# Služba vzdáleného pečetění I.CA RemoteSeal

Ing. Roman Kučera
První certifikační autorita, a.s.
5. 4. 2018

# I.CA RemoteSeal

Hovořit budeme o splnění povinnosti veřejnoprávního podepisujícího danou § 8 zákona č. 297/2016 Sb.:

- 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.
- **Tato povinnost platí nejpozději od 20. září 2018.**

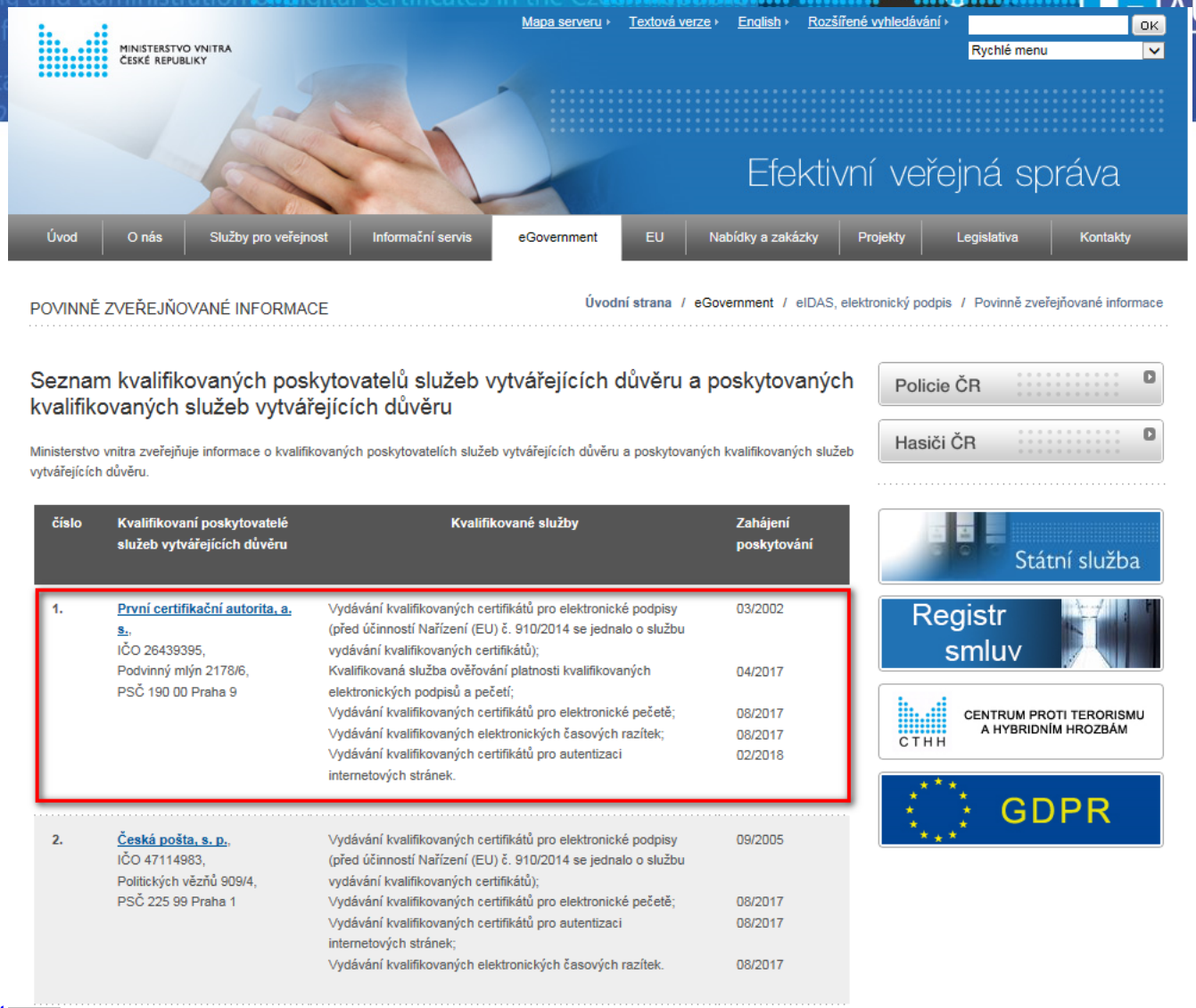
## Co to je kvalifikovaná elektronická pečeť?

- Dle článku 3 bodu 27) eIDAS je to:

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

Kvalifikovaný certifikát pro elektronickou pečeť může vydat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který byl auditován a služba zařazena na TL list státu EU (LoTL).

# Seznam kvalifikovaných poskytovatelů v ČR



MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Mapa serveru | Textová verze | English | Rozšířené vyhledávání | OK | Rychlé menu

Efektivní veřejná správa

Úvod | O nás | Služby pro veřejnost | Informační servis | eGovernment | EU | Nabídky a zakázky | Projekty | Legislativa | Kontakty

POVINNĚ ZVEŘEJŇOVANÉ INFORMACE

Úvodní strana / eGovernment / eIDAS, elektronický podpis / Povinně zveřejňované informace

## Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru

Ministerstvo vnitra zveřejňuje informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru.

| číslo | Kvalifikovaní poskytovatelé služeb vytvářejících důvěru | Kvalifikované služby | Zahájení poskytování |
|---|---|---|---|
| 1. | První certifikační autorita, a. s.,<br>IČO 26439395,<br>Podvinný mlýn 2178/6,<br>PSČ 190 00 Praha 9 | Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů);<br>Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečetí;<br>Vydávání kvalifikovaných certifikátů pro elektronické pečetě;<br>Vydávání kvalifikovaných elektronických časových razítek;<br>Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek. | 03/2002<br>04/2017<br>08/2017<br>08/2017<br>02/2018 |
| 2. | Česká pošta, s. p.,<br>IČO 47114983,<br>Politických vězňů 909/4,<br>PSČ 225 99 Praha 1 | Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů);<br>Vydávání kvalifikovaných certifikátů pro elektronické pečetě;<br>Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek;<br>Vydávání kvalifikovaných elektronických časových razítek. | 09/2005<br>08/2017<br>08/2017<br>08/2017 |

Policie ČR

Hasiči ČR

Státní služba

Registr smluv

CTHH CENTRUM PROTI TERORISMU A HYBRIDNÍM HROZBÁM

GDPR

http://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx

## Kde lze zjistit, že se jedná o kvalifikovaný prostředek pro vytváření elektronických pečetí (QSealCD)?

## „Compilation of Member States notification on SSCDs and QSCDs“

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

- Uvedena certifikovaná QSigCDs a QSealCDs podle nařízení eIDAS

# QSealCD

CERTIFICATION AUTHORITY

**List of QSCDs**

| | |
|---|---|
| **Name:** | **PrimeSign Remote Signing Device/Core für qualifizierte Signaturen und Siegel** |
| Applicant | PrimeSign GmbH |
| **Qualified Signature Creation Device (QSigCD)** | yes<br>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 | Zentrum für sichere Informationstechnologie - Austria (A-SIT) |
| QSigCD designation date | 20.11.2017 |
| QSigCD designation expiry | Valid up to revocation by A-SIT |
| QSigCD designation report reference | A-SIT-VIG-17-067 |
| QSigCD designation report | https://www.a-sit.at/pdfs/qscd/VIG-17-067_qsee_bescheinigung_primesign_signed.pdf |
| Art.30.3.(b) notified alternative certification method | https://www.a-sit.at/pdfs/merkblatt_de.pdf<br>https://www.a-sit.at/pdfs/merkblatt_en.pdf |
| CC certification report reference | none |
| **Qualified Seal Creation Device (QSealCD)** | yes<br>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 | Zentrum für sichere Informationstechnologie - Austria (A-SIT) |
| QSealCD designation date | 20.11.2017 |
| QSealCD designation expiry | Valid up to revocation by A-SIT |
| QSealCD designation report reference | A-SIT-VIG-17-067 |
| QSealCD designation report | https://www.a-sit.at/pdfs/qscd/VIG-17-067_qsee_bescheinigung_primesign_signed.pdf |
| Art.30.3.(b) notified alternative certification method | https://www.a-sit.at/pdfs/merkblatt_de.pdf<br>https://www.a-sit.at/pdfs/merkblatt_en.pdf |
| CC certification report reference | none |

SafeNet Luna PCI-E

| | |
|---|---|
| **Name:** | **Qualified Signature and Seal Creation Device (QSCD) LuxTrust's Qualified Remote Signature and Seal Creation Device, version 1.0** |
| Applicant | LuxTrust S.A., IVY Building, 13-15 Parc d'activités, L-8308 Capellen, Luxembourg |
| **Qualified Signature Creation Device (QSigCD)** | yes<br>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 | Zentrum für sichere Informationstechnologie - Austria (A-SIT) |
| QSigCD designation date | 14.12.2017 |
| QSigCD designation expiry | Valid up to revocation by A-SIT |
| QSigCD designation report reference | A-SIT-VIG-17-060 |
| QSigCD designation report | https://www.a-sit.at/pdfs/qscd/VIG-17-060_QSCD_Certificate_LuxTrust_signed.pdf |
| Art.30.3.(b) notified alternative certification method | https://www.a-sit.at/pdfs/merkblatt_de.pdf<br>https://www.a-sit.at/pdfs/merkblatt_en.pdf |
| CC certification report reference | HSM (subcomponent) certified by OCSI |
| **Qualified Seal Creation Device (QSealCD)** | yes<br>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 | Zentrum für sichere Informationstechnologie - Austria (A-SIT) |
| QSealCD designation date | 14.12.2017 |
| QSealCD designation expiry | Valid up to revocation by A-SIT |
| QSealCD designation report reference | A-SIT-VIG-17-060 |
| QSealCD designation report | https://www.a-sit.at/pdfs/qscd/VIG-17-060_QSCD_Certificate_LuxTrust_signed.pdf |
| Art.30.3.(b) notified alternative certification method | https://www.a-sit.at/pdfs/merkblatt_de.pdf<br>https://www.a-sit.at/pdfs/merkblatt_en.pdf |
| CC certification report reference | HSM (subcomponent) certified by OCSI<br>http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf |

THALES nSHIELD SOLO/SOLO+

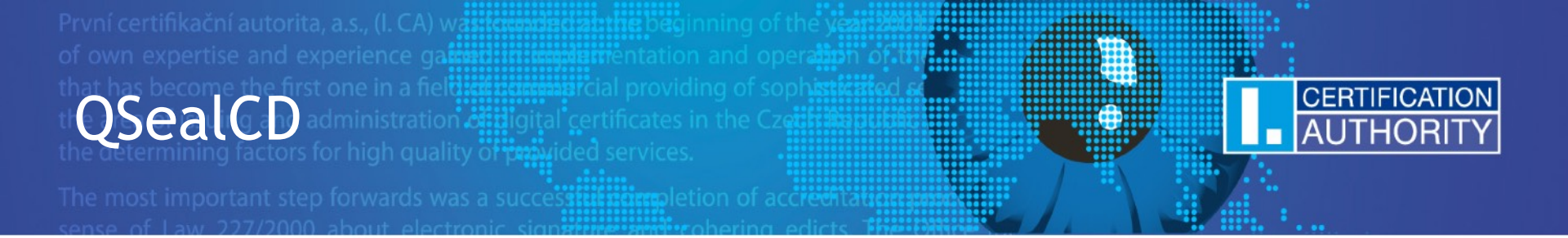
# QSealCD

| Name: | Qualified Signature and Seal Creation Device (QSCD) AliasLab CryptoAccelerator, release 3.5.1 |
|---|---|
| Applicant | AliasLab SpA, via Cremona 27/6, 46100 Mantova, Italy |
| Qualified Signature Creation Device (QSigCD) | yes<br>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 | Zentrum für sichere Informationstechnologie - Austria (A-SIT) |
| QSigCD designation date | 20.12.2017 |
| QSigCD designation expiry | Valid up to revocation by A-SIT |
| QSigCD designation report reference | A-SIT-VIG-17-083 |
| QSigCD designation report | https://www.a-sit.at/pdfs/qscd/VIG-17-083_QSCD_Certificate_CryptoAccelerator_signed.pdf |
| Art.30.3.(b) notified alternative certification method | https://www.a-sit.at/pdfs/merkblatt_de.pdf<br>https://www.a-sit.at/pdfs/merkblatt_en.pdf |
| CC certification report reference | HSM (subcomponent) certified by OCSI<br>http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf |
| Qualified Seal Creation Device (QSealCD) | yes<br>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 | Zentrum für sichere Informationstechnologie - Austria (A-SIT) |
| QSealCD designation date | 20.12.2017 |
| QSealCD designation expiry | Valid up to revocation by A-SIT |
| QSealCD designation report reference | A-SIT-VIG-17-083 |

| | |
|---|---|
| QSealCD designation report | https://www.a-sit.at/pdfs/qscd/VIG-17-083_QSCD_Certificate_CryptoAccelerator_signed.pdf |
| Art.30.3.(b) notified alternative certification method | https://www.a-sit.at/pdfs/merkblatt_de.pdf<br>https://www.a-sit.at/pdfs/merkblatt_en.pdf |
| CC certification report reference | HSM (subcomponent) certified by OCSI<br>http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf |

Solo, Solo+ and Solo XC resp. Connect, Connect+ and Connect XC; Firmware Versions: 2.50.16 and 2.55.1 as well as 3.3.21 and 3.4.1; Manufacturer: Thales

# QSealCD



| List of QSCDs | |
|---|---|
| **Name:** | - |
| **Name:** | **ARX CoSign v8.2** |
| Applicant | ARX (Algorithmic Research, Ltd.) |
| **Qualified Signature Creation Device (QSigCD)** | yes<br>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<br>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 |

# I.CA RemoteSeal

## Jaké jsou možnosti pečetění?

1. QSealCD v držení pečetící osoby (pokud jsou data pro vytváření elektronických pečetí uchovávána v prostředí spravovaném zcela, nikoli však výhradně uživatelem) - certifikované čipové karty či HSM
2. QSealCD na dálku (pokud data pro vytváření elektronických pečetí spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru jménem pečetící osoby)
3. Zahraniční kvalifikovaní poskytovatelé.

**Služba I.CA RemoteSeal představuje variantu 2.**

# I.CA RemoteSeal

## Výhody využití služby pečetění na dálku

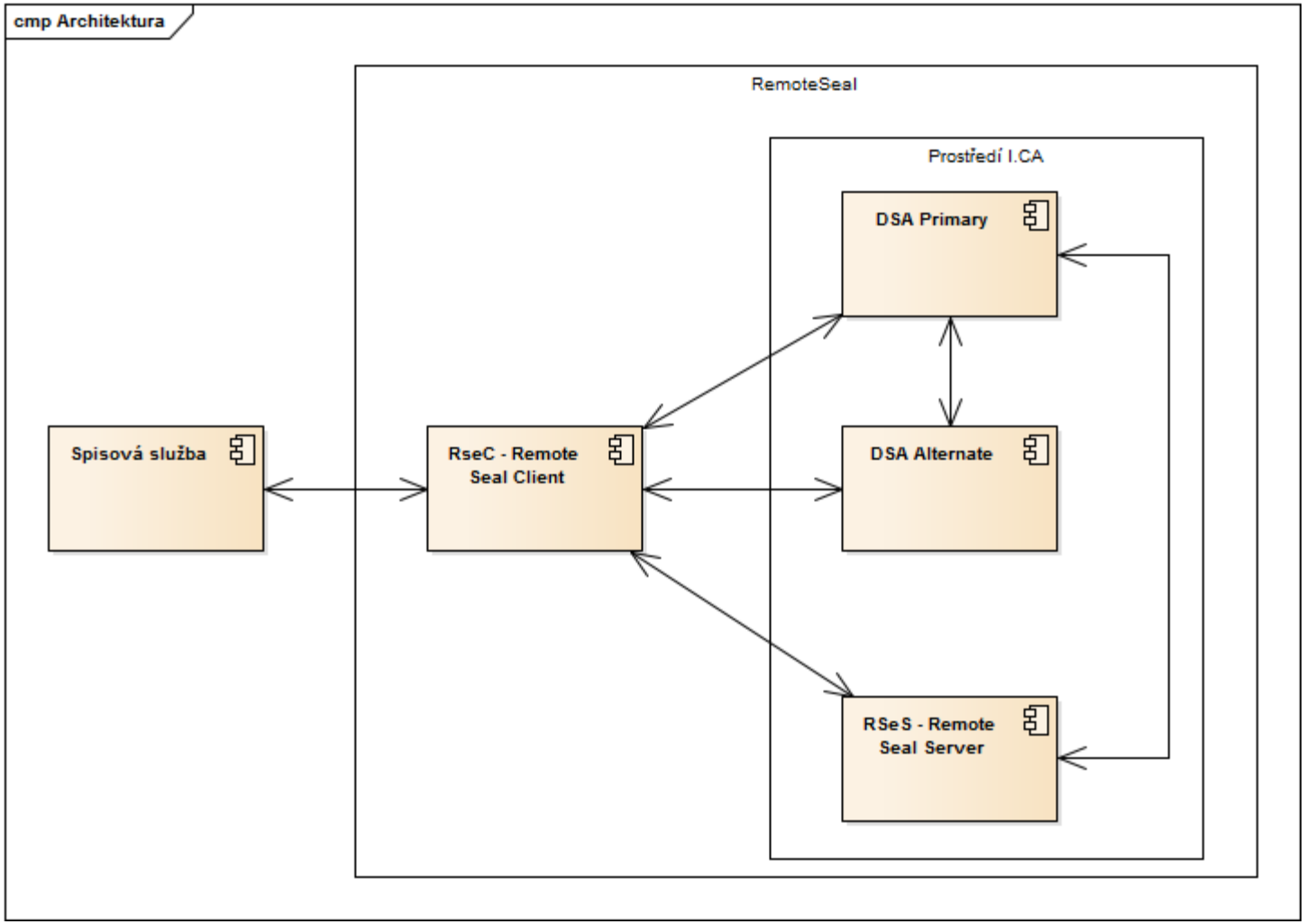
- uživatelé nemusí mít detailní technické znalosti HSM modulu a jeho ovládání
- není třeba zajistit investiční prostředky na nákup HSM modulu/ů, což znamená výraznou úsporu a minimální technické nároky.

# I.CA RemoteSeal

**Předpokládáme, že služba I.CA RemoteSeal bude auditována a orgánem dohledu zařazena na seznam služeb poskytovaných kvalifikovaným poskytovatelem služeb vytvářejících důvěru.**

# I.CA RemoteSeal

## Základní schéma služby:



# I.CA RemoteSeal

Základní popis:

1. Zřízení služby
2. Aktivace RemoteSeal klienta
3. Opečetění dokumentu
4. Automatické prodloužení služby
5. Vydání následného kvalifikovaného certifikátu pro elektronickou pečeť
6. Cenový model
7. Testování služby.

# I.CA RemoteSeal

## 1. Zřízení služby

- Mezi I.CA a klientem bude uzavřena smlouva.
- Oprávněná osoba klienta navštíví pobočku Registrační autority (RA).
- Operátor RA vydá klientovi prvotní autentizační komerční technologický certifikát na aktivační čipovou kartu . Certifikát je zaveden 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 RemoteSeal klienta založí pro klienta uživatele na HSM
  - ICARA provede aktivaci uživatelského účtu v HSM
  - ICARA provede pod účtem uživatele  generování párových dat pro vydání prvotního pečetícího certifikátu.
- Operátor RA pomocí ICARA podepíše žádost o vydání pečetícího certifikátu privátním klíčem párových dat na HSM

# I.CA RemoteSeal

## 1. Zřízení služby

- Oprávněná osoba klienta zadá PIN na pinpadové čtečce
- Na základě žádosti proběhne vydání pečetícího certifikátu
- Pečetící certifikát:
  - Je zaslán na e-mailovou adresu uživatele
  - ICARA uloží na čipovou kartu/token uživatele.
  - ICARA uloží do HSM
- Oprávněná osoba klienta odchází z RA s aktivační kartou.

## 2. Aktivace RemoteSeal klienta

- Pro aktivaci RemoteSeal klienta spustí oprávněná osoba klienta dodávanou GUI utilitu
- Utilita vyzve uživatele k vložení aktivační karty, načež utilita:
  - Naváže spojení s RemoteSeal klientem pomocí oboustranně autentizovaného HTTPS s prvotním autentizačním certifikátem (uživatel je vyzván k zadání PINu)
  - Automaticky vytvoří žádost o vydání následného autentizačního certifikátu, která je podepsána prvotním autentizačním certifikátem; privátní klíč je generován v RemoteSeal klientovi (nikoliv na kartě)
  - Žádost je odeslána ke zpracování do I.CA, kde se obratem vydá následný certifikát a ten se stáhne zpět do utility
- Následně utilita vytvoří aktivační soubor, kde bude uložen následný autentizační certifikát včetně privátního klíče
- Uživatel tento aktivační soubor následně načte do aplikace volající RemoteSeal klienta (např. spisové služby).

# I.CA RemoteSeal

## 3. Opečetění dokumentu

- Proces opečetění dokumentu inicializuje volající aplikace (např. spisová služba), která má integrovanou knihovnu RemoteSeal klient
- Spisová služba předá do RemoteSeal klienta dokument k opečetění spolu s nastavením pečetění (viditelný/neviditelný podpis, formát, přidání TS, atp.) + aktivační soubor vzniklý při aktivaci RemoteSeal klienta
- RemoteSeal klient připraví dokument k podpisu - sestaví žádost o opečetění (obsahující jednoznačný textový identifikátor – např. č.j.), parametry podpisu, hash původního dokumentu a hash, který bude vstupem pro výpočet kryptogramu
- Tato žádost bude podepsána pomocí následného autentizačního certifikátu
- Následně RemoteSeal klient naváže oboustranně autentizovaný TLS kanál pro komunikaci s RemoteSeal serverem v I.CA

## 3. Opečetění dokumentu

- Navázaným kanálem předá podepsanou žádost o opečetění RemoteSeal serveru
- Následně je na HSM vytvořen kryptogram pomocí privátního klíče pečetícího certifikátu
- RemoteSeal klient využije kryptogram pro kompletaci podepsaného dokumentu
- Pokud je vyžadován podpis s časovým razítkem, je TS do dokumentu přidáno nyní, přičemž RemoteSeal klient se vůči TSA autentizuje pomocí následného autentizačního certifikátu
- Hotový opečetěný dokument je vrácen volající aplikaci/spisové službě.

## 4. Automatické prodloužení služby

- Součástí RemoteSeal klienta je funkcionalita automatické obnovy následného autentizačního certifikátu a nahrání nově vydaného certifikátu do RemoteSeal klienta.

## 5. Vydání následného kvalifikovaného certifikátu pro elektronickou pečeť

- V rámci automatického prodloužení služby bude také probíhat automatická obnova pečetícího certifikátu
- RemoteSeal klient s určitým předstihem před expirací certifikátu vygeneruje v HSM nový pár klíčů a vytvoří žádost o vydání následného certifikátu, kterou opečetí původním certifikátem
- Žádost o následný certifikát se zpracuje v I.CA standardní cestou
- RemoteSeal klient následně uloží do HSM následný certifikát a od toho okamžiku jej začne pro pečetění využívat.

## 6. Cenový model

Půjde o kombinaci paušálního poplatku a jednotkové ceny za jedno opečetění v množstevních pásmech obdobných časovým razítkům.

Aktivační čipová karta/token, autentizační certifikáty (prvotní i následné), pečetící certifikáty, pomoc při implementaci RemoteSeal klienta – jsou poskytovány zdarma v rámci služby.

## 7. Testování

Pro zájemce bude služba pro testování k dispozici do cca 2 týdnů, je možné se obrátit na remoteseal@ica.cz.

# Závěr

Děkuji za pozornost.

Ing. Roman Kučera
kucera@ica.cz