Smlouva

o poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal v2

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:	XXX
	XXX
IČ:	264 39 395
DIČ:	CZ26439395
Bankovní spojení:	XXX
Číslo účtu:	XXX

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

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

a

Česká republika – Státní ústav pro kontrolu léčiv, organizační složka státu

Se sídlem:	Šrobárova 49/48, 100 41 Praha 10
Zastoupená:	Mgr. Irenou Storovou, MHA, ředitelkou
IČ:	00023817
Bankovní spojení:	Česká národní banka
Číslo účtu:	623101/0710

(dále též „**Objednatel**“)

(dále jednotlivě také jako **„Smluvní strana“** a společně také jako „**Smluvní strany**“)

uzavírají níže uvedeného dne, měsíce a roku tuto Smlouvu o poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal v2 (dále jen „**Smlouva**“).

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, 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. Vzhledem k tomu, že služba I.CA RemoteSeal v2 není přímo v nařízení eIDAS definována, nemůže být auditována jako kvalifikovaná služba. Nicméně byla posouzena orgánem dohledu, Ministerstvem vnitra, a jeho rozhodnutím čj. MV-210370-5/EG-2022 ze dne 8.12.2022 bylo I.CA povoleno poskytovat službu vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal v2 v souladu s politikou této služby a v souladu s technickou a uživatelskou dokumentací zařízení Entrust nShield Connect XC se SAM modulem. Dále bylo 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 I.
Předmět Smlouvy

1. Předmětem plnění této Smlouvy je zajištění provozu 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 (dále také „**Služba**“ nebo „**I.CA RemoteSeal**“). Obchodní označení Služby je I.CA RemoteSeal.

2. Účelem této smlouvy je zabezpečení vhodných podmínek pro výkon činnosti Objednatele a plnění jeho úkolů.

Článek II.
Povinnosti Objednatele

1. I.CA poskytuje Službu v souladu se závazným prohlášením uvedeným v Preambuli této Smlouvy. Objednatel se zavazuje zabezpečit dodržování platné Politiky služby vytváření kvalifikovaných elektronických pečetí na dálku (dále jen „**Politika**“). Veškeré změny a doplňky této Politiky jsou vůči Objednateli účinné po podpisu dodatku k této Smlouvě podepsaného zástupci obou Smluvních stran.

2. Objednatel je povinen nahradit újmu na jmění Poskytovatele vzniklou v důsledku nedodržení Politiky Objednatelem.

3. Objednatel se zavazuje neposkytovat plnění poskytnuté I.CA dalším osobám bez souhlasu I.CA a nezneužívat poskytování služeb I.CA.

Článek III.
Povinnosti I.CA

1. I.CA poskytuje Objednateli Službu 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.

2. I.CA se zavazuje poskytovat Službu v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 99,5 % a kapacitou až 30 vytvořených pečetí za minutu.

3. I.CA se zavazuje poskytovat:

   a) technickou podporu při provozu Služby, řešení nestandardních situací a poradenství související s předmětem této Smlouvy prostřednictvím e-mailové adresy remoteseal@ica.cz a telefonní linky XXX v rozsahu Po – Pá 8:00 až 17:00 hod,
   b) provozní pohotovost Služby v režimu 24/7 na telefonním čísle XXX,
   c) právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celé Služby, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS,
   d) 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 10 vytvořených pečetí za minutu.

4. 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.

5. I.CA se zavazuje vést pro Objednatele přehled o počtu Službou vydaných kvalifikovaných elektronických pečetí, který bude Objednateli dostupný způsobem umožňujícím dálkový přístup.

6. Pokud to bude vyžadovat poskytování Služby, že I.CA se zavazuje, že poskytne Objednateli v rámci ceny Služby oprávnění k užívání programového vybavení Služby ve smyslu § 2358 a násl. Občanského zákoníku, a to jako licenci nevýhradní, přenositelnou, po celou dobu poskytování Služby, včetně práva užití všech budoucích upgrade a update daného programového vybavení Služby.

7. I.CA se zavazuje při plnění této Smlouvy spolupracovat s jakýmikoliv experty nebo jinými odborníky, které určí Objednatel, tak aby bylo dosaženo účelu této Smlouvy.

8. I.CA potvrzuje, že ke dni podpisu této Smlouvy má uzavřenu pojistnou smlouvu na pojištění odpovědnosti za škodu způsobenou při výkonu své podnikatelské činnosti na minimální částku 1.000.000,- Kč (slovy jeden milion korun českých) se spoluúčastí nejvýše 10 %, a že tuto pojistnou smlouvu bude udržovat účinnou po dobu trvání této Smlouvy a dále nejméně 6 měsíců po ukončení činnosti podle této Smlouvy. Na žádost Objednatele je I.CA bez zbytečného odkladu povinna předložit Objednateli pojistnou smlouvu či pojistný certifikát příslušné pojišťovny.

Článek IV.
Smluvní cenové podmínky

1. Cena za poskytování Služby, 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 v 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 v Kč bez DPH/měsíc	Cena za 1 ks pečetění v Kč bez DPH
1 - 100	500	2,00
101 - 300	1000	1,80
301 - 500	1500	1,50
501 - 1.000	2000	1,30
1.001 - 3.000	3500	1,10
3.001 - 5.000	4500	1,00
5.001 - 10.000	6000	0,80
10.001 - 30.000	9000	0,65
30.001 - 50.000	12000	0,50
50.001 - 100.000	15000	0,30
100.001 - 300.000	18000	0,20
300.001 - 500.000	21000	0,15
500.001 - 1.000.000	25000	0,10
1.000.001 - 5.000.000	29000	0,08
5.000.001 - 10.000.000	35000	0,05

2. Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady I.CA související s poskytováním Služby. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.

3. Úhrada poskytování Služby bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA vytvořila kvalifikované elektronické pečetě, a to podle počtu skutečně provedených a poskytnutých vytvořených pečetí. Daňový doklad bude obsahovat počet skutečně vytvořených pečetí.

4. Celková cena veškerých Služeb, poskytnutých na základě této Smlouvy, nesmí ve svém souhrnu překročit limit částky 200 000,- Kč bez DPH za kalendářní rok.

5. 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.

6. Objednatel je povinen uhradit daňové doklady převodem na účet I.CA do 30 dnů ode dne doručení daňového dokladu, vystaveného I.CA, na adresu sídla Objednatele a doručeného písemně na adresu sídla Objednatele podle údajů v této Smlouvě nebo na adresu posta@sukl.cz.

7. Daňový doklad musí mít náležitosti daňových a účetních dokladů stanovených platnými a účinnými právními předpisy. Objednatel je oprávněn daňový doklad, který nebude splňovat náležitosti podle platných a účinných právních předpisů, vrátit I.CA. I.CA je povinna nedostatky daňového dokladu odstranit a vystavit nový daňový doklad. V případě vrácení vadně vystaveného daňového dokladu ve smyslu tohoto odstavce se Objednatel neocitá v prodlení s jeho úhradou. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu.

Článek V.
Sankční ustanovení, odstoupení od Smlouvy

1. V případě zaviněného nedodržení parametru dostupnosti Služby (SLA) uvedeného v článku III. 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 stanovenou hodnotu. Měsíční výše Smluvní pokuty však nepřesáhne výši měsíční ceny za poskytování Služby.

2. V případě nesplnění povinností uvedených v článku III. odstavci 3. 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 III. odstavci 3. písm. c) tohoto ujednání je I.CA povinna uhradit Objednateli Smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.

4. Každá ze Smluvních stran má právo odstoupit od této Smlouvy, pokud druhá ze Smluvních stran poruší 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 prokazatelně 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 újma na jmění druhé Smluvní strany. V takovém případě má Smluvní strana za povinnost pokračovat v plnění Smlouvy a zabezpečit předmět Smlouvy takovým způsobem, aby bylo odstraněno nebezpečí shora uvedené újmy na jmění. Odstoupení od Smlouvy se řídí § 2001 a násl. Občanského zákoníku.

Článek VI.
Zvláštní ujednání

1. Dodržování předpisů
   I.CA se zavazuje, že jí pověření zaměstnanci při plnění této Smlouvy v objektech Objednatele budou dodržovat veškeré obecně závazné předpisy, vztahující se k vykonávané činnosti, zejména předpisy o bezpečnosti práce a o požární bezpečnosti, interní předpisy Objednatele, předpisy o vstupu do objektů Objednatele, o ochraně osobních údajů a o bezpečnosti systémů, a budou se řídit organizačními pokyny zaměstnance, pověřeného Objednatelem.

2. Ochrana osobních údajů
   V případě, že se při zajišťování předmětu této Smlouvy dostanou zaměstnanci I.CA do styku s interními aplikacemi či informačními systémy Objednatele, zavazuje se I.CA v souladu s nařízením Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES a zákonem č. 110/2019 Sb., o zpracování osobních údajů, přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Pokud jde o personální opatření, zavazuje se I.CA zajistit u fyzických osob – svých kmenových zaměstnanců, případně jiných fyzických osob, pokud by vykonávaly některé

činnosti v rámci předmětu této Smlouvy pro I.CA, že tyto činnosti budou vykonávat pouze osoby bezúhonné a zavázané povinností mlčenlivosti.

3. Obchodní tajemství
   Pokud I.CA získá (bez ohledu na způsob) od Objednatele informace, které mají povahu obchodního tajemství (dále též „**chráněné informace**“ nebo „**obchodní tajemství**“), bude s těmito chráněnými informacemi nakládat jako s vlastním obchodním tajemstvím, aniž by bylo nutné takové informace jako chráněné informace vždy jednotlivě označovat, což nevylučuje možnost v jednotlivých případech při zvýšeném zájmu toto nebo jiné označení (např. “diskrétní“) pro jednotlivé informace, resp. jejich nosiče, výslovně použít. I.CA se zavazuje, že nepoužije chráněné informace k jinému účelu, než k jakému jí byly poskytnuty a že kmenové zaměstnance, kteří přijdou s chráněnými informacemi do styku, případně smluvní partnery, kterým se svolením druhé Smluvní strany chráněné informace zpřístupní, o povinnosti uchovávat takové informace v tajnosti dostatečně poučí a odpovídajícím způsobem smluvně zajistí jejich utajení.

   Ustanovení této Smlouvy, která se týkají ochrany obchodního tajemství, budou v plném rozsahu platná a účinná po neomezenou dobu od ukončení smluvního vztahu založeného touto Smlouvou.

4. Poskytování informací
   I.CA se zavazuje, že informace ani jakékoliv technické nebo jiné podklady, získané při plnění této Smlouvy, nepoužije pro jiné než touto Smlouvou stanovené účely, ani je neposkytne nebo k nim neumožní přístup třetím osobám bez předchozího písemného souhlasu Objednatele. Tento závazek se vztahuje na všechny zaměstnance společnosti I.CA a další zaměstnance, kteří se budou případně podílet na plnění předmětu této Smlouvy a seznámí se s těmito informacemi nebo budou držiteli těchto podkladů. Tento závazek bude trvat po neomezenou dobu od ukončení platnosti této Smlouvy.

5. Objednatel v souladu s § 4a odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti o změně souvisejících zákonů, ve znění pozdějších předpisů (dále jen „**ZoKB**“) informuje Poskytovatele, že systém kvalifikovaného pečetění, jehož součástí je i služba vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal v2, je podpůrným systémem systému kritické informační infrastruktury a významných informačních systémů ve smyslu § 2 písm. b) a d) ZoKB a Objednatel je ve smyslu § 2 písm. e) ZoKB správcem zmíněných systémů kritické informační infrastruktury a významných informačních systémů, přičemž Poskytovatel bere toto na vědomí. Poskytovatel rovněž bere na vědomí, že se po dobu účinnosti této Smlouvy stává provozovatelem podpůrného systému systému kritické informační infrastruktury a významných informačních systémů ve smyslu § 2 písm. g) ZoKB a dle § 3 písm. e) rovněž osobou, jíž jsou v této souvislosti ZoKB a příslušnými prováděcími předpisy ukládány povinnosti v oblasti kybernetické bezpečnosti. Při plnění této Smlouvy je povinen plnit Bezpečnostní pravidla pro významné dodavatele, které tvoří Přílohu č. 2 této Smlouvy. V případě rozporu mezi ustanovením Smlouvy a ustanovením Přílohy č. 2 je rozhodující ustanovení Smlouvy.

Článek VII.
Oprávněné osoby, komunikace

1. Kontaktní údaje pro oznamování incidentů a příjem požadavků na:

    a) technickou podporu při provozu služby, řešení nestandardních situací a poradenství související s předmětem této Smlouvy v rozsahu Po – Pá 8:00 až 17:00 hod.:
    e-mail: remoteseal@ica.cz,
    telefon: XXX

    b) provozní pohotovost Služby v režimu 24/7:
    telefon: XXX

2. Oprávněnými pracovníky Objednatele jsou následující osoby:

    XXX
    XXX
    XXX
    XXX

3. Smluvní strany jsou oprávněny jednostranně změnit oprávněné osoby, resp. kontaktní údaje, jsou však povinny na takovou změnu druhou Smluvní stranu předem písemně upozornit.

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. Smluvní strany souhlasí s uveřejněním této Smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů a rovněž na profilu Objednatele, případně i na dalších místech, kde tak stanoví právní předpis.

Uveřejnění této Smlouvy prostřednictvím registru smluv ve lhůtě stanovené zákonem zajistí Objednatel.

5. Smluvní strany souhlasí s tím, že v registru smluv bude zveřejněn celý rozsah Smlouvy, vyjma osobních údajů, a to na dobu neurčitou.

6. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami.

7. Tato Smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv.

8. Tato Smlouva se uzavírá na dobu neurčitou.

9. Místem plnění Smlouvy je sídlo Objednatele a jeho níže uvedená odloučená pracoviště:

   - Benešovská 2538/40, 101 00 Praha 10;
   - 17. listopadu 1790, 708 52 Ostrava – Poruba;
   - B. Němcové 585/54, 370 87 České Budějovice
   - Stará 25, 602 00 Brno;
   - Křížkovského 3, 772 00 Olomouc;
   - Resslova 745, 500 09 Hradec Králové;
   - Klicperova 9, 301 00 Plzeň.

10. Kterákoli ze smluvních stran je oprávněna za dodržení níže uvedených podmínek Smlouvu písemně vypovědět:

    a) Objednatel je oprávněn Smlouvu zcela vypovědět bez uvedení důvodu, přičemž výpovědní doba pro Objednatele činí 3 měsíce a počíná běžet dnem bezprostředně následujícím po dni prokazatelného doručení výpovědi druhé smluvní straně,
    b) Poskytovatel je oprávněn Smlouvu zcela vypovědět z důvodu prodlení Objednatele se zaplacením faktury vystavené Poskytovatelem po uskutečnění plnění, tj. po řádném a včasném poskytnutí Služeb v souladu s touto Smlouvou; prodlení Objednatele musí činit více než 60 dní. Výpovědní doba pro Poskytovatele činí v takovém případě 3 měsíce a počíná běžet dnem bezprostředně následujícím po dni prokazatelného doručení výpovědi druhé smluvní straně,
    c) Poskytovatel je dále oprávněn Smlouvu zcela vypovědět bez uvedení důvodu, přičemž výpovědní doba pro Poskytovatele činí v takovém případě 6 měsíců a počíná běžet dnem bezprostředně následujícím po dni prokazatelného doručení výpovědi druhé smluvní straně.

11. Za řádné doručení výpovědi se považuje jeho doručení prostřednictvím poskytovatele poštovních služeb, kurýra nebo jeho doručení do datové schránky druhé smluvní strany.

12. Ukončením Smlouvy nejsou Smluvní strany zbaveny povinnosti vyrovnat veškeré závazky vzniklé v souvislosti s plněním této Smlouvy v době její platnosti a účinnosti a učinit veškeré úkony, které nesnesou odkladu a které jsou nutné k zabránění vzniku újmy na straně kterékoli ze Smluvních stran.

13. Smluvní strany se dohodly, že se ve vztazích mezi I.CA a Objednatelem vyplývajících z této Smlouvy neuplatní §§ 1895 – 1900 zák. č. 89/2012 Sb., občanského zákoníku.

14. Tato Smlouva může být změněna dohodou obou Smluvních stran. Dohoda o změně Smlouvy nebo o jejím zrušení musí mít písemnou formu označenou jako vzestupně číslované dodatky a musí být podepsána oprávněnými zástupci obou Smluvních stran.

15. Smluvní strany mohou zveřejnit ve svých informačních materiálech, že I.CA je poskytovatelem služby I.CA RemoteSeal pro Objednatele.

16. Tato Smlouva je vyhotovena ve dvou vyhotoveních, z nichž obě Smluvní strany obdrží po jednom vyhotovení, popř. v jediném oboustranně elektronicky podepsaném originále.

17. Seznam příloh, které tvoří nedílnou součást této Smlouvy:
    a) Příloha č. 1 – Popis služby I.CA RemoteSeal,
    b) Příloha č. 2 - Bezpečnostní pravidla pro významné dodavatele.

V Praze dne 5.5.2023 V Praze dne 8.6.2023

Za Poskytovatele:

……..
XXX

……
XXX

Za Objednatele:

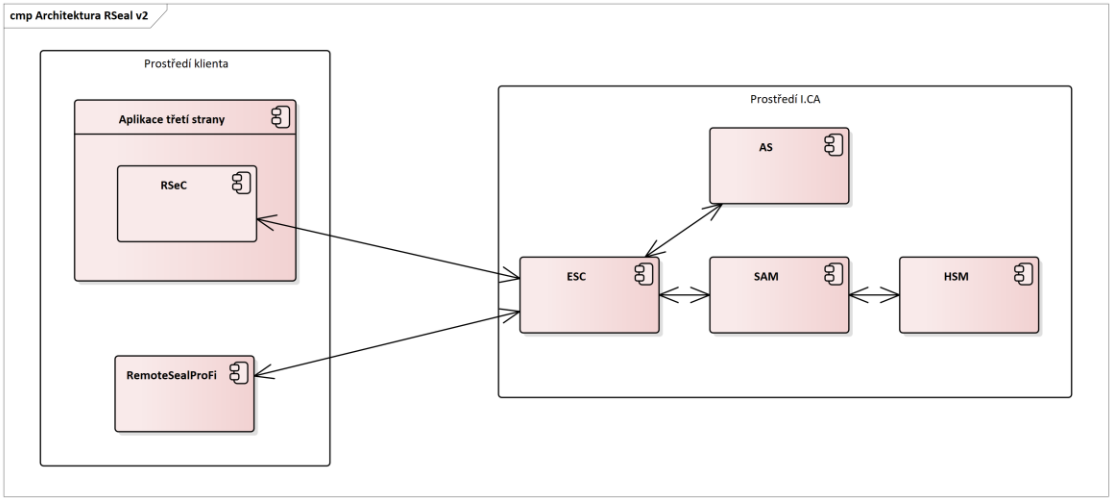
……
Mgr. Irena Storová
ředitelka
Státního ústavu pro kontrolu léčiv

Popis služby I.CA RemoteSeal v2

Co je služba I.CA RemoteSeal v2

Služba I.CA RemoteSeal v2 (dále už jen „RemoteSeal“ nebo „služba“) je služba vytváření kvalifikovaných elektronických pečetí na dálku. Služba umožňuje vygenerovat a držet data pro vytváření elektronických pečetí (tj. zejména privátní klíč) v QSealCD certifikovaném HSM zařízení ve správě I.CA a k němu pak zprostředkovat přístup pro účely vytváření kvalifikovaných elektronických pečetí. Klient (tj. právnická osoba) má k dispozici klientskou komponentu a příslušné autentizační markanty, pomocí kterých může dokument opatřit kvalifikovanou elektronickou pečetí. Samotný obsah dokumentu přitom neopouští klientskou komponentu, a tudíž ani prostředí klienta.

Architektura

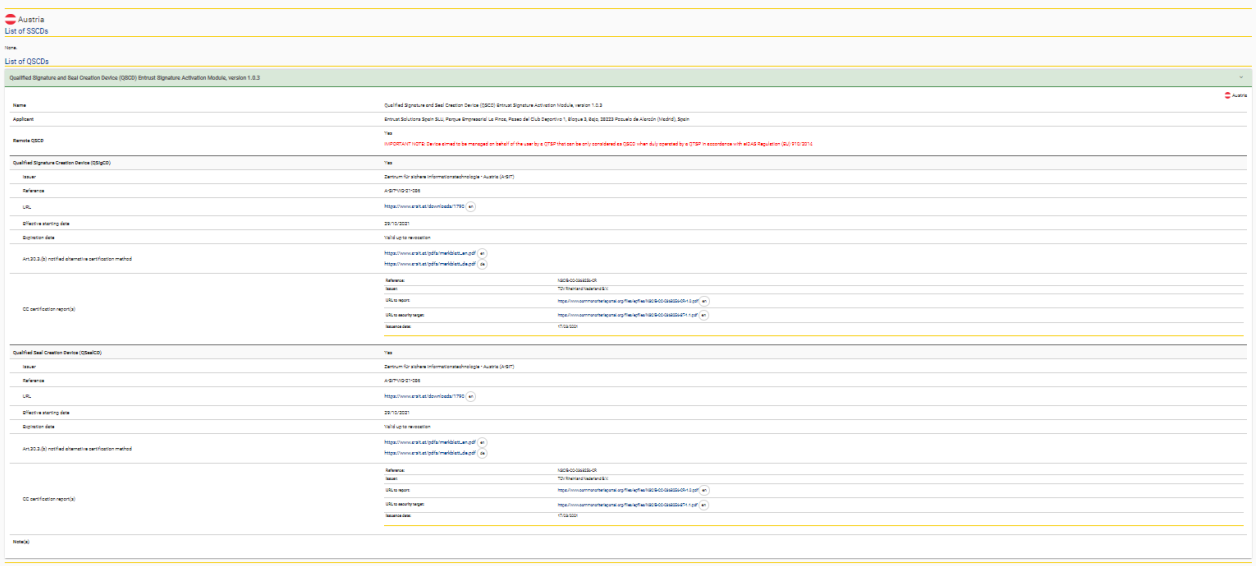


- **RSeC** (RemoteSeal Client) - klientská komponenta určená pro strojové pečetění dokumentů a pro integraci do spisové služby nebo jiného systému, který potřebuje autonomně vytvářet kvalifikované pečeti. Existuje ve vícero variantách pro snadnou integraci do různých systémů.
- **RemoteSealProFi** - klientská desktop aplikace pro Windows, která slouží ke správě pečetění dané organizace a ručnímu vytváření kvalifikovaných pečetí.
- **ESC** (Evolved Signature Core) - základní aplikační server provozovaný I.CA, přes který jdou veškeré komunikace týkající se pečetění z klientských komponent.
- **SAM** (Signature Activation Module) - povinná součást QSCD pro vzdálený podpis/pečeť, který zajišťuje kontrolu přístupu ke klíčům uloženým na HSM modulu
- **HSM** (Hardware Security Module) - povinná součást QSCD pro vzdálený podpis/pečeť, která zajišťuje samotné bezpečné generování, uchovávání a používání privátních klíčů.
- **AS** (Authorization Server) - aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření SAD (Signature Activation Data) tj. datové struktury autorizující použití příslušného privátního klíče pro podpis příslušných dat pro SAM.

Použité QSCD

Služba využívá certifikované Remote QSealCD skládající se ze:

- SAM modulu Entrust SAM
  - https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD



- HSM modulu Entrust nShield Connect XC

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 Parts 1, 2 & 3 (ISO/IEC 15408-1, ISO/IEC 15408-2 & ISO/IEC 15408-3)
Certificate number	**CC-21-0368256**
	TÜV Rheinland Nederland B.V. certifies:
Certificate holder	**Entrust** **Minneapolis1187 Park Place, Shakopee, MN 55379, USA**
TOE developer	**nCipher Security Limited (an Entrust company)** **One Station Square, Cambridge CB1 2GA, UK**
Product and assurance level	**nShield Solo XC Hardware Security Module v12.60.15** Assurance Package: ▪ EAL4 augmented with AVA_VAN.5 and ALC_FLR.2 Protection Profile Conformance: ▪ EN419221-5 Protection Profiles for TSP Cryptographic Modules - Part 5, Version 1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020
Project number	**0368256**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2 and ALC_FLR.3

SOGIS Mutual Recognition Agreement for components up to EAL7 and ALC_FLR.3

Validity	Date of 1st issue : **17-03-2021** Certificate expiry : **17-03-2026**

PRODUCTS RvA C 078
Accredited by the Dutch Council for Accreditation

[redacted]

TÜVRheinland®
Precisely Right.

www.tuv.com/nl

Version 2020-4

Varianty klientských komponent

RemoteSeal poskytuje několik variant klientských komponent, které je možné rozdělit do dvou skupin:

- Klientské komponenty pro ruční pečetění uživatelem, tedy člověkem
- Klientské komponenty pro automatizované/strojové pečetění

Klientské komponenty pro ruční pečetění uživatelem, tedy člověkem

Pro ruční pečetění člověkem - tj. zaměstnanci dané organizace existuje desktopová GUI aplikace pro Windows RemoteSealProFi, která umožňuje ručně vybrat dokument/dokumenty a opatřit je kvalifikovanou elektronickou pečetí.
Aplikace RemoteSealProFi má zároveň správcovskou (administrátorskou) funkci - uživatel s rolí správce pečetění organizace pomocí aplikace spravuje instance RSeC, další uživatele a obnovu pečetícího certifikátu.

Klientské komponenty pro automatizované/strojové pečetění

Klientské komponenty pro automatizované/strojové pečetění souhrnně nazýváme RSeC (Remote Seal Client) a jsou určeny pro integraci do informačního systému/aplikace třetí strany, který má autonomně pečetit dokumenty jejichž je organizace původcem.
RSeC je vždy založen na nativním (C/C++) jádře, ke kterému je pak nadstavba pro danou platformu:

- **jRSeC** (Linux i Windows) - nadstavba nad RSeC určená pro integraci do aplikací v jazyce Java formou Java class library.
- **RSeC.NET** (Linux i Windows) - nadstavba nad RSeC určená pro integrací do aplikací v jazyce .NET
- **RSeProxy** (Windows) - serverová aplikace určená pro instalaci do sítě klienta, která do vnitřní sítě klienta poskytuje SOAP webové služby pro funkcionalitu pečetění, přičemž vůči systému RemoteSeal vystupuje jako klientská komponenta RSeC.

Zřízení služby

1. Prvním krokem je uzavření smlouvy mezi organizací a I.CA.
2. Oprávněná osoba žadatele (tj. organizace) dohodne se zástupcem I.CA způsob vydání osobního autentizačního komerčního certifikátu – obvykle navštíví pobočku RA v sídle společnosti I.CA s potřebnými doklady ke zřízení služby I.CA RemoteSeal na danou organizaci.
3. Operátor RA vydá oprávněné osobě osobní autentizační komerční certifikát na čipovou kartu Starcos 3.5 nebo 3.7. Tato osoba se tímto automaticky stává prvním (a v tento okamžik prozatím také jediným) správcem služby pečetění pro danou organizaci.
4. Operátor RA provede zřízení služby I.CA RemoteSeal vč. vydání kvalifikovaného pečetícího certifikátu (kvalifikovaný certifikát pro elektronickou pečeť) pro danou organizaci, přičemž privátní klíč pro tento certifikát je generován a spravován QSCD zařízením služby I.CA RemoteSeal.
5. V rámci vydání pečetícího certifikátu oprávněná osoba žadatele podepisuje dokumentaci k vydání certifikátu, přičemž tyto mohou být podepsány:
   - klasicky vlastnoručním podpisem na papír, nebo
   - bezpapírově/elektronicky pomocí osobního autentizačního komerčního certifikátu oprávněné osoby (v tom případě žadatel podepisuje pouze smlouvu)

6. Oprávněná osoba žadatele odchází z RA s čipovou kartou s autentizačním komerčním certifikátem.

Uživatelské účty RemoteSealProFi

Aplikace RemoteSealProFi umožňuje na jednom PC (přesněji jednomu uživateli Windows na daném PC) mít současně vytvořeno více uživatelských účtů a při startu aplikace se přihlásit do uživatelského účtu dle volby.

Uživatelské účty jsou dvojího druhu:

- Přenosný uživatelský účet
- Fixní uživatelský účet

Přenosný uživatelský účet

Přenosný uživatelský účet není vázán na jedno konkrétní PC, ale je možné k němu přistupovat z různých PC, na nichž je nainstalována aplikace RemoteSealProFi.
Pro autentizaci uživatele slouží:

- čipová karta Starcos 3.5 nebo 3.7 s (autentizačním) osobním komerčním certifikátem
- PIN k čipové kartě
- heslo uživatele ke službě RemoteSeal

Uživatel, jenž pro autentizaci používá výše uvedené, si může na libovolném množství PC založit přenosný uživatelský účet a pomocí čipové karty atd. se do aplikace přihlásit a dále s ní pracovat. Bez čipové karty však přihlášení k přenosnému uživatelskému účtu není možné.

Aktivace přenosného uživatelského účtu

Pro aktivaci přenosného uživatelského účtu je potřeba mít čipovou kartu s komerčním certifikátem, na který byl uživatelský účet založen (buďto na RA nebo správcem pečetění).
K aktivaci přenosného uživatelského účtu dojde při prvním pokusu o přihlášení do RemoteSealProFi pomocí příslušné čipové karty s komerčním certifikátem. Tedy:

1. Uživatel zvolí přidání uživatelského profilu => přenosný profil
2. Vloží čipovou kartu, případně vybere příslušný certifikát
3. Zadá PIN
4. Aplikace detekuje, že tento uživatelský účet ještě nebyl aktivován a vyzve uživatele k volbě hesla pro službu RemoteSeal
5. Po dvojím zadání hesla proběhne aktivace a uživatel se může standardně přihlásit do aplikace.

Poznámka

To je případ i prvotní aktivace oprávněnou osobou, jež navštívila RA pro zřízení služby.

Fixní uživatelský účet

Fixní uživatelský účet je oproti tomu vázán na konkrétní PC, resp. na konkrétní uživatelský profil v OS Windows, na kterém proběhla aktivace a jinde se k němu není možné přihlásit.
K přihlášení však nejsou potřeba žádné fyzické markanty, postačuje:

- data uložená na daném PC (a uživatelském profilu Windows) jež vznikla při aktivaci
- heslo uživatele ke službě RemoteSeal

Použití fixních uživatelských účtů však vyžaduje použití doplňkového zabezpečení zdroje komunikace (viz níže).

Aktivace fixního uživatelského účtu

Po zřízení nového fixního uživatelského účtu (správcem pečetění) obdrží uživatel tzv. aktivační mail, který v příloze obsahuje tzv. aktivační soubor. Tento slouží pro provedení aktivace následovně:

1. Uživatel zvolí přidání uživatelského profilu => fixní profil
2. Vloží aktivační soubor (jež dostal mailem)
3. Následně mu na telefonní číslo (uvedené při zřízení účtu) přijde tzv. aktivační SMS kód
4. Tento kód uživatel přepíše do aplikace
5. V případě správného zadání je následně vyzván k volbě hesla pro službu RemoteSeal
6. Po dvojím zadání hesla proběhne aktivace a uživatel se může standardně přihlásit do aplikace.

Uživatelské role RemoteSealProFi

Jednotliví uživatelé aplikace RemoteSealProFi mají v rámci daného pečetícího accountu dané organizace vždy jednu ze dvou rolí:

- **správce pečetění**
  - Má přístup do administrátorské sekce RemoteSealProFi, kde může:
    - spravovat instance RSeC (přidávání, (od)blokace, přejmenování, zrušení)
    - požádat o vydání následného pečetícího certifikátu
    - vidět a nastavovat okamžik nasazení nového (následného) pečetícího certifikátu
    - spravovat další uživatele pod daným pečetícím accountem (přidávání, (od)blokace, zrušení, nastavení role) *(a to vč. možnosti přidat dalšího správce pečetění)*
  - Může libovolně vytvářet kvalifikované elektronické pečetě.
- **běžný uživatel**
  - Nemá přístup do administrátorské sekce RemoteSealProFi.
  - Může libovolně vytvářet kvalifikované elektronické pečetě.

Aktivace RSeC

Komponenta RSeC pro autentizaci vůči systému RemoteSeal vyžaduje:

- přístupový soubor tzv. RSealAccessFile
- heslo (pro instanci RSeC definovanou daným přístupovým souborem)

Držitel certifikátu (organizace) může současně provozovat více různých aplikací, které pečetí pomocí stejného accountu RemoteSeal, tj. stejného pečetícího certifikátu. Tedy může provozovat více samostatných instancí RSeC, přičemž pro každou je potřeba vygenerovat dvojici přístupový soubor + heslo.

Generování přístupového souboru provádí uživatel (typicky zaměstnanec dané organizace) s rolí správce pečetění dané organizace v administrátorské části aplikace RemoteSealProFi:

1. Uživatel se přihlásí do aplikace RemoteSealProFi
2. Otevře administrátorskou část aplikace => správa RSeC => Přidat nový
3. Pro ověření zadá své heslo a následně vyplní
   - název nové instance RSeC (určeno zejména pro interní identifikaci v rámci dané organizace - např.: "Spisová služba - server 1")
   - heslo pro novou instanci RSeC
   - znovu heslo pro novou instanci RSeC
4. RemoteSealProFi poté provede založení nové instance RSeC a po dokončení nabídne uložení vygenerovaného aktivačního souboru na disk

Do komponenty RSeC se pak přístupový soubor a heslo předávají přes API příslušné knihovny - způsob jejich vložení/uložení do příslušné aplikace je tedy odvislý od implementace v dané aplikaci. Z principu je možné, aby přístupový soubor "ležel" někde na disku daného stroje, na kterém probíhá pečetění přes RSeC. Heslo by však mělo být danou aplikací uloženo bezpečnějším způsobem a nikdy by nemělo ležet v plaintextu někde v souboru.
Volající aplikace pak předává přístupový soubor a heslo k němu pro každé pečetění, resp. pro každou inicializaci objektu třídy SealClient. RSeC si sám nezajišťuje žádnou persistenci přístupového souboru ani hesla.

Opečetění dokumentu

Opečetění dokumentu přes RSeC

1. Volající aplikace vytvoří instanci třídy SealClient z RSeC, které předá přístupový soubor a heslo k němu
2. Volající aplikace předá do RSeC 1 až N dokumentů k opečetění spolu s nastavením opečetění jednotlivých dokumentů (viditelný/neviditelný podpis, formát, přidání časového razítka, atp.)
3. RSeC připraví dokumenty k podpisu, založí pro každý dokument pečetící transakci, autorizuje použití privátního klíče na HSM modulu, získá z backendu vytvořenou podpisovou strukturu vč. případného časového razítka a sestaví kompletní podepsané dokumenty
4. Sestavené podepsané dokumenty RSeC vrátí volající aplikaci

Opečetění dokumentu přes RemoteSealProFi

1. Uživatel se přihlásí do aplikace RemoteSealProFi
2. Uživatel vybere "profil pečetě" podle kterého chce pečetit
   - profil pečetě jsou de-facto uložené parametry vytvářené pečetě (viditelný podpis, vložení časového razítka, atp), které mohou sloužit jako fixně předepsané parametry pro druh dokumentu (např.: všechna potvrzení o studiu mají stejné parametry) - jako základní nastavení parametrů, které jsou pro daný případ uživatele následně upraveny a je možné je sdílet s dalšími uživateli pod stejným pečetícím accountem.
3. Volitelně uživatel upraví parametry pečetě
4. Následně uživatel vybere dokumenty, které se mají opečetit a potvrdí
5. RemoteSealProFi postupně opečetí všechny vybrané dokumenty

Obnova pečetícího certifikátu

S předstihem před koncem platnosti aktuální pečetícího certifikátu (30, 15 a 5 dní) jsou uživatelé s rolí správce pečetění informováni e-mailem o blížícím se konci platnosti pečetícího certifikátu. Správce pečetění:

1. Se přihlásí do aplikace RemoteSealProFi a otevře administrátorskou část aplikace => správa pečetícího certifikátu
2. Stiskne tlačítko obnovit certifikát
3. Aplikace zajistí vytvoření žádosti o následný certifikát a zobrazí uživateli detail servisní transakce k podpisu žádosti o vydání následného certifikátu
4. Uživatel stiskne tlačítko podepsat a zadá své heslo ke službě RemoteSeal
5. Služba následně zajistí vydání následného pečetícího certifikátu a po jeho vydání naplánuje odložené nasazení nově vydaného pečetícího certifikátu (za + 15 dní)
6. Správce pečetění si může po vydání certifikátu v aplikaci zobrazit informace o novém certifikátu, uložit si nový certifikát do souboru, vidět přesný čas plánovaného nasazení nového certifikátu a tento čas může v aplikace také změnit.

Podporované formáty podpisu

- **CAdES**
  - CAdES-B-B, CAdES-B-T
  - Dle normy EN 319 122, ve variantách:
    - Interní
    - Externí
- **PAdES**
  - PAdES-B-B, PAdES-B-T
  - Dle normy EN 319 142, ve variantách:
    - Neviditelný
    - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
- **XAdES**
  - 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.
- **ASiC-E XAdES**
  - ASiC-E XAdES-B a ASiC-E XAdES-T
  - Dle normy ETSI TS 103 174, přičemž:

- Je možné opečetit právě jeden datový objekt právě jednou kvalifikovanou pečetí
- Není podporováno rozšíření stávajícího ASiC-E souboru o další pečeť/podpis, ani několik podpisů/pečetí v rámci jednoho ASiC-E souboru.
- Pro soubory typu .txt, .pdf, .xml, .png je implicitně doplněn příslušný mimetype odpovídající dané příponě. Tuto implicitní volbu je možné v rozhraní explicitně přenastavit na jiný mimetype, popř. lze explicitní cestou nastavit mimetype pro ostatní (implicitně nepodporované) typy datových objektů.
- Samotná XAdES pečeť uvnitř ASiC-E kontejneru obsahuje pouze minimální nezbytně nutnou množinu podepisovaných a nepodepisovaných properties vyžadovanou danou ETSI normou.

Doplňkové zabezpečení zdroje komunikace

Pro jednotlivé pečetící accounty je možné nastavit doplňkové zabezpečení zdroje komunikace, které umožňuje omezit, "odkud" může daná aplikace pro daný account kontaktovat službu RemoteSeal - např.: že fixní uživatelské účty RemoteSealProFi musejí komunikovat přes určitou VPN mezi klientem a I.CA, nebo musí být tato komunikace zabezpečena mTLS spojením s konkrétním klientským certifikátem atp.

Dostupnost:

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

Příloha č. 2

BEZPEČNOSTNÍ PRAVIDLA PRO VÝZNAMNÉ DODAVATELE dle ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI (č. 181/2014 Sb.) a VYHLÁŠKY č. 82/2018 Sb.

1 PERSONÁLNÍ BEZPEČNOST

1.1 Smluvní partner Státního ústavu pro kontrolu léčiv (dále jen „SÚKL“) a jeho případní subdodavatelé (smluvní partner a subdodavatelé dále jen souhrnně „dodavatel“) mají povinnost ve svých interních procesech realizovat tato opatření:

a) mít stanoven vlastní plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí a který obsahuje formu, obsah a rozsah:

i. poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
ii. potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role, nebo zajišťujících podporu provozu informačního systému SÚKL;

b) mít určeny osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;

c) v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;

d) pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti;

e) v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;

f) zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;

g) v případě ukončení smluvního vztahu s administrátory a osobami podílejících se na podpoře vývoje či provozu systému SÚKL či jakékoliv jeho infrastrukturní části, zajišťovat předání odpovědností, zrušení jejich přístupových účtů a informovat SÚKL o této skutečnosti;

h) stanovit interní pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany administrátorů a osob zastávajících bezpečnostní role;

i) vést o provedených školeních přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.2 SÚKL si vyhrazuje právo vést záznamy a prověřovat činnosti dodavatele, vést záznamy o incidentech a nestandardních činnostech zaměstnanců a dalších osob působících ve prospěch dodavatele (dále jen „zaměstnanci dodavatele“). Na základě těchto záznamů má oprávnění vyhodnocovat důvěryhodnost a spolehlivost zaměstnanců dodavatele, zejména při situacích vzniklých bezpečnostních incidentů. V případě identifikovaného rizika oznámí SÚKL nesoulad dodavateli a obě strany vejdou v jednání pro řešení této situace.

1.3 Kvalifikace zaměstnanců dodavatele musí odpovídat vykonávané pracovní pozici (vykonávané práci a úrovni zabezpečení).

2 FYZICKÁ BEZPEČNOST, POŽÁRNÍ OCHRANA A BOZP

2.1 Dodavatel jako zaměstnavatel při provádění prací při plnění smlouvy odpovídá za dodržování předpisů BOZP a PO svými zaměstnanci v prostorách SÚKL, popř. dalšími fyzickými osobami vykonávajícími práci v jeho prospěch a odpovídá za dodržování podmínek vstupu osob a vjezdu vozidel do areálů, objektů a na pozemky SÚKL a bezpečnostního režimu pro ně stanoveného.

3 BEZPEČNOSTNÍ POVĚDOMÍ

3.1 Každý zaměstnanec dodavatele musí být prokazatelně proškolen a mít znalosti příslušných interních předpisů SÚKL souvisejících s předmětem plnění smlouvy. Za proškolení zaměstnanců dodavatele (v roli provozovatele) a za jejich prokazatelné seznámení s požadavky smlouvy a jejích příloh odpovídá dodavatel.

4 IDENTIFIKACE

4.1 Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své ICT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých určených systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji. Na technická zařízení, se kterými zaměstnanci dodavatele přistupují do vymezených částí vnitřní infrastruktury SÚKL, se ze strany SÚKL pohlíží jako na BYOD a pro jejich konfiguraci se vyžaduje dodržování minima dle vnitřního předpisu SÚKL S-069, který je dodavateli předán.

4.2 Každý zaměstnanec dodavatele, pokud přistupuje k interním systémům SÚKL, má u SÚKL veden a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy.

5 AUTENTIZACE

5.1 Podmínky pro autentizaci při využití ICT infrastruktury SÚKL:

a) k jednoznačné identifikaci privilegovaných uživatelů určených systémů se preferovaně využívá vícefaktorová autentizace;

b) ověření heslem - pokud není možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace heslem o minimální délce 17 znaků, kdy mezi znaky musí být minimálně jedno velké písmeno, jedno malé písmeno, jedna číslice a jeden metaznak z možností: #, $, &, %, !, ?, +, - Heslo musí být měněno nejpozději po 18 měsících, případně v kratším intervalu vyžadovaném aktuálně nastavenou politikou hesel, a nesmí se následně zopakovat v následných 12ti změnách.

5.2 Pro vzdálený přístup zaměstnanců dodavatele předkládá dodavatel podklady pro vyplnění žádosti o vzdálený přístup, podle které jsou poté nastavena oprávnění. Žádost podepisuje oprávněná osoba dodavatele jednat ve věcech plnění smlouvy.

5.3 Dodavatel odpovídá za činnosti svých zaměstnanců, popřípadě dalších fyzických osob vykonávajících práci v jeho prospěch, které musí být v souladu s pravidly, předanými ze strany SÚKL. Veškeré škody, které vzniknou porušením těchto pravidel zaměstnanci dodavatele nebo dalšími fyzickými osobami vykonávajícími práci v jeho prospěch, jdou k tíži dodavatele, který je povinen tyto škody v plném rozsahu SÚKL nahradit.

6 AUTORIZACE

6.1 Zaměstnanci dodavatele jsou povinni v ICT infrastruktuře SÚKL využívat privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé ani administrátoři nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou určeného systému a v žádném případě nesmí umožnit pracovat pod tímto účtem jiným osobám.

6.2 Zaměstnanci dodavatele jsou informováni SÚKL, ke kterým chráněným informacím SÚKL mají při plnění smlouvy přístup a jak s nimi mohou nakládat. Tyto informace vyplývají ze smlouvy a dodavatel je oprávněn a povinen své zaměstnance s příslušnými částmi smlouvy prokazatelně seznámit. Jakékoliv manipulace a další operace s chráněnými informacemi SÚKL, které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povoleny.

7 KONCOVÁ PRACOVNÍ STANICE

7.1 Pro přístup k systémům SÚKL jsou standardně použity vlastní prostředky dodavatele (HW, SW). Dodavatel odpovídá za to, že nejsou používány v rozporu s licenčními podmínkami produktů.
7.2 Přístup výpočetní techniky dodavatele (PC, notebooky) k chráněným interním informacím a k informačním a telekomunikačním systémům je podmíněn schválením příslušného pracoviště SÚKL a odpovědnou osobou systému.
7.3 Pracovní stanice dodavatele přistupující prostřednictvím VPN musí splňovat podmínky uvedené pro používání BYOD v interní směrnici SÚKL S-069.

8 UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

8.1 Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou následující:
a) užití pouze kryptografických prostředků podle doporučení vydávaných a aktualizovaných NÚKIB
b) šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA nebo CA, které explicitně důvěřují obě strany;
c) pro webové servery prezentující data pocházející z určených informačních systémů mimo samotný systém používat HTTPS protokol;
d) pro webové servery prezentující data pocházející z určených systémů pro uživatele mimo SÚKL se používá certifikát obecně uznávané certifikační autority.

9 MONITORING

9.1 Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům SÚKL může být nepřetržitě zaznamenáván, monitorován a vyhodnocován. Události v systémech jsou SÚKL zaznamenávány do logů.
9.2 Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.
9.3 V souladu s příslušnými ustanoveními smlouvy je dodavatel povinen neprodleně po zjištění hlásit SÚKL každý nastalý bezpečnostní incident.

10 OCHRANA MÉDIÍ

10.1 Uložení chráněných informací SÚKL na přenosná média a případný transport médií mimo prostory SÚKL podléhá jeho schválení.
10.2 V případě ukládání chráněných informací SÚKL na přenosná média má dodavatel povinnost, pokud je to technicky možné, ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.
10.3 Dodavatel je povinen zajistit likvidaci operativních dat obsahujících chráněné informace SÚKL ihned po pominutí účelu jejich zpracování a/nebo uložení způsobem dle právních předpisů či metodik vydaných NÚKIB, případně ÚOOÚ. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vést protokol.

11 BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

11.1 Dodavatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události:
a) odpovědné osobě SÚKL (osoba oprávněná jednat ve věcech plnění smlouvy a manager kybernetické bezpečnosti). Ohlášení provede mailem (případně telefonicky) v termínu bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události / incidentu.
b) v ohlášení uvede:
   i. datum a čas zjištění;
   ii. povahu události / incidentu;
   iii. zdroje události;

iv. cíle / oběti události;
v. okamžité i potencionální dopady;
vi. přijatá či navrhovaná opatření k omezení dopadů, případně eliminaci opakování.

12 AUDIT DODAVATELE (PRAVIDLA ZÁKAZNICKÉHO AUDITU)

12.1 OPRÁVNĚNÍ K PROVEDENÍ AUDITU DODAVATELE

a) SÚKL si v souladu s ustanovením smlouvy vyhrazuje právo provádět audity dodavatele.

b) SÚKL s dostatečným předstihem alespoň 5 pracovních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že SÚKL se zavazuje postupovat tak, aby nenarušil provozní potřeby dodavatele.

c) SÚKL si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele) v souvislosti s plněním smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.

d) Dokumentace auditů prováděných SÚKL tvoří pro každý audit:

i. oznámení o auditu a plán auditu;
ii. dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné);
iii. zpráva z auditu;
iv. písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem (pokud je nezbytné pro dokumentování nálezů);
v. záznam o zjištění (nápravných opatřeních a následné kontrole).

f) Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění:

i. dodavatel navrhne na základě zjištění uvedených v závěrečné auditní zprávě návrh opatření a termíny řešení a předá jejich seznam SÚKL k odsouhlasení;
ii. SÚKL potvrdí souhlas s navrženými opatřeními. Souhlas vydává osoba oprávněná jednat ve věcech smlouvy.

12.2 NÁPRAVNÁ OPATŘENÍ

a) Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření;

b) Zprávu o realizovaných opatřeních dodavatel oznamuje a předává SÚKL cestou člena jeho auditního týmu.

13 PODMÍNKY PŘI UKONČENÍ SMLOUVY

13.1 V případě ukončení smluvního vztahu musí být ukončeny veškeré přístupy dodavatele a jeho zaměstnanců k aktivům společnosti (VPN, systémy, informace) nejpozději k termínu ukončení smluvního vztahu.

13.2 Pokud byla zaměstnancům dodavatele poskytnuta aktiva SÚKL, musí být tato aktiva vrácena nejpozději k termínu ukončení smluvního vztahu.

13.3 Pokud byla dodavateli poskytnuta informační aktiva (data) SÚKL, musí být nejpozději k termínu ukončení smluvního vztahu vrácena a beze zbytku smazána způsobem určeným v právních předpisech o kybernetické bezpečnosti, či metodice NÚKIB, resp. ÚOOÚ, ze všech systémů dodavatele a nosičů dodavatele taková aktiva obsahujících. O smazání či předání takových aktiv musí být vypracován protokol, který je předán SÚKL.

13.4 V případě předčasného ukončení smluvního vztahu jiným způsobem než splněním závazku (např. výpovědí, odstoupením od smlouvy, dohodou o ukončení smlouvy apod.), mohou být přístupy dodavatele, pokud je to nutné, ze strany SÚKL ukončeny před uplynutím doby trvání smluvního vztahu.