



MPACSS01148087

Městský úřad Pacov

Č. ev.:

Č. j.:

MP/0777/2022

Došlo:

17. 01. 2022

Počet listů / příloh

3/1

Spisový a skart. znak / skart. lhůta

Smlouva

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

uzavřená podle ustanovení § 1746 odst. 2 zák. č. 89/2012 Sb., občanského zákoníku
(dále jen „Občanský zákoník“)

První certifikační autorita, a.s.

Se sídlem: Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
Zastoupená: Ing. Petrem Budišem, Ph.D., předsedou představenstva
Ing. Romanem Kučerou, členem představenstva
IČ: 264 39 395
DIČ: CZ26439395
Bankovní spojení: Československá obchodní banka, a.s.
Číslo účtu: 168457418/0300
zapsaná v obchodním rejstříku, vedeném Městským soudem v Praze, spisová značka B,
vložka 7136.

(dále též „I.CA“ nebo „Poskytovatel“)

a

Město Pacov

Se sídlem: Pacov, náměstí Svobody 320, PSČ 39501
Zastoupená: Tomášem Kocourem, starostou města
IČ: 00248789
DIČ:
Bankovní spojení: Česká spořitelna, a. s.
Číslo účtu: 27-0622171349/0800

(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 pečeti, kvalifikovaných certifikátů pro autentizaci internetových stránek a kvalifikované služby ověřování platnosti kvalifikovaných elektronických podpisů a pečeti. 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 pečeti 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 pečeti podle certifikační politiky vydávání kvalifikovaných certifikátů pro elektronické pečeti 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 pečeti na dálku v souladu s platnou Politikou služby vytváření kvalifikovaných elektronických pečeti 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 pečeti na dálku v souladu se závazným prohlášením uvedeným v Preambuli této Smlouvy. Objednatel se zavazuje zabezpečit dodržování platné Politiky služby vytváření kvalifikovaných elektronických pečeti 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 pečeti 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 99,5 % a kapacitou až 30 vytvořených pečeti 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 [REDACTED] 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 [REDACTED]
 - 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 5 vytvořených pečeti za minutu.
4. I.CA garantuje a nese odpovědnost za vytvoření kvalifikované elektronické pečeti pouze za předpokladu, že data nutná k vytvoření pečeti (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 pečeti, bude stanovena podle počtu vytvořených kvalifikovaných elektronických pečeti 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 pečeti 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	500	2,00
101 - 300	1 000	1,80
301 - 500	1 500	1,50
501 - 1.000	2 000	1,30
1.001 - 3.000	3 500	1,10
3.001 - 5.000	4 500	1,00
5.001 - 10.000	6 000	0,80
10.001 - 30.000	9 000	0,65
30.001 - 50.000	12 000	0,50
50.001 - 100.000	15 000	0,30
100.001 - 300.000	18 000	0,20
300.001 - 500.000	21 000	0,15
500.001 - 1.000.000	25 000	0,10
1.000.001 - 5.000.000	29 000	0,08
5.000.001 - 10.000.000	35 000	0,05

2. Ceny uvedené v odst. 1. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady I.CA související s poskytováním služby 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 pečeti, 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. Objednatel je povinen uhradit daňové doklady převodem na účet I.CA do 30 dnů ode dne doručení daňového dokladu, vystaveného I.CA, na adresu sídla objednatele a doručeného písemně na adresu sídla objednatele podle údajů v této Smlouvě.
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 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.

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 99,5 % za kalendářní den, je I.CA povinna uhradit objednateli smluvní pokutu ve výši 1.000,- Kč bez DPH za každých započatých 0,1%, o kterých klesne dostupnost poskytované služby pod 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.

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 smířčí jednání k vyřešení sporu, bude soudní spor veden u příslušného obecného soudu ČR.
2. Pokud jakýkoli závazek dle Smlouvy nebo kterékoli ustanovení Smlouvy je nebo se stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních závazků a ustanovení dle Smlouvy a smluvní strany se zavazují takovýto neplatný nebo nevymahatelný závazek či ustanovení nahradit novým, platným a vymahatelným závazkem, nebo ustanovením, jehož předmět bude nejlépe odpovídat předmětu a ekonomickému účelu původního závazku či ustanovení
3. V případě, že by se některá ustanovení Smlouvy stala neplatnými v důsledku legislativních změn, nestává se neplatnou celá Smlouva. V takovém případě sjednají smluvní strany nové znění dotčených ustanovení tak, aby vystihovalo co nejpřesněji podstatu původního ujednání a aby co nejlépe odpovídalo duchu Smlouvy.
4. Smluvní strany souhlasí s uveřejněním této Smlouvy v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů a rovněž na profilu objednatele, případně i na dalších místech, kde tak stanoví právní předpis. Uveřejnění této Smlouvy prostřednictvím registru smluv ve lhůtě stanovené zákonem zajistí objednatel.
5. Smluvní strany souhlasí s tím, že v registru smluv bude zveřejněn celý rozsah Smlouvy, včetně osobních údajů, a to na dobu neurčitou.
6. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami.
7. Tato Smlouva nabývá účinnosti dnem jejího uveřejnění v informačním systému veřejné správy, který slouží k uveřejňování smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv.
8. Smluvní strany souhlasí s tím, že v registru smluv bude zveřejněn celý rozsah Smlouvy, včetně osobních údajů, a to na dobu neurčitou.
9. Tato Smlouva se uzavírá na dobu neurčitou.
10. Místem plnění Smlouvy je sídlo objednatele.
11. 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.
12. 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.
13. 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.
14. Smluvní strany se dohodly, že se ve vztazích mezi I.CA a objednatelem vyplývajících z této Smlouvy neuplatní §§ 1895 – 1900 zák. č. 89/2012 Sb., občanského zákoníku.
15. 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.
16. Smluvní strany mohou zveřejnit ve svých informačních materiálech, že I.CA je poskytovatelem služby I.CA RemoteSeal pro objednatele.
17. Tato Smlouva je vyhotovena ve dvou vyhotoveních, z nichž obě smluvní strany obdrží po jednom vyhotovení.
18. Seznam příloh, které tvoří nedílnou součást této smlouvy:
a) Příloha č. 1 – Popis služby I.CA RemoteSeal.

V Praze dne 12.1.2022

V Pacově dne 17.1.2022

Za poskytovatele:

Za objednatele:

Ing. Petr Budiš, Ph.D.
předseda představenstva

Tomáš Kocour
starosta města

Ing. Roman Kučera
člen představenstva

MĚSTO PACOV
15

Služba vytváření kvalifikovaných elektronických pečetí na dálku I.CA RemoteSeal

Východisko služby

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

Právní základ

Povinnost používat kvalifikované elektronické pečeteř 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 pečeteř.“

Kvalifikovaná elektronická pečeteř dle bodu 27) článku 3 nařízení eIDAS:

„Zaručená elektronická pečeteř, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeteř.“

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 tyto 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).

Existují dva typy QSealCD:

1. QSealCD v držení pečeteřící 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 pečeteřící osoby).

Služba I.CA RemoteSeal představuje variantu 2 s tím, že certifikace na základě alternativního procesu – musí používat srovnatelnou úroveň bezpečnosti a zároveň certifikační orgán daný postup oznámil Komisi. Alternativní postup může být použit pouze v případě, že příslušné normy neexistují.

Seznam EU pro QSealCD

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

- Seznam je spravován Komisí.

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

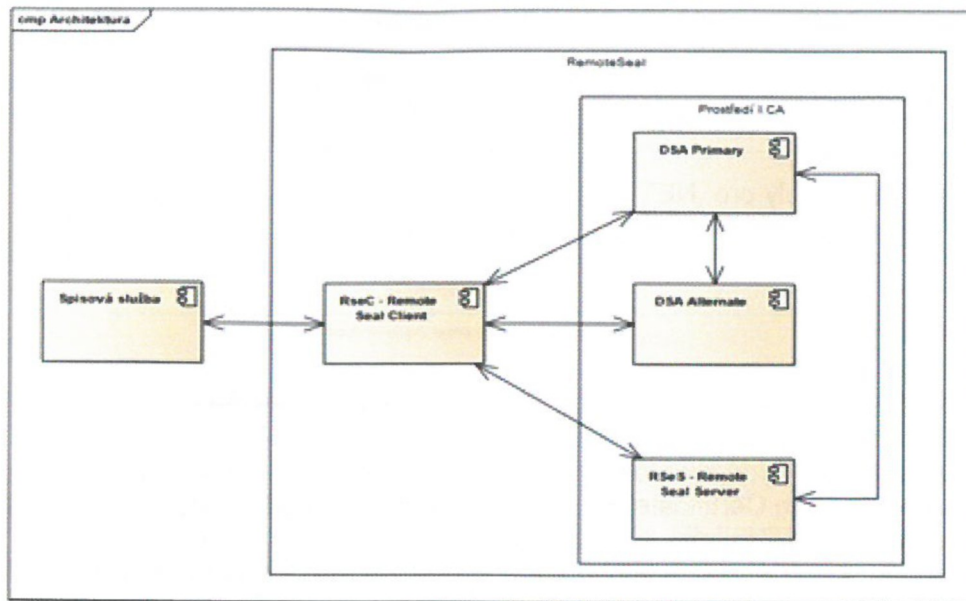
Výběr QSealCD pro službu I.CA RemoteSeal

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

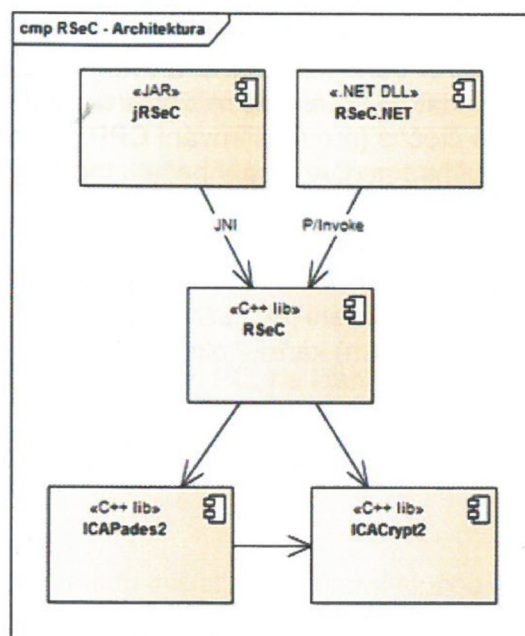
List of QSCDs	
Name:	
Name:	ARX CoSign v8.2
Applicant	ARX (Algorithmic Research, Ltd.)
Qualified Signature Creation Device (QSigCD)	yes
	IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance 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/ax/arc_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/ax/rc_ax_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/ax/st_ax_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/ax/arc_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/ax/rc_ax_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/ax/st_ax_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.

Zřízení služby

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 kartu/token (viz [návosloví](#)). FAC je nutné zavést do AUTHu jako autentizační certifikát pro RemoteSeal pro daného uživatele (budou provádět ručně obchodníci na základě SN certifikátu, které jim zašle klient).
- Operátor RA připraví žádost o pečetící certifikát pro uživatele.
- Operátor RA vygeneruje párová data pro pečetící certifikát (z pohledu operátora atomická operace) což obnáší:
 - 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 **CSK_{FAC}** (Ciphered Secret Key)
 - ICARA následně uloží do RSeS kryptogramy **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 (zde můžeme teoreticky zapojit uživatele aby zadal PIN na pinpadové čtečce (pro rozšifrování **CPP** pomocí privátního klíče **FAC**))
- Na základě žádosti proběhne na CA vydání pečetícího certifikátu.
- Pečetící certifikát:
- CA pošle na mailovou adresu uživatele.
- ICARA uloží na čipovou kartu uživatele.
- ICARA uloží na DSA (díky přihlášení jako uživatel)
- Klient odchází z RA s aktivační(m) kartou/tokenem.

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 (potažmo aktivačního tokenu), načtež 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 **CSK_{FAC}** (drží se pouze v RAM)
 - Pomocí privátního klíče **FAC** na aktivační kartě dešifruje **CSK_{FAC}** na **SK** (drží se pouze v RAM)
 - Zašifruje pomocí RSAES_PKCS#1 v1.5 klíč **SK** veřejným klíčem **SACi** do výsledku **CSK_{SACi}**
 - Utilita následně uloží do RSeS kryptogram **CSK_{SACi}**
- Utilita může případně uživatele vyzvat k dalším nastavením RSeC, pokud nějaká budou (např.: přidávání TS, viditelný podpis, reason, location pokud se tyto nebudou nastavovat pomocí RSeCAPI)
- 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 4.0

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 a 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 **CSK_{SACi}** a **CPP**, které budou v RSeC drženy pouze v RAM
- RSeC pomocí **SACi** rozšifruje **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 bude funkcionalita automatické obnovy **SACi** (obdobné řešení jako v QVerify)
- Nejprve se z RSeS stáhne **CSK_{SACi}**
- Pomocí nově vygenerované veřejného klíče se vygeneruje **CSK_{SACj}** 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 (zakotveného ve Smlouvě) bude také probíhat automatická obnova pečetícího certifikátu
- RSeC s určitým předstihem před vypršením certifikátu vygeneruje 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

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 něž 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.

Dostupnost:

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