Úřad vlády České republiky

Číslo smlouvy: 18/166-0
Č.j.: 29644/2018-OIT-2

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

uzavřená podle ustanovení § 1746 odst. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „Občanský zákoník)

První certifikační autorita, a.s.

Zastoupená:	Ing. Petrem Budišem, Ph.D., předsedou představenstva Ing. Romanem Kučerou, členem představenstva
Se sídlem:	Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
IČ:	264 39 395
DIČ:	CZ26439395
Bankovní spojení:	Československá obchodní banka, a.s.
Číslo účtu:	XXXXXXXXXX

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

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

a

Česká republika – Úřad vlády České republiky

Zastoupená:	Ing. Tomášem Kučerou, zástupcem ředitele, na základě vnitřního předpisu
Se sídlem:	nábřeží Edvarda Beneše 128/4, 118 01 Praha 1 – Malá Strana
IČ:	00006599
DIČ:	CZ00006599
Bankovní spojení:	Česká národní banka
Číslo účtu:	XXXXXXXXXX

(dále též „**Objednatel**“)

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

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

Článek I.
Preambule

1. Poskytovatel prohlašuje, že je kvalifikovaným poskytovatelem služeb vytvářejících důvěru podle Nařízení Evropského parlamentu a Rady č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické

transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES („eIDAS“) a zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, pro oblast vydávání kvalifikovaných certifikátů pro elektronické podpisy, kvalifikovaných elektronických časových razítek, kvalifikovaných certifikátů pro elektronické pečetě, kvalifikovaných certifikátů pro autentizaci internetových stránek a kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečetí. Služba I.CA RemoteSeal, vzhledem k tomu, že není přímo v nařízení eIDAS definována, nemůže být auditována jako kvalifikovaná služba. Nicméně byla posouzena orgánem dohledu, ministerstvem vnitra, a jeho rozhodnutím čj. MV-68158-6/EG-2018 ze dne 21. června 2018 bylo I.CA povoleno poskytovat službu vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal v souladu s politikou této služby a v souladu s technickou a uživatelskou dokumentací zařízení ARX CoSign v8.2 a DocuSign Signature Appliance v8.4. Dále bylo stejným Rozhodnutím povoleno I.CA vydávat kvalifikované certifikáty pro elektronické pečetě podle certifikační politiky vydávání kvalifikovaných certifikátů pro elektronické pečetě na dálku (algoritmus RSA), verze 1.00 (identifikátor 1.3.6.1.4.1.23624.10.1.38.1.0). Identifikátor této služby byl uveřejněn v důvěryhodném seznamu České republiky u služby „(78) I.CA – vydávání kvalifikovaných certifikátů“ společně s identifikátorem „QCQSCDManagedOnBehalf“ podle kap. 5.5.9.2.3 technických specifikací ETSI TS 119 612 v2.1.1. Důvěryhodný seznam je veden na https://tsl.gov.cz/publ/TSL_CZ.xtsl.

Článek II.
Předmět smlouvy

1. Předmětem plnění této Smlouvy je 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. Obchodní označení služby je I.CA RemoteSeal.

Článek III.
Povinnosti objednatele

1. I.CA poskytuje službu vytváření kvalifikovaných elektronických pečetí na dálku v souladu se závazným prohlášením uvedeným v Preambuli této Smlouvy. Objednatel se zavazuje zabezpečit dodržování platné Politiky služby vytváření kvalifikovaných elektronických pečetí na dálku („Politika“). 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 vzniklou v souvislosti s nedodržením Politiky.
3. Objednatel se zavazuje neposkytovat plnění poskytnuté I.CA dalším osobám bez souhlasu I.CA a nezneužívat poskytování služeb I.CA.

Článek IV.
Povinnosti I.CA

1. I.CA poskytuje objednateli službu vytváření kvalifikovaných elektronických pečetí na dálku (dále též „I.CA RemoteSeal“) v souladu s bodem 52 recitálu, články 29 a 39, Přílohou II body 3 a 4 a Přílohou III nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce

na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS). Popis služby je uveden v příloze č. 1 této Smlouvy.

2. I.CA se zavazuje poskytovat službu I.CA RemoteSeal v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 98 % 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 284 081 933.
   b) Hotline v rozsahu Po – Pá 8:00 – 17:00 hod. na výše uvedených kontaktech a provozní pohotovost služby v režimu 24/7 na telefonním čísle 731 657 586.
   c) právní a technickou aktuálnost komponenty pro zajištění komunikace s I.CA, jakož i celou službu I.CA RemoteSeal, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.
   d) za účelem otestování nových verzí služby I.CA RemoteSeal před nasazením do ostrého provozu službu I.CA TRemoteSeal 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.

Článek V.
Smluvní cenové podmínky

1. Cena za poskytování služby I.CA RemoteSeal, tj. za vytvoření kvalifikované elektronické pečetě, bude stanovena podle počtu vytvořených kvalifikovaných elektronických pečetí v daném kalendářním měsíci podle příslušného objemového pásma, a to jako součin „Ceny za 1 ks pečetění Kč bez DPH“ a počtu skutečně vytvořených kvalifikovaných elektronických pečetí v příslušném pásmu dle přiloženého rozpisu za kalendářní měsíc. K této ceně bude připočten paušální poplatek ve výši pro dané množstevní pásmo. K celkové ceně bude připočteno DPH podle aktuálně platných předpisů.

počet pečetění od - do za měsíc	paušální poplatek Kč bez DPH/měsíc	Cena za 1 ks pečetění Kč bez DPH
1 - 100	1 000	4,00
101 - 300	2 000	3,50
301 - 500	3 000	3,00
501 - 1.000	5 000	2,50
1.001 - 3.000	7 000	2,10
3.001 - 5.000	9 000	1,70
5.001 - 10.000	11 000	1,40
10.001 - 30.000	14 000	1,10
30.001 - 50.000	17 000	0,80
50.001 - 100.000	21 000	0,50
100.001 - 300.000	24 000	0,30
300.001 - 500.000	29 000	0,20
500.001 - 1.000.000	35 000	0,16
1.000.001 - 5.000.000	42 000	0,12

5.000.001 - 10.000.000	49 000	0,08

2. Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady I.CA související s poskytováním služby I.CA RemoteSeal. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.
3. Úhrada poskytování služby I.CA RemoteSeal 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; cena bude stanovena jako součin „Ceny za 1 pečetění Kč bez DPH“ a počtu skutečně vytvořených pečetí v příslušném pásmu za kalendářní měsíc dle rozpisu uvedeného v odst. 1. tohoto článku + paušální poplatek v příslušném pásmu. DPH bude vyjádřeno dle aktuálně platné legislativy.
4. 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.
5. Daňový doklad musí obsahovat náležitosti obchodní listiny dle § 435 občanského zákoníku a daňového dokladu dle zák. č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „ZDPH“). Na faktuře musí být uvedeno evidenční číslo této smlouvy uvedené Objednatelem v záhlaví této smlouvy.
6. 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. Na základě vadně vystaveného daňového dokladu ve smyslu tohoto odstavce se Objednatel neocitá v prodlení. Lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného daňového dokladu. Poskytovatel je oprávněn fakturu včetně všech jejích příloh vystavit v elektronické formě dle § 26 odst. 4 ZDPH, a to ve formátu ISDOC nebo ISDOCX verze 5.2 nebo vyšší. Elektronickou fakturu je možné zaslat datovou schránkou (identifikace: trfaa33) nebo elektronickou poštou na adresu posta@vlada.cz a v případě e-mailů opatřených zaručeným elektronickým podpisem taktéž na adresu edesk@vlada.cz.
7. Objednatel uhradí fakturu Poskytovatele bezhotovostně převodem na účet, přičemž splatnost faktury je 21 dnů ode dne jejího doručení Objednateli na adresu sídla Objednatele a doručeného písemně na adresu sídla Objednatele podle údajů v této Smlouvě. Povinnost Objednatele zaplatit fakturovanou částku dle této smlouvy je splněna odepsáním příslušné částky z účtu Objednatele. Objednatel neposkytuje zálohové platby.

Článek VI.

Sankční ustanovení, odstoupení od smlouvy

1. V případě zaviněného nedodržení parametru SLA dostupnosti služby I.CA RemoteSeal uvedeného v článku IV. odstavci 2. této Smlouvy, tj. pokud dostupnost služby klesne pod 98 % za kalendářní den, je I.CA povinna uhradit objednateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každých započatých 0,1%, o kterých klesne dostupnost poskytované služby pod požadovanou hodnotu. Měsíční výše smluvní pokuty však nepřesáhne výši měsíční ceny za poskytování služby.
2. V případě nesplnění povinností uvedených v článku IV. 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 IV. 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 v případě, poruší-li jedna ze smluvních stran své závazky a povinnosti stanovené touto Smlouvou, a to podstatným nebo opakovaným způsobem. Odstoupení musí mít písemnou formu s uvedením důvodů odstoupení a musí být doručeno druhé smluvní straně, jinak je odstoupení neplatné. Odstoupení od Smlouvy má právní účinky dnem doručení. Od toho dne nesmí smluvní strana, které takto bylo odstoupení doručeno, pokračovat v plnění předmětu Smlouvy vyjma případů, kdy by nečinností hrozila 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 VII.
Povinnost mlčenlivosti

1. Obě smluvní strany se zavazují dodržet důvěrný charakter všech informací (bez ohledu na formu jejich zachycení) o činnostech a záležitostech druhé smluvní strany, které získaly během jednání vedoucích k uzavření této smlouvy, nebo které získaly během plnění této smlouvy a to i po ukončení smlouvy, vyjma informací, které:
   - je strana povinna sdělit ze zákona;
   - jsou již v držení druhé smluvní strany, ne však následkem porušení této povinnosti;
   - jsou veřejně známé, a to ne v důsledku porušení této povinnosti nebo
   - které smluvní strana, jíž se informace týkají, písemně výslovně označí jako nedůvěrné.
2. Každá smluvní strana se zavazuje druhé učinit všechna nezbytná opatření, aby zajistila, že tuto povinnost dodržují i její zaměstnanci, spolupracující osoby a Poskytovatele.
3. Poskytovatel je povinen zavázat povinností mlčenlivosti podle odst. 1 tohoto článku všechny osoby, které se budou podílet na plnění předmětu veřejné zakázky dle této smlouvy. Za porušení povinnosti mlčenlivosti osobami, které se budou podílet na plnění předmětu smlouvy, odpovídá poskytovatel, jako by povinnost porušil sám.
4. Povinnost mlčenlivosti trvá i po skončení účinnosti smlouvy.

Článek VIII.
Závěrečná ustanovení, termín a místo plnění smlouvy

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. Tuto Smlouvu lze měnit nebo doplňovat pouze formou vzestupně číslovaných písemných dodatků, podepsaných oprávněnými zástupci smluvních stran na jedné listině.
5. Obě smluvní strany podpisem této Smlouvy vylučují, aby nad rámec jejích výslovných ustanovení a ustanovení jejích příloh byla jakákoliv jejich práva či povinnosti dovozovány z dosavadní či budoucí praxe zavedené mezi smluvními stranami.
6. Poskytovatel převzal na sebe nebezpečí změny okolností po uzavření této Smlouvy, a proto mu nepřísluší domáhat se práv uvedených v § 1765 odst. 1 a § 2620 odst. 2 Občanského zákoníku.
7. Poskytovatel souhlasí se zveřejněním této smlouvy, včetně všech jejích případných dodatků, především na profilu zadavatele a v Registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (dále je „Registr smluv“). Objednatel je dále v souladu se ZZVZ povinen na profilu zadavatele uveřejnit skutečně uhrazenou cenu.
8. Smluvní strany souhlasí s uveřejněním této Smlouvy, včetně všech jejích případných dodatků, v Registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále je „Registr smluv“) 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.
9. Smluvní strany souhlasí s tím, že v Registru smluv bude zveřejněn celý rozsah Smlouvy, včetně osobních údajů, a to na dobu neurčitou.
10. Tato smlouva nabývá platnosti dnem jejího podpisu smluvními stranami a účinnosti dnem jejího uveřejnění v Registru smluv.
11. Tato Smlouva se uzavírá na dobu neurčitou.
12. Místem plnění Smlouvy je sídlo Objednatele.
13. Smlouvu je možné ukončit:
    a) písemnou dohodou smluvních stran;
    b) písemnou výpovědí některé ze smluvních stran, zaslanou druhé smluvní straně, a to buď výpovědí s důvodem, kterým je podstatné porušení ustanovení této Smlouvy druhou smluvní stranou, nebo výpovědí bez uvedení důvodu. V obou případech se uplatní výpovědní doba v délce 30 kalendářních dnů počínající běžet prvním dnem následujícím po dni, kdy bylo písemné vyhotovení výpovědi prokazatelně doručeno druhé smluvní straně.
14. Písemnou dohodou smluvních stran je Smlouva ukončena ke dni v této dohodě uvedené a není-li v dohodě takový den uveden, pak ke dni podpisu dohody oběma smluvními stranami.
15. Ukončením Smlouvy nejsou smluvní strany zbaveny povinnosti vyrovnat veškeré závazky vzniklé v důsledku platnosti a účinnosti této Smlouvy a učinit veškeré úkony, které nesnesou odkladu a které jsou nutné k zabránění vzniku škody na straně jedné ze smluvních stran.
16. Smluvní strany se dohodly, že se ve vztazích mezi I.CA a objednatelem vyplývajících z této Smlouvy neuplatní §§ 1895 – 1900 Oobčanského zákoníku.
17. Smluvní strany mohou zveřejnit ve svých informačních materiálech, že I.CA je poskytovatelem služby I.CA RemoteSeal pro Objednatele.

18. Tato Smlouva je vyhotovena ve čtyřech vyhotoveních, z nichž Objednatel obdrží po třech vyhotoveních a Poskytovatel po jednom. Seznam příloh, které tvoří nedílnou součást této smlouvy:
    a) Příloha č. 1 – Popis služby I.CA RemoteSeal.

V Praze dne 08.10.2018

Za poskytovatele:

……..
Ing. Petr Budiš, Ph.D.
předseda představenstva

……
Ing. Roman Kučera
člen představenstva

V Praze dne 12.10.2018

Za objednatele:

……
Ing. Tomáš Kučera
zástupce ředitele Odboru informatiky

Příloha č. 1

Služba vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal

Východisko služby

Nařízení Evropského parlamentu a Rady č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS), konkrétně bod 52 recitálu, články 29 a 39, body 3 a 4 Přílohy II a Příloha III.

Právní základ

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

Kvalifikovaná elektronická pečeť dle bodu 27) článku 3 nařízení eIDAS:
„Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť."

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

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

Prostředky pro vytváření kvalifikovaných elektronických pečetí musí být uvedeny na seznamu vedeném Evropskou komisí:
„Compilation of Member States notification on SSCDs and QSCDs"
https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

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

Existují dva typy QSealCD:

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

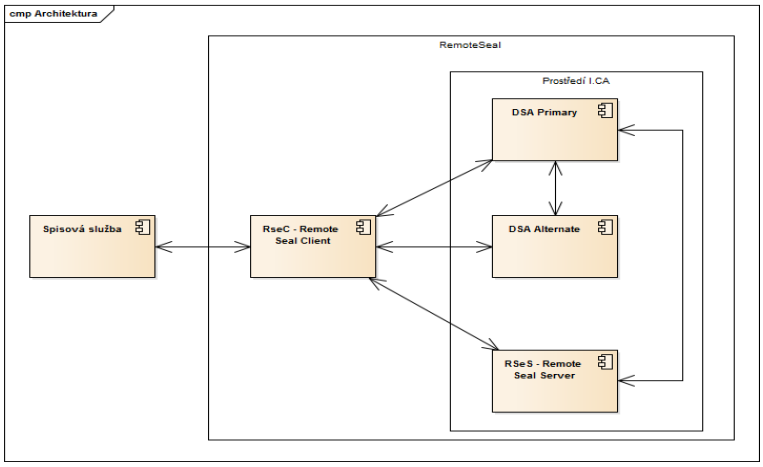
Služba I.CA RemoteSeal představuje variantu 2. Na HSM modulu v prostředí I.CA leží privátní klíč pečetícího certifikátu k jehož použití se využije autentizační certifikát vydaný danému klientovi. V prostředí klienta je instalována komponenta, která zasílá do prostředí I.CA požadavky na opečetění (hash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

Realizace služby I.CA RemoteSeal je založena na zařízení:

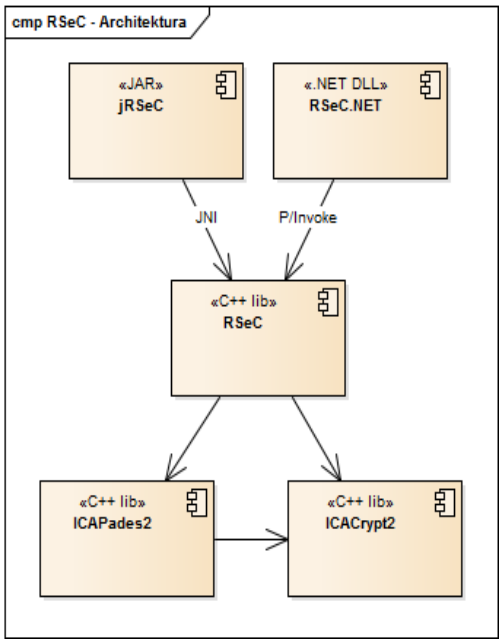
- ARX (Algorithmic Research) CoSign v8.2
- Společnost ARX koupena v roce 2015 společností DocuSign
- Produkt nadále prodáván pod názvem DocuSign Signature Appliance v8.2

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

Architektura služby



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



RemoteSeal Client

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

Postup zřízení služby

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

Zřízení služby bude probíhat na vybraných pobočkách RA následujícím způsobem:

- Klient navštíví pobočku RA.
- Operátor RA vydá klientovi prvotní autentizační komerční certifikát (**FAC** - First Authentication Certificate) na aktivační čipovou kartu. FAC bude zaveden v systému I.CA jako autentizační certifkát pro RemoteSeal pro daného uživatele
- Operátor RA připraví žádost o pečetící certifikát pro uživatele.
- Operátor RA vygeneruje párová data pro pečetící certifikát:

- ICARA pomocí **RSeS** (RemoteSealServer) založí pro klienta uživatele na DSA včetně prvotního hesla **FP** (First Password).
- ICARA náhodně vygeneruje nové heslo **PP** (Production Password) (drženo pouze v RAM)
- ICARA náhodně vygeneruje 256b AES šifrovací klíč **SK** (Secret Key)
- ICARA zašifruje pomocí AES-KW (kde **K** je **SK** a **PP** je **W**) do výsledku **CPP** (Ciphered Production Password)
- ICARA zašifruje pomocí RSAES_PKCS#1 v1.5 klíč **SK** veřejným klíčem **FAC** do výsledku $\mathbf{CSK_{FAC}}$ (Ciphered Secret Key)
- ICARA následně uloží do RSeS kryptogramy $\mathbf{CSK_{FAC}}$ a **CPP**
- ICARA provede aktivaci uživatelského účtu v DSA pomocí FP (a tudíž i změnu hesla na PP).
- ICARA provede pod účtem uživatele (s heslem PP) generování párových dat pro vydání prvotního pečetícího certifikátu.

- Operátor RA pomocí ICARA podepíše žádost o vydání pečetícího certifikátu privátním klíčem párových dat na DSA po zadání PIN klientem na pinpadové čtečce
- Na základě žádosti proběhne na CA vydání pečetícího certifikátu.
- Pečetící certifikát:
  - CA pošle na mailovou adresu uživatele.
  - ICARA uloží na aktivační kartu uživatele.
  - ICARA uloží na DSA
- Klient odchází z RA s aktivační kartou.

Aktivace RSeC

- Pro aktivaci RSeC spustí uživatel (např.: oprávněná osoba úřadu) dodávanou GUI utilitu RSeActivationUtil (dále jen utilita)
- Utilita vyzve uživatele k vložení aktivační karty, načež utilita:
  - Naváže spojení s RSeS pomocí oboustranně autentizovaného HTTPS za pomoci **FAC** (uživatel bude vyzván k zadání PINu)
  - Automaticky vytvoří žádost o vydání následného certifikátu **SACi** (Secondary Authentication Certificate číslo i), která bude podepsána **FAC** a privátní klíč k **SACi** se bude generovat v SW (nikoliv na kartě)
  - Žádost se odešle ke zpracování na CA, kde se obratem vydá následný certifikát **SACi** a ten se stáhne zpět do utility
  - Utilita si z RSeS stáhne $\mathbf{CSK_{FAC}}$ (drží se pouze v RAM)
  - Pomocí privátního klíče **FAC** na aktivační kartě dešifruje $\mathbf{CSK_{FAC}}$ na **SK** (drží se pouze v RAM)
  - Zašifruje pomocí RSAES_PKCS#1 v1.5 klíč **SK** veřejným klíčem **SACi** do výsledku $\mathbf{CSK_{SACi}}$
  - Utilita následně uloží do RSeS kryptogram $\mathbf{CSK_{SACi}}$
- Následně utilita vytvoří aktivační soubor, kde bude uložen certifikát **SACi** včetně privátního klíče.

- Uživatel tento aktivační soubor následně načte do spisové služby (obecně do aplikace volající RSeC), která jej bude pro použití RemoteSeal předávat do RSeC.

Technické parametry RSeActivationUtil

- Jednoduchá Windows GUI utilita.
- Nemusí být spouštěna na stejném PC, na kterém je provozován RSeC.
- Vyžaduje: .NET 4.5.2

Opečetění dokumentu

- Proces opečetění dokumentu inicializuje spisová služba (obecně volající aplikace), která má integrovanou knihovnu RSeC.
- Spisová služba předá do RSeC dokument k opečetění spolu s nastavením pečetění (viditelný/neviditelný podpis, formát, přidání TS, atp.) + aktivační soubor vzniklý při aktivaci RSeC
- RSeC připraví dokument k podpisu: sestaví žádost o opečetění (obsahující číslo jednací dokumentu (obecně jednoznačný textový identifikátor), parametry podpisu, hash původního dokumentu a hash který bude vstupem pro výpočet kryptogramu)
- Tato žádost bude podepsána pomocí **SACi**
- Následně RSeC naváže oboustraně autentizovaný TLS kanál pro komunikaci s RSeS pomocí **SACi**
- Navázaným kanálem předá podepsanou žádost o opečetění na RSeS
- RSeS obratem vrátí do RSeC kryptogramy $\mathbf{CSK_{SACi}}$ a **CPP**, které budou v RSeC drženy pouze v RAM
- RSeC pomocí **SACi** rozšifruje $\mathbf{CSK_{SACi}}$ na **SK** a pomocí něj rozšifruje **CPP** na **PP** (vše pouze v RAM, po dešifrování **PP** možno ostatní z RAM uvolnit)
- RSeC následně naváže anonymní HTTPS na DSA s aplikováním certificate pinningu na ověření autenticity DSA
- Následně tímto kanálem po autentizaci pomocí **PP** vytvoří na DSA kryptogram pomocí privátního klíče pečetícího certifikátu
- Po vytvoření kryptogramu se z RAM odstraní **PP**
- RSeC využije kryptogram pro kompletaci podepsaného dokumentu
- Pokud je vyžadován podpis s časovým razítkem, je TS do dokumentu přidáno nyní, přičemž RSeC se vůči TSA autentizuje pomocí **SACi**
- Hotový opečetěný dokument je vrácen spisové službě.

Automatické prodloužení služby

- Součástí RSeC je funkcionalita automatické obnovy **SACi**
- Nejprve se z RSeS stáhne $\mathbf{CSK_{SACi}}$
- Pomocí nově vygenerované veřejného klíče se vygeneruje $\mathbf{CSK_{SACi}}$ a spolu s veřejným klíčem se nahraje na RSeS.
- Následně je možné provést standardní obnovu a nahrát nově vydaný certifikát SACj na RSeS

Obnova pečetícího certifikátu

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

Technické normy

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

Podporované formáty podpisu:

- CAdES-B-B, CAdES-B-T
  - Dle normy EN 319 122, ve variantách:
  - Interní
  - Externí
- PAdES-B-B, PAdES-B-T
  - Dle normy EN 319 142, ve variantách:
  - Neviditelný
  - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
- XAdES-B a XAdES-T
  - dle normy ETSI TS 103 171, a to ve variantě enveloped, přičemž:
  - • Na vstupu bude XML dokument, který bude kompletně použit jakožto vstup podepisovaných data.
  - • Na vstupu bude určeno ID elementu, do nějž bude jakožto poslední child element přidán element Signature obsahující nově vytvořenou kvalifikovanou elektronickou pečeť.
    • Na vstupu bude definice požadovaných transformací, digest metody a mime-type referencovaných dat pro element Reference s id="xadesReference".
  - • Na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512)
  - • Na vstupu bude možnost volby podpisu typu XAdES-B/XAdES-T tedy bez nebo s časovým razítkem.

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

Dostupnost:

- Služba je poskytována v režimu 24/7 s SLA 98% a kapacitou až 30 vytvořených pečetí za minutu.