Řízení letového provozu
České republiky

Rámcová smlouva o poskytování služby vytváření kvalifikovaných elektronických pečetí

uzavřená ve smyslu ustanovení § 1746 odst. 2 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**občanský zákoník**")

(dále jen „**smlouva**")

1. Smluvní strany

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)
se sídlem: Navigační 787, 252 61 Jeneč
zastoupený: Ing. Miloslavou Mezerovou, výkonnou ředitelkou Útvaru finančně správního
IČO: 49710371
DIČ: CZ699004742
bankovní spojení: ČSOB Praha 5, č.ú. 88153/0300
SWIFT kód: CEKOCZPP
zapsaný v obchodním rejstříku vedeném u Městského soudu v Praze, v oddíle A, vložce 10771

(dále jen „**objednatel**")

a

První certifikační autorita, a.s.
se sídlem: Podvinný Mlýn 2178/6, 190 00 Praha 9
zastoupena: Ing. Petrem Budišem, Ph.D.,MBA, předsedou představenstva a
Ing. Romanem Kučerou, členem představenstva
IČO: 26439395
DIČ: CZ26439395
bankovní spojení: [redacted]
zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, v oddíle B, vložce 7136

(dále jen „**poskytovatel**")

Objednatel a poskytovatel rovněž jako „**smluvní strany**" nebo jednotlivě „**smluvní strana**".

[redacted]

2. Preambule

2.1 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 vytváření kvalifikovaných elektronických pečetí, vzhledem k tomu, že není přímo v nařízení eIDAS definována, nemůže být auditována jako kvalifikovaná služba. Nicméně byla posouzena orgánem dohledu, ministerstvem vnitra, a zařazena na seznam služeb poskytovaných kvalifikovanými poskytovateli služeb vytvářejících důvěru.

3. Předmět smlouvy

3.1 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.

4. Povinnosti objednatele

4.1 Poskytovatel se zavazuje poskytovat 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 (dále jen „**Politika**"). Veškeré změny a doplňky této Politiky jsou vůči objednateli účinné po podpisu dodatku k této smlouvě podepsaného zástupci obou smluvních stran.

4.2 Objednatel je povinen nahradit újmu na jmění vzniklou v souvislosti s nedodržením Politiky.

4.3 Objednatel se zavazuje neposkytovat plnění poskytnuté poskytovatelem dalším osobám bez souhlasu poskytovatele a nezneužívat poskytování služeb poskytovatele.

5. Povinnosti poskytovatele

5.1 Poskytovatel se zavazuje poskytovat objednateli službu vytváření kvalifikovaných elektronických pečetí na dálku (dále též „**služba pečetění**") 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.

5.2 Poskytovatel se zavazuje poskytovat službu pečetění v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 99,9 % a kapacitou až 30 vytvořených pečetí za minutu.

5.3 Poskytovatel se zavazuje poskytovat:

5.3.1. technickou podporu při provozu služby pečetění, řešení nestandardních situací a poradenství související s předmětem této smlouvy prostřednictvím e-mailové adresy remoteseal@ica.cz a telefonní linky 284 081 933.

5.3.2. 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.

5.3.3. právní a technickou aktuálnost komponenty pro zajištění komunikace s poskytovatelem, jakož i celou službu pečetění, s relevantními právními a technickými předpisy a normami v návaznosti na eIDAS.

5.3.4. za účelem otestování nových verzí služby pečetění před nasazením do ostrého provozu službu pečetění v testovacím prostředí s funkcionalitou obdobnou službě pečetění v ostrém prostředí, pro testovací prostředí platí SLA 95% a kapacita 10 vytvořených pečetí za minutu.

5.4 Poskytovatel garantuje a nese odpovědnost za vytvoření kvalifikované elektronické pečetě pouze za předpokladu, že data nutná k vytvoření pečetě (odesílaná do prostředí poskytovatele), generovaná komponentou dodanou poskytovatelem nebyla jakkoliv pozměněna a nebylo s nimi nijak manipulováno.

6. Smluvní cenové podmínky

6.1 Cena za poskytování služby pečetění, 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 pečetě 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 pečetí od - do za měsíc	paušální poplatek Kč bez DPH/měsíc	Cena za 1 ks pečetí Kč bez DPH
1 - 100	1 250,00	[redacted]
101 - 300	2 500,00	
301 - 500	3 750,00	
501 - 1.000	6 250,00	
1.001 - 3.000	8 750,00	
3.001 - 5.000	11 250,00	
5.001 - 10.000	13 750,00	
10.001 - 30.000	17 500,00	

6.2 Ceny uvedené v odst. 6.1 této smlouvy jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady poskytovatele související s poskytováním služby pečetění. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkající se DPH, a to nejvýše o částku odpovídající této legislativní změně.

6.3 Úhrada poskytování služby pečetění bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž poskytovatel vytvořil kvalifikované elektronické pečetě, a to podle počtu skutečně provedených a poskytnutých vytvořených pečetí včetně paušálního poplatku. Daňový doklad bude obsahovat počet skutečně vytvořených pečetí; cena bude stanovena jako součin „Ceny za 1 ks pečetě Kč bez DPH" a počtu skutečně vytvořených pečetí v příslušném pásmu za kalendářní měsíc dle rozpisu uvedeného v odst. 6.1 této smlouvy + paušální poplatek v příslušném pásmu. DPH bude vyjádřeno dle aktuálně platné legislativy.

6.4 Poskytovatel je povinen vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služby pečetění.

6.5 Objednatel je povinen uhradit daňové doklady převodem na účet poskytovatele do 30 dnů ode dne doručení daňového dokladu, vystaveného poskytovatelem, na adresu sídla objednatele a doručeného písemně na adresu sídla objednatele podle údajů v čl. 1 této smlouvy.

6.6 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 poskytovateli. Poskytovatel je povinen 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.

7. Sankční ustanovení, odstoupení od smlouvy

7.1 V případě zaviněného nedodržení parametru SLA dostupnosti služby pečetění uvedeného v odst. 5.2 této smlouvy, tj. pokud dostupnost služby klesne pod 99,9 % za kalendářní den, je poskytovatel povinen 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.

7.2 V případě nesplnění povinností uvedených v odst. 5.3.1 a 5.3.2 této smlouvy je poskytovatel povinen uhradit objednateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každé takové porušení.

7.3 V případě nesplnění povinností uvedených v odst. 5.3.3 této smlouvy je poskytovatel povinen uhradit objednateli smluvní pokutu ve výši 10.000,- Kč bez DPH za každé takové porušení.

7.4 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.

8. Závěrečná ustanovení, termín a místo plnění smlouvy

8.1 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.

8.2 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

8.3 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 této smlouvy.

8.4 Uveřejňování

Poskytovatel bere na vědomí, že objednatel je povinen uveřejnit tuto smlouvu ve smyslu 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. Poskytovatel bere dále na vědomí, že objednatel je povinným subjektem podle zákona č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Při uveřejnění této smlouvy v registru smluv budou v jejím textu znečitelněny zejména tyto údaje: bankovní spojení poskytovatele, podpisy na smlouvě, dále obchodní tajemství ve smyslu § 504 občanského zákoníku specifikované v odst. 8.6 této smlouvy.

8.5 Bezpečnost v civilním letectví

Poskytovatel podpisem smlouvy bere na vědomí, že není oprávněn sdělovat či jakkoliv šířit informace, kterými by mohla být narušena bezpečnost v civilním letectví, a to z důvodu požadavků na zachování bezpečnosti v civilním letectví, které vyplývají z příslušných právních předpisů

[redacted]

(zejména Letecký předpis L 17), a které ukládají poskytovatelům letových provozních služeb přijmout taková adekvátní opatření, na základě kterých bude zajištěna ochrana civilního letectví před protiprávními činy. Poskytovatel nesmí zejména jakkoliv reprodukovat a dále šířit informace, o nichž se dozvěděl v souvislosti s plněním této smlouvy.

8.6 Obchodní tajemství

Podle § 504 občanského zákoníku je obchodním tajemstvím kalkulace cena za 1 ks pečeti obsažená v odst. 6.1 této smlouvy, a proto nebude uveřejněna ani poskytnuta dle odst. 8.4 této smlouvy.

8.7 Ochrana osobních údajů

Objednatel i poskytovatel respektují pravidla o ochraně osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tj. nařízení GDPR, a dalších obecně závazných právních předpisů upravujících ochranu osobních údajů. Bližší informace o ochraně osobních údajů na straně objednatele jsou k dispozici na webových stránkách

http://www.rlp.cz/spolecnost/osobniudaje/Stranky/default.aspx

8.8 Náhrada majetkové a nemajetkové újmy

Pro náhradu majetkové újmy (škody) a nemajetkové újmy platí příslušná ustanovení občanského zákoníku. Majetková újma se nahrazuje v penězích, nedohodnou-li se strany v konkrétním případě jinak. Smluvní strany prohlašují, že dojde-li porušením povinností smluvní strany ke vzniku újmy na pověsti nebo obchodní firmě druhé smluvní strany či k jiné nemajetkové újmě, uhradí porušující strana poškozené smluvní straně přiměřené zadostiučinění.

8.9 Vyšší moc (vis maior)

8.9.1. Smluvní strany se osvobozují od odpovědnosti za částečné nebo úplné nesplnění smluvních závazků, jestliže se tak prokazatelně stalo v důsledku vyšší moci. Za vyšší moc se pokládají okolnosti, které vznikly po uzavření této smlouvy v důsledku smluvními stranami nepředvídaných a neodvratitelných událostí, mimořádné povahy a mají bezprostřední vliv na plnění předmětu této smlouvy. Nastanou-li výše uvedené okolnosti, jsou obě smluvní strany povinny se neprodleně o těchto okolnostech vzájemně informovat.

8.9.2. Lhůty pro plnění povinností podle smlouvy se prodlužují o dobu, po kterou prokazatelně trvá okolnost vylučující odpovědnost za částečné nebo úplné nesplnění smluvních závazků.

8.9.3. Jestliže důsledky vyplývající ze zásahu vyšší moci prokazatelně trvají déle než tři měsíce, může kterákoliv ze smluvních stran od smlouvy odstoupit s tím, že se nároky smluvních stran vyrovnají tak, aby žádné ze smluvních stran nevzniklo bezdůvodné obohacení.

8.10 Tato smlouva nabývá platnosti oběma smluvními stranami a účinnosti dnem 19. 9. 2018, přičemž uvedené datum nabytí účinnosti této smlouvy musí následovat až po jejím uveřejnění v registru smluv.

8.11 Tato smlouva se uzavírá na dobu neurčitou.

8.12 Místem plnění smlouvy je sídlo objednatele.

8.13 Smlouvu je možné ukončit:

8.13.1. písemnou dohodou smluvních stran;

8.13.2. 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.

8.14 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.

8.15 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.

8.16 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.

8.17 Tato smlouva je vyhotovena ve čtyřech (4) vyhotoveních, z nichž obě smluvní strany obdrží po dvou (2) vyhotovení.

8.18 Seznam příloh, které tvoří nedílnou součást této smlouvy:

Příloha č. 1 – Popis služby vytváření kvalifikovaných elektronických pečetí na dálku

V Jenči dne 12-09

[redacted]

Řízení let

V Praze dne 11. 9. 2

[redacted]

Příloha č. 1 ke smlouvě evidenční číslo smlouvy ŘLP ČR, s.p.: 265/2018/PS/096 - Popis služby vytváření kvalifikovaných elektronických pečetí na dálku

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

Právní základ
Povinnost používat kvalifikované elektronické pečetě orgány veřejné moci počínaje 20.9.2018 je dána § 8 zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce:
„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:

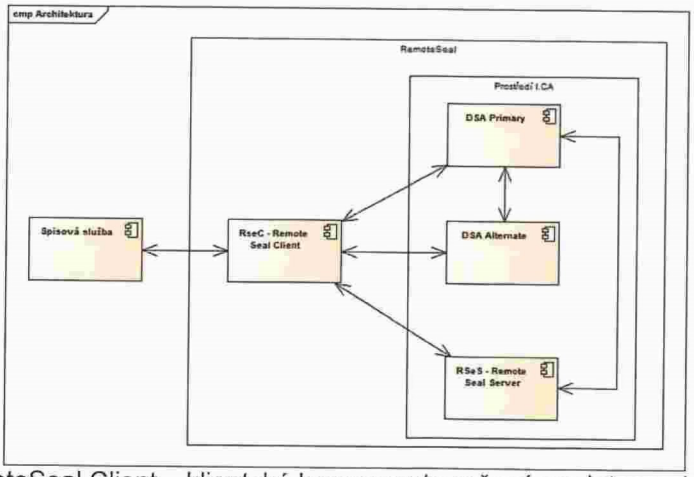
- ARX (Algorithmic Research) CoSign v8.2

- 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.

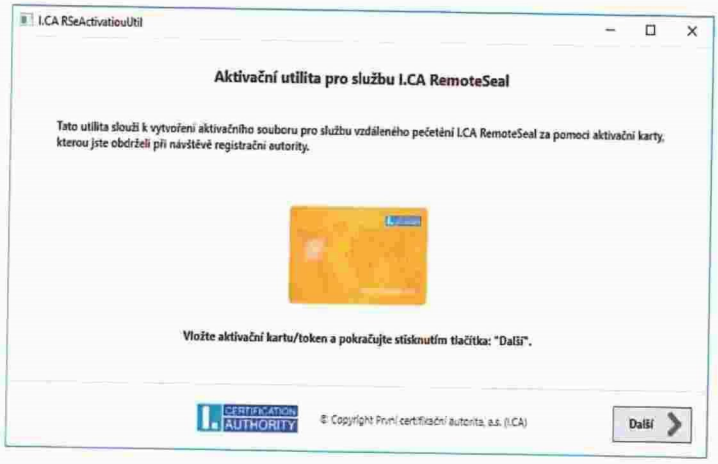
Postup zřízení služby

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, kde operátor vydá na aktivační čipovou kartu autentizační komerční certifikát, vygeneruje párová data pečetícího certifikátu na HSM modulu a vydá pečetící certifikát
- Pečetící certifikát:
  - CA pošle na mailovou adresu uživatele.
  - ICARA uloží na aktivační kartu uživatele.
- 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
- Následně utilita vytvoří aktivační soubor a uživatel tento aktivační soubor následně načte do spisové služby (obecně do aplikace volající RSeC), která jej bude pro použití RemoteSeal předávat do RSeC.

Technické parametry RSeActivationUtil

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

- Vyžaduje: .NET 4.0

Opečetění dokumentu

- 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)
- Následně RSeC naváže oboustraně autentizovaný TLS kanál pro komunikaci s RSeS, předá podepsanou žádost o opečetění na RSeS
- Na DSA k vytvoření kryptogramu pomocí privátního klíče pečetícího certifikátu
- RSeC využije kryptogram pro kompletaci podepsaného dokumentu
- Hotový opečetěný dokument je vrácen spisové službě.

Automatické prodloužení služby

- Součástí RSeC je funkcionalita automatické obnovy autentizačního certifikátu, která probíhá zcela automaticky. Proces inicializuje RSeC a vydaný certifikát je do něj následně uložen.

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 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 99,9% a kapacitou až 30 vytvořených pečetí za minutu.