**SMLOUVA O POSKYTOVÁNÍ SLUŽEB ELEKTRONICKÉ PEČETĚNÍ A ČASOVÁ RAZÍTKA**

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku (dále jen „**Smlouva**“)

Smluvní strany

Objednatel:

|  |  |
| --- | --- |
| Obchodní firma | **Institut plánování a rozvoje hlavního města Prahy** |
| Se sídlem | Vyšehradská 2077/57, 128 00 Praha 2 – Nové město |
| Zapsaná | v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. Pr 63 |
| IČ | 70883858 |
| DIČ | CZ70883858 |
| Zastoupená | Mgr. Adamem Švejdou, zástupcem ředitele pro ekonomickou  a provozní činnost |
| Bankovní spojení |  |

(dále jen „**Objednatel**“)

## a

Poskytovatel:

|  |  |
| --- | --- |
| Obchodní firma | **ICZ.DMS a.s.** |
| Se sídlem | Na hřebenech II 1718/10, Nusle, 140 00 Praha 4 |
| Zapsaná | v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 23140 |
| IČ | 06696805 |
| DIČ | CZ699000372 |
| Zastoupená | Antonínem Drahovzalem, na základě plné moci |
| Bankovní spojení |  |

(dále jen „**Poskytovatel**“)

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

1. Předmět Smlouvy
   1. Předmětem smlouvy je závazek Poskytovatele poskytovat nebo zprostředkovat poskytnutí služby kvalifikovaných elektronických pečetí a časových razítek (dále „**Služby**“) a závazek Objednatele tyto Služby převzít a zaplatit za ně sjednané ceny. Bližší specifikace Služeb je uvedena v Příloze č. 1 Smlouvy.
2. Termín zahájení poskytování služeb
   1. Poskytovatel se zavazuje zahájit poskytování Služby (zprovoznit Služby) v prostředí Objednatele nejpozději do 21 dnů od účinnosti této smlouvy za předpokladu poskytnutí nezbytné součinnosti ze strany Objednatele.
3. Cena Služeb a platební podmínky
   1. Cena za poskytování Služby se skládá z paušálního poplatku a ceny za 1 ks pečetění s ohledem na množství odebraných elektronických pečetí a časových razítek dle specifikace uvedené v Příloze č. 2 Smlouvy. Dále pak z jednorázové platby za zprovoznění služby také uvedena v Příloze č. 2 Smlouvy
   2. Ceny uvedené ve Smlouvě jsou uvedeny bez a včetně DPH ve výši platné ke dni uzavření této Smlouvy. Dojde-li ke změně sazby DPH, bude Poskytovatelem DPH účtována podle právních předpisů platných a účinných v době uskutečnění zdanitelného plnění. Takováto změna Smlouvy nemusí být sjednána formou písemného dodatku k této Smlouvě.
   3. Poskytovatel vystaví a zašle Objednateli příslušnou fakturu za poskytnuté Služby vždy bez zbytečného odkladu v **měsíci** následujícím po skončení příslušného ukončeného **měsíce**, ve kterém byla poskytována příslušná služba, a to včetně výkazu poskytnutých služeb.
   4. Faktury jsou splatné do patnácti (15) kalendářních dnů od jejich doručení. K uhrazení faktury dojde připsáním částky z účtu Objednatele ve prospěch účtu Poskytovatele.
   5. Jednotlivé faktury musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných právních předpisů, zejména § 29 zák. č. 235/2004 Sb., o dani z přidané hodnoty v platném znění a § 435 zák. č. 89/2012 Sb., občanského zákoníku (dále „**Občanský zákoník**“).
4. Práva a povinnosti Smluvních stran
   1. V rámci realizace předmětu plnění Smlouvy má každá Smluvní strana zejména následující povinnosti:
      1. vzájemně spolupracovat a poskytovat druhé Smluvní straně veškeré informace potřebné pro řádné plnění svých povinností vyplývajících ze Smlouvy;
      2. neprodleně informovat druhou Smluvní stranu o vzniku nebo hrozícím vzniku překážky plnění mající významný vliv na řádné a včasné plnění dle Smlouvy;
      3. poskytovat druhé Smluvní straně úplné, pravdivé a včasné informace o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění dle Smlouvy;
      4. plnit své povinnosti vyplývající ze Smlouvy tak, aby nedocházelo k prodlení s plněním povinností vázaných k jednotlivým termínům a úhradě splatných jednotlivých peněžních dluhů.
5. Ochrana informací
   1. Objednatel i Poskytovatel jsou si vědomi toho, že v rámci plnění této Smlouvy:

### si mohou vzájemně úmyslně nebo i opomenutím poskytnout informace, které budou považovány za důvěrné, přičemž tyto informace mohou též představovat předmět obchodního tajemství ve smyslu ustanovení § 504 Občanského zákoníku (dále jen „Důvěrné informace“);

### mohou jejich zaměstnanci získat vědomou činností druhé Smluvní strany nebo i jejím opominutím přístup k Důvěrným informacím druhé strany.

* 1. Důvěrné informace nezahrnují informace již veřejně známé a informace získané od třetí strany, která byla oprávněna tyto informace šířit.
  2. Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace.

1. OCHRANA OSOBNÍCH ÚDAJŮ
   1. Objednatel a Poskytovatel shodně prohlašují, že v rámci realizace plnění dle této Smlouvy může docházet ke zpracování osobních údajů Objednatelem i Poskytovatelem ve smyslu zákona č. 110/2019 Sb., o zpracování osobních údajů (dále jen „**ZZOÚ**“) či ve smyslu Nařízení Evropského parlamentu a rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů) (dále jen „**GDPR**“). Smluvní strany se proto dohodly na podmínkách zpracování osobních údajů odpovídajících zejména požadavkům § 28 odst. 1 a 3 GDPR, které řeší vztahy mezi Objednatelem jako správcem, případně zpracovatelem ve vztahu k osobním údajům jiných správců zapojených do projektu a Poskytovatelem jako zpracovatelem, případně dalším zpracovatelem.
   2. Poskytovatel jakožto zpracovatel se v případě, že v rámci realizace plnění dle této Smlouvy bude zpracovávat osobní údaje, zavazuje se je zpracovávat v souladu s požadavky GDPR a ZZOÚ, zejména:

* zohledňovat povahu zpracování,
* být nápomocen při vyřizování žádostí subjektu údajů,
* být nápomocen v plnění povinností dle čl. 32 až 36 GDPR
* umožnit audity, vč. inspekcí prováděných správcem či jím pověřenou osobou a poskytnout součinnost u těchto auditů.
  1. Typ zpracovávaných osobních údajů a kategorie subjektu údajů jsou stanoveny zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů a dalšími prováděcími předpisy, zejména se jedná o následující osobní údaje:
  2. adresát/odesílatel: jméno, příjmení, kontaktní údaje,
  3. uživatel informačního systému: jméno, příjemní, kontaktní údaje, login.
  4. Obecné zásady zpracování osobních údajů subjektů údajů: Objednatel jako správce pověřuje Poskytovatele zpracováváním osobních údajů v rozsahu nezbytném pro plnění Smlouvy a výhradně za účelem vyplývajícím z účelu Smlouvy a z účelu plnění poskytovaného dle Smlouvy, a to na základě pokynů správce. Toto pověření se vztahuje i na poddodavatele s tím, že Poskytovatel výslovně prohlašuje, že pokud do zpracování osobních údajů zapojí dalšího poddodavatele, bude tento poskytovat dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování osobních údajů splňovalo požadavky GDPR a ZZOÚ a zaváže jej smlouvou ke stejným povinnostem, které má ve vztahu k Objednateli. Poskytovatel výslovně prohlašuje, že v případě, pokud povinnost dále zapojený zpracovatel nesplní – odpovídá pak za všechny povinnosti ve vztahu k Objednateli on.
  5. Povinnosti Poskytovatele týkající se ochrany osobních údajů se Poskytovatel zavazuje plnit po dobu účinnosti Smlouvy, pokud z ustanovení Smlouvy výslovně nevyplývá, že mají trvat i po zániku její účinnosti.
  6. Poskytovatel je povinen postupovat při zpracování osobních údajů v souladu s touto Smlouvou a ZZOÚ a GDPR, a zpracovávat osobní údaje výlučně pro účel a v rozsahu, ve kterém mu byly předány, a při zpracování postupovat s řádnou péčí.
  7. V případě ukončení této Smlouvy je Poskytovatel povinen předat Objednateli protokolárně veškeré hmotné nosiče obsahující osobní údaje a smazat veškeré osobní údaje v elektronické podobě v jeho dispozici, neobdrží-li Poskytovatel od Objednatele písemně jiné pokyny.
  8. Poskytovatel je povinen dbát, aby žádný subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu subjektů údajů před neoprávněným zasahováním do soukromého a osobního života a zajistit veškerá práva subjektu údajů, která je z pozice zpracovatele povinen zajišťovat dle ZZOÚ a GDPR.
  9. Poskytovatel se zavazuje dodržovat všechny povinnosti, které mu jako zpracovateli vyplývají ze ZZOÚ a GDPR, jakož i z interních předpisů Objednatele, se kterými byl prokazatelně seznámen a jeho pokynů vydaných v souladu s účinnými právními předpisy.
  10. Pokud Poskytovatel zjistí, že Objednatel porušuje povinnosti stanovené ZZOÚ nebo GDPR, je povinen jej na to neprodleně upozornit.
  11. V případě, kdy je ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu provedena kontrola zpracování osobních údajů Poskytovatelem či v případě zahájení správního řízení ze strany Úřadu pro ochranu osobních údajů či jiného správního orgánu ve vztahu k zpracování osobních údajů Poskytovatelem dle této Smlouvy, je Poskytovatel tuto skutečnost povinen oznámit Objednateli a poskytnout mu veškeré informace o průběhu a výsledcích této kontroly, resp. průběhu a výsledcích takového řízení.
  12. Poskytovatel není oprávněn osobní údaje subjektů údajů jím zpracovávané či k nimž mu byl umožněn přístup žádným způsobem ukládat, kopírovat, tisknout, opisovat, činit z nich výpisky či opisy či je pozměňovat, pokud toto není nezbytné pro plnění jeho povinností dle této Smlouvy.
  13. Poskytovatel je povinen umožnit Objednateli na vyžádání kontrolu dodržování povinností dle tohoto článku Smlouvy.
  14. Záruky o technickém a organizačním zabezpečení osobních údajů subjektů údajů: Poskytovatel je povinen zabezpečit řádnou technickou a organizační ochranu zpracovávaných osobních údajů a výslovně prohlašuje, že odpovídá za zavedení nezbytných technických a organizačních opatření dle pokynů správce, které mu byly předloženy, tak, aby zpracování osobních údajů splňovalo v přiměřené míře požadavky ZZOÚ a GDPR.
  15. Poskytovatel je povinen při zpracování osobních údajů zajistit ochranu osobních údajů minimálně na takové úrovni, aby byly dodrženy veškeré záruky o technickém a organizačním zabezpečení osobních údajů uvedené v tomto článku Smlouvy.
  16. Poskytovatel se zavazuje zajistit taková opatření, aby nemohlo dojít k neoprávněnému ani nahodilému přístupu k osobním údajům, k jejich úplné ani částečné změně, zničení či ztrátě, neoprávněným přenosům či sdružení s jinými osobními údaji, či k jinému neoprávněnému zpracování v rozporu s touto Smlouvou. Poskytovatel zároveň užije taková opatření, která umožní určit a ověřit, komu byly osobní údaje předány.
  17. Poskytovatel se za účelem ochrany osobních údajů zavazuje zajistit zejména, že:
      1. Přístup k osobním údajům bude umožněn výlučně pověřeným osobám, které budou předem prokazatelně seznámeny s povahou osobních údajů a rozsahem a účelem jejich zpracování a budou povinny zachovávat mlčenlivost o všech okolnostech, o nichž se dozví v souvislosti se zpřístupněním osobních údajů a jejich zpracováním (dále jen „**pověřené osoby**“). Poskytovatel u pověřených osob zajistí zachování mlčenlivosti o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, a to i pro dobu po skončení zaměstnání nebo příslušných prací pověřených osob.
      2. Při zpracování osobních údajů budou osobní údaje vhodným způsobem zabezpečeny, jedná-li se o osobní údaje v elektronické podobě.
      3. Při zpracování osobních údajů v jiné než elektronické podobě budou osobní údaje uchovány v místnostech s vhodnou úrovní zabezpečení.
      4. Přístup k osobním údajům bude pověřeným osobám umožněn výlučně pro účely zpracování osobních údajů v rozsahu a za účelem stanoveným touto Smlouvou.
  18. Poskytovatel se zavazuje na písemnou žádost Objednatele přijmout v přiměřené lhůtě další vhodné a přiměřené záruky za účelem technického a organizačního zabezpečení osobních údajů, zejména přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům.
  19. Poskytovatel se zavazuje dokumentovat přijatá a provedená technickoorganizační opatření k zajištění ochrany osobních údajů v souladu se ZZOÚ a GDPR i jinými právními předpisy, přičemž zajišťuje, kontroluje a odpovídá zejména za:
      1. plnění pokynů pro zpracování osobních údajů pověřenými osobami, které mají bezprostřední přístup k osobním údajům;
      2. zabránění neoprávněným osobám přistupovat k osobním údajům nakládat s nimi a
      3. opatření, která umožní určit a ověřit, jak byly osobní údaje zpracovány.
  20. V případě zjištění porušení záruk dle této Smlouvy je Poskytovatel povinen zajistit stav odpovídající zárukám neprodleně poté, co zjistí, že záruky porušuje.
  21. V oblasti automatizovaného zpracování osobních údajů je Poskytovatel v rámci opatření podle předchozích odstavců povinen také:
      1. zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze pověřené osoby,
      2. zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob,
      3. zabránit neoprávněnému přístupu k datovým nosičům.
  22. Poskytovatel se zavazuje, že přijme přiměřená opatření k zabezpečení zpracování, případně včetně:
      1. schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;
      2. schopnosti obnovit dostupnost osobních údajů a přístup k nim v případě fyzických či technických incidentů;
      3. procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.
  23. Jestliže vznikne v souvislosti se zavedením opatření k zajištění ochrany osobních údajů podle právních předpisů uvedených v tomto článku potřeba uzavřít dodatek k této Smlouvě nebo zvláštní smlouvu, zavazuje se Poskytovatel poskytnout veškerou součinnost nezbytnou k formulaci obsahu takového dodatku, resp. smlouvy, a k uzavření takového dodatku, resp. smlouvy.

1. Oprávněné osoby Smluvních stran
   1. Každá ze Smluvních stran jmenuje oprávněnou osobu. Oprávněné osoby budou zastupovat příslušnou Smluvní stranu ve smluvních, obchodních a technických záležitostech souvisejících s plněním této Smlouvy (dále „**Oprávněné osoby**“).
   2. Oprávněné osoby jsou oprávněny jménem Smluvních stran provádět veškeré úkony v rámci, objednávání Služeb, vyjednávaní podmínek a komunikace, akceptačních procedur, zastupovat Smluvní strany ve změnovém řízení a připravovat dodatky ke Smlouvě pro jejich písemné schválení a podpis osobami oprávněnými zavazovat Smluvní strany (statutární orgán), nebo jejich zplnomocněnými zástupci.
   3. Jména oprávněných osob jako i rozsah jejich oprávnění jsou uvedena v Příloze č. 3 této Smlouvy.
   4. Smluvní strany jsou oprávněny jednostranně změnit Oprávněné osoby bez nutnosti uzavření dodatku ke Smlouvě. V takovém případě jsou povinny na takovou změnu druhou Smluvní stranu předem písemně upozornit, jinak tato změna nemá vůči druhé Smluvní straně právní účinky.
2. Trvání Smlouvy a možnosti jejího ukončení
   1. Smlouva nabývá platnosti dnem jejího podpisu poslední ze Smluvních stran a uzavírá se na dobu neurčitou od účinnosti smlouvy.
   2. Tuto Smlouvu lze ukončit:

### Písemnou dohodou Smluvních stran, jejíž součástí je i vypořádání vzájemných závazků.

### Písemným odstoupením od této Smlouvy v případě nepodstatného porušení této Smlouvy druhou Smluvní stranou za podmínek dále stanovených. Jestliže kterákoli Smluvní strana poruší nepodstatným způsobem tuto Smlouvu, je druhá Smluvní strana oprávněna písemně vyzvat porušující Smluvní stranu ke splnění jejích závazků z této Smlouvy. Pokud do třiceti (30) dnů od doručení této výzvy Smluvní strana, která porušila tuto Smlouvu, neučiní uspokojivé kroky k nápravě nebo pokud do šedesáti (60) dnů od této výzvy, nebo do jakékoli delší doby písemně dohodnuté Smluvními stranami, tato Smluvní strana neodstraní porušení závazků této Smlouvy, může druhá Smluvní strana od této Smlouvy odstoupit, aniž by se tím zbavovala výkonu jakýchkoli jiných práv nebo prostředků k dosažení nápravy.

### písemnou výpovědí některé ze Smluvních stran, zaslanou druhé Smluvní straně, a to výpovědí bez uvedení důvodu. Výpovědní doba v délce 30 kalendářních dnů počínající běžet prvním dnem následujícím po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé Smluvní straně

* 1. Smluvní strany jsou povinny do třiceti (30) dnů od ukončení účinnosti této Smlouvy vypořádat písemnou dohodou své vzájemné závazky.

1. Závěrečná ustanovení
   1. Tato Smlouva nabývá účinnosti ke dni zveřejnění v registru smluv s tím, že Objednatel se zavazuje zveřejnit tuto Smlouvu, jakož i veškeré její případné dodatky v souladu se zákonem o registru smluv. Strany potvrzují, že Příloha č. 2 představuje obchodní tajemství Poskytovatele, a proto nebude uveřejněna v registru smluv.
   2. Smluvní strany se dohodly, že žádná z nich není oprávněna postoupit svá práva a povinnosti vyplývající z této Smlouvy třetí straně bez předchozího písemného souhlasu druhé Smluvní strany.
   3. Smlouva představuje úplné ujednání mezi Smluvními stranami a nahrazuje všechny dosavadní smlouvy, dohody a ujednání vztahující se k předmětu této Smlouvy, která byla v minulosti učiněna, ať v písemné nebo ústní formě.
   4. Smlouva je vyhotovena v elektronické podobě v 1 (slovy: jednom) vyhotovení v českém jazyce s elektronickými podpisy obou Smluvních stran v souladu se zákonem č. 297/202016 Sb., O službách vytvářejících důvěru pro elektronické transakce ve znění pozdějších předpisů.
   5. Nedílnou součást Smlouvy tvoří následující přílohy:

Příloha č. 1 - Specifikace Služeb

Příloha č. 2 – Cena Služeb

Příloha č. 3 - Oprávněné osoby

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

\*\*\*

|  |  |  |
| --- | --- | --- |
| V Praze dne dle elektronického podpisu |  | V Praze dne dle elektronického podpisu |
| **Za Objednatele:** |  | **Za Poskytovatele:** |
|  |  |  |
| **Mgr. Adam Švejda,**  Zástupce ředitele pro ekonomickou  a provozní činnost  Institut plánování a rozvoje hlavního města Prahy |  | Antonín Drahovzal  na základě plné moci  ICZ. DMS. a.s. |

**Příloha č. 1**

**Specifikace služeb**

**Služba vytváření kvalifikovaných elektronických pečetí na dálku a kvalifikovaných časových razítek**

**I.CA RemoteSeal v 2**

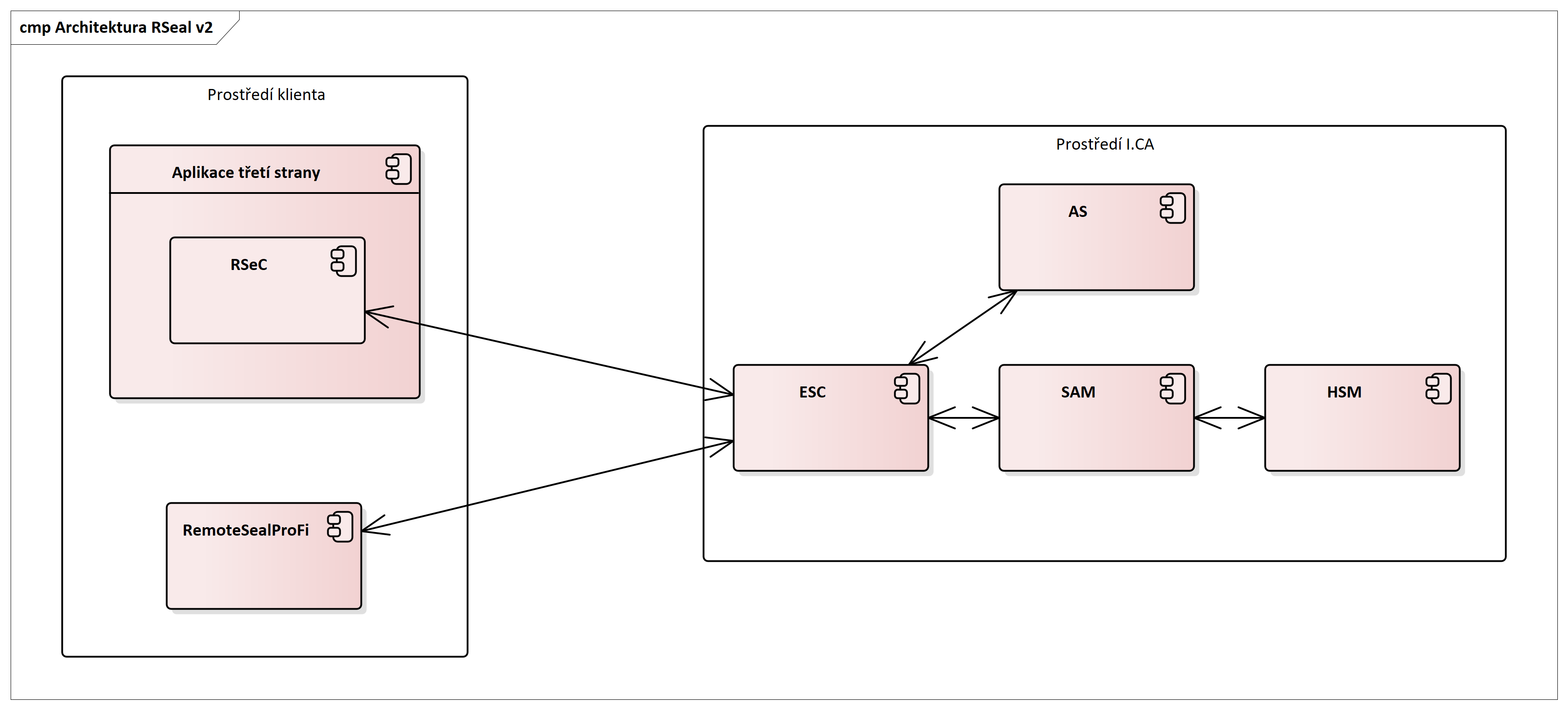
**Nabízené řešení:**

Implementace řešení spočívá v konfiguraci a nastavení modulu ICZ eIDAS, propojení se službou I.CA a vytvoření kvalifikované pečetě viz specifiakce níže.

## 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.

## 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

## 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.

**Příloha č. 2**

**Cena Služeb**

**Příloha č. 3**

**Oprávněné osoby**

Oprávněné osoby Objednatele:

|  |  |  |
| --- | --- | --- |
| **Jméno** | **Oblast pravomocí** | **Kontaktní informace** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Oprávněné osoby Poskytovatele:

|  |  |  |
| --- | --- | --- |
| **Jméno** | **Oblast pravomocí** | **Kontaktní informace** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |