	0,80

50.001 - 100.000	21 000	0,50
100.001 - 300.000	24 000	0,30
300.001 - 500.000	29 000	0,20
500.001 - 1.000.000	35 000	0,16
1.000.001 - 5.000.000	42 000	0,12
5.000.001 - 10.000.000	49 000	0,08

- 6.3. Celková cena z odstavce 6.1 je stanovena jako cena nejvýše přípustná a konečná. Cena za plnění díla zahrnuje veškeré související náklady zhotovitele, např. náklady na dopravu, pojištění, předání a záruční servis.
- 6.4. Celková cena byla stanovena na základě provedeného výběrového řízení čj. 20645/2020.

VII. Platební podmínky

- 7.1. Zhotovitel bude fakturovat cenu za dílo postupně, jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž zhotovitel vytvořil kvalifikované elektronické pečeti, a to podle počtu skutečně provedených a poskytnutých vytvořených pečeti, vždy do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby I.CA RemoteSeal.
- 7.2. Výpočet měsíční fakturované částky na základě počtu vytvořených kvalifikovaných pečeti je stanoven v čl. VI. odst. 6.2 této smlouvy.
- 7.3. Daňový doklad (faktura) musí obsahovat všechny náležitosti daňového dokladu podle § 435 OZ, podle § 7 zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů, podle zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů, a podle § 21 a § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a odkaz na tuto smlouvu, příslušné akceptační protokoly a identifikaci zástupce zhotovitele. Faktura včetně příslušných akceptačních protokolů musí být zaslána elektronicky – cestou datové schránky s následujícím parametrem: ID datové schránky „Generální ředitelství cel“: **7puaa4c**
- 7.4. Faktura musí obsahovat evidenční číslo této smlouvy a jako přílohu akceptační protokol dle vzoru v Příloze č. 3 podepsaný oprávněnými zástupci obou smluvních stran. Pokud faktura nebude obsahovat stanovené náležitosti dle této smlouvy, nebo v ní nebudou správně uvedené údaje, je objednatel oprávněn vrátit ji ve lhůtě 10 (slovy: deseti) pracovních dnů od jejího obdržení zhotoviteli s uvedením chybějících náležitostí nebo nesprávných údajů. V takovém případě bude faktura zhotovitelem opravena a nová lhůta splatnosti začne plynout doručením opravené faktury zpět objednateli. V případě, že objednatel fakturu vrátí, přestože faktura je správná a předepsané náležitosti obsahuje, zůstává v platnosti původní lhůta splatnosti faktury a pokud objednatel fakturu nezplatí v původním termínu splatnosti, je v prodlení.
- 7.5. Doba splatnosti faktury je sjednána na 30 (slovy: třicet) kalendářních dnů od data doručení faktury na adresu objednatele. Takto sjednaná doba splatnosti, není-li průkazně dohodnuto jinak, nahrazuje den splatnosti uvedený na faktuře. V případě, že poslední den splatnosti faktury připadne na den pracovního klidu, resp. volna, bude se za den splatnosti považovat nejbližší následující pracovní den.

- 7.6. Peněžní závazek objednatele se považuje za včas splněný dnem připsání příslušné částky ve prospěch účtu zhotovitele. Platba faktury bude provedena bezhotovostním převodem na bankovní účet zhotovitele, jenž je uvedený na faktuře.
- 7.7. Smluvní strany si dojednaly, že objednatel je oprávněn provést zajišťovací úhradu daně z přidané hodnoty ve smyslu ust. § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, na účet příslušného správce daně, jestliže se zhotovitel stane ke dni poskytnutí úplaty za uskutečněné zdanitelné plnění nespolehlivým plátcem daně ve smyslu ust. § 106a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

VIII. Smluvní sankce

- 8.1. V případě nedodržení parametru SLA dostupnosti služby I.CA RemoteSeal uvedeného v článku III. odstavci 3.1 této smlouvy, tj. pokud dostupnost služby klesne pod 99,5 % za každý kalendářní den či pod 30 vytvořených pečetí za každou minutu, je zhotovitel povinen uhradit objednateli smluvní pokutu ve výši 1.000,- Kč (slovy: jeden tisíc korun českých) za každých započatých 0,1%, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu, a smluvní pokutu ve výši 1000 Kč (slovy: jeden tisíc korun českých) za každý případ nedodržení parametru 30 podpisů za minutu.
- 8.2. V případě nesplnění povinností uvedených v článku III. odstavci 3.2 a 3.3 této smlouvy je zhotovitel povinen uhradit objednateli smluvní pokutu ve výši 1.000,- Kč (slovy: jeden tisíc korun českých) za každé takové porušení.
- 8.3. V případě nesplnění povinností uvedených v článku III. odstavci 3.4 této smlouvy je zhotovitel povinen uhradit objednateli smluvní pokutu ve výši 10.000,- Kč (slovy: deset tisíc korun českých) za každé takové porušení.
- 8.4. V případě porušení povinnosti mlčenlivosti dle článku IX. odst. 9.2. a 9.3. této smlouvy je druhá smluvní strana oprávněna požadovat zaplacení smluvní sankce ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každý jednotlivý případ porušení.
- 8.5. Ustanoveními o smluvní sankci není dotčeno právo objednatele na náhradu vzniklé škody. Smluvní sankce je splatná do 10 dnů ode dne doručení jejího vyúčtování zhotoviteli.
- 8.6. Smluvní sankci je objednatel oprávněn započíst proti pohledávce zhotovitele.
- 8.7. V případě, že objednatel bude v prodlení s jakoukoli platbou dle této smlouvy o více než 30 (slovy: třicet) dnů a nedoloží prokazatelně, že zpoždění spočívá v systémových překážkách objednatelem neovlivnitelných, je zhotovitel oprávněn žádat po objednateli zaplacení úroku z prodlení ve výši stanovené nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob. Smluvní strany výslovně sjednávají, že v takovém případě výše úroků odpovídá náhradě škody.
- 8.8. Výslovně se touto smlouvou sjednávají výše stanovené smluvní sankce. Smluvní strany si výslovně ujednaly, že k jiným než zde uvedeným a dále např. ústně sjednaným smluvním sankcím, jakož i k smluvním sankcím sjednaným dodatečně nebude přihlíženo.

8.9. Smluvní strany si výslovně ujednaly vyloučení aplikace ust. § 1806 OZ tzn. že úroky z úroků nelze požadovat.

IX. Omezení odpovědnosti zhotovitele, mlčenlivost

9.1. Zhotovitel neodpovídá za nemožnost plnit předmět této smlouvy a případnou škodu z toho vzniklou v případě, že objednatel:

- a) neposkytl zhotoviteli potřebnou součinnost a informace,
- b) ani po písemné výzvě zhotovitele nepředal zhotoviteli pravdivé a úplné podklady nebo poskytl zhotoviteli nevhodné podklady a tyto nedoplnil či nenahradil na základě oznámení dle čl. II. odst. 2.1. písm. d) vhodnými podklady,
- c) nerespektoval písemná doporučení a pokyny zhotovitele vydaná v souladu se zákonem.

9.2. Zhotovitel se zavazuje po celou dobu trvání této smlouvy, jakož i po jejím uplynutí respektovat a dodržovat mlčenlivost o skutečnostech dle čl. II. bod 2.1. písm. e) a písm. f).

9.3. V této souvislosti se zhotovitel zejména zavazuje:

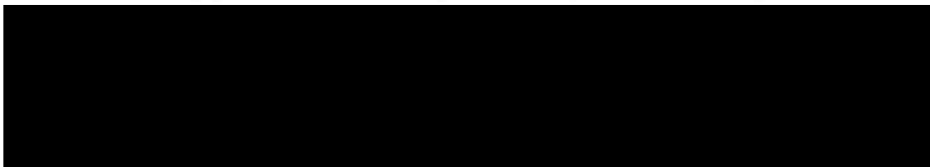
- a) nesdělít údaje, které objednatel označil jako důvěrné či neveřejné, ani jiné údaje, které se od objednatele při plnění této smlouvy dozvěděl, třetím osobám, s výjimkou osob uvedených v čl. X. odst. 10.1. této smlouvy,
- b) zajistit, aby uvedené údaje nebyly zpřístupněny třetím osobám, s výjimkou osob uvedených v čl. X. odst. 10.1. této smlouvy,
- c) zabezpečit listiny včetně fotokopií obsahující uvedené údaje před zneužitím třetími osobami.

9.4. Smluvní strany se zavazují, že obchodní a další údaje, s nimiž se při plnění závazků z této smlouvy seznámily, nezpřístupní třetím osobám, mimo osob uvedených v čl. X. odst. 10.1. této smlouvy, bez písemného souhlasu druhé smluvní strany.

9.5. Zhotovitel garantuje a nese odpovědnost za vytvoření kvalifikované elektronické pečeti pouze za předpokladu, že data nutná k vytvoření pečeti (odesílaná do prostředí zhotovitele), generovaná komponentou dodanou zhotovitelem, nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno.

X. Součinnost a komunikace smluvních stran

10.1. Při plnění této smlouvy jsou na straně objednatele pověřeni rolí **oprávněné osoby**:



Tyto oprávněné osoby budou vyvíjet součinnost se zhotovitelem při plnění předmětu smlouvy, a to ve věcech smluvních (s právem předávat zhotoviteli všechny informace potřebné pro plnění smluvního závazku zhotovitele, o které ke splnění závazků v souladu s touto smlouvou požádá, a přebírat od něho všechna plnění uskutečněná dle této smlouvy).

10.2. Při plnění této smlouvy jsou na straně zhotovitele pověřeni rolí **oprávněné osoby**:



Tyto oprávněné osoby budou vyvíjet součinnost s objednatelům při plnění předmětu smlouvy, a to ve věcech smluvních (s právem přebírat všechny informace potřebné pro plnění tohoto smluvního závazku od objednatele, o které ke splnění závazků v souladu s touto smlouvou požádá a předávat mu všechna plnění uskutečněná dle této smlouvy).

XI. Platnost a účinnost smlouvy

- 11.1. Smlouva se uzavírá na dobu určitou do 31. 5. 2021.
- 11.2. Tato smlouva nabývá platnosti podpisem statutárních zástupců obou smluvních stran a účinnosti dnem zveřejnění v registru smluv, nejdříve však dne 1. 6. 2020.
- 11.3. Tuto smlouvu je možno ukončit písemnou dohodou obou smluvních stran.
- 11.4. Shledá-li objednatel nebo zhotovitel podstatné porušení plnění předmětu smlouvy druhou stranou, má právo na okamžité odstoupení od smlouvy, jehož písemné vyhotovení musí být druhé straně doručeno.
- 11.5. Za podstatné porušení smlouvy ze strany objednatele se zejména považuje, pokud objednatel:
 - a) nevystaví pro zhotovitele plnou moc dle čl. II odst. 2.8 této smlouvy,
 - b) bude v prodlení s úhradou ceny déle než 30 dní,
 - c) poruší obchodní tajemství nebo jiný závazek mlčenlivosti dle této smlouvy.
- 11.6. Za podstatné porušení smlouvy ze strany zhotovitele se zejména považuje, pokud zhotovitel:
 - a) opakovaně nesplní některou z povinností dle této smlouvy,
 - b) poruší obchodní tajemství nebo jiný závazek mlčenlivosti dle této smlouvy,
 - c) uvedl ve svém prohlášení učiněném v odst. 2.5. této smlouvy nepravdivé skutečnosti nebo stane-li se toto prohlášení nepravdivým kdykoliv v době účinnosti této smlouvy.
- 11.7. Odstoupení od smlouvy je platné dnem doručení oznámení o odstoupení. Strana, kvůli jejímuž porušení smlouvy došlo k odstoupení od smlouvy, je povinna zaplatit odstupující straně na základě faktury vystavené odstupující stranou do 14 (slovy: čtrnácti) dnů ode dne doručení takové faktury veškeré náklady odstupující strany jakožto přímý důsledek odstoupení od smlouvy.
- 11.8. Strany souhlasí s tím, že v případě předčasného ukončení účinnosti této smlouvy z jakýchkoliv důvodů bude dokončeno plnění dle v okamžiku předčasného ukončení této smlouvy schválených požadavků za podmínek uvedených v této smlouvě.
- 11.9. Ustanovení článků této smlouvy, jejichž cílem je upravit vztahy mezi smluvními stranami po ukončení účinnosti této smlouvy, zůstanou platná i po ukončení této smlouvy.

XII. Zvláštní ujednání

- 12.1. Žádná ze smluvních stran není odpovědná za škodu způsobenou okolnostmi vylučujícími odpovědnost ve smyslu § 2913 odst. 2 OZ.
- 12.2. Objednatel souhlasí s tím, že zhotovitel má právo zmiňovat tuto smlouvu jako referenci vůči třetím stranám, avšak při dodržení závazků mlčenlivosti dle této smlouvy.
- 12.3. Zhotovitel výslovně prohlašuje, že je v plném rozsahu pojištěn minimálně do výše 10 mil. Kč pro případ škody způsobené porušením závazků zhotovitele dle této smlouvy. Tuto pojistnou ochranu se zhotovitel zavazuje udržovat po celou dobu možnosti trvání této smlouvy.
- 12.4. Zhotovitel souhlasí s tím, že obsah této smlouvy není obchodním tajemstvím a objednatel jej může zveřejnit, zejména v rozsahu a za podmínek vyplývajících ze zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. V souladu se zákonem č. 340/2015 Sb., o registru smluv, se strany dohodly, že objednatel zašle tuto smlouvu správci registru smluv k uveřejnění ve lhůtě stanovené tímto zákonem. Osobní údaje stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.
- 12.5. Zhotovitel je povinen poskytnout objednateli veškeré doklady související s realizací projektu a plněním závazných ukazatelů v rámci předmětu činnosti zhotovitele, které si vyžádají příslušné kontrolní orgány, zejména příslušný finanční úřad, Ministerstvo financí ČR, Nejvyšší kontrolní úřad.

XIII. Okolnosti vylučující odpovědnost

- 13.1. Pro účely této smlouvy „okolnosti vylučující odpovědnost“ znamenají událost, vymezenou v § 2913 odst. 2 OZ.
- 13.2. Jestliže vznikne situace zaviněná okolnostmi vylučujícími odpovědnost, dotčená strana okamžitě uvědomí druhou smluvní stranu písemně o takových podmínkách a jejich příčině. Pokud není jinak stanoveno písemně ze strany dotčené, bude druhá smluvní strana pokračovat v realizaci svých závazků podle smlouvy tak, jak je to možné a bude hledat veškeré rozumné alternativní prostředky pro realizaci části, kde nebrání okolnosti vylučující odpovědnost.
- 13.3. Žádná ze smluvních stran nebude odpovídat za nesplnění kteréhokoliv ze svých smluvních závazků dle této smlouvy či jejich dodatků v důsledku okolností vylučujících odpovědnost. Platební závazky vzniklé před okolností vylučující odpovědnost nebudou okolností vylučující odpovědnost prominuty. Žádná ze smluvních stran není oprávněna požadovat zaplacení smluvní sankce druhou smluvní stranou za porušení povinností z této smlouvy okolnostmi vylučujícími odpovědnost.
- 13.4. Trvají-li okolnosti vylučující odpovědnost déle než 3 (slovy: tři) měsíce, smluvní strany mohou odstoupit od smlouvy písemně s účinností ke dni doručení odstoupení druhé smluvní straně.
- 13.5. Smluvní strany si výslovně ujednaly vyloučení aplikace ust. § 2914 OZ.

XIV. Závěrečná ujednání

- 14.1. Veškeré právní jednání směřující ke změně i části této smlouvy, jakož i k jejímu zrušení, musí mít formu vzestupně číslovaných písemných dodatků, schválených

statutárními zástupci smluvních stran. Dodatek se po schválení stává nedílnou součástí této smlouvy.

- 14.2. Stanou-li se některá ustanovení této smlouvy zcela nebo zčásti neplatná nebo pokud by některá ustanovení chyběla, není tím dotčena platnost zbývajících ustanovení. Místo neplatného ustanovení platí jako dohodnuté takové ustanovení, které odpovídá smyslu a účelu neplatného ustanovení. Schází-li ustanovení zcela, platí za dohodnuté takové ustanovení, které odpovídá tomu, co by podle smyslu a účelu této Smlouvy bylo ujednáno, kdyby tato skutečnost byla známa od počátku. Totéž platí, vyskytnou-li se ve smlouvě či jejích dodatcích případné mezery.
- 14.3. Tato smlouva a veškeré záležitosti z ní vyplývající nebo s ní související se řídí právním řádem České republiky a spadá pod jurisdikci soudů České republiky. Smluvní strany se zavazují, že případné rozpory vzniklé při realizaci této smlouvy budou řešit korektním způsobem a v souladu s právními předpisy a pravidly slušnosti. Každá ze smluvních stran se dále zavazuje, že k soudnímu řešení uvedených sporů přistoupí až po vyčerpání možností jejich vyřízení mimosoudní cestou.
- 14.4. Smluvní strany podle § 89a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů určují jako místně příslušný soud Obvodní soud pro Prahu 1; v případě, že podle procesních předpisů je k rozhodování věci v prvním stupni příslušný krajský soud, určují smluvní strany jako místně příslušný soud Městský soud v Praze.
- 14.5. Pokud se jedna ze smluvních stran vzdá určitého nároku na nápravu v případě porušení nebo nedodržení ustanovení této smlouvy ze strany druhé smluvní strany nebo se zdrží či opomene uplatnit či využít kteréhokoli práva nebo výsady, jež jí podle této smlouvy náleží nebo náležet může, nesmí být takový úkon, a to bez výjimky, považován nebo uplatňován jako precedens do budoucna pro jakýkoli další případ, ani nelze považovat takové jednání za vzdání se jakéhokoli nároku, práva či výsady jednou pro vždy.
- 14.6. Zhotovitel výslovně souhlasí s tím, že objednatel tuto smlouvu uveřejní na svém profilu v plném znění v souladu se ZZVZ.
- 14.7. Smluvní strany si ujednaly, že závazky vyplývající z této smlouvy se promlčují ve lhůtě deset let ode dne, kdy smluvní strana mohla poprvé toto právo uplatnit.
- 14.8. Smluvní strany si výslovně ujednaly, že tuto smlouvu nelze postoupit na řad. Žádná ze smluvních stran není oprávněna vtělit jakékoliv právo plynoucí jí ze smlouvy nebo z jejího porušení do podoby cenného papíru.
- 14.9. Smluvní strany prohlašují, že si tuto smlouvu přečetly, že byla uzavřena po vzájemném projednání. Autentičnost této smlouvy potvrzují svým podpisem.
- 14.10. Tato smlouva je vyhotovena ve čtyřech stejnopisech s platností originálu, z nichž každá smluvní strana obdrží po dvou vyhotoveních.
- 14.11. Přílohy jsou nedílnou součástí této smlouvy. V případě rozporu mezi touto smlouvou a jejími přílohami platí smlouva.

14.12. Tato smlouva obsahuje následující přílohy:

Příloha č. 1 „I.CA RemoteSeal - Služba vytváření kvalifikovaných elektronických pečetí na dálku“

Příloha č. 2 „Politika_PecetNaDalku_1v00“

Příloha č. 3 „Akceptační protokol“ – vzor

14.13. Smluvní strany na důkaz svého souhlasu připojují své podpisy.

za zhotovitele

za objednatele

V Praze dne:

V Praze dne:

**Petr
Budiš**

Digitálně podepsal
Petr Budiš
Datum: 2020.05.04
11:00:30 +02'00'

Podpis: _____

Jméno : Ing. Petr Budiš, Ph.D.

Funkce : předseda představenstva

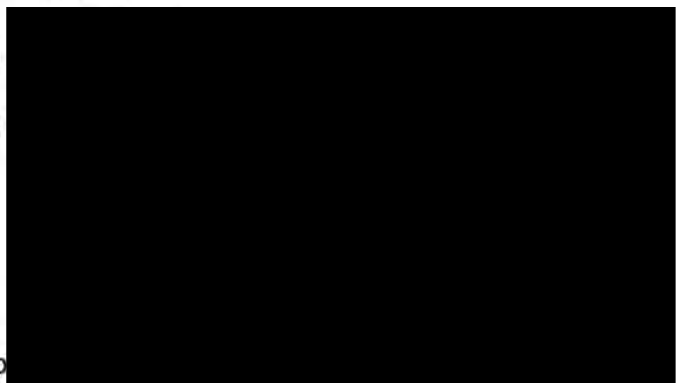
**Ing. Roman
Kučera**

Digitálně podepsal
Ing. Roman Kučera
Datum: 2020.05.04
10:59:21 +02'00'

Podpis: _____

Jméno : Ing. Roman Kučera

Funkce : člen představenstva



Služba vytváření kvalifikovaných elektronických pečeti na dálku I.CA RemoteSeal

Východisko služby

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), konkrétně bod 52 recitálu, články 29 a 39, body 3 a 4 Přílohy II a Příloha III.

Právní základ

Povinnost používat kvalifikované elektronické pečeti orgány veřejné moci počínaje 20.9.2018 je dána § 8 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce: „Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečetí.“

Kvalifikovaná elektronická pečeť dle bodu 27) článku 3 nařízení eIDAS:

„Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečeti a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.“

Požadavky na kvalifikované prostředky pro vytváření elektronických pečeti (QSealCD):

- prostřednictvím „mutatis mutandis“ stanoveny v příloze II. nařízení eIDAS
- jedná se o stejné požadavky jako na kvalifikované prostředky pro vytváření elektronických podpisů
- stejné funkční požadavky jako pro SSCD prostředky dle směrnice 1999/93/ES pro ty prostředky, které jsou v držení osoby
- v případě prostředků pro vytváření kvalifikovaných elektronických pečeti na dálku dodatečné požadavky na kvalifikované poskytovatele (odst. 3 a 4 přílohy II. nařízení eIDAS).

Prostředky pro vytváření kvalifikovaných elektronických pečeti musí být uvedeny na seznamu vedeném Evropskou komisí:

„Compilation of Member States notification on SSCDs and QSCDs“

<https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>

- Seznam je spravován Evropskou komisí
- Komise figuruje pouze v roli editora seznamu
- Mohou přispívat pouze ty členské státy, které měly nebo mají nahlášeny certifikační orgány
- Je na zodpovědnosti členských států nahlášovat prostředky Komisi a případné změny jejich certifikace
- Seznam nemá konstitutivní hodnotu, jedná se pouze o informativní seznam.

Existují dva typy QSealCD:

1. QSealCD v držení pečetící osoby (pokud jsou data pro vytváření elektronických pečeti uchovávána v prostředí spravovaném zcela, nikoli však nutně výhradně uživatelem).
2. QSealCD na dálku (pokud data pro vytváření elektronických pečeti spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru jménem pečetící osoby).

Služba I.CA RemoteSeal představuje variantu 2. Na HSM modulu v prostředí I.CA leží privátní klíč pečetícího certifikátu k jehož použití se využije autentizační certifikát vydaný danému klientovi. V prostředí klienta je instalována komponenta, která zasílá do prostředí I.CA požadavky na opečetění (hash dat, nikoli obsah dokumentu) a zpět jsou vrácena data, jež komponenta použije pro vytvoření opečetěného dokumentu.

Příloha č. 1

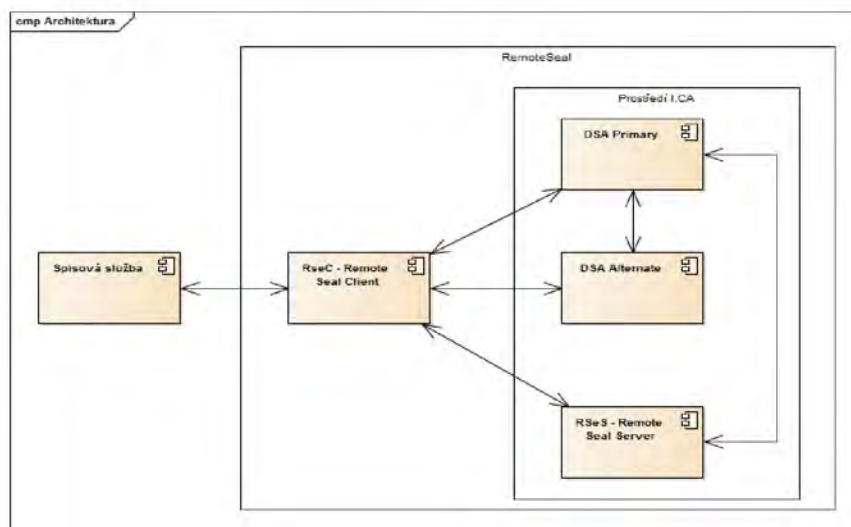
Realizace služby I.CA RemoteSeal je založena na zařízení:

- ARX (Algorithmic Research) CoSign v8.2
- Společnost ARX koupena v roce 2015 společností DocuSign
- Produkt nadále prodáván pod názvem DocuSign Signature Appliance v8.2

List of QSCDs	
Name:	-
Name:	ARX CoSign v8.2
Applicant	ARX (Algorithmic Research, Ltd.)
Qualified Signature Creation Device (QSigCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSigCD designation by	OCSI
QSigCD designation date	07.02.2017
QSigCD designation expiry	-
QSigCD designation report reference	OCSI/ACC/ARX/01/2017/RA
QSigCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/arn/ac_rda_eidas_cosign_82_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/IMQ/05/2016/RC
CC certification body	-
CC certification date	12.09.2016
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/arn/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/arn/st_arx_cosign_82_v2.6.pdf
Conformity Protection Profile	-
Evaluation criteria and version	-
Evaluation level	-
Developers	-
Qualified Seal Creation Device (QSealCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSealCD designation by	OCSI
QSealCD designation date	07.02.2017
QSealCD designation expiry	-
QSealCD designation report reference	OCSI/ACC/ARX/01/2017/RA
QSealCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/arn/ac_rda_eidas_cosign_82_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/IMQ/05/2016/RC
CC certification body	-
CC certification date	12.09.2016
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/arn/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/arn/st_arx_cosign_82_v2.6.pdf



Architektura služby



Příloha č.1

- **RSeC** – RemoteSeal Client – klientská komponenta určená pro integraci do volající aplikace, typicky do spisové služby.
- **RSeS** – RemoteSeal Server – základní aplikační server provozovaný I.CA, který realizuje první vrstvu autentizace volající aplikace a udržuje evidenci provedených transakcí (opečetění).
- DSA Primary - DocuSign Signature Appliance Primary - primární HSM modul, který drží privátní klíče uživatelů a podepisuje
- DSA Alternate - DocuSign Signature Appliance Alternate - záložní HSM modul, který udržuje repliku databáze privátních klíčů a v případě výpadku primárního HSM zastoupí primární HSM pro podepisování
- **RSeActivationUtil** – Aktivační utilita sloužící k aktivaci RSeC pomocí tzv. aktivační karty.

RemoteSeal Client

- Klientská komponenta sloužící k zadávání transakcí (požadavků na opečetění dat) do systému RemoteSeal.
- Nativní C++ jádro
- Distribuováno ve formě:
 - JAR pro Java
 - .NET assembly pro .NET
 - V případě zájmu možno volat přímo nativní jádro.

Postup zřízení služby

Předpokladem zřízení služby je uzavření smlouvy mezi I.CA a klientem.

Zřízení služby bude probíhat na vybraných pobočkách RA následujícím způsobem:

- Klient navštíví pobočku RA, kde operátor vydá na aktivační čipovou kartu autentizační komerční certifikát, vygeneruje párová data pečetičního certifikátu na HSM modulu a vydá pečetiční certifikát
- Pečetiční certifikát:
 - CA pošle na mailovou adresu uživatele.
 - ICARA uloží na aktivační kartu uživatele.
- Klient odchází z RA s aktivační kartou.

Aktivace RSeC



- Pro aktivaci RSeC spustí uživatel (např.: oprávněná osoba úřadu) dodávanou GUI utilitu RSeActivationUtil (dále jen utilita)

Příloha č.1

- Utilita vyzve uživatele k vložení aktivační karty
- Následně utilita vytvoří aktivační soubor a uživatel tento aktivační soubor následně načte do spisové služby (obecně do aplikace volající RSeC), která jej bude pro použití RemoteSeal předávat do RSeC.

Technické parametry RSeActivationUtil

- Jednoduchá Windows GUI utilita.
- Nemusí být spouštěna na stejném PC, na kterém je provozován RSeC.
- Vyžaduje: .NET 4.0

Opečetění dokumentu

- Proces opečetění dokumentu inicializuje spisová služba (obecně volající aplikace), která má integrovanou knihovnu RSeC.
- Spisová služba předá do RSeC dokument k opečetění spolu s nastavením pečetění (viditelný/neviditelný podpis, formát, přidání TS, atp.) + aktivační soubor vzniklý při aktivaci RSeC
- RSeC připraví dokument k podpisu: sestaví žádost o opečetění (obsahující číslo jednací dokumentu (obecně jednoznačný textový identifikátor), parametry podpisu, hash původního dokumentu a hash který bude vstupem pro výpočet kryptogramu)
- Následně RSeC naváže oboustraně autentizovaný TLS kanál pro komunikaci s RSeS, předá podepsanou žádost o opečetění na RSeS
- Na DSA k vytvoření kryptogramu pomocí privátního klíče pečetícího certifikátu
- RSeC využije kryptogram pro kompletaci podepsaného dokumentu
- Hotový opečetěný dokument je vrácen spisové službě.

Automatické prodloužení služby

- Součástí RSeC je funkcionality automatické obnovy autentizačního certifikátu, která probíhá zcela automaticky. Proces inicializuje RSeC a vydaný certifikát je do něj následně uložen.

Obnova pečetícího certifikátu

- V rámci automatického prodloužení služby bude také probíhat automatická obnova pečetícího certifikátu
- RSeC s určitým předstihem před vypršením platnosti certifikátu vygeneruje na DSA nový pár klíčů a vytvoří žádost o vydání následného certifikátu, kterou opečetí původním certifikátem
- Žádost o následný certifikát se zpracuje standardní cestou
- RSeC následně uloží do DSA následný certifikát a od toho okamžiku jej začne pro pečetění využívat.

Technické normy

Pro systémy vzdáleného podepisování existuje standard CEN/TS 419241 z roku 2014, bude nahrazen normou (nyní v draftu) prEN 419241.

Podporované formáty podpisu:

- CAdES-B-B, CAdES-B-T
 - Dle normy EN 319 122, ve variantách:
 - Interní
 - Externí

Příloha č.1

- PAdES-B-B, PAdES-B-T
 - Dle normy EN 319 142, ve variantách:
 - Neviditelný
 - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
- XAdES-B a XAdES-T
 - dle normy ETSI TS 103 171, a to ve variantě enveloped, přičemž:
 - Na vstupu bude XML dokument, který bude kompletně použit jakožto vstup podepisovaných data.
 - Na vstupu bude určeno ID elementu, do nějž bude jakožto poslední child element přidán element Signature obsahující nově vytvořenou kvalifikovanou elektronickou pečeť.
 - Na vstupu bude definice požadovaných transformací , digest metody a mime-type referencovaných dat pro element Reference s id="xadesReference".
 - Na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512)
 - Na vstupu bude možnost volby podpisu typu XAdES-B/XAdES-T tedy bez nebo s časovým razítkem.

Podpisovaná data nikdy neopouští volající systém/prostředí klienta (komponentu RSeC)!

První certifikační autorita, a.s.



Politika

služby vytváření kvalifikovaných elektronických pečetí
na dálku

Politika služby vytváření kvalifikovaných elektronických pečetí na dálku je veřejným dokumentem, který je vlastnictvím společnosti První certifikační autorita, a.s., a byl vypracován jako nedílná součást komplexní bezpečnostní dokumentace. Žádná část tohoto dokumentu nesmí být kopírována bez písemného souhlasu majitele autorských práv.

Verze 1.00

OBSAH

1	Úvod	7
1.1	Přehled	7
1.2	Název a jednoznačné určení dokumentu.....	8
1.3	Participující subjekty	8
1.3.1	Poskytovatel služeb.....	8
1.3.2	Kontaktní místa	8
1.3.3	Spoléhající se strany	8
1.3.4	Jiné participující subjekty.....	8
1.4	Použití služby.....	9
1.4.1	Přípustné použití služby.....	9
1.4.2	Omezení použití služby	9
1.5	Správa politiky.....	9
1.5.1	Organizace spravující politiku nebo prováděcí směrnici.....	9
1.5.2	Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici.....	9
1.5.3	Osoba rozhodující o souladu prováděcí směrnice s politikou služby.....	9
1.5.4	Postupy při schvalování prováděcí směrnice	9
1.6	Přehled použitých pojmů a zkratk.....	9
2	Odpovědnost za zveřejňování a úložiště informací a dokumentace.....	12
2.1	Úložiště informací a dokumentace.....	12
2.2	Zveřejňování informací a dokumentace.....	12
2.3	Periodicita zveřejňování informací.....	12
2.4	Řízení přístupu k jednotlivým typům úložišť	12
3	Identifikace a autentizace ke službě	13
3.1	Počáteční ověření identity	13
3.1.1	Ověřování identity právnické osoby	13
3.1.2	Pověřené osoby	13
3.1.3	Ověřování identity fyzické osoby	13
3.2	Ověření identity při prodloužení služby.....	14
3.3	Změna údajů	14
4	Požadavky na životní cyklus služby.....	15
4.1	Uzavření smlouvy a zřízení služby	15
4.1.1	Proces uzavření smlouvy a odpovědnosti.....	15
4.1.2	Povinnosti Klienta	15

4.1.3	Povinnosti Osoby.....	15
4.1.4	Zřízení služby	16
4.2	Aktivace Služby.....	16
4.3	Tvorba kvalifikované elektronické pečete	16
4.4	Automatické prodloužení služby.....	16
4.5	Účtování provedených operací.....	16
5	Postupy správy, řízení a provozu	17
5.1	Fyzická bezpečnost.....	17
5.1.1	Umístění a konstrukce.....	17
5.1.2	Fyzický přístup	17
5.1.3	Elektřina a klimatizace.....	17
5.1.4	Vlivy vody	17
5.1.5	Protipožární opatření a ochrana	17
5.1.6	Ukládání médií	18
5.1.7	Nakládání s odpady.....	18
5.1.8	Zálohy mimo budovu	18
5.2	Procesní bezpečnost.....	18
5.2.1	Důvěryhodné role	18
5.2.2	Počet osob požadovaných na zajištění jednotlivých činností	18
5.2.3	Identifikace a autentizace pro každou roli	19
5.2.4	Role vyžadující rozdělení povinností.....	19
5.3	Personální bezpečnost.....	19
5.3.1	Požadavky na kvalifikaci, zkušenosti a bezúhonnost.....	19
5.3.2	Posouzení spolehlivosti osob	19
5.3.3	Požadavky na školení.....	20
5.3.4	Požadavky a periodičita doškolování.....	20
5.3.5	Periodičita a posloupnost rotace pracovníků mezi různými rolemi	20
5.3.6	Postihy za neoprávněné činnosti zaměstnanců	20
5.3.7	Požadavky na nezávislé dodavatele	20
5.3.8	Dokumentace poskytovaná zaměstnancům.....	20
5.4	Postupy zpracování auditních záznamů	21
5.4.1	Typy zaznamenávaných událostí.....	21
5.4.2	Periodičita zpracování záznamů	21
5.4.3	Doba uchování auditních záznamů.....	21
5.4.4	Ochrana auditních záznamů.....	21
5.4.5	Postupy pro zálohování auditních záznamů.....	21

5.4.6	System shromažďování auditních záznamů (interní nebo externí).....	21
5.4.7	Postup při oznamování události subjektu, který ji způsobil.....	22
5.4.8	Hodnocení zranitelnosti	22
5.5	Uchovávání záznamů.....	22
5.5.1	Typy uchovávaných záznamů.....	22
5.5.2	Doba uchování záznamů	22
5.5.3	Ochrana úložiště záznamů	22
5.5.4	Postupy při zálohování záznamů	22
5.5.5	Požadavky na používání časových razítek při uchovávání záznamů.....	22
5.5.6	System shromažďování uchovávaných záznamů (interní nebo externí)	23
5.5.7	Postupy pro získání a ověření uchovávaných informací	23
5.6	Obnova po havárii nebo kompromitaci	23
5.6.1	Postup ošetření incidentu nebo kompromitace	23
5.6.2	Poškození výpočetních prostředků, softwaru nebo dat	23
5.6.3	Schopnost obnovit činnost po havárii.....	23
5.7	Ukončení činnosti poskytovatele služeb	23
6	Řízení technické bezpečnosti.....	25
6.1	Počítačová bezpečnost	25
6.1.1	Specifické technické požadavky na počítačovou bezpečnost	25
6.1.2	Hodnocení počítačové bezpečnosti	25
6.2	Technické řízení životního cyklu.....	26
6.2.1	Řízení vývoje systému pro poskytování služby.....	26
6.2.2	Řízení správy bezpečnosti.....	26
6.2.3	Řízení bezpečnosti životního cyklu.....	26
6.3	Řízení bezpečnosti sítě	26
6.4	Ochrana proti padělání a odcizení dat.....	27
7	Hodnocení shody a jiná hodnocení	28
7.1	Periodicita hodnocení nebo okolnosti pro provedení hodnocení.....	28
7.2	Identita a kvalifikace hodnotitele.....	28
7.3	Vztah hodnotitele k hodnocenému subjektu	28
7.4	Hodnocené oblasti	28
7.5	Postup v případě zjištění nedostatků.....	28
7.6	Sdělování výsledků hodnocení.....	28
8	Ostatní obchodní a právní záležitosti.....	30
8.1	Poplatky	30

8.1.1	Poplatky za využívání služby	30
8.1.2	Poplatky za další služby	30
8.1.3	Postup při refundování.....	30
8.2	Finanční odpovědnost	30
8.2.1	Krytí pojištěním.....	30
8.2.2	Další aktiva.....	30
8.2.3	Pojištění nebo krytí zárukou pro koncové uživatele	30
8.3	Důvěrnost obchodních informací.....	31
8.3.1	Rozsah důvěrných informací	31
8.3.2	Informace mimo rámec důvěrných informací	31
8.3.3	Odpovědnost za ochranu důvěrných informací.....	31
8.4	Ochrana osobních údajů	31
8.4.1	Politika ochrany osobních údajů	31
8.4.2	Informace považované za osobní údaje	31
8.4.3	Informace nepovažované za osobní údaje.....	31
8.4.4	Odpovědnost za ochranu osobních údajů.....	32
8.4.5	Oznámení o používání osobních údajů a souhlas s jejich zpracováním	32
8.4.6	Poskytování osobních údajů pro soudní či správní účely	32
8.4.7	Jiné okolnosti zpřístupňování osobních údajů.....	32
8.5	Práva duševního vlastnictví.....	32
8.6	Zastupování a záruky	32
8.6.1	Zastupování a záruky I.CA	32
8.6.2	Zastupování a záruky ostatních zúčastněných subjektů	32
8.7	Zřeknutí se záruk	32
8.8	Omezení odpovědnosti	33
8.9	Záruky a odškodnění.....	33
8.10	Doba platnosti, ukončení platnosti.....	34
8.10.1	Doba platnosti	34
8.10.2	Ukončení platnosti	34
8.10.3	Důsledky ukončení a přetrvání závazků	34
8.11	Individuální upozorňování a komunikace se zúčastněnými subjekty.....	34
8.12	Novelizace	34
8.12.1	Postup při novelizaci.....	34
8.12.2	Postup a periodicita oznamování.....	34
8.12.3	Okolnosti, při kterých musí být změněn OID	34

8.13	Ustanovení o řešení sporů	34
8.14	Rozhodné právo.....	35
8.15	Shoda s právními předpisy	35
8.16	Další ustanovení	35
8.16.1	Rámcová dohoda	35
8.16.2	Postoupení práv	35
8.16.3	Oddělitelnost ustanovení	35
8.16.4	Zřeknutí se práv.....	35
8.16.5	Vyšší moc.....	35
8.17	Další opatření.....	35
9	Závěrečná ustanovení.....	36

tab. 1 - Vývoj dokumentu

Verze	Datum vydání	Schválil	Poznámka
1.00	19.06.2018	Ředitel společnosti První certifikační autorita, a.s.	První vydání.

1 ÚVOD

Tento dokument stanoví zásady, které První certifikační autorita, a.s., (dále též I.CA) uplatňuje v souladu s platnými právními předpisy a mezinárodně uznávanými technickými normami při zajištění služby vytváření kvalifikovaných elektronických pečetí na dálku (dále též Služba).

Pozn.: Pokud jsou v dalším textu uváděny odkazy na standardy nebo zákony, jedná se vždy buď o uvedený standard nebo zákon, resp. standard či zákon, který ho nahrazuje. Pokud by byla tato politika v rozporu se standardy nebo zákony, které nahradí dosud platné, bude vydána její nová verze.

Zákonné požadavky na Službu jsou definovány:

- nařízením 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),
- legislativou týkající se ochrany osobních údajů, v souladu se směrnicí č. 95/46/ES, resp. s nařízením Evropského parlamentu a Rady (EU) 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, po nabytí jeho platnosti 25.5.2018).

Služba společnosti První certifikační autorita, a.s., zajišťující vytváření kvalifikovaných elektronických pečetí na dálku je poskytována právníckým osobám (dále též Klient) na základě uzavřeného smluvního vztahu. I.CA dále nijak neomezuje potenciální Klienty, poskytování služby je nediskriminační, včetně jejího zpřístupnění pro osoby se zdravotním postižením.

1.1 Přehled

Dokument **Politika služby vytváření kvalifikovaných elektronických pečetí na dálku** (dále též Politika) vypracovaný společností První certifikační autorita, a. s., se zabývá skutečnostmi, vztahujícími se ke Službě s přihlédnutím k platným standardům Evropské unie a k právu České republiky v dané oblasti. Dokument je rozdělen do devíti kapitol, jejichž stručný popis je uveden v následujícím seznamu:

- Kapitola 1 identifikuje tento dokument, obecně popisuje subjekty, které participují na poskytování Služby a definuje přípustné využití Služby.
- Kapitola 2 popisuje problematiku odpovědností za zveřejňování informací, resp. dokumentace.
- Kapitola 3 popisuje procesy identifikace a autentizace ke Službě.
- Kapitola 4 definuje procesy životního cyklu Služby, technické parametry, až po ukončení poskytování služby.
- Kapitola 5 zahrnuje problematiku fyzické, procesní a personální bezpečnosti, včetně definování množiny zaznamenávaných událostí, uchovávání těchto záznamů a reakce po haváriích nebo kompromitaci.
- Kapitola 6 je zaměřena na technickou bezpečnost včetně počítačové a síťové ochrany.
- Kapitola 7 je zaměřena na problematiku hodnocení poskytované Služby.
- Kapitola 8 zahrnuje problematiku obchodní a právní, včetně ochrany osobních údajů.

- Kapitola 9 obsahuje závěrečná ustanovení.

Bližší podrobnosti o Službě poskytované podle této Politiky mohou být uvedeny v odpovídající Prováděcí směrnici služby vytváření kvalifikovaných elektronických pečetí na dálku (dále též Směrnice).

1.2 Název a jednoznačné určení dokumentu

Název a identifikace dokumentu: Politika služby vytváření kvalifikovaných elektronických pečetí na dálku, verze 1.00

OID politiky: není přiřazeno

1.3 Participující subjekty

1.3.1 Poskytovatel služeb

Společnost První certifikační autorita, a.s., jako kvalifikovaný poskytovatel služeb vytvářejících důvěru.

1.3.2 Kontaktní místa

Kontaktními místy jsou určené registrační autority I.CA (nikoli všechny registrační autority), kde je na základě smlouvy o poskytování Služby mezi I.CA a Klientem osobě zastupující Klienta (dále též Osoba) vydán jednak prvotní autentizační komerční certifikát na aktivací kartu/token a dále vygenerována párová data a zprostředkováno vydání pečeti certifikátu Klienta. Dále kontaktní místa:

- Poskytují potřebné informace, přijímají reklamace atd.
- Jsou oprávněna z naléhavých provozních nebo technických důvodů pozastavit zcela nebo zčásti výkon své činnosti.

1.3.3 Spoléhající se strany

Spoléhající se stranou je subjekt, který se spoléhá na kvalifikovanou elektronickou pečeť vytvořenou Klientem v rámci Služby.

1.3.4 Jiné participující subjekty

Jinými participujícími subjekty jsou orgány činné v trestním řízení, případně orgány dohledu a další, kterým to podle platné legislativy přísluší.

1.4 Použití služby

1.4.1 Přípustné použití služby

Službu provozovanou podle této Politiky lze využívat v procesech vytváření kvalifikované elektronické pečeti v souladu s platnou legislativou.

1.4.2 Omezení použití služby

Služba provozovaná podle této Politiky nesmí být používána v rozporu s přípustným použitím popsáním v kapitole 1.4.1 a dále pro jakékoliv nelegální účely.

1.5 Správa politiky

1.5.1 Organizace spravující politiku nebo prováděcí směrnici

Tuto Politiku, resp. jí odpovídající Směrnici, spravuje společnost První certifikační autorita, a.s.

1.5.2 Kontaktní osoba organizace spravující politiku nebo prováděcí směrnici

Kontaktní osoba společnosti První certifikační autorita, a.s., v souvislosti s touto Politikou, resp. s odpovídající Směrnicí, je uvedena na internetové adrese (viz kapitola 2.2).

1.5.3 Osoba rozhodující o souladu prováděcí směrnice s politikou služby

Jedinou osobou, která je odpovědná za rozhodování o souladu postupů společnosti První certifikační autorita, a.s., uvedených ve Směrnici s touto Politikou, je ředitel společnosti První certifikační autorita, a.s.

1.5.4 Postupy při schvalování prováděcí směrnice

Pokud je potřebné provést změny v příslušné Směrnici a vytvořit její novou verzi, určuje ředitel společnosti První certifikační autorita, a.s., osobu, která je oprávněna tyto změny provést. Nabytí platnosti nové verze Směrnice předchází její schválení ředitelem společnosti První certifikační autorita, a.s.

1.6 Přehled použitých pojmů a zkratk

tab. 2 - Pojmy

Pojem	Vysvětlení
elektronická pečeť	v tomto dokumentu kvalifikovaná elektronická pečeť dle platné legislativy
legislativa pro služby vytvářející důvěru	nařízení eIDAS a aktuálně platná relevantní legislativa Evropské unie

orgán dohledu	orgán dohledu nad dodržováním legislativy pro služby vytvářející důvěru v ČR
smlouva	text smlouvy v elektronické nebo listinné podobě
zákon o ochraně utajovaných informací	zákon České republiky č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
zákoník práce	zákon České republiky č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

tab. 3 - Zkratky

Pojem	Vysvětlení
ČR	Česká republika
ČSN	označení českých technických norem
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
EN	European Standard, typ ETSI standardu
EPS	elektrická požární signalizace
ETSI	European Telecommunications Standards Institute, evropský standardizační institut v oblasti informačních a komunikačních technologií
EU	Evropská unie
EZS	elektronická zabezpečovací signalizace
GDPR	Global Data Protection Regulation, 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 (obecné nařízení o ochraně osobních údajů)
http	Hypertext Transfer Protocol, protokol pro výměnu textových dokumentů ve formátu html
https	Hypertext Transfer Protocol Secure, protokol pro zabezpečenou výměnu textových dokumentů ve formátu html
IEC	International Electrotechnical Commission, světová organizace publikující standardy pro elektrotechniku, elektroniku, sdělovací techniku a příbuzné obory
ISMS	Information Security Management System, systém řízení bezpečnosti informací
ISO	International Organization for Standardization, mezinárodní organizace sdružující národní standardizační organizace, označení standardů
OID	Object Identifier, objektový identifikátor, číselná identifikace

	objektu
PCO	pult centrální ochrany
PDCA	Plan-Do-Check-Act, Plánování-Zavedení-Kontrola-Využití, Demingův cyklus, metoda neustálého zlepšování
QSealCD	kvalifikované zařízení pro tvorbu elektronických pečetí (v souladu s eIDAS)
TS	Technical Specification, typ ETSI standardu
UPS	Uninterruptible Power Supply/Source, zdroj nepřerušovaného napájení
ZOOÚ	legislativa týkající se ochrany osobních údajů, v souladu se směrnicí č. 95/46/ES, resp. s GDPR, tj. s nařízením Evropského parlamentu a Rady (EU) 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, po nabytí jeho platnosti 25.5.2018)

2 ODPOVĚDNOST ZA ZVEŘEJŇOVÁNÍ A ÚLOŽIŠTĚ INFORMACÍ A DOKUMENTACE

2.1 Úložiště informací a dokumentace

Společnost První certifikační autorita, a.s., zřizuje a provozuje úložiště informací a dokumentace.

2.2 Zveřejňování informací a dokumentace

Základní adresy (dále též informační adresy), na nichž lze nalézt veřejné informace o společnosti První certifikační autorita, a.s, případně odkazy pro zjištění dalších informací, jsou:

- adresa sídla společnosti:
První certifikační autorita, a.s.
Podvinný mlýn 2178/6
190 00 Praha 9
Česká republika
- internetová adresa <http://www.ica.cz>.

Elektronická adresa, která slouží pro kontakt veřejnosti s I.CA, je info@ica.cz.

Na výše uvedené internetové adrese lze získat také informace o Službě.

Povolenými protokoly pro přístup k veřejným informacím jsou http a https. I.CA může bez udání důvodu přístup k některým informacím zrušit nebo pozastavit.

2.3 Periodicita zveřejňování informací

I.CA zveřejňuje informace s následující periodicitou:

- politika Služby - po schválení a vydání nové verze,
- prováděcí směrnice Služby - neprodleně,
- ostatní veřejné informace – není předem určeno, obecně však platí, že tyto informace musí reflektovat aktuální stav poskytovaných služeb vytvářejících důvěru.

2.4 Řízení přístupu k jednotlivým typům úložišť

Veškeré veřejné informace zpřístupňuje I.CA bezplatně bez omezení.

Neveřejné informace jsou dostupné pouze pověřeným zaměstnancům I.CA, nebo subjektům definovaným platnou legislativou. Přístup k těmto informacím je řízen pravidly uvedenými v interní dokumentaci.

3 IDENTIFIKACE A AUTENTIZACE KE SLUŽBĚ

3.1 Počáteční ověření identity

Službu mohou využívat Klienti, kteří mají s I.CA uzavřenou platnou smlouvu o využívání této Služby (dále též Smlouva). Pravidla uvedená v následujících podkapitolách platí i pro vydání kvalifikovaného pečetičího certifikátu, který je ve Službě využíván.

3.1.1 Ověřování identity právnické osoby

Ověřování identity právnické osoby Klienta je prováděno před uzavřením Smlouvy, pokud ověření řádně neproběhne, není možné Smlouvu uzavřít. Pro ověření identity Klienta musí být předložen:

- originál nebo úředně ověřená kopie výpisu z obchodního nebo jiného zákonem určeného rejstříku/registru, živnostenského listu, zřizovací listiny, resp. jiného dokladu stejné právní váhy, nebo
- vytištěný výtah z veřejně dostupných registrů, který předloží žadatel nebo jej vyhotoví operátor RA.

Tento dokument musí obsahovat úplné obchodní jméno, identifikační číslo (je-li přiřazeno), adresu sídla, jméno/jména osoby/osob oprávněné/oprávněných k zastupování (statutárních zástupců).

3.1.2 Pověřené osoby

Pověřené osoby Klienta oprávněné k využívání Služby (dále Osoby) jsou buď uvedeny ve Smlouvě, nebo jsou vybaveny plnou mocí k zastupování Klienta podepsanou statutárním zástupcem Klienta. Tyto Osoby jsou oprávněny požádat o vydání prvotního autentizačního komerčního certifikátu na aktivační kartě/tokenu a o vydání kvalifikovaného pečetičího certifikátu. Postup ověřování jejich identity je popsán dále.

3.1.3 Ověřování identity fyzické osoby

Primárním osobním dokladem pro občany ČR musí být platný občanský průkaz nebo cestovní pas. Primárním osobním dokladem pro cizince je platný cestovní pas, nebo jím v případě občanů členských států EU může být platný osobní doklad, sloužící k prokazování totožnosti na území příslušného státu.

Z tohoto dokladu jsou ověřovány následující údaje:

- celé občanské jméno,
- datum a místo narození, nebo rodné číslo, je-li v primárním dokladu uvedeno,
- číslo předloženého primárního osobního dokladu,
- adresa trvalého bydliště (je-li v primárním dokladu uvedena).

Sekundární osobní doklad musí být jednoznačným způsobem (rodné číslo, číslo občanského průkazu atd.) svázán s primárním osobním dokladem a musí obsahovat alespoň jeden z následujících údajů:

- datum narození (nebo rodné číslo, je-li uvedeno),

- adresu trvalého bydliště,
- fotografii obličeje.

Údaje v sekundárním osobním dokladu sloužící k jednoznačné identifikaci Osoby musí být shodné s těmito údaji v primárním osobním dokladu.

Pokud Osoba není uvedena jako zástupce Klienta přímo ve Smlouvě musí předložit plnou mocí k zastupování Klienta podepsanou statutárním zástupcem Klienta.

3.2 Ověření identity při prodloužení služby

Prodloužení Služby probíhá automatizovaně.

3.3 Změna údajů

Pokud vzhledem ke změně údajů není možné provést prodloužení Služby, musí dojít k uzavření dodatku ke smlouvě a vydání nového autentizačního i pečetíčního certifikátu.

4 POŽADAVKY NA ŽIVOTNÍ CYKLUS SLUŽBY

V následujících podkapitolách je popsán životní cyklus služby.

4.1 Uzavření smlouvy a zřízení služby

4.1.1 Proces uzavření smlouvy a odpovědnosti

Klient uzavírající smlouvu o využívání Služby (a kterému potom při návštěvě Osoby na kontaktním místě budou vydány prvotní autentizační komerční certifikát a kvalifikovaný pečetící certifikát je povinen zejména:

- seznámit se s touto Politikou, resp. s příslušnou Směrnicí a smluvně se zavázat jednat podle nich,
- poskytovat pravdivé a úplné informace pro uzavření Smlouvy,
- překontrolovat, zda údaje uvedené ve Smlouvě jsou správné a odpovídají požadovaným.

I.CA je povinna zejména:

- před uzavřením Smlouvy informovat Klienta o smluvních podmínkách,
- uzavírat s Klientem Smlouvu obsahující náležitosti požadované platnou legislativou a technickými standardy,
- zveřejňovat veřejné informace v souladu s ustanoveními kapitoly 2.2,
- činnosti spojené se Službou poskytovat v souladu s platnou legislativou, touto Politikou, příslušnou Směrnicí a provozní dokumentací.

4.1.2 Povinnosti Klienta

Povinností Klientů (držitelů certifikátů) je zejména:

- dodržovat veškerá relevantní ustanovení Smlouvy,
- používat službu v souladu s ustanoveními kapitoly 1.4,
- nakládat s údaji pro identifikaci a autentizaci ke Službě (prvotní autentizační komerční certifikát, resp. jemu odpovídající soukromý klíč na aktivační kartě/tokenu, případně následný autentizační certifikát, resp. jemu odpovídající soukromý klíč uložený šifrovaně v konfiguračním souboru) tak, aby nemohlo dojít k jejímu zneužití,
- neprodleně uvědomit poskytovatele Služby o změnách údajů uvedených ve Smlouvě (a v certifikátu),
- neprodleně uvědomit poskytovatele Služby o podezření, že údaje pro identifikaci a autentizaci ke Službě byly zneužity.

4.1.3 Povinnosti Osoby

Povinností Osoby je v případě požadavku na ukončení Služby, informovat o této skutečnosti I.CA a po vzájemné dohodě sjednanou formou smlouvu ukončit.

4.1.4 Zřízení služby

Zřízení služby probíhá na kontaktních místech, kterými jsou vybrané registrační autority I.CA. Osoba zastupující klienta ji navštíví, je provedeno ověření její identity - viz kapitola 3.1.3 - a potom vydán prvotní autentizační komerční certifikát na aktivační kartě/tokenu (je zde uložen včetně soukromého klíče) a pečeticí kvalifikovaný certifikát, který je uložen na tutéž kartu/token. Soukromý klíč odpovídající pečeticímu certifikátu je vygenerován a uložen v zařízení typu QSealCD spravovaném poskytovatelem služby, do tohoto QSealCD je uložen i odpovídající certifikát.

4.2 Aktivace Služby

Aktivace Služby se provede spuštěním dodávané GUI utility s využitím aktivační karty/tokenu, utilita k jejímu vložení vyzve. Výsledným produktem aktivace Služby je nainstalování klientské aplikace (dále jen Aplikace), vygenerování klíčového páru a vystavení sekundárního autentizačního certifikátu a vytvoření konfiguračního souboru, který musí být následně načten do Aplikace. Soukromý klíč odpovídající sekundárnímu autentizačnímu certifikátu je zde uložen šifrovaně.

4.3 Tvorba kvalifikované elektronické pečeti

Vytváření pečeti iniciuje spisová služba (obecně volající aplikace) klienta. Klientská Aplikace vytvoří šifrovaný kanál k zařízení typu QSealCD, tímto kanálem předá žádost o vytvoření kvalifikované elektronické pečeti a vytvořená kvalifikovaná elektronická pečeť je stejným kanálem vrácena Aplikaci, která sestaví výsledný dokument opatřený pečetí. Pokud je požadován podpis opatřený kvalifikovaným časovým razítkem, je to provedeno v tomto okamžiku, následuje vrácení výsledného dokumentu spisové službě.

4.4 Automatické prodloužení služby

V pravidelných intervalech, pokud je automatické prodloužení zakotveno ve Smlouvě, je s určitým předstihem před vypršením platnosti pečeticího certifikátu provedeno:

- vygenerování nových párových dat pro sekundární autentizační certifikát,
- vygenerování nových párových dat pro vzdálené pečetení a vydán nový kvalifikovaný pečeticí certifikát (soukromý klíč je vygenerován a uložen v zařízení typu QSealCD spravovaném poskytovatelem Služby).

4.5 Účtování provedených operací

Všechny žádosti o kvalifikované elektronické pečeti jsou ukládány do databáze. V pravidelných intervalech jsou získávány záznamy o provedených operacích ze zařízení typu QSealCD, údaje jsou párovány se žádostmi a na základě toho je účtováno. Vedlejším efektem je, že pokud k operaci v QSealCD neexistuje odpovídající žádost, je situace řešena jako potenciální útok.

5 POSTUPY SPRÁVY, ŘÍZENÍ A PROVOZU

Management bezpečnosti je zaměřen především na:

- systém poskytované Služby,
- veškeré procesy podporující poskytování Služby.

Oblasti managementu provozní a fyzické bezpečnosti jsou řešeny jak v základních dokumentech Celková bezpečnostní politika, tato Politika, odpovídající Směrnice a Plán pro zvládání krizových situací a plán obnovy, tak v upřesňujících interních dokumentech. Uvedené dokumenty reflektují výsledky periodicky prováděné analýzy rizik.

5.1 Fyzická bezpečnost

5.1.1 Umístění a konstrukce

Objekty provozního pracoviště jsou umístěny v geograficky odlišných lokalitách, které jsou dále jiné než ředitelství společnosti, obchodní a vývojová pracoviště, pracoviště kontaktních a obchodních míst.

Zařízení určená k výkonu Služby jsou umístěna ve vyhrazených prostorách provozních pracovišť. Tyto prostory jsou zabezpečené obdobně, jako zabezpečené oblasti kategorie „Důvěrné“ podle zákona o ochraně utajovaných informací.

5.1.2 Fyzický přístup

Požadavky na fyzický přístup do jednotlivých vyhrazených prostor (chráněných mechanickými a elektronickými prostředky) provozních pracovišť jsou uvedeny v interní dokumentaci společnosti. Ochrana objektů je řešena elektronickým zabezpečovacím systémem (EZS), připojením na pult centrální ochrany (PCO) a případně speciálním systémem pro sledování pohybu osob a dopravních prostředků.

5.1.3 Elektřina a klimatizace

V prostorách určených k výkonu Služby je dostatečně dimenzovaná aktivní klimatizace, která udržuje celoroční teplotu v rozmezí $20^{\circ}\text{C} \pm 5^{\circ}\text{C}$. Přívod elektrické energie je jističen pomocí UPS (Uninterruptible Power Supply) a diesel agregátu.

5.1.4 Vlivy vody

Všechny kritické systémy provozních pracovišť jsou umístěny takovým způsobem, aby nemohly být zaplaveny ani stoupačkou vodou. Provozní pracoviště jsou podle potřeby vybavena čidly průniku vody pro případ zaplavení vodou z topení, nebo vodou ze střechy při prudkém dešti.

5.1.5 Protipožární opatření a ochrana

V objektech provozních pracovišť a pracovišť pro uchovávání informací je instalována elektronická požární signalizace (EPS). Vstupní dveře vyhrazených prostor, ve kterých jsou

umístěna zařízení určená k výkonu Služby, jsou opatřeny protipožární vložkou. V samotných prostorách se nachází hasicí přístroj.

5.1.6 Ukládání médií

Paměťová média, obsahující provozní zálohy a záznamy v elektronické podobě, jsou ukládána v kovových skříních, popř. trezorech. Kopie jsou ukládány v jiné geografické lokalitě, než kde je umístěno provozní pracoviště.

Papírová média, která je nutno archivovat, jsou skladována v jiné geografické lokalitě, než je umístěno provozní pracoviště.

5.1.7 Nakládání s odpady

Veškerý papírový kancelářský odpad je před opuštěním provozních pracovišť I.CA znehodnocen skartováním.

5.1.8 Zálohy mimo budovu

Kopie provozních a pracovních záloh jsou uloženy na místě určeném ředitelem I.CA a popsaném v interní dokumentaci.

5.2 Procesní bezpečnost

5.2.1 Důvěryhodné role

Pro vybrané činnosti jsou v I.CA definovány důvěryhodné role. Postup jmenování zaměstnanců do důvěryhodných rolí, specifikace těchto rolí včetně odpovídajících činností a odpovědností jsou uvedeny v interní dokumentaci.

Všichni zaměstnanci I.CA v důvěryhodných rolích nesmí být ve střetu zájmů, které by mohly ohrozit nestrannost operací I.CA. Postupy jmenování zaměstnanců do důvěryhodných rolí a specifikace těchto rolí jsou uvedeny v interní dokumentaci.

5.2.2 Počet osob požadovaných na zajištění jednotlivých činností

Pro procesy související s citlivými daty Klientů nutnými pro provoz Služby jsou definovány činnosti, které musí být vykonány za účasti více než jediné osoby. Jedná se zejména o:

- inicializaci kryptografického modulu pro generování a ukládání citlivých dat nutných pro provoz Služby,
- zálohování těchto dat uložených v kryptografickém modulu,
- obnovu těchto dat do kryptografického modulu.

Pro provádění ostatních úloh není počet přítomných osob určen, musí však jít výhradně o pověřené pracovníky.

5.2.3 Identifikace a autentizace pro každou roli

Pracovníkům každé role jsou přiděleny prostředky pro řádnou identifikaci a autentizaci k těm komponentám, které jsou pro jejich činnost nezbytné.

Pro vybrané činnosti využívají pracovníci v důvěryhodných rolích dvoufaktorovou autentizaci.

5.2.4 Role vyžadující rozdělení povinností

Role vyžadující rozdělení povinností, včetně popisu náplně jejich činnosti, jsou popsány v interní dokumentaci.

5.3 Personální bezpečnost

5.3.1 Požadavky na kvalifikaci, zkušenosti a bezúhonnost

Zaměstnanci I.CA v důvěryhodných rolích jsou vybíráni a přijímáni na základě dále popsaných personálních kritérií:

- naprostá občanská bezúhonnost - prokazováno tím, že tyto osoby nemají žádný záznam v rejstříku trestů (výpis z rejstříku trestů, nebo čestné prohlášení),
- vysokoškolské vzdělání v rámci akreditovaného bakalářského nebo magisterského studijního programu a nejméně tři roky praxe v oblasti informačních a komunikačních technologií, nebo středoškolské vzdělání a nejméně pět let praxe v oblasti informačních a komunikačních technologií, přičemž z toho nejméně jeden rok v oblasti poskytování certifikačních/důvěryhodných služeb,
- znalost v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Ostatní zaměstnanci I.CA podílející se na zajištění služeb vytvářejících důvěru Služby jsou přijímáni na základě následujících kritérií:

- vysokoškolské vzdělání v rámci akreditovaného bakalářského, resp. magisterského studijního programu, nebo středoškolské vzdělání,
- základní orientace v oblasti infrastruktury veřejných klíčů a informační bezpečnosti.

Popis konkrétní činnosti zaměstnance je definován pracovní smlouvou.

Dokud nejsou dokončeny veškeré vstupní kontroly zaměstnance, není mu umožněn logický ani fyzický přístup k důvěryhodným systémům.

Pro vykonávání řídicí funkce musí mít vedoucí zaměstnanci zkušenosti získané praxí nebo odbornými školeními s ohledem na důvěryhodnost Služby, znalost bezpečnostních postupů s odpovědností za bezpečnost a zkušenosti s bezpečností informací a hodnocením rizik.

5.3.2 Posouzení spolehlivosti osob

Zdrojem informací o všech zaměstnancích I.CA jsou:

- sami tito zaměstnanci,
- osoby, které tyto zaměstnance znají,
- veřejné zdroje informací.

Zaměstnanci poskytují prvotní informace osobním pohovorem při přijímání do pracovního poměru, ty jsou aktualizovány při periodických pohovorech s nadřízeným pracovníkem v průběhu pracovního poměru.

5.3.3 Požadavky na školení

Zaměstnanci I.CA jsou odborně zaškoleni pro používání určeného programového vybavení a speciálních zařízení. Zaškolení se provádí kombinací metody samostudia a metodickým vedením již zaškoleným pracovníkem. Školení zahrnuje oblasti informační bezpečnosti, ochrany osobních údajů a další relevantní témata.

5.3.4 Požadavky a periodicita doškolování

Dvakrát za 12 měsíců jsou zaměstnancům I.CA poskytovány aktuální informace o vývoji v předmětných oblastech.

Pracovníci kontaktních míst jsou průběžně formou novinek a sdělení distribuovaných v rámci aplikačního vybavení registrační autority informováni o všech relevantních skutečnostech nutných pro správnou činnost kontaktního místa.

5.3.5 Periodicita a posloupnost rotace pracovníků mezi různými rolemi

Z důvodů možné zastupitelnosti v mimořádných případech jsou zaměstnanci I.CA motivováni k získávání znalostí potřebných pro zastávání jiné role v I.CA.

5.3.6 Postihy za neoprávněné činnosti zaměstnanců

Při zjištění neautorizované činnosti je s dotyčným zaměstnancem postupováno způsobem popsáným v interních dokumentech společnosti a řídicím se zákoníkem práce (tento proces nebrání případnému trestnímu stíhání, pokud tomu odpovídá závažnost zjištěné neautorizované činnosti).

5.3.7 Požadavky na nezávislé dodavatele

I.CA může nebo musí některé činnosti zajišťovat smluvně, za činnost nezávislých dodavatelů plně odpovídá. Tyto obchodně právní vztahy jsou ošetřeny bilaterálními obchodními smlouvami. Jedná se např. o zhotovitele programového aplikačního vybavení, dodavatele hardware, systémového programového vybavení, externí auditory atd. Tyto subjekty jsou povinny se řídit odpovídajícími veřejnými politikami, relevantními částmi interní dokumentace I.CA, které jim budou poskytnuty a předepsanými normativními dokumenty. V případě porušení povinností stanovených v uvedených dokumentech jsou vyžadovány smluvní pokuty, případně je s dodavatelem okamžitě ukončena smlouva.

5.3.8 Dokumentace poskytovaná zaměstnancům

Zaměstnanci I.CA mají k dispozici, kromě Politiky a Směrnice služby, bezpečnostní a provozní dokumentaci, veškeré další příslušné normy, směrnice, příručky a metodické pokyny, potřebné pro výkon jejich činnosti.

5.4 Postupy zpracování auditních záznamů

5.4.1 Typy zaznamenávaných událostí

Zaznamenávány jsou veškeré události požadované platnou legislativou pro služby vytvářející důvěru a příslušnými technickými standardy a normami.

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 integritu těchto 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

Auditní záznamy jsou kontrolovány a vyhodnocovány v intervalech definovaných v interní dokumentaci, v případě bezpečnostního incidentu okamžitě.

5.4.3 Doba uchování auditních záznamů

Nestanoví-li relevantní legislativa jinak, jsou auditní záznamy uchovávány po dobu nejméně 10 let od jejich vzniku.

5.4.4 Ochrana auditních záznamů

Auditní záznamy v elektronické a papírové podobě jsou uloženy způsobem zajišťujícím ochranu před jejich změnami, krádeží a zničením (ať již úmyslným nebo neúmyslným).

Elektronické auditní záznamy jsou ukládány ve dvou kopiích, každá kopie je umístěna v jiné místnosti provozního pracoviště. Minimálně jedenkrát měsíčně se provádí uložení těchto auditních záznamů na médium, které je umístěno mimo provozní prostory I.CA.

Auditní záznamy v papírové formě jsou umístěny mimo provozní prostory I.CA.

Ochrana výše uvedených typů auditních záznamů je popsána v interní dokumentaci.

5.4.5 Postupy pro zálohování auditních záznamů

Zálohování elektronických auditních záznamů probíhá obdobným způsobem, jako zálohování ostatních elektronických informací. Zálohování auditních záznamů v papírové formě prováděno není.

5.4.6 Systém shromažďování auditních záznamů (interní nebo externí)

Systém shromažďování auditních záznamů je z pohledu informačních systémů Služby interní.

5.4.7 Postup při oznamování události subjektu, který ji způsobil

Subjekt není o zapsání události do auditního záznamu informován.

5.4.8 Hodnocení zranitelnosti

Hodnocení zranitelnosti je ve společnosti První certifikační autorita, a.s., prováděno v periodických intervalech jako součást analýzy rizik. Sledování zranitelnosti zařízení a programového vybavení souvisejících se službami vytvářejícími důvěru je popsáno v interní dokumentaci.

5.5 Uchovávání záznamů

Uchovávání záznamů, tj. informací a dokumentace, je u I.CA prováděno podle interní dokumentace.

5.5.1 Typy uchovávaných záznamů

I.CA uchovává níže uvedené záznamy (v elektronické nebo listinné podobě), které souvisejí s poskytovanou Službou, zejména:

- smlouvy s Klienty a jejich případné dodatky související se Službou,
- záznam o manipulaci s informacemi (např. převzetí, předání, uložení, kontrola, konverze do elektronické podoby atd.),
- aplikační programové vybavení, provozní a bezpečnostní dokumentace.

5.5.2 Doba uchování záznamů

Záznamy jsou uchovávány v souladu s ustanoveními kapitoly 5.4.3.

Postupy při uchovávání záznamů jsou upraveny interní dokumentací.

5.5.3 Ochrana úložiště záznamů

Prostory, ve kterých se uchovávají záznamy nacházejí, jsou zabezpečeny způsobem vycházejícím z požadavků provedené analýzy rizik a ze zákona o ochraně utajovaných informací.

Postupy při ochraně úložiště uchovávaných záznamů jsou upraveny interní dokumentací I.CA.

5.5.4 Postupy při zálohování záznamů

Postupy při zálohování záznamů jsou upraveny interní dokumentací.

5.5.5 Požadavky na používání časových razítek při uchovávání záznamů

V případě, že jsou využívána časová razítka, jedná se o kvalifikovaná elektronická časová razítka vydávaná I.CA.

5.5.6 Systém shromažďování uchovávaných záznamů (interní nebo externí)

Záznamy jsou ukládány na místo určené ředitelem I.CA.

Samotná problematika přípravy a způsobu ukládání záznamů v elektronické i písemné podobě je upravena interními normami a směrnicemi. Shromažďování uchovávaných záznamů je evidováno.

5.5.7 Postupy pro získání a ověření uchovávaných informací

Uchovávané informace a záznamy jsou umístěny v lokalitách k tomu určených a jsou přístupné:

- zaměstnancům I.CA, pokud je to k jejich činnosti vyžadováno
- oprávněným kontrolním subjektům, orgánům činným v trestním řízení a soudům, pokud je to právními normami vyžadováno.

O každém takto povoleném přístupu je pořizován písemný záznam.

5.6 Obnova po havárii nebo kompromitaci

5.6.1 Postup ošetření incidentu nebo kompromitace

V případě výskytu těchto událostí postupuje I.CA v souladu s interním plánem pro zvládání krizových situací a plánem obnovy a případně s další relevantní interní dokumentací.

5.6.2 Poškození výpočetních prostředků, softwaru nebo dat

Viz kapitola 5.6.1.

5.6.3 Schopnost obnovit činnost po havárii

Viz kapitola 5.6.1.

5.7 Ukončení činnosti poskytovatele služeb

Pro ukončování činnosti kvalifikovaného poskytovatele služby vytvářející důvěru platí následující pravidla:

- ukončení činnosti kvalifikovaného poskytovatele služby vytvářející důvěru musí být písemně oznámeno orgánu dohledu a všem subjektům, které mají uzavřenou Smlouvu na využívání Služby.
- ukončení činnosti poskytovatele služby vytvářející důvěru musí být zveřejněno na internetové adrese podle kapitoly 2.2,
- ukončování činnosti je řízený proces probíhající podle předem připraveného plánu, jehož součástí je popis postupu uchování a zpřístupňování informací pro poskytování důkazů v soudním a správním řízení a pro účely zajištění kontinuity služeb.

V případě bankrotu je postupováno v souladu s příslušnou legislativou.

V případě odnětí statutu kvalifikovaného poskytovatele služeb vytvářejících důvěru dle platné legislativy:

- informace o odnětí statutu musí být písemně nebo elektronicky oznámena všem subjektům, které mají uzavřenou Smlouvu na využívání Služby,
- informace o odnětí statutu musí být zveřejněna v souladu s kapitolou 2.2,
- o dalším postupu rozhodne ředitel I.CA na základě rozhodnutí orgánu dohledu.

6 ŘÍZENÍ TECHNICKÉ BEZPEČNOSTI

6.1 Počítačová bezpečnost

6.1.1 Specifické technické požadavky na počítačovou bezpečnost

Úroveň bezpečnosti komponent použitých pro poskytování Služby je definována platnou legislativou pro služby vytvářející důvěru, resp. v ní odkazovanými technickými standardy a normami.

6.1.2 Hodnocení počítačové bezpečnosti

Hodnocení počítačové bezpečnosti I.CA je založeno na požadavcích uvedených v mezinárodních a národních standardech, zejména:

- prEN 419241-1 Trustworthy Systems Supporting Server Signing - Part 1: Security Requirements.
- prEN 419241-2 Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing.
- CEN/TS 419 261 Security requirements for trustworthy systems managing certificates and time-stamps.
- ČSN ETSI EN 319 401 Elektronické podpisy a infrastruktury (ESI) - Obecné požadavky politiky pro poskytovatele důvěryhodných služeb.
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ČSN ETSI EN 319 403 Elektronické podpisy a infrastruktury (ESI) - Posuzování shody poskytovatelů důvěryhodných služeb - Požadavky na orgány posuzování shody posuzující poskytovatele důvěryhodných služeb.
- ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- ETSI TS 119 101 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation
- ISO/IEC 17021 Conformity assessment -- Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17065 Conformity assessment -- Requirements for bodies certifying products, processes and services.

6.2 Technické řízení životního cyklu

6.2.1 Řízení vývoje systému pro poskytování služby

Při vývoji systému je postupováno v souladu s interní dokumentací.

6.2.2 Řízení správy bezpečnosti

Kontrola řízení bezpečnosti informací, včetně kontroly souladu se standardy, je prováděna v rámci periodických kontrol bezpečnostní shody podle platné legislativy a dále formou interních a externích auditů systému řízení bezpečnosti informací (ISMS).

Bezpečnost informací se v I.CA řídí těmito normami:

- ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.
- ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.
- ČSN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.
- ČSN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.

6.2.3 Řízení bezpečnosti životního cyklu

Řízení bezpečnosti životního cyklu je v I.CA je prováděno procesním přístupem typu „Plánování-Zavedení-Kontrola-Využití“ (Plan-Do-Check-Act, PDCA), který se skládá z navazujících procesů:

- vybudování - stanovení rozsahu a hranic, kterých se řízení bezpečnosti informací týká, určení bezpečnostní politiky, plánů a výběr bezpečnostních opatření v závislosti na vyhodnocených rizicích, to vše v souladu s celkovou bezpečnostní politikou,
- implementace a provoz - účelné a systematické prosazení vybraných bezpečnostních opatření,
- monitorování a přehodnocování - zajištění zpětné vazby, pravidelné sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací, předávání poznatků vedení společnosti k posouzení,
- údržba a zlepšování - provádění opatření k nápravě a zlepšování, na základě rozhodnutí vedení organizace.

6.3 Řízení bezpečnosti sítě

V prostředí I.CA nejsou důvěryhodné systémy určené k podpoře služeb vytvářejících důvěru umístěné na provozních pracovištích I.CA přímo dostupné z veřejné sítě Internet. Tyto systémy jsou chráněny komerčním produktem typu firewall s integrovaným systémem IPS (Intrusion Prevention System). Veškerá komunikace mezi klientskou částí aplikace a provozními pracovišti je vedena šifrovaně. Podrobnosti jsou popsány v interní dokumentaci.

6.4 Ochrana proti padělání a odcizení dat

Opatření proti padělání a odcizení dat jsou součástí celého systému řízení bezpečnosti informací nejen Služby, ale všech systémů I.CA. Spolupodílí se řízení počínaje managementem společnosti, přes vedoucí zaměstnance až po zaměstnance v důvěryhodných rolích s příslušnými oprávněními.

7 HODNOCENÍ SHODY A JINÁ HODNOCENÍ

7.1 Periodicita hodnocení nebo okolnosti pro provedení hodnocení

Periodicita hodnocení, včetně okolností pro provádění hodnocení, je dána platnou legislativou pro služby vytvářející důvěru a jí odkazovanými technickými standardy a normami, dle kterých je hodnocení prováděno.

Periodicita jiných hodnocení je dána příslušnými technickými standardy a normami.

7.2 Identita a kvalifikace hodnotitele

Identita (akreditovaný subjekt posuzování shody) a kvalifikace hodnotitele provádějícího hodnocení podle platné legislativy pro služby vytvářející důvěru, je dána touto legislativou a jí odkazovanými technickými standardy a normami.

Kvalifikace hodnotitele provádějícího jiná hodnocení je dána příslušnými technickými standardy a normami.

7.3 Vztah hodnotitele k hodnocenému subjektu

V případě interního hodnotitele platí, že tento není ve vztahu podřízenosti vůči organizační jednotce, která zajišťuje provoz Služby.

V případě externího hodnotitele platí, že se jedná o subjekt, který není s I.CA majetkově ani organizačně svázán.

7.4 Hodnocené oblasti

V případě provádění hodnocení požadovaného platnou legislativou pro služby vytvářející důvěru jsou hodnocené oblasti konkretizovány touto legislativou, v ostatních případech jsou hodnocené oblasti dány technickými standardy a normami, podle kterých je hodnocení prováděno.

7.5 Postup v případě zjištění nedostatků

Se zjištěními všech typů prováděných hodnocení je seznámen bezpečnostní manažer I.CA, který je povinen zajistit odstranění případných nedostatků. Pokud by byly zjištěny nedostatky, které by zásadním způsobem znemožňovaly poskytovat Službu, přeruší I.CA její poskytování do doby, než budou tyto nedostatky odstraněny.

7.6 Sdělování výsledků hodnocení

Sdělování výsledků hodnocení podléhá požadavkům legislativy pro služby vytvářející důvěru a příslušných technických standardů a norem.

Sdělování výsledků hodnocení je prováděno formou písemné závěrečné zprávy, která je hodnotícím subjektem předána řediteli, resp. bezpečnostnímu manažerovi I.CA.

V nejbližším možném termínu svolá bezpečnostní manažer I.CA schůzi bezpečnostního výboru, na které musí být přítomni členové vedení společnosti, které s obsahem závěrečné zprávy seznámí.

8 OSTATNÍ OBCHODNÍ A PRÁVNÍ ZÁLEŽITOSTI

8.1 Poplatky

8.1.1 Poplatky za využívání služby

Poplatky za využívání Služby jsou upraveny ve Smlouvě uzavřené mezi I.CA a Klientem.

8.1.2 Poplatky za další služby

Není relevantní pro tento dokument.

8.1.3 Postup při refundování

Není relevantní pro tento dokument.

8.2 Finanční odpovědnost

8.2.1 Krytí pojištěním

Společnost První certifikační autorita, a.s., prohlašuje, že má uzavřené pojištění podnikatelských rizik takovým způsobem, aby byly pokryty případné finanční škody.

Společnost První certifikační autorita, a.s., sjednala pro všechny zaměstnance pojištění odpovědnosti za škody způsobené zaměstnavateli v rozsahu, určeném představenstvem společnosti.

8.2.2 Další aktiva

Společnost První certifikační autorita, a.s., prohlašuje, že má k dispozici dostatečné finanční zdroje a jiná finanční zajištění na poskytování služeb vytvářejících důvěru s ohledem na riziko vzniku odpovědnosti za škodu.

Podrobné informace o aktivech společnosti První certifikační autorita, a.s., je možno získat z Výroční zprávy společnosti První certifikační autorita, a.s..

8.2.3 Pojištění nebo krytí zárukou pro koncové uživatele

Není relevantní pro tento dokument, služba není poskytována.

8.3 Důvěrnost obchodních informací

8.3.1 Rozsah důvěrných informací

Důvěrnými informacemi I.CA jsou veškeré informace, které nejsou označeny jako veřejné a nejsou zveřejňovány způsobem uvedeným v kapitole 2.2, zejména:

- veškeré kryptografické informace sloužící v procesu poskytování Služby,
- obchodní informace I.CA,
- veškeré interní informace a dokumentace,
- veškeré osobní údaje.

8.3.2 Informace mimo rámec důvěrných informací

Za veřejné se považují pouze informace označené jako veřejné včetně těch, které jsou zveřejňovány způsobem uvedeným v kapitole 2.2.

8.3.3 Odpovědnost za ochranu důvěrných informací

Žádný zaměstnanec I.CA, který přijde do styku s citlivými a důvěrnými informacemi, je nesmí bez souhlasu ředitele I.CA poskytnout třetí straně.

8.4 Ochrana osobních údajů

8.4.1 Politika ochrany osobních údajů

Ochrana osobních údajů a dalších neveřejných informací je v I.CA řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

8.4.2 Informace považované za osobní údaje

Osobními informacemi jsou veškeré osobní údaje podléhající ochraně ve smyslu příslušných zákonných norem, tedy ZOOÚ.

Zaměstnanci I.CA, případně subjekty definované platnou legislativou přicházející do styku s osobními údaji, jsou povinni zachovávat mlčenlivost o těchto údajích a datech a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení těchto údajů a dat. Povinnost mlčenlivosti trvá i po skončení pracovního, nebo jiného obdobného poměru, nebo po provedení příslušných prací.

8.4.3 Informace nepovažované za osobní údaje

Za osobní údaje nejsou považovány informace, které nespádají do působnosti příslušných zákonných norem, tedy ZOOÚ.

8.4.4 Odpovědnost za ochranu osobních údajů

Za ochranu osobních údajů je odpovědný ředitel I.CA.

8.4.5 Oznámení o používání osobních údajů a souhlas s jejich zpracováním

Problematika oznamování o používání osobních údajů a souhlasu s jejich zpracováním je v I.CA řešena v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

8.4.6 Poskytování osobních údajů pro soudní či správní účely

Poskytování osobních údajů pro soudní, resp. správní účely je v I.CA řešeno v souladu s požadavky příslušných zákonných norem, tedy ZOOÚ.

8.4.7 Jiné okolnosti zpřístupňování osobních údajů

V případě zpřístupňování osobních údajů postupuje I.CA striktně podle požadavků příslušných zákonných norem, tedy ZOOÚ.

8.5 Práva duševního vlastnictví

Tato Politika, veškeré související dokumenty, obsah webových stránek a procedury, zajišťující provoz systému poskytujícího Službu, jsou chráněny autorskými právy společnosti První certifikační autorita, a.s., a představují její významné know-how.

8.6 Zastupování a záruky

8.6.1 Zastupování a záruky I.CA

I.CA zaručuje, že poskytuje:

- technickou podporu při provozu Služby, řešení nestandardních situací a poradenství související s provozem Služby prostřednictvím kontaktních údajů uvedených na adrese www.ica.cz,
- Službu vždy právně a technicky aktuální dle relevantních právních předpisů a technických standardů a norem.

Veškeré záruky a z nich plynoucí plnění je možné uznat jen tehdy, pokud subjekt využívající Službu neporušil povinnosti plynoucí mu ze Smlouvy a této Politiky.

8.6.2 Zastupování a záruky ostatních zúčastněných subjektů

Není relevantní pro tento dokument.

8.7 Zřeknutí se záruk

Společnost První certifikační autorita, a.s., poskytuje pouze záruky, uvedené v kapitole 8.6.

8.8 Omezení odpovědnosti

Společnost První certifikační autorita, a.s., neodpovídá za škody způsobené spoléhajícím se stranám v případech, kdy nesplnily povinnosti požadované touto Politikou, podle které byla Služba poskytována. Dále neodpovídá za škody vzniklé v důsledku porušení závazků I.CA z důvodu vyšší moci.

8.9 Záruky a odškodnění

Pro poskytování služeb vytvářejících důvěru platí relevantní ustanovení platné legislativy a dále takové záruky, které byly sjednány Smlouvou mezi společností První certifikační autorita, a.s., a uživatelem Služby. Smlouva nesmí být v rozporu s platnou legislativou a musí být vždy v elektronické nebo listinné formě.

Společnost První certifikační autorita, a.s.:

- se zavazuje, že splní veškeré povinnosti definované jak platnou legislativou, tak příslušnými politikami,
- poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování Služby,
- souhlasí s tím, že dodavatelé aplikačního programového vybavení, se kterými má platnou smlouvu na distribuci kořenového certifikátu, nepřebírají žádné závazky nebo odpovědnosti, s výjimkou případů, kdy poškození či ztráta byly přímo způsobeny programovým vybavením tohoto dodavatele,
- další možné náhrady škody vycházejí z ustanovení příslušné legislativy a o jejich výši může rozhodnout soud.

Společnost První certifikační autorita, a.s., **neodpovídá** za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování Služby Klientem, zejména za využívání v rozporu s podmínkami uvedenými v této Politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení,

Reklamací je možné podat těmito způsoby:

- e-mailem na adresu reklamace@ica.cz,
- prostřednictvím datové schránky I.CA,
- doporučenou poštovní zásilkou na adresu sídla společnosti,
- osobně v sídle společnosti.

Reklamující osoba je povinna uvést:

- co nejvýstižnější popis závady,
- bližší popis reklamované služby
- požadovaný způsob vyřízení reklamace.

O reklamaci rozhodne I.CA nejpozději do tří pracovních dnů od doručení reklamace a vyrozumí o tom reklamujícího (formou elektronické pošty, nebo doporučenou zásilkou), pokud se strany nedohodnou jinak.

Reklamací, včetně vady, bude vyřízena bez zbytečných odkladů, a to nejpozději do třiceti dnů ode dne uplatnění reklamace, pokud se strany nedohodnou jinak.

8.10 Doba platnosti, ukončení platnosti

8.10.1 Doba platnosti

Tato Politika nabývá platnosti dnem uvedeným v kapitole 9 a platí minimálně po dobu poskytování Služby, nebo do nahrazení Politiky novou verzí.

8.10.2 Ukončení platnosti

Jedinou osobou, která je oprávněna schvalovat ukončení platnosti této Politiky je ředitel společnosti První certifikační autorita, a.s.

8.10.3 Důsledky ukončení a přetrvání závazků

Po ukončení platnosti této Politiky přetrvávají z ní vyplývající závazky I.CA, a to po dobu platnosti posledního podle ní vydaného Certifikátu.

8.11 Individuální upozorňování a komunikace se zúčastněnými subjekty

Pro individuální oznámení a komunikaci se zúčastněnými subjekty může I.CA využít jimi dodané e-mailové adresy, poštovní adresy, telefonní čísla, osobní jednání atd.

Komunikovat s I.CA lze taktéž způsoby uvedenými na internetové informační adrese.

8.12 Novelizace

8.12.1 Postup při novelizaci

Postup je realizován řízeným procesem popsáním v interním dokumentu.

8.12.2 Postup a periodicita oznamování

Vydání nové verze Politiky je vždy oznámeno formou zveřejňování informací.

8.12.3 Okolnosti, při kterých musí být změněn OID

OID není Politice přiřazen. V případě jakýchkoliv změn v tomto dokumentu je vždy změněna jeho verze.

8.13 Ustanovení o řešení sporů

V případě, že Klient nebo spoléhající se strana nesouhlasí s návrhem na vyřešení sporu, mohou použít následující stupně odvolání:

- odpovědný pracovník kontaktního místa,
- odpovědný pracovník I.CA (nutné elektronické nebo listinné podání),

- ředitel I.CA (nutné elektronické nebo listinné podání).

Uvedený postup dává nesouhlasící straně možnost prosazovat svůj názor rychlejším způsobem než soudní cestou.

8.14 Rozhodné právo

Obchodní činnost společnosti První certifikační autorita, a.s., se řídí právním řádem České republiky.

8.15 Shoda s právními předpisy

Systém poskytování služeb vytvářejících důvěru je provozován ve shodě s legislativními požadavky EU, České republiky a dále s relevantními mezinárodními standardy.

8.16 Další ustanovení

8.16.1 Rámcová dohoda

Není relevantní pro tento dokument.

8.16.2 Postoupení práv

Není relevantní pro tento dokument.

8.16.3 Oddělitelnost ustanovení

Pokud soud, nebo veřejnoprávní orgán, v jehož jurisdikci jsou aktivity pokryté touto Politikou, stanoví, že provádění některého povinného požadavku je nelegální, potom je rozsah tohoto požadavku omezen tak, aby požadavek byl platný a legální.

8.16.4 Zřeknutí se práv

Není relevantní pro tento dokument.

8.16.5 Vyšší moc

Společnost První certifikační autorita, a.s., neodpovídá za porušení svých povinností vyplývajících ze zásahu vyšší moci, např. přírodních nebo lidskou činností způsobených katastrof velkého rozsahu, stávek či občanských nepokojů vždy spojených s vyhlášením nouzového stavu, nebo vyhlášení stavu ohrožení státu nebo válečného stavu, popř. výpadku komunikačního spojení.

8.17 Další opatření

Není relevantní pro tento dokument.

9 ZÁVĚREČNÁ USTANOVENÍ

Tato Politika služby vytváření kvalifikovaných elektronických pečetí na dálku vydaná společností První certifikační autorita, a.s., nabývá platnosti a účinnosti dnem 19.6.2018.

Příloha č. 3 ke smlouvě o dílo č. 20/600/0174 s názvem „Zajištění služby kvalifikovaných pečeti na dálku pro systém AISG“

AKCEPTAČNÍ PROTOKOL – vzor

Objednatel:	Generální ředitelství cel	Číslo smlouvy:	
Zhotovitel:	Jméno zhotovitele		

Předmět akceptace

(Specifikace akceptovaného plnění včetně uvedení)

1.

2.

3.

4.

Podpisem tohoto Akceptačního protokolu potvrzuje Oprávněná osoba Objednatele, že uvedený předmět k uvedenému dni řádně akceptovala v souladu s ustanoveními smlouvy. Podpisem tohoto Akceptačního protokolu potvrzuje Oprávněná osoba Zhotovitele, že uvedený předmět k uvedenému dni řádně akceptovala v souladu s ustanoveními smlouvy.

Objednatel:		
Oprávněná osoba:	Telefon, E-mail:	Datum:

Zhotovitel		
Oprávněná osoba:	Telefon, E-mail:	Datum: