**Ev. č. 18/166-1**

 **Čj. 8529/2024-UVCR**

**Dodatek č. 1**

**ke Smlouvě o poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal čj. 29644/2018-OIT-2**

**První certifikační autorita, a.s.**

se sídlem Podvinný mlýn 2178/6, 190 00 Praha 9

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

IČ: 26439395

DIČ: CZ26439395

zastoupená: Ing. Petrem Budišem, Ph.D., MBA, předsedou představenstva a

Ing. Romanem Kučerou, členem představenstva

Bankovní spojení: Československá obchodní banka, a.s.

Číslo účtu: XXXXXX

(dále jen „Poskytovatel“)

**a**

**Česká republika – Úřad vlády České republiky**

se sídlem nábřeží Edvarda Beneše 128/4, 118 01 Praha 1 – Malá Strana

IČ: 00006599

DIČ: CZ00006599

zastoupená: Ing. Jitkou Křupkovou, ředitelkou Odboru informatiky, na základě vnitřního předpisu

Bankovní spojení Česká národní banka

Číslo účtu: 4320001/0710

(dále jen „Objednatel“)

(dále také jen „smluvní strany“)

**uzavírají níže uvedeného dne, měsíce a roku tento dodatek č. 1** **ke Smlouvě o poskytování služby vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal, čj. 29644/2018-OIT-2 (dále jen „Dodatek“).**

**I. Předmět dodatku**

A) V Článku V. se stávající odstavec 1. nahrazuje novým odstavcem 1., který zní:

„1. Úhrada za poskytování služby I.CA RemoteSeal je realizována formou nákupu předplaceného balíčku pečetí, případně předplaceného balíčku časových razítek. Cena balíčků závisí na počtu kvalifikovaných elektronických pečetí či časových razítek a řídí se následující tabulkou.

|  |  |  |
| --- | --- | --- |
| Velikost balíčku (ks) | Cena za balíček kvalifikovaných pečetí I.CA RemoteSeal (Kč bez DPH) | Cena za balíček časových razítek (Kč bez DPH) |
| 50 000 | 37 000 |  25 000 |
| 100 000 | 45 000 | 30 000 |
| 200 000  |  58 000 |  40 000 |
| 500 000 |  96 000 |  75 000 |

Balíček pečetí či časových razítek je nutné vyčerpat maximálně do tří let od zahájení jeho čerpání.“

B) Příloha č. 1 se nahrazuje novou přílohou č. 1 reflektující aktuální technické řešení služby.

**II. Závěrečná ustanovení**

* 1. Ostatní ustanovení smlouvy, nedotčená tímto Dodatkem, zůstávají beze změny.

Tento Dodatek nabývá platnosti dnem jeho podpisu oběma smluvními stranami a účinnosti dnem jeho uveřejnění v Registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv. Tento Dodatek je uzavřen elektronicky. Objednatel a Poskytovatel obdrží elektronický originál uzavřeného dodatku.

2. Smluvní strany prohlašují, že si tento Dodatek přečetly, jeho obsahu rozumí a na základě své svobodné vůle připojují své podpisy.

V Praze 29. 02. 2024 V Praze 01. 03. 2024

**První certifikační autorita, a.s. Česká republika – Úřad vlády České republiky**

……………………………………………….. …………………………………………

 Ing. Petr Budiš, Ph.D., MBA, v. r. Ing. Jitka Křupková v. r.

 ředitelka Odboru informatiky

 předseda představenstva

………………………………………………....

 Ing. Roman Kučera v. r.

 člen představenstva

**Příloha č. 1**

**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
* HSM modulu Entrust nShield Connect XC



## 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/nevidititelný 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

### Připojení časového razítka

§ 11 odst. 2 zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce stanoví, že veřejnoprávní podepisující, který zapečetil elektronický dokument, kterým činí úkon nebo právně jedná, způsobem podle § 8, a osoba, která zapečetila elektronický dokument, kterým činí úkon při výkonu své působnosti, způsobem podle § 8, opatří zapečetěný elektronický dokument kvalifikovaným elektronickým časovým razítkem. Časové razítko je možné připojit jak v rámci pečetící transakce, tak samostatným procesem. Časová razítka zakoupená v rámci balíčku časových razítek je možné čerpat jak v rámci pečetících transakcí, tak pro samostatné připojení časového razítka.

## Obnova pečetícího certifikátu

S předstihem před koncem platnosti aktuálního 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 aplikaci 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.