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

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

Číslo smlouvy objednatele: 1616 / 23 / 16 / SIS

První certifikační autorita, a.s.

se sídlem:	Praha 9, Podvinný mlýn 2178/6, PSČ 190 00
zastoupená:	Ing. Petrem Budišem, Ph.D., MBA, předsedou představenstva a 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

Fakultní nemocnice Plzeň

se sídlem:	Edvarda Beneše 1128/13, 301 00 Plzeň - Bory
zastoupená:	MUDr. Václavem Šimánkem, Ph.D., ředitelem
IČ:	00669806
DIČ:	CZ00669806
Bankovní spojení:	ČNB
Číslo účtu:	33739311/0710

(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 a kvalifikovaných elektronických podpisů na dálku I.CA RemoteSign (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.

Článek II.
Předmět smlouvy

1. Předmětem plnění této Smlouvy je zajištění provozu služby vytváření kvalifikovaných elektronických pečetí na dálku (obchodní označení služby je I.CA RemoteSeal) v souladu s platnou Politikou služby I.CA RemoteSeal a zajištění provozu služby vytváření kvalifikovaných elektronických podpisů (obchodní označení služby je I.CA RemoteSign) na dálku v souladu s platnou Politikou služby I.CA RemoteSign. Aktuální verze politik jsou vždy k dispozici k dispozici na www.ica.cz.

Článek III.
Povinnosti objednatele

1. I.CA poskytuje službu vytváření kvalifikovaných elektronických pečetí na dálku a vytváření kvalifikovaných elektronických podpisů na dálku v souladu se závazným prohlášením uvedeným v Preambuli této Smlouvy. Objednatel se zavazuje zabezpečit dodržování platných politik služeb, tj. Politiky služby I.CA RemoteSeal a Politiky služby I.CA RemoteSign (dále též „Politiky“). Veškeré změny a doplňky těchto Politik 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 Politik.

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“) a službu vytváření kvalifikovaných elektronických podpisů (dále též „I.CA RemoteSign“) v souladu s nařízením 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 služeb je uveden v příloze č. 1 a v příloze č. 2 této Smlouvy.

2. I.CA se zavazuje poskytovat služby I.CA RemoteSeal a I.CA RemoteSign v režimu 24/7, tedy 24 hodin denně, 7 dní v týdnu, s SLA 99,5 % a kapacitou až 30 vytvořených pečetí a podpisů za minutu.

3. I.CA se zavazuje poskytovat:

    a) technickou podporu při provozu služeb, 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 komponent pro zajištění komunikace s I.CA, jakož i celou službu I.CA RemoteSeal a I.CA RemoteSign, v souladu 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.
    e) Za účelem otestování nových verzí služby I.CA RemoteSign před nasazením do ostrého provozu službu I.CA TRemoteSign v testovacím prostředí s funkcionalitou obdobnou službě I.CA RemoteSign v ostrém prostředí.

4. I.CA garantuje a nese odpovědnost za vytvoření kvalifikované elektronické pečetě nebo kvalifikovaného elektronického podpisu pouze za předpokladu, že data nutná k vytvoření pečetě nebo podpisu (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, a to jako součin „Ceny za 1 ks pečetění bez DPH“ a počtu skutečně vytvořených kvalifikovaných elektronických pečetí za kalendářní měsíc. K této ceně bude připočten měsíční paušální poplatek. K celkové ceně bude připočteno DPH podle aktuálně platných předpisů. Za měsíc, ve kterém nebyla prostřednictvím služby I.CA RemoteSeal vytvořena žádná kvalifikovaná elektronická pečeť, nebude paušální poplatek účtován.

   Cena za 1 ks pečetění bez DPH činí 2,00 Kč.
   Měsíční paušální poplatek činí 500 Kč.

2. Cena za poskytování služby I.CA RemoteSign, tj. za vytvoření kvalifikovaného elektronického podpisu, bude stanovena podle počtu vytvořených kvalifikovaných elektronických podpisů v daném kalendářním měsíci, a to jako součin „Ceny za vytvoření 1 ks podpisu bez DPH“ a počtu skutečně vytvořených kvalifikovaných elektronických podpisů za kalendářní měsíc. K této ceně bude připočten měsíční paušální poplatek. K celkové ceně bude připočteno DPH podle aktuálně platných předpisů. Za měsíc, ve kterém nebyl prostřednictvím služby I.CA RemoteSign vytvořen žádný kvalifikovaný elektronický podpis, nebude paušální poplatek účtován.

   Cena za vytvoření 1 ks podpisu bez DPH činí 2,00 Kč.
   Měsíční paušální poplatek činí 500 Kč.

3. Ceny uvedené v odst. 1. a 2. tohoto článku jsou cenami neměnnými, nejvýše přípustnými a zahrnují veškeré náklady I.CA související s poskytováním služeb I.CA RemoteSeal a I.CA RemoteSign. Ceny mohou být změněny pouze v souvislosti se změnou daňových předpisů týkajících se DPH, a to nejvýše o částku odpovídající této legislativní změně.

4. Úhrada za poskytování služeb I.CA RemoteSeal a I.CA RemoteSign bude prováděna vždy jednou měsíčně zpětně za uplynulý kalendářní měsíc, v němž I.CA vytvořila kvalifikované elektronické pečetě a kvalifikované elektronické podpisy, a to podle počtu skutečně provedených a poskytnutých vytvořených pečetí a podpisů. Daňový doklad bude obsahovat počet skutečně vytvořených pečetí a podpisů; cena bude stanovena dle odst. 1. a 2. DPH bude vyjádřeno dle aktuálně platné legislativy.

5. I.CA je povinna vystavit řádný daňový doklad do 15. dne kalendářního měsíce následujícího po kalendářním měsíci, za který je účtována cena za poskytování služeb I.CA RemoteSeal a I.CA RemoteSign.

6. 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.

7. 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 služeb I.CA RemoteSeal a RemoteSign 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 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. 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 a účinnosti dnem jejího podpisu oběma smluvními stranami.

7. Tato Smlouva se uzavírá na dobu určitou od 1. 1. 2024 do 31. 12. 2024. Účinnosti nabývá dnem zveřejnění v registru smluv.

8. Místem plnění Smlouvy je sídlo objednatele.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. Smluvní strany mohou zveřejnit ve svých informačních materiálech, že I.CA je poskytovatelem služby I.CA RemoteSeal pro objednatele.

15. Tato Smlouva je vyhotovena ve dvou vyhotoveních, z nichž obě smluvní strany obdrží po jednom vyhotovení.

16. Seznam příloh, které tvoří nedílnou součást této smlouvy:
   a) Příloha č. 1 – Popis služby I.CA RemoteSeal,
   b) Příloha č. 2 – Popis služby I.CA RemoteSign.

V Praze dne …….

Za poskytovatele:

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

……..
Ing. Roman Kučera
člen představenstva

V Plzni dne …….

Za objednatele:

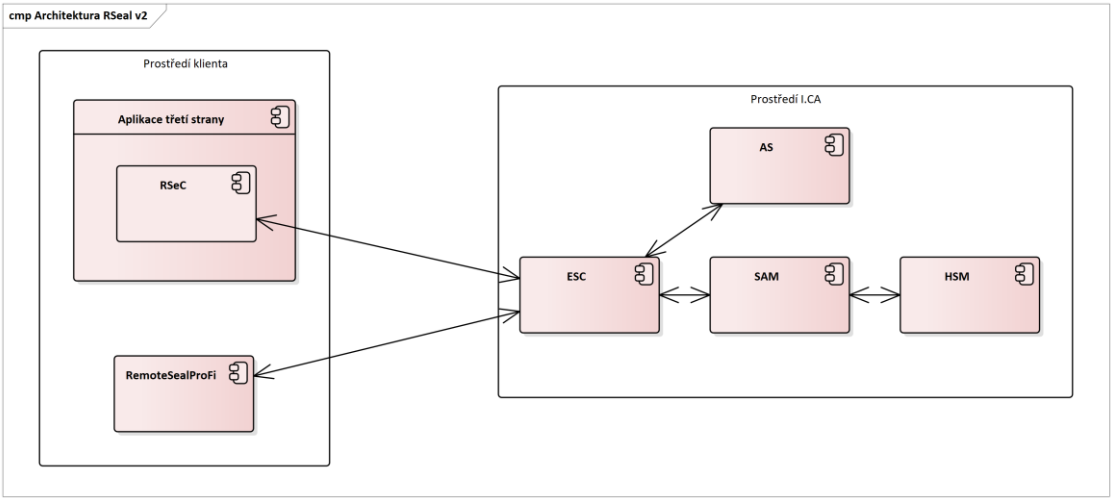
……
MUDr. Václav Šimánek, Ph.D.
ředitel

Popis služby I.CA RemoteSeal

I.CA RemoteSeal 2.0

Služba I.CA RemoteSeal v2 (dále už jen „RemoteSeal“ nebo „služba“) je služba vytváření kvalifikovaných elektronických pečetí na dálku. Služba umožňuje vygenerovat a držet data pro vytváření elektronických pečetí (tj. zejména privátní klíč) v QSealCD certifikovaném HSM zařízení ve správě I.CA a k němu pak zprostředkovat přístup pro účely vytváření kvalifikovaných elektronických pečetí. Klient (tj. právnická osoba) má k dispozici klientskou komponentu a příslušné autentizační markanty, pomocí kterých může dokument opatřit kvalifikovanou elektronickou pečetí. Samotný obsah dokumentu přitom neopouští klientskou komponentu, a tudíž ani prostředí klienta.

Architektura

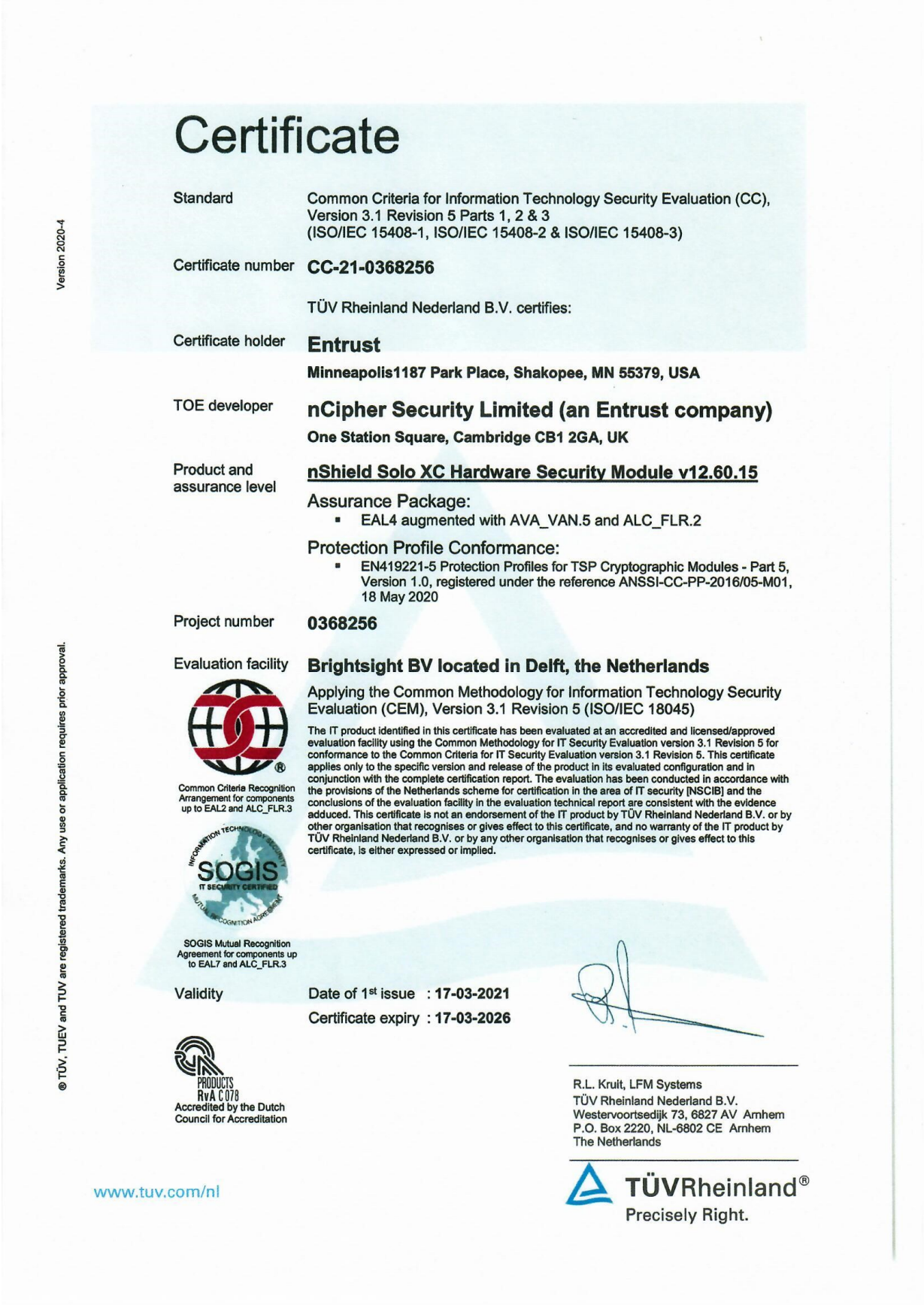


- **RSeC** (RemoteSeal Client) - klientská komponenta určená pro strojové pečetění dokumentů a pro integraci do spisové služby nebo jiného systému, který potřebuje autonomně vytvářet kvalifikované pečeti. Existuje ve vícero variantách pro snadnou integraci do různých systémů.
- **RemoteSealProFi** - klientská desktop aplikace pro Windows, která slouží ke správě pečetění dané organizace a ručnímu vytváření kvalifikovaných pečetí.
- **ESC** (Evolved Signature Core) - základní aplikační server provozovaný I.CA, přes který jdou veškeré komunikace týkající se pečetění z klientských komponent.
- **SAM** (Signature Activation Module) - povinná součást QSCD pro vzdálený podpis/pečeť, který zajišťuje kontrolu přístupu ke klíčům uloženým na HSM modulu
- **HSM** (Hardware Security Module) - povinná součást QSCD pro vzdálený podpis/pečeť, která zajišťuje samotné bezpečné generování, uchovávání a používání privátních klíčů.
- **AS** (Authorization Server) - aplikační server, který zajišťuje ověření autentizace koncového uživatele (držitele klíče) a vytváření SAD (Signature Activation Data) tj. datové struktury autorizující použití příslušného privátního klíče pro podpis příslušných dat pro SAM.

Použité QSCD

Služba využívá certifikované Remote QSealCD skládající se ze:

- SAM modulu Entrust SAM
  - https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD
- HSM modulu Entrust nShield Connect XC



Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 Parts 1, 2 & 3 (ISO/IEC 15408-1, ISO/IEC 15408-2 & ISO/IEC 15408-3)

Certificate number: **CC-21-0368256**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder: **Entrust**

Minneapolis1187 Park Place, Shakopee, MN 55379, USA

TOE developer: **nCipher Security Limited (an Entrust company)**

One Station Square, Cambridge CB1 2GA, UK

Product and assurance level: **nShield Solo XC Hardware Security Module v12.60.15**

Assurance Package:
- EAL4 augmented with AVA_VAN.5 and ALC_FLR.2

Protection Profile Conformance:
- EN419221-5 Protection Profiles for TSP Cryptographic Modules - Part 5, Version 1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020

Project number: **0368256**

Evaluation facility: **Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2 and ALC_FLR.3

SOGIS Mutual Recognition Agreement for components up to EAL7 and ALC_FLR.3

Validity: Date of 1st issue : **17-03-2021**

Certificate expiry : **17-03-2026**

PRODUCTS RvA C 078 Accredited by the Dutch Council for Accreditation

R.L. Kruit, LFM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

Version 2020-4

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Varianty klientských komponent

RemoteSeal poskytuje několik variant klientských komponent, které je možné rozdělit do dvou skupin:

- Klientské komponenty pro ruční pečetění uživatelem, tedy člověkem
- Klientské komponenty pro automatizované/strojové pečetění

Klientské komponenty pro ruční pečetění uživatelem, tedy člověkem

Pro ruční pečetění člověkem - tj. zaměstnanci dané organizace existuje desktopová GUI aplikace pro Windows RemoteSealProFi, která umožňuje ručně vybrat dokument/dokumenty a opatřit je kvalifikovanou elektronickou pečetí.

Aplikace RemoteSealProFi má zároveň správcovskou (administrátorskou) funkci - uživatel s rolí správce pečetění organizace pomocí aplikace spravuje instance RSeC, další uživatele a obnovu pečetícího certifikátu.

Klientské komponenty pro automatizované/strojové pečetění

Klientské komponenty pro automatizované/strojové pečetění souhrnně nazýváme RSeC (Remote Seal Client) a jsou určeny pro integraci do informačního systému/aplikace třetí strany, který má autonomně pečetit dokumenty jejichž je organizace původcem.

RSeC je vždy založen na nativním (C/C++) jádře, ke kterému je pak nadstavba pro danou platformu:

- **jRSeC** (Linux i Windows) - nadstavba nad RSeC určená pro integraci do aplikací v jazyce Java formou Java class library.
- **RSeC.NET** (Linux i Windows) - nadstavba nad RSeC určená pro integrací do aplikací v jazyce .NET
- **RSeProxy** (Windows) - serverová aplikace určená pro instalaci do sítě klienta, která do vnitřní sítě klienta poskytuje SOAP webové služby pro funkcionalitu pečetění, přičemž vůči systému RemoteSeal vystupuje jako klientská komponenta RSeC.

Zřízení služby

1. Prvním krokem je uzavření smlouvy mezi organizací a I.CA.
2. Oprávněná osoba žadatele (tj. organizace) dohodne se zástupcem I.CA způsob vydání osobního autentizačního komerčního certifikátu – obvykle navštíví pobočku RA v sídle společnosti I.CA s potřebnými doklady ke zřízení služby I.CA RemoteSeal na danou organizaci.
3. Operátor RA vydá oprávněné osobě osobní autentizační komerční certifikát na čipovou kartu Starcos 3.5 nebo 3.7. Tato osoba se tímto automaticky stává prvním (a v tento okamžik prozatím také jediným) správcem služby pečetění pro danou organizaci.
4. Operátor RA provede zřízení služby I.CA RemoteSeal vč. vydání kvalifikovaného pečetícího certifikátu (kvalifikovaný certifikát pro elektronickou pečeť) pro danou organizaci, přičemž privátní klíč pro tento certifikát je generován a spravován QSCD zařízením služby I.CA RemoteSeal.
5. V rámci vydání pečetícího certifikátu oprávněná osoba žadatele podepisuje dokumentaci k vydání certifikátu, přičemž tyto mohou být podepsány:
   - klasicky vlastnoručním podpisem na papír, nebo
   - bezpapírově/elektronicky pomocí osobního autentizačního komerčního certifikátu oprávněné osoby (v tom případě žadatel podepisuje pouze smlouvu)
6. Oprávněná osoba žadatele odchází z RA s čipovou kartou s autentizačním komerčním certifikátem.

Uživatelské účty RemoteSealProFi

Aplikace RemoteSealProFi umožňuje na jednom PC (přesněji jednomu uživateli Windows na daném PC) mít současně vytvořeno více uživatelských účtů a při startu aplikace se přihlásit do uživatelského účtu dle volby.

Uživatelské účty jsou dvojího druhu:

- Přenosný uživatelský účet
- Fixní uživatelský účet

Přenosný uživatelský účet

Přenosný uživatelský účet není vázán na jedno konkrétní PC, ale je možné k němu přistupovat z různých PC, na nichž je nainstalována aplikace RemoteSealProFi.

Pro autentizaci uživatele slouží:

- čipová karta Starcos 3.5 nebo 3.7 s (autentizačním) osobním komerčním certifikátem
- PIN k čipové kartě
- heslo uživatele ke službě RemoteSeal

Uživatel, jenž pro autentizaci používá výše uvedené, si může na libovolném množství PC založit přenosný uživatelský účet a pomocí čipové karty atd. se do aplikace přihlásit a dále s ní pracovat. Bez čipové karty však přihlášení k přenosnému uživatelskému účtu není možné.

Aktivace přenosného uživatelského účtu

Pro aktivaci přenosného uživatelského účtu je potřeba mít čipovou kartu s komerčním certifikátem, na který byl uživatelský účet založen (buďto na RA nebo správcem pečetění).
K aktivaci přenosného uživatelského účtu dojde při prvním pokusu o přihlášení do RemoteSealProFi pomocí příslušné čipové karty s komerčním certifikátem. Tedy:

1. Uživatel zvolí přidání uživatelského profilu => přenosný profil
2. Vloží čipovou kartu, případně vybere příslušný certifikát
3. Zadá PIN
4. Aplikace detekuje, že tento uživatelský účet ještě nebyl aktivován a vyzve uživatele k volbě hesla pro službu RemoteSeal
5. Po dvojím zadání hesla proběhne aktivace a uživatel se může standardně přihlásit do aplikace.

Poznámka

To je případ i prvotní aktivace oprávněnou osobou, jež navštívila RA pro zřízení služby.

Fixní uživatelský účet

Fixní uživatelský účet je oproti tomu vázán na konkrétní PC, resp. na konkrétní uživatelský profil v OS Windows, na kterém proběhla aktivace a jinde se k němu není možné přihlásit.
K přihlášení však nejsou potřeba žádné fyzické markanty, postačuje:

- data uložená na daném PC (a uživatelském profilu Windows) jež vznikla při aktivaci
- heslo uživatele ke službě RemoteSeal

Použití fixních uživatelských účtů však vyžaduje použití doplňkového zabezpečení zdroje komunikace (viz níže).

Aktivace fixního uživatelského účtu

Po zřízení nového fixního uživatelského účtu (správcem pečetění) obdrží uživatel tzv. aktivační mail, který v příloze obsahuje tzv. aktivační soubor. Tento slouží pro provedení aktivace následovně:

1. Uživatel zvolí přidání uživatelského profilu => fixní profil
2. Vloží aktivační soubor (jež dostal mailem)
3. Následně mu na telefonní číslo (uvedené při zřízení účtu) přijde tzv. aktivační SMS kód
4. Tento kód uživatel přepíše do aplikace
5. V případě správného zadání je následně vyzván k volbě hesla pro službu RemoteSeal
6. Po dvojím zadání hesla proběhne aktivace a uživatel se může standardně přihlásit do aplikace.

Uživatelské role RemoteSealProFi

Jednotliví uživatelé aplikace RemoteSealProFi mají v rámci daného pečetícího accountu dané organizace vždy jednu ze dvou rolí:

- **správce pečetění**
  - Má přístup do administrátorské sekce RemoteSealProFi, kde může:
    - spravovat instance RSeC (přidávání, (od)blokace, přejmenování, zrušení)
    - požádat o vydání následného pečetícího certifikátu
    - vidět a nastavovat okamžik nasazení nového (následného) pečetícího certifikátu
    - spravovat další uživatele pod daným pečetícím accountem (přidávání, (od)blokace, zrušení, nastavení role) *(a to vč. možnosti přidat dalšího správce pečetění)*
  - Může libovolně vytvářet kvalifikované elektronické pečetě.
- **běžný uživatel**
  - Nemá přístup do administrátorské sekce RemoteSealProFi.
  - Může libovolně vytvářet kvalifikované elektronické pečetě.

Aktivace RSeC

Komponenta RSeC pro autentizaci vůči systému RemoteSeal vyžaduje:

- přístupový soubor tzv. RSealAccessFile
- heslo (pro instanci RSeC definovanou daným přístupovým souborem)

Držitel certifikátu (organizace) může současně provozovat více různých aplikací, které pečetí pomocí stejného accountu RemoteSeal, tj. stejného pečetícího certifikátu. Tedy může provozovat více samostatných instancí RSeC, přičemž pro každou je potřeba vygenerovat dvojici přístupový soubor + heslo.

Generování přístupového souboru provádí uživatel (typicky zaměstnanec dané organizace) s rolí správce pečetění dané organizace v administrátorské části aplikace RemoteSealProFi:

1. Uživatel se přihlásí do aplikace RemoteSealProFi
2. Otevře administrátorskou část aplikace => správa RSeC => Přidat nový
3. Pro ověření zadá své heslo a následně vyplní
   - název nové instance RSeC (určeno zejména pro interní identifikaci v rámci dané organizace - např.: "Spisová služba - server 1")
   - heslo pro novou instanci RSeC
   - znovu heslo pro novou instanci RSeC
4. RemoteSealProFi poté provede založení nové instance RSeC a po dokončení nabídne uložení vygenerovaného aktivačního souboru na disk

Do komponenty RSeC se pak přístupový soubor a heslo předávají přes API příslušné knihovny - způsob jejich vložení/uložení do příslušné aplikace je tedy odvislý od implementace v dané aplikaci. Z principu je možné, aby přístupový soubor "ležel" někde na disku daného stroje, na kterém probíhá pečetění přes RSeC. Heslo by však mělo být danou aplikací uloženo bezpečnějším způsobem a nikdy by nemělo ležet v plaintextu někde v souboru.

Volající aplikace pak předává přístupový soubor a heslo k němu pro každé pečetění, resp. pro každou inicializaci objektu třídy SealClient. RSeC si sám nezajišťuje žádnou persistenci přístupového souboru ani hesla.

Opečetění dokumentu

Opečetění dokumentu přes RSeC

1. Volající aplikace vytvoří instanci třídy SealClient z RSeC, které předá přístupový soubor a heslo k němu
2. Volající aplikace předá do RSeC 1 až N dokumentů k opečetění spolu s nastavením opečetění jednotlivých dokumentů (viditelný/nevidititelný podpis, formát, přidání časového razítka, atp.)
3. RSeC připraví dokumenty k podpisu, založí pro každý dokument pečetící transakci, autorizuje použití privátního klíče na HSM modulu, získá z backendu vytvořenou podpisovou strukturu vč. případného časového razítka a sestaví kompletní podepsané dokumenty
4. Sestavené podepsané dokumenty RSeC vrátí volající aplikaci

Opečetění dokumentu přes RemoteSealProFi

1. Uživatel se přihlásí do aplikace RemoteSealProFi
2. Uživatel vybere "profil pečetě" podle kterého chce pečetit
   - profil pečetě jsou de-facto uložené parametry vytvářené pečetě (viditelný podpis, vložení časového razítka, atp), které mohou sloužit jako fixně předepsané parametry pro druh dokumentu (např.: všechna potvrzení o studiu mají stejné parametry) - jako základní nastavení parametrů, které jsou pro daný případ uživatele následně upraveny a je možné je sdílet s dalšími uživateli pod stejným pečetícím accountem.
3. Volitelně uživatel upraví parametry pečetě
4. Následně uživatel vybere dokumenty, které se mají opečetit a potvrdí
5. RemoteSealProFi postupně opečetí všechny vybrané dokumenty

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 aplikaci také změnit.

Podporované formáty podpisu

- **CAdES**
  - CAdES-B-B, CAdES-B-T
  - Dle normy EN 319 122, ve variantách:
    - Interní
    - Externí
- **PAdES**
  - PAdES-B-B, PAdES-B-T
  - Dle normy EN 319 142, ve variantách:
    - Neviditelný
    - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí

- **XAdES**
  - XAdES-B a XAdES-T
  - Dle normy ETSI TS 103 171 a to ve variantě enveloped, přičemž:
    - Na vstupu bude XML dokument, který bude kompletně použit jakožto vstup podepisovaných data.
    - Na vstupu bude určeno ID elementu, do nějž bude jakožto poslední child element přidán element Signature obsahující nově vytvořenou kvalifikovanou elektronickou pečeť.
    - Na vstupu bude definice požadovaných transformací , digest metody a mime-type referencovaných dat pro element Reference s id="xadesReference".
    - Na vstupu bude volba hash algoritmu podpisu (SHA256/SHA384/SHA512)
    - Na vstupu bude možnost volby podpisu typu XAdES-B/XAdES-T tedy bez nebo s časovým razítkem.
- **ASiC-E XAdES**
  - ASiC-E XAdES-B a ASiC-E XAdES-T
  - Dle normy ETSI TS 103 174, přičemž:
    - Je možné opečetit právě jeden datový objekt právě jednou kvalifikovanou pečetí
    - Není podporováno rozšíření stávajícího ASiC-E souboru o další pečeť/podpis, ani několik podpisů/pečetí v rámci jednoho ASiC-E souboru.
    - Pro soubory typu .txt, .pdf, .xml, .png je implicitně doplněn příslušný mimetype odpovídající dané příponě. Tuto implicitní volbu je možné v rozhraní explicitně přenastavit na jiný mimetype, popř. lze explicitní cestou nastavit mimetype pro ostatní (implicitně nepodporované) typy datových objektů.
    - Samotná XAdES pečeť uvnitř ASiC-E kontejneru obsahuje pouze minimální nezbytně nutnou množinu podepisovaných a nepodepisovaných properties vyžadovanou danou ETSI normou.

Doplňkové zabezpečení zdroje komunikace

Pro jednotlivé pečetící accounty je možné nastavit doplňkové zabezpečení zdroje komunikace, které umožňuje omezit, "odkud" může daná aplikace pro daný account kontaktovat službu RemoteSeal - např.: že fixní uživatelské účty RemoteSealProFi musejí komunikovat přes určitou VPN mezi klientem a I.CA, nebo musí být tato komunikace zabezpečena mTLS spojením s konkrétním klientským certifikátem, atp.

Popis služby I.CA RemoteSign

a) Služba vytváření kvalifikovaných elektronických podpisů na dálku (dále též RemoteSign) umožňuje vygenerovat a držet data pro vytváření elektronických podpisů (tj. zejména privátní klíč) v certifikovaném HSM zařízení ve správě I.CA, které je kvalifikovaným prostředkem pro vytváření elektronických podpisů (QSCD), a k němu pak zprostředkovat přístup pro účely vytváření kvalifikovaných elektronických podpisů. Odběratel má k dispozici klientskou komponentu RSiCon a příslušné autentizační markanty, pomocí kterých může elektronický dokument opatřit kvalifikovaným elektronickým podpisem. Samotný obsah elektronického dokumentu přitom neopouští klientskou komponentu, a tudíž ani prostředí klienta.

b) Vytváření elektronických podpisů je možné realizovat prostřednictvím mobilních telefonů s operačními systémy Android a iOS, případně PC desktop aplikací.

c) RemoteSign využívá certifikované QSCD uvedené na seznamu vedeném Evropskou komisí: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd, které se skládá ze:
   i. SAM modulu Entrust SAM
   ii. HSM modulu Entrust nShield Connect XC

d) QSCD splňuje požadavky norem:
   i. EN 419 241-2:2019 — Trustworthy Systems Supporting Server Signing — Part 2: Protection Profile for QSCD for Server Signing.
   ii. EN 419 221-5:2018 – Protection Profiles for TSP Cryptographic Modules - Part 5 – Cryptographic Module for Trust Services.

e) Služba RemoteSign podporuje formáty elektronických podpisů podle Prováděcího rozhodnutí Komise (EU) č. 2015/1506, tj. podporuje formáty:

   i. PAdES-B-B, PAdES-B-T, dle normy EN 319 142, ve variantách:
      - Neviditelný
      - Viditelný – Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí

   ii. CAdES-B-B, CAdES-B-T, dle normy EN 319 122, ve variantách:
      - Interní
      - Externí

f) Dále RemoteSign podporuje též podpis e-Receptu ve formátu specifikovaném Státním ústavem pro kontrolu léčiv.