**Smlouva**

**o poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal

uzavřená podle ustanovení § 1746 odst, 2 zák. č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „Občanský zákoník“)**

**První certifikační autorita, a.s.**

Se sídlem: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00

Zastoupená: Ing. Petrem Budišem, Ph.D., předsedou představenstva

 Ing. Romanem Kučerou, členem představenstva

IČ: 264 39 395

DIČ: CZ26439395

Bankovní spojení: ČSOB, a.s.

Číslo účtu: XXXXXXXXX/XXXX

zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B, vložka 7136.

(dále též „**I.CA**“ nebo „**Poskytovatel**“)

a

**Česká republika – Ministerstvo průmyslu a obchodu**

Se sídlem: Na Františku 32, 110 15 Praha 1,

Zastoupená: Ing. Miloslavem Marčanem, ředitelem odboru informatiky

IČ: 47609109

Bankovní spojení: Česká národní banka

Číslo účtu: XXXXXXXXXX/XXXX

(dále též „**Objednatel**“)

(dále jednotlivě také jako **„Strana“** a společně také jako „**Strany**“)

uzavírají níže uvedeného dne, měsíce a roku tuto Smlouvu o poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal (dále jen „Smlouva“).

**Článek I.**

**Preambule**

1. Poskytovatel 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, ve znění pozdějších předpisů, pro oblast vydávání kvalifikovaných certifikátů pro elektronické podpisy, kvalifikovaných elektronických časových razítek, kvalifikovaných certifikátů pro elektronické pečetě, kvalifikovaných certifikátů pro autentizaci internetových stránek a kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí. 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 pečetí 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 pečetě podle certifikační politiky vydávání kvalifikovaných certifikátů pro elektronické pečetě 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>.

**Článek II.**

**Předmět smlouvy**

1. Předmětem plnění této Smlouvy je poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku v souladu s platnou Politikou služby vytváření kvalifikovaných elektronických pečetí na dálku, která je vždy v aktuální verzi k dispozici na [www.ica.cz](http://www.ica.cz). Obchodní označení služby je I.CA RemoteSeal.
2. I.CA poskytuje objednateli službu vytváření kvalifikovaných elektronických pečetí na dálku (dále též „I.CA RemoteSeal“) v souladu s bodem 52 recitálu, články 29 a 39, Přílohou II body 3 a 4 a Přílohou III nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS). Popis služby je uveden v příloze č. 1 této Smlouvy.
3. I.CA se zavazuje poskytovat službu I.CA RemoteSeal v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 99,5 % a kapacitou až 30 vytvořených pečetí za minutu.
4. I.CA se zavazuje poskytovat:
5. technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem této smlouvy prostřednictvím e-mailové adresy remotseal@ica.cz a telefonní linky 284 081 933.
6. Hotline v rozsahu Po – Pá 8:00 – 17:00 hod. na výše uvedených kontaktech a provozní pohotovost služby v režimu 24/7 na telefonním čísle 731 657 586.
7. právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celou službu I.CA RemoteSeal, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
8. službu I.CA TRemoteSeal v testovacím prostředí s funkcionalitou obdobnou službě I.CA RemoteSeal v ostrém prostředí, aby bylo zajištěno otestování nových verzí služby I.CA RemoteSeal před nasazením do ostrého provozu. Pro testovací prostředí platí SLA 95% a kapacita 10 vytvořených pečetí za minutu.

**Článek III.**

**Povinnosti objednatele**

1. I.CA poskytuje službu vytváření kvalifikovaných elektronických pečetí na dálku v souladu se závazným prohlášením uvedeným v Preambuli této Smlouvy. Objednatel se zavazuje zabezpečit dodržování platné Politiky služby vytváření kvalifikovaných elektronických pečetí na dálku („Politika“), jež tvoří přílohu č. 2 této Smlouvy. Veškeré změny a doplňky této Politiky jsou vůči objednateli účinné po podpisu dodatku k této Smlouvě podepsaného zástupci Stran.
2. Objednatel se zavazuje neposkytovat plnění poskytnuté I.CA dalším osobám bez souhlasu I.CA a nezneužívat poskytování služeb I.CA.

**Článek IV.**

**Povinnosti I.CA**

1. I.CA garantuje a nese odpovědnost za vytvoření kvalifikované elektronické pečetě pouze za předpokladu, že data nutná k vytvoření pečetě (odesílaná do prostředí I.CA), generovaná komponentou dodanou I.CA, nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno.
2. I.CA se zavazuje, že bude zachovávat mlčenlivost o veškerých skutečnostech obchodní, finanční či účetní povahy, které se dozvěděl v době trvání této smlouvy a které se týkají Objednatele a dalších osob ve vztahu k Objednateli.
3. I.CA se zavazuje plnit právní požadavky a povinnosti v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů v souvislosti se svojí činností při plnění této Smlouvy. I.CA se současně zavazuje, že bude při plnění této Smlouvy, postupovat v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („GDPR“). Povinnosti I.CA při zpracování osobních údajů jsou stanoveny v příloze č. 3. Smlouvy.
4. Předání a převzetí výsledků činnosti I.CA dle článku V. odst. 1 Smlouvy potvrdí vždy objednatel v přehledu jednotlivých činností I.CA. I.CA zpracuje po uplynutí kalendářního měsíce výkaz provedených pečetí a to do 10 pracovních dnů. V případě, že budou v odevzdaném výkazu během této doby shledány nedostatky, vrátí výkaz Objednatel I.CA k přepracování, případně k doplnění. I.CA je povinen přepracovat či doplnit výsledky své činnosti v  termínu do 10 pracovních dnů od obdržení informace o jeho nedostatcích. Původní lhůta bude tímto momentem zastavena. Schválení výkazu provedených pečetí oznámí kontaktní osoba Objednatele kontaktní osobě I.CA. Objednatel stvrzuje výkaz provedených pečetí svým podpisem v v tomto výkazu.
5. Schválený výkaz provedených pečetí je podmínkou pro proplacení ceny dle čl. V. odst. 6. Smlouvy.

**Článek V.**

**Smluvní cenové podmínky**

1. Cena za poskytování služby I.CA RemoteSeal, tj. za vytvoření kvalifikované elektronické pečetě, bude stanovena podle počtu vytvořených kvalifikovaných elektronických pečetí v daném kalendářním měsíci podle příslušného objemového pásma, a to jako součin „Ceny za 1 ks pečetění Kč 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.

|  |  |  |
| --- | --- | --- |
| počet pečetění od - do za měsíc | paušální poplatek Kč bez DPH/měsíc | Cena za 1 ks pečetění Kč 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 |

1. Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady I.CA související s poskytováním služby I.CA RemoteSeal. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.
2. Úhrada poskytování služby I.CA RemoteSeal bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA vytvořila kvalifikované elektronické pečetě. DPH bude vyjádřeno dle aktuálně platné legislativy.
3. I.CA je povinna vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby I.CA RemoteSeal.
4. Objednatel je povinen uhradit daňové doklady převodem na účet I.CA do 30 dnů ode dne prokazatelného doručení daňového dokladu, vystaveného I.CA Objednateli na adresu sídla objednatele a doručeného písemně na adresu sídla objednatele podle údajů v této Smlouvě.
5. Daňový doklad bude mít náležitosti daňových dokladů podle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, § 11 zákona č. 563/1991 Sb., o účetnictví a náležitosti obchodní listiny podle § 435 zákona č. 89/2012 Sb., občanského zákoníku, to vše ve znění pozdějších předpisů. Nebude-li daňový doklad obsahovat zákonem nebo Smlouvou stanovené náležitosti nebo nebude-li přiložena kopie potvrzeného výkazu provedených pečetí, popř. bude-li obsahovat chybné údaje, je objednatel oprávněn fakturu vrátit poradci k přepracování. I.CA je povinna podle povahy závad daňový doklad opravit, nebo nově vyhotovit. Oprávněným vrácením daňového dokladu přestává běžet původní lhůta splatnosti. Nová lhůta splatnosti běží znovu ode dne doručení opraveného nebo nově vyhotoveného daňového dokladu.

**Článek VI.**

**Sankční ustanovení, odstoupení od smlouvy**

1. V případě zaviněného nedodržení parametru SLA dostupnosti služby I.CA RemoteSeal uvedeného v článku IV. odstavci 2. této Smlouvy, tj. pokud dostupnost služby klesne pod 99,5 % za kalendářní den, je I.CA povinna uhradit objednateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každých započatých 0,1 %, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu.
2. V případě nesplnění povinností uvedených v článku II. odstavci 4. písm. a) a b) této Smlouvy je I.CA povinna uhradit objednateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každé takové porušení.
3. V případě nesplnění povinností uvedených v článku II. odstavci 4. písm. c) tohoto ujednání je I.CA povinna uhradit objednateli smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.
4. Pro případ porušení povinnosti I.CA zachovávat mlčenlivost dle článku IV. odst. 2 se sjednává smluvní pokuta ve výši 10 000 Kč, a to za každý jednotlivý případ.
5. Pro případ porušení povinnosti I.CA o ochraně osobních údajů dle článku IV. odst. 3 se sjednává smluvní pokuta ve výši 10 000 Kč, a to za každý jednotlivý případ ve výši uvedené v článku VI. odst. 2 Přílohy č. 3.
6. Uhrazením smluvní pokuty není dotčeno právo poškozené smluvní strany domáhat se náhrady újmy, která jí vznikla porušením smluvní povinnosti, které se smluvní pokuta týká, a to v plné výši, tedy i ve výši přesahující smluvní pokutu. Uhrazená výše smluvní pokuty se nezapočítává do výše újmy, která má být uhrazena.
7. Smluvní pokuta nebo úrok z prodlení je splatný do čtrnácti (14) dnů ode dne zaslání písemné výzvy jednou smluvní stranou druhé.
8. V případě, že objednatel bude v prodlení s úhradou daňového dokladu, sjednávají Strany úrok z prodlení v zákonné výši.
9. Každá ze smluvních stran má právo odstoupit od této Smlouvy v případě, poruší-li jedna ze smluvních stran své závazky a povinnosti stanovené touto Smlouvou, a to podstatným nebo opakovaným způsobem. Odstoupení musí mít písemnou formu s uvedením důvodů odstoupení a musí být doručeno druhé smluvní straně, jinak je odstoupení neplatné. Odstoupení od Smlouvy má právní účinky dnem doručení. Od toho dne nesmí smluvní strana, které takto bylo odstoupení doručeno, pokračovat v plnění předmětu Smlouvy vyjma případů, kdy by nečinností hrozila škoda či jiná újma druhé smluvní straně. V takovém případě má smluvní strana za povinnost pokračovat v plnění Smlouvy a zabezpečit předmět Smlouvy takovým způsobem, aby bylo odstraněno nebezpečí škody či jiné újmy. Odstoupení od smlouvy se řídí § 2001 a násl. občanského zákoníku.

## **Článek VII.**

## **Ukončení smlouvy**

1. Platnost smlouvy je možno ukončit písemnou dohodou, odstoupením nebo výpovědí kteroukoliv smluvní stranou.
2. Objednatel má možnost smlouvu z jakéhokoliv důvodu nebo bez uvedení důvodu vypovědět s výpovědní dobou 1 měsíc, a to s účinností ke konci kalendářního měsíce následujícího po měsíci, v němž byla výpověď doručena poradci.
3. Objednatel může od smlouvy odstoupit v případě podstatného porušení povinností vyplývajících z této smlouvy ze strany I.CA, za něž je považováno zejména:
	1. prodlení s plněním lhůt dle této smlouvy o více jak 7 kalendářních dní;
	2. skutečnost, že byly Objednatelem zjištěny zásadní vady a nedostatky při plnění této Smlouvy a I.CA je ani po písemném upozornění Objednatelem neodstranil;
	3. porušení povinnosti zachovávat mlčenlivost podle této Smlouvy;
	4. nedodržení povinnosti být pojištěn pro případ odpovědnosti za škodu podle této Smlouvy.
4. V případě výpovědi či odstoupením od této Smlouvy zaplatí Objednatel I.CA poměrnou část ceny, která odpovídá řádně doloženým a účelně vynaloženým nákladům, vzniklým v rozsahu tohoto dílčího plnění do dne ukončení smlouvy, a to pouze za předpokladu, že poskytnuté plnění je pro Objednatele využitelné.
5. Při ukončení platnosti této smlouvy je I.CA vždy povinen upozornit Objednatele na opatření potřebná k tomu, aby se zabránilo vzniku škody či újmy bezprostředně hrozící Objednateli nedokončením činností souvisejících s poskytováním služeb dle této Smlouvy.
6. I.CA se zavazuje vrátit Objednateli v případě ukončení tohoto smluvního vztahu veškeré poskytnuté písemnosti a nosiče informací, a to v případě výpovědi ze strany Objednatele do 3 dnů od ukončení platnosti této Smlouvy, v ostatních případech nejpozději k datu ukončení účinnosti této Smlouvy.
7. Ukončením platnosti této smlouvy nejsou dotčena ustanovení smlouvy týkající se nároků z odpovědnosti za škodu a nároků na zaplacení smluvní pokuty, ustanovení o zachování mlčenlivosti, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku platnosti této smlouvy.

**Článek VIII.**

**Závěrečná ustanovení**

1. Tato Smlouva a vztahy z ní vyplývající se řídí českým právním řádem. Veškeré spory vyplývající z této Smlouvy se smluvní strany budou snažit řešit smírnou cestou. Teprve nepovede-li takové smírčí jednání k vyřešení sporu, bude soudní spor veden u příslušného obecného soudu ČR.
2. Pokud jakýkoli závazek dle Smlouvy nebo kterékoli ustanovení Smlouvy je nebo se stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních závazků a ustanovení dle Smlouvy a smluvní strany se zavazují takovýto neplatný nebo nevymahatelný závazek či ustanovení nahradit novým, platným a vymahatelným závazkem, nebo ustanovením, jehož předmět bude nejlépe odpovídat předmětu a ekonomickému účelu původního závazku či ustanovení
3. V případě, že by se některá ustanovení Smlouvy stala neplatnými v důsledku legislativních změn, nestává se neplatnou celá Smlouva. V takovém případě sjednají smluvní strany nové znění dotčených ustanovení tak, aby vystihovalo co nejpřesněji podstatu původního ujednání a aby co nejlépe odpovídalo duchu Smlouvy.
4. Strany souhlasí s uveřejněním plného znění této smlouvy včetně jejích příloh v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, a rovněž na profilu Objednatele, případně i na dalších místech, kde tak stanoví právní předpis. Uveřejnění Smlouvy prostřednictvím registru smluv zajistí Objednatel.
5. Strany souhlasí s tím, že v registru smluv bude zveřejněn celý rozsah Smlouvy, včetně osobních údajů, a to na dobu neurčitou.
6. Tato Smlouva nabývá platnosti dnem jejího podpisu Smluvními stranami a účinnosti dnem zveřejnění v registru smluv.
7. Tato Smlouva se uzavírá v rámci veřejné zakázky malého rozsahu na dobu neurčitou, a to až do vyčerpání finančního limitu pro čerpání služeb dle této Smlouvy ve výši 579 000 Kč (slovy: pět set sedmdesát devět tisíc korun českých) bez DPH.
8. Za plnění dle této smlouvy se považuje i poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku za období od 1. 4. 2021 do nabytí účinnosti této Smlouvy od 1. 7. 2021.
9. Místem plnění Smlouvy je sídlo objednatele.
10. Platnost Smlouvy je možné ukončit:
	1. písemnou dohodou Stran;
	2. písemnou výpovědí některé ze smluvních stran, zaslanou druhé smluvní straně, a to bez uvedení důvodu. Výpovědní doba činí 30 kalendářních dnů a počíná běžet prvním dnem následujícím po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé smluvní straně.
11. Písemnou dohodou Stran je Smlouva ukončena ke dni v této dohodě uvedené a není-li v dohodě takový den uveden, pak ke dni podpisu dohody oběma Stranami.
12. Ukončením platnosti Smlouvy nejsou Strany zbaveny povinnosti vyrovnat veškeré závazky vzniklé v důsledku platnosti a účinnosti této Smlouvy a učinit veškeré úkony, které nesnesou odkladu a které jsou nutné k zabránění vzniku škody na straně jedné ze smluvních stran.
13. Strany se dohodly, že se ve vztazích mezi I.CA a Objednatelem vyplývajících z této Smlouvy neuplatní §§ 1895–1900 občanského zákoníku.
14. Strany přebírají riziko změny okolností ve smyslu § 1765 odst. 2 občanského zákoníku.
15. Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.
16. Tato Smlouva může být změněna dohodou Stran. Dohoda o změně Smlouvy nebo o jejím zrušení musí mít písemnou formu označenou jako vzestupně číslované dodatky a musí být podepsána oprávněnými zástupci Stran.
17. Strany mohou zveřejnit ve svých informačních materiálech, že I.CA je poskytovatelem služby I.CA RemoteSeal pro objednatele.
18. I.CA odpovídá Objednateli za veškeré škody I.CA způsobené neplněním nebo porušením povinností dle této Smlouvy v plném rozsahu. O náhradě škody platí příslušná ustanovené občanského zákoníku
19. Právní vztahy v této Smlouvě neupravené nebo upravené jen částečně se řídí právním řádem České republiky, zejména příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a předpisy souvisejícími.
20. Žádná ze stran není odpovědná za prodlení s porušením povinností stanovených Smlouvou, pokud bylo způsobeno okolnostmi vylučujícími odpovědnost (vyšší moc). Za vyšší moc dle Smlouvy se považují mimořádné okolnosti bránící dočasně nebo trvale splnění v ní stanovených povinností, pokud nastaly po jejím uzavření nezávisle na vůli povinné strany a jestliže nemohly být tyto okolnosti nebo jejich následky povinnou stranou odvráceny ani při vynaložení veškerého úsilí, které lze na ni v dané situaci spravedlivě požadovat.
21. Tato Smlouva je vyhotovena ve dvou vyhotoveních s platností originálu, z nichž každá Strana obdrží po jednom vyhotovení.
22. Seznam příloh, které tvoří nedílnou součást této smlouvy:
23. Příloha č. 1 – Popis služby I.CA RemoteSeal.
24. Příloha č.2 – Politika služby vytváření kvalifikovaných elektronických pečetí na dálku.
25. Příloha č. 3 – Ochrana osobních údajů a bezpečnostní opatření pro smluvní vztahy

V Praze dne dle elektronického podpisu

Za Poskytovatele: Za Objednatele:

…………………………………….. ………………………………………

 Ing. Petr Budiš, Ph.D. Ing. Miloslav Marčan

 předseda představenstva ředitel odboru informatiky

……………………………………

 Ing. Roman Kučera

 člen představenstva

**Příloha č. 1**

**Popis služby I.CA RemoteSeal**

**Služba vytváření kvalifikovaných elektronických pečetí na dálku**

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 pečetě orgány veřejné moci počínaje 20.9.2018 je dána § 8 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce ve znění zákona č. 183/2017 Sb.:

„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 pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.“

Požadavky na kvalifikované prostředky pro vytváření elektronických pečetí (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 pečetí na dálku dodatečné požadavky na kvalifikované poskytovatele (odst. 3 a 4 přílohy II. nařízení eIDAS).

Existují dva typy QSealCD:

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

Služba I.CA RemoteSeal představuje variantu 2 s tím, že certifikace na základě alternativního procesu – musí používat srovnatelnou úroveň bezpečnosti a zároveň certifikační orgán daný postup oznámil Komisi. Alternativní postup může být použit pouze v případě, že příslušné normy neexistují.

Seznam EU pro QSealCD

**„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 Komisí.
* Komise pouze v roli editora seznamu.
* Mohou přispívat pouze ty ČS, které měly nebo mají nahlášeny certifikační orgány.
* Je na zodpovědnosti členských států nahlašovat prostředky Komisi a případné změny jejich certifikace.
* Seznam nemá konstitutivní hodnotu, jedná se pouze o informativní seznam.

Výběr QSealCD pro službu I.CA RemoteSeal

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





Architektura služby



* **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.

**Zřízení služby**[**¶**](https://info.zlin.ica.cz/projects/remseal/wiki/AnalysisBasicConcepts#Zřízení-služby)

Zřízení služby bude probíhat na vybraných pobočkách RA následujícím způsobem:

* Klient navštíví pobočku RA.
* Operátor RA vydá klientovi prvotní autentizační komerční certifikát (**FAC** - First Authentication Certificate) na aktivační kartu/token (viz [názvosloví](https://info.zlin.ica.cz/projects/remseal/wiki/ServiceTerminology)). FAC je nutné zavést do AUTHu jako autentizační certifkát pro RemoteSeal pro daného uživatele (budou provádět ručně obchodníci na základě SN certifikátu, které jim zašle klient).
* Operátor RA připraví žádost o pečetící certifikát pro uživatele.
* Operátor RA vygeneruje párová data pro pečetící certifikát (z pohledu operátora atomická operace) což obnáší:
	+ ICARA pomocí **RSeS** (RemoteSealServer) založí pro klienta uživatele na DSA včetně prvotního hesla **FP** (First Password).
	+ ICARA náhodně vygeneruje nové heslo **PP** (Production Password) (drženo pouze v RAM)
	+ ICARA náhodně vygeneruje 256b AES šifrovací klíč **SK** (Secret Key)
	+ ICARA zašifruje pomocí [AES-KW](https://info.zlin.ica.cz/projects/podpdal/wiki/SecurityConcepts#AES-Key-Wrap) (kde **K** je **SK** a **PP** je **W**) do výsledku **CPP** (Ciphered Production Password)
	+ ICARA zašifruje pomocí RSAES\_PKCS#1 v1.5 klíč **SK** veřejným klíčem **FAC** do výsledku **CSKFAC** (Ciphered Secret Key)
	+ ICARA následně uloží do RSeS kryptogramy **CSKFAC** a **CPP**
	+ ICARA provede aktivaci uživatelského účtu v DSA pomocí FP (a tudíž i změnu hesla na PP).
	+ ICARA provede pod účtem uživatele (s heslem PP) generování párových dat pro vydání prvotního pečetícího certifikátu.
* Operátor RA pomocí ICARA podepíše žádost o vydání pečetícího certifikátu privátním klíče párových dat na DSA (zde můžeme teoreticky zapojit uživatele aby zadal PIN na pinpadové čtečce (pro rozšifrování **CPP** pomocí privátního klíče **FAC**)
* Na základě žádosti proběhne na CA vydání pečetícího certifikátu.
* Pečetící certifikát:
	+ CA pošle na mailovou adresu uživatele.
	+ ICARA uloží na čipovou kartu uživatele.
	+ ICARA uloží na DSA (díky přihlášení jako uživatel)
* Klient odchází z RA s aktivační(m) kartou/tokenem.

**Aktivace RSeC[¶](https://info.zlin.ica.cz/projects/remseal/wiki/AnalysisBasicConcepts%22%20%5Cl%20%22Aktivace-RSeC)**



* Pro aktivaci RSeC spustí uživatel (např.: oprávněná osoba úřadu) dodávanou GUI utilitu RSeActivationUtil (dále jen utilita)
* Utilita vyzve uživatele k vložení aktivační karty (potažmo aktivačního tokenu), načež utilita:
	+ Naváže spojení s RSeS pomocí oboustranně autentizovaného HTTPS za pomoci **FAC** (uživatel bude vyzván k zadání PINu)
	+ Automaticky vytvoří žádost o vydání následného certifikátu **SACi** (Secondary Authentication Certificate číslo i), která bude podepsána **FAC** a privátní klíč k **SACi** se bude generovat v SW (nikoliv na kartě)
	+ Žádost se odešle ke zpracování na CA, kde se obratem vydá následný certitifikát **SACi** a ten se stáhne zpět do utility
	+ Utilita si z RSeS stáhne **CSKFAC** (drží se pouze v RAM)
	+ Pomocí privátního klíče **FAC** na aktivační kartě dešifruje **CSKFAC** na **SK** (drží se pouze v RAM)
	+ Zašifruje pomocí RSAES\_PKCS#1 v1.5 klíč **SK** veřejným klíčem **SACi** do výsledku **CSKSACi**
	+ Utilita následně uloží do RSeS kryptogram **CSKSACi**
* Utilita může případně uživatele vyzvat k dalším nastavením RSeC, pokud nějaká budou (např.: přidávání TS, viditelný podpis, reason, location pokud se tyto nebudou nastavovat pomocí RSeCAPI)
* Následně utilita vytvoří aktivační soubor, kde bude uložen certifikát **SACi** včetně privátního klíče.
* 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**[**¶**](https://info.zlin.ica.cz/projects/remseal/wiki/AnalysisBasicConcepts#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)
* Tato žádost bude podepsána pomocí **SACi**
* Následně RSeC naváže oboustraně autentizovaný TLS kanál pro komunikaci s RSeS pomocí **SACi**
* Navázaným kanálem předá podepsanou žádost o opečetění na RSeS
* RSeS obratem vrátí do RSeC kryptogramy **CSKSACi** a **CPP**, které budou v RSeC drženy pouze v RAM
* RSeC pomocí **SACi** rozšifruje **CSKSACi** na **SK** a pomocí něj rozšifruje **CPP** na **PP** (vše pouze v RAM, po dešifrování **PP** možno ostatní z RAM uvolnit)
* RSeC následně naváže anonymní HTTPS na DSA s aplikováním certificate pinningu na ověření autenticity DSA
* Následně tímto kanálem po autentizaci pomocí **PP** vytvoří na DSA kryptogram pomocí privátního klíče pečetícího certifikátu
* Po vytvoření kryptogramu se z RAM odstraní **PP**
* RSeC využije kryptogram pro kompletaci podepsaného dokumentu
* Pokud je vyžadován podpis s časovým razítkem, je TS do dokumentu přidáno nyní, přičemž RSeC se vůči TSA autentizuje pomocí **SACi**
* Hotový opečetěný dokument je vrácen spisové službě

**Automatické prodloužení služby**[**¶**](https://info.zlin.ica.cz/projects/remseal/wiki/AnalysisBasicConcepts#Automatické-prodloužení-služby)

* Součástí RSeC bude funkcionalita automatické obnovy **SACi** (obdobné řešení jako v QVerify)
* Nejprve se z RSeS stáhne **CSKSACi**
* Pomocí nově vygenerované veřejného klíče se vygeneruje **CSKSACj** a spolu s veřejným klíčem se nahraje na RSeS.
* Následně je možné provést standardní obnovu a nahrát nově vydaný certifikát SACj na RSeS

**Obnova pečetícího certifikátu**[**¶**](https://info.zlin.ica.cz/projects/remseal/wiki/AnalysisBasicConcepts#Obnova-pečetícího-certifikátu)

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

Pro systémy vzdáleného podepisování existuje standard CEN/TS 419241 z roku 2014, který by měl být nahrazen normou prEN 419241 z roku 2017.

Podporované formáty podpisu:

* CAdES-B-B, CAdES-B-T
	+ Dle normy EN 319 122, ve variantách:
	+ Interní
	+ Externí
* PAdES-B-B, PAdES-B-T
	+ Dle normy EN 319 142, ve variantách:
	+ Neviditelný
	+ Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
* Podepisovaná data (business obsah) nikdy neopouští volající systém (komponentu RSeC)!

**Bezpečnostní požadavky a jejich splnění:**

Důvěrnost:

* Ověřovaná data nejsou v systému ukládána
* Důvěrnost dat je řešena:
	+ Při přenosu dat: prostřednictvím SSL protokolu.
	+ Při zpracování požadavku na ověření na serveru: s ověřovanými daty se pracuje pouze v paměti a nejsou v žádném kroku fyzicky uložena do souboru (ani dočasného) nebo databáze. Po procesu ověření jsou data z paměti vymazána.
	+ Celý proces ověření je logován.

Integrita:

* Ověřovaná data nejsou v systému ukládána. Integrita vstupních dat při přenosu je řešena na úrovni datové struktury webové služby (vstupem je hash ověřovaných dat a hash z podpisu) a jejich kontrolou na serveru.

Dostupnost:

* Služba je poskytována v režimu 24/7 s SLA 99,5% a kapacitou až 30 ověření za minutu.

**Příloha č. 2**

**Politika služby vytváření kvalifikovaných elektronických pečetí na dálku**



**Příloha č. 3**

**Ochrana osobních údajů a bezpečnostní opatření pro smluvní vztahy**

**Článek I.Definice pojmů**

|  |  |
| --- | --- |
| **Obecné nařízení** | Nařízení Evropského parlamentu a rady 2016/679 ze dne 27.4.2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „obecné nařízení“). |
| **Správce** | Správcem je ten, kdo určuje účely a prostředky zpracování osobních údajů. |
| **Zpracovatel** | Zpracovatel zpracovává údaje pro Správce, dle jeho pokynů. |
| **Osobní údaje** | Veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, např. jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo jeden či více prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. |
| **Subjekt údajů** | Identifikované nebo identifikovatelná fyzická osoba. |
| **Zpracování** | Jakákoliv operace nebo soubor operací s osobními údaji nebo se soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, výmaz, omezení nebo zničení. |

**Článek II.**

**Předmět ochrany osobních údajů**

1. Předmětem ochrany osobních údajů je úprava vztahů mezi Správcem osobních údajů a Zpracovatelem osobních údajů, zejména pak vymezení rozsahu osobních údajů, které budou zpracovávány, účelu, pro který budou osobní údaje zpracovávány, a specifikace podmínek a záruk Zpracovatele z hlediska technického a organizačního zabezpečení ochrany osobních údajů.
2. Na základě tohoto Dodatku zmocňuje Správce Zpracovatele ke zpracovávání osobních údajů potřebných k vydání certifikátů a zajištění ukládání dokumentů Správce, v prostředí datového centra I.CA.
3. Správce určuje pro Zpracovatele v souladu s nařízením GDPR a zákonem o ochraně osobních údajů tento způsob a tyto prostředky zpracování osobních údajů:

 Správce opravňuje Zpracovatele po dobu účinnosti Smlouvy ke zpracování Osobních údajů zaměstnanců Správce (dále též „Subjekt údajů“) v souvislosti s plněním povinností dle Smlouvy, kdy Osobní údaje potřebné pro vydání certifikátů budou Zpracovateli předávané Subjektem údajů za výše uvedeným Účelem smlouvy v podobě elektronických a/nebo tištěných dokumentů, které mohou obsahovat níže uvedené kategorie Osobních údajů:

* + 1. jméno nebo jména,
		2. příjmení,
		3. titul (před i za jménem),
		4. údaje o adrese trvalého pobytu
		5. datum narození,
		6. rodné číslo,
		7. e-mailová adresa
		8. číslo a místo vydání dokladů totožnosti (občanský průkaz ev. pas).
1. Osobní údaje v elektronické podobě jsou Zpracovatelem ukládány v prostředí datového centra I.CA.
2. Zpracovatel je povinen a zavazuje se zajistit šifrování osobních dat takovým způsobem, aby nebyl Zpracovatel, jeho zaměstnanci ani žádné třetí osoby, které budou pověřeny Zpracovatelem ke zpracování osobních údajů, s výjimkou Správce, schopen zpracovat předané osobní údaje a ani na tyto osobní údaje nahlížet.
3. Přístup do datového centra I.CA mají pouze oprávněné a evidované osoby, a to na základě zvláštních uživatelských oprávnění, jedinečného ID, zřízeného výlučně pro každou osobu a tak, aby elektronické záznamy umožnily vždy určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zpracovány (Přístupový klíč).
4. Po dobu účinnosti Smlouvy umožní Zpracovatel bez zbytečného odkladu Správci opravu, odstranění, zablokování nebo změnu osobních údajů zpracovávaných na základě Smlouvy. Zpracovatel je oprávněn provádět opravy, odstranění nebo blokování osobních údajů ve smyslu předchozí věty jménem Správce pouze v souladu s příslušnými právními předpisy.
5. Zpracovatel je oprávněn zpracovávat osobní údaje, nebo výjimečně z důvodu naplnění Smlouvy pověřit zpracováváním dalšího zpracovatele, a to i mimo území České republiky, v souladu s platnými právními předpisy (dále Další zpracovatel). Zpracovatel se zavazuje předem informovat Správce o každém Dalším zpracovateli.

**Článek III.**

**Povinnosti zpracovatele při zpracování osobních údajů**

1. Zpracovatel se zavazuje přijmout všechna bezpečnostní, technická, organizační a jiná opatření požadovaná v Čl. 32 Obecného nařízení, přitom přihlédne ke stavu techniky, nákladům na provedení, povaze zpracování, rozsahu zpracování, kontextu zpracování a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických.
2. Zpracovatel se zavazuje zpracovávat osobní údaje v souladu s Nařízením GDPR a pokyny Správce, pokud jsou v souladu s právními předpisy.
3. Zpracovatel se zavazuje nezapojit do zpracování žádné další osoby bez předchozího písemného souhlasu Správce.
4. Zpracovatel se zavazuje zpracovávat osobní údaje pouze na základě doložených pokynů Správce (včetně předání údajů do třetích zemí a mezinárodním organizacím). Výjimkou jsou pouze případy, kdy jsou určité povinnosti Zpracovateli uloženy přímo právním předpisem. Jiný účel není Smluvními stranami sjednán ani povolen. Zpracovávání osobních údajů může zahrnovat odstranění potíží za účelem zabránění, vyhledávání a opravy problémů s fungováním Služeb. Může také zahrnovat zlepšování funkcí vyhledávání hrozeb uživatelů a ochrany uživatelů. Osobní údaje nebudou bez výslovného a písemného svolení Správce použity, ani z nich nebudou odvozovány informace pro žádné reklamní či jiné komerční účely (reklamy, marketingu atp.).
5. Zpracovatel bude zpracovávat osobní údaje zejména v rozsahu údajů poskytnutých Správcem a dále osobní údaje zaměstnanců Správce, kteří jsou odpovědni za plnění Smlouvy a tohoto Dodatku.
6. Zpracovatel se zavazuje zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti.
7. Zpracovatel se zavazuje být Správci bez zbytečného odkladu nápomocen při plnění povinností Správce, zejména povinnosti reagovat na žádosti o výkon práv Subjektů údajů, povinnosti ohlašovat případy porušení zabezpečení osobních údajů dozorovému úřadu dle čl. 33 Obecného nařízení, povinnosti oznamovat případy porušení zabezpečení osobních údajů subjektu údajů dle čl. 34 Obecného nařízení, povinnosti posoudit vliv na ochranu osobních údajů dle čl. 35 Obecného nařízení a povinnosti provádět předchozí konzultace dle čl. 36 Obecného nařízení, a že za tímto účelem Zpracovatel zajistí nebo přijme vhodná technická a organizační opatření, o kterých ihned informuje Správce.
8. Zpracovatel se zavazuje po ukončení poskytování služeb spojených se zpracováním osobních údajů dle potřeb Správce všechny tyto osobní údaje vymazat, anebo je vrátit Správci a vymazat veškeré existující kopie. Výjimkou jsou dokumenty související s vydáváním kvalifikovaných certifikátů, které je Zpracovatel povinen uchovávat po dobu 10 let a údaje, na základě kterých byla ověřena totožnost žadatele o kvalifikovaný certifikát, které je Zpracovatel povinen uchovávat po dobu dalších 15 let, oboje na základě § 3 zákona č. 297/2016 Sb.
9. Zpracovatel se zavazuje poskytnout Správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené Správci právními předpisy.
10. Zpracovatel se zavazuje umožnit audity či inspekce prováděné Správcem nebo jiným auditorem, kterého Správce pověří.
11. Zpracovatel se zavazuje poskytnout bez zbytečného odkladu nebo ve lhůtě, kterou stanoví Správce, součinnost potřebnou pro plnění zákonných povinností Správce spojených s ochranou osobních údajů, jejich zpracováním a s plněním Dodatku o zpracování osobních údajů.

**Článek IV.**

**Záruky zpracovatele**

1. Za účelem ochrany osobních údajů Správce před neoprávněným nebo nahodilým přístupem, použitím, zveřejněním nebo zničením, resp. před jejich náhodnou ztrátou či změnou, anebo neoprávněným přenosům anebo neoprávněnému zpracování, jakož i k jinému zneužití, uplatňuje Zpracovatel technická a organizační bezpečnostní opatření, interní kontroly a rutiny zabezpečení osobních údajů, zajišťující splnění všech povinností dle zákona o ochraně osobních údajů.
2. Zpracovatel se zavazuje zajistit informovanost svých zaměstnanců a spolupracujících osob o povinnostech vyplývajících z této Smlouvy a tohoto Dodatku.
3. Zpracovatel se zavazuje zajistit, aby jeho zaměstnanci a spolupracující osoby, kteří budou přicházet do styku s osobními údaji poskytnutými na základě Smlouvy, stejně jako zaměstnanci Dalšího zpracovatele, kteří budou přicházet do styku s osobními údaji poskytnutými na základě této Smlouvy, byli smluvně vázáni povinností mlčenlivosti a poučeni o možných následcích porušení těchto povinností s tím, že povinnost důvěrnosti bude jimi dodržována i po skončení jejich pracovního poměru nebo jiného smluvně založeného vztahu.
4. Zpracovatel nese odpovědnost za jednání osob, které použil v souvislosti s plněním Smlouvy, bez ohledu na to, zda se jedná o jeho vlastní zaměstnance nebo smluvní partnery.

**ČLÁNEK V.**

**Ochrana osobních údajů**

1. Zpracovatel se zavazuje zachovávat mlčenlivost o všech skutečnostech, o nichž se dozví u Správce při plnění závazků dle Smlouvy nebo v souvislosti s ním, jakož i o osobních údajích, osobních údajích zvláštní kategorie a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních a citlivých údajů ve smyslu zejména Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Nařízení GDPR). V tomto odstavci definovaný́ závazek mlčenlivosti a ochrany důvěrných informací platí i po dobu 25 let po ukončení smluvního vztahu založeného Smlouvou.
2. Ustanovení Článku IV., odst. 1, se nevztahuje na informace, které byly v době uzavření Smlouvy obecně známé, nebo se obecně známými stanou později, anebo které je třeba v nezbytně nutném rozsahu poskytnout podle zvláštních právních předpisů (např. zákon č. 106/1999 Sb.) či pravomocných soudních rozhodnutí.
3. Zpracovatel se zavazuje, že nepoužije jakýkoliv osobní údaj nebo osobní údaj zvláštní kategorie, s nímž přijde do styku při plnění závazků dle Smlouvy, a ani neumožní použití třetí osobě.
4. Zpracovatel se zavazuje plně respektovat bezpečnostní požadavky Správce k zajištění ochrany osobních, o nichž je Zpracovatel průkazně informován.
5. Zpracovatel prohlašuje, že přijal bezpečnostní opatření k zajištění ochrany předaných osobních údajů před jejich zneužitím nebo únikem prostřednictvím svých zaměstnanců nebo smluvních partnerů.
6. Zpracovatel prohlašuje, že jeho zaměstnanci a/nebo smluvní partneři přicházející při výkonu své práce do styku s předanými osobními údaji, byli náležitě poučeni o povoleném způsobu nakládání s takovými údaji a byli seznámeni s následky jednání, které by bylo v rozporu se zákonnou úpravou a bezpečnostními směrnicemi Správce, s nimiž byli prokazatelně seznámeni.
7. Zpracovatel nese odpovědnost za řízení přístupu Uživatelů Správce k osobním údajům a osobním údajům zvláštní kategorie, ukládaným a zpracovávaným v rámci poskytování Služby, ve smyslu Nařízení GDPR, a to včetně tvorby a správy bezpečných hesel k přístupům Správce i Uživatelů.

**ČLÁNEK VI.**

**Sankce**

1. V případě, že Zpracovatel poruší jakoukoliv povinnost stanovenou v článku IV odst. 3. Smlouvy, s ohledem na ochranu a povinnosti vztahující se ke zpracování Osobních údajů, může se Správce domáhat okamžitého odstranění závadného stavu.
2. V případě, že Zpracovatel poruší jakoukoliv povinnost stanovenou v článku IV.odst.3. Smlouvy, je Správce dále oprávněn požadovat smluvní pokutu ve výši 20.000,- Kč za každý jednotlivý případ a Zpracovatel je povinen tuto pokutu uhradit.

**Článek VII.**

**Bezpečnostní opatření pro smluvní vztahy**

1. I.CA je povinna zabezpečit údaje potřebné pro vydání certifikátů takovým způsobem, aby nedošlo k jakémukoli porušení důvěrnosti, dostupnosti a integrity údajů. Tyto údaje uchovává a zpracovává v souladu s 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) a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
2. I.CA je oprávněna užívat údaje potřebné pro vydání certifikátů výhradně pro účely ověření totožnosti žadatele o certifikát.
3. MPO je oprávněno na základě předchozího písemného upozornění provést kontrolu a audit prostor I.CA, ve kterých jsou uchovávány údaje potřebné pro vydání certifikátů.
4. Veškeré činnosti dle této Smlouvy zajišťuje I.CA sama svými zaměstnanci, a to v rámci činnosti kvalifikovaného poskytovatele služeb vytvářejících důvěru, bez poddodavatelů.
5. V případě vydávání certifikátů v prostorách MPO je I.CA povinna dodržovat bezpečnostní politiky či pravidla definovaná MPO.
6. Tato Smlouva je v souladu s obecně závaznými právními předpisy ČR a přímo vykonatelnými nařízeními EU, speciálně s 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) a zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
7. I.CA je povinna informovat MPO o kybernetických bezpečnostních incidentech souvisejících s plněním Smlouvy, způsobu řízení rizik na straně I.CA a o zbytkových rizicích souvisejících s plněním Smlouvy a o významných změnách ovládání I.CA podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných I.CA k plnění podle Smlouvy.
8. Při ukončení Smlouvy zůstávají vydané certifikáty a kvalifikovaná elektronická časová razítka platná po dobu jejich platnosti, I.CA není oprávněna je zneplatnit.
9. V případě požadavku MPO na předání seznamu vydaných certifikátů či kvalifikovaných elektronických časových razítek za definované časové období vyhotoví I.CA tyto seznamy v lidsky čitelné podobě ve formátu .xlsx či .docx.
10. Doba uchovávání údajů potřebných pro vydání certifikátů se řídí ustanovením § 3 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce. Likvidace musí probíhat protokolárním způsobem a být potvrzena dozorovým orgánem kvalifikovaných poskytovatelů služeb vytvářejících důvěru ministerstvem vnitra ČR.
11. V případě významných změn kontroly nad dodavatelem nebo změn kontroly nad zásadními aktivy využívanými I.CA k plnění podle Smlouvy je MPO oprávněno od Smlouvy jednostranně odstoupit. Odstoupení musí mít písemnou formu a být podepsáno oprávněnou osobou. Právní účinky odstoupení nastávají prvním dnem měsíce následujících po měsíci, kdy bylo odstoupení prokazatelně doručeno I.CA. K tomuto datu se obě smluvní strany zavazují vypořádat všechny své vzájemné závazky.
12. V případě porušení ustanovení této Smlouvy je MPO oprávněno uplatnit vůči I.CA sankce relevantní konkrétnímu porušení, a to na základě dohody obou stran.“.