



# Služba vzdáleného pečetění I. CA RemoteSeal

Ing. Roman Kučera  
První certifikační autorita, a.s.  
24. 4. 2019



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 od 20. září 2018.**

**Ve zkratce - kde je dnes značka, musí být pečet'**

## e- značka *versus* e-pečet'

- Elektronickou pečetí může dokument opatřit pouze **původce dokumentu** - pozor při příjmu elektronických dokumentů.
- Kvalifikovaný certifikát pro elektronickou pečet' nelze vydat na fyzickou osobu, ale pouze na **právníckou osobu**.
- Elektronickou značku (založena na systémovém certifikátu) není možné použít od 20.9.2018 pro označování odchozích dokumentů orgány veřejné moci. **Je nutné použít kvalifikovanou elektronickou pečet'.**

## 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



## POVINNÉ ZVLÁŠŤOVANÉ INFORMACE

Úvodní strana / Kvalifikovaní / CIDAS, digitální podpis / Vybírat kvalifikované informace

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

Můžete využít naše webové stránky a kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru.

Police ČR 0

Hasiči ČR 0

Státní služba

Registr smluv

CENTRUM PROTI TERORISMU A HYBRIDNÍM HROZBÁM

GDPR

Číslo	Kvalifikovaný poskytovatel služeb vytvářejících důvěru	Kvalifikované služby	Zahájení poskytování
1.	<b>První certifikační autorita, a.s.</b> IČU 26432035, Průmyslová ul. 717/16, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů pro elektronický podpis (příloha č. 1 k vyhlášce č. 112/2014 ze dne 10. 1. 2014) a) jakožto o službu vydávání kvalifikovaných certifikátů, Kvalifikované služby vykazování přílohy č. 1 k vyhlášce č. 112/2014 ze dne 10. 1. 2014 pro elektronický podpis a pečeti Vydávání kvalifikovaných certifikátů pro elektronický podpis, Vydávání kvalifikovaných certifikátů pro elektronický podpis a pečeti, Vydávání kvalifikovaných certifikátů pro elektronický podpis Internetových stránek	01/2007 04/2017 01/2017 01/2017 02/2018
2.	<b>Česká pošta, a.s.</b> IČU 47114283, I. Národní tř. 42/10 100 04, PSČ 200 99 Praha 1	Vydávání kvalifikovaných certifikátů pro elektronický podpis (příloha č. 1 k vyhlášce č. 112/2014 ze dne 10. 1. 2014) a) jakožto o službu vydávání kvalifikovaných certifikátů, Vydávání kvalifikovaných certifikátů pro elektronický podpis Vydávání kvalifikovaných certifikátů pro elektronický podpis internálních stránek, Vydávání kvalifikovaných certifikátů pro elektronický podpis	01/2005 01/2017 01/2017 08/2017

<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

## 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 (malí klienti) či HSM (velcí klienti disponující odborným zázemím)
2. QSealCD na dálku - pokud data pro vytváření elektronických pečetí spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru jménem pečetící osoby = velcí klienti

**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.



**Služba I.CA RemoteSeal byla auditována a orgánem  
dohledu v červnu 2018 zařazena na seznam služeb  
poskytovaných  
kvalifikovaným poskytovatelem služeb vytvářejících  
důvěru.**

Identifikátor 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.

# I.CA RemoteSeal



Služba umožňuje pečetění dokumentů kvalifikovanou elektronickou pečetí s privátním klíčem uloženým v certifikovaném HSM modulu.

HSM modul je umístěn v prostředí I.CA, v prostředí klienta je instalován klient RSeC, který komunikuje se serverem RSeS a HSM modulem.

Služba umožňuje pečetit dokumenty ve formátech:

CAdES-B-B, CAdES-B-T PAdES-B-B, PAdES-B-T XAdES-B a XAdES-T

K pečetěnému dokumentu je možné připojit kvalifikované elektronické časové razítko I.CA.

*Oceněna časopisem ComputerWorld jako IT produkt roku 2018 v kategorii on-line služby.*

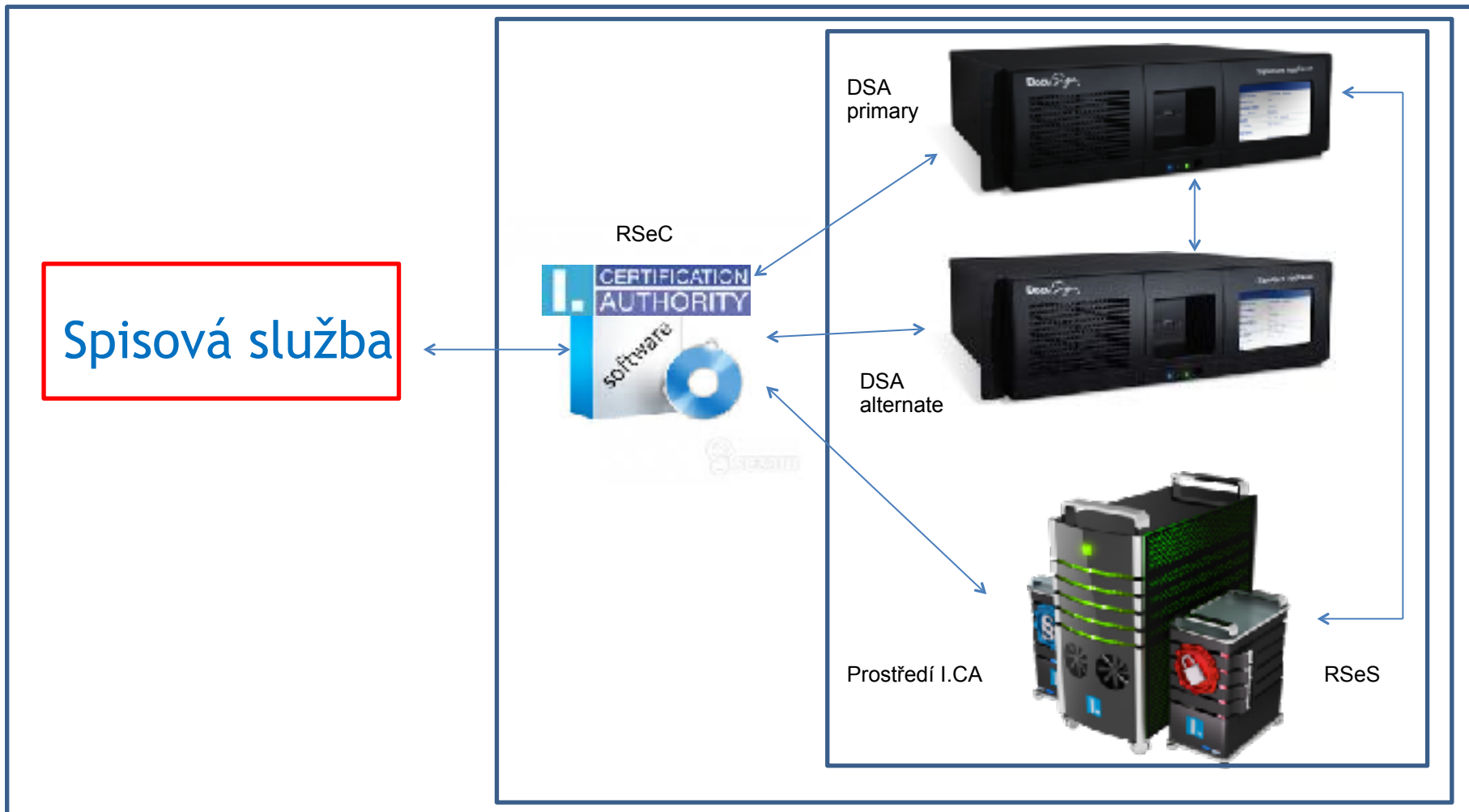
# I.CA RemoteSeal



# I.CA RemoteSeal



## Základní schéma služby:



# Architektura - popis komponent systému



Model architektury vychází z draftu normy EN 419 241-1 z roku 2017, resp. normy publikované v červenci 2018.

Norma definuje základní bezpečnostní požadavky na vytváření podpisu/pečetě na dálku jménem podepisující/pečetící osoby.

Tyto požadavky musela I.CA dodržet při návrhu řešení a byly též předmětem auditu.

# Architektura - popis komponent systému



- **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** - DocuSign Signature Appliance - certifikovaný QSealCD HSM modul.
- **RSeActivationUtil** - Aktivační utilita sloužící k aktivaci RSeC pomocí tzv. aktivační karty.

# Proces opečetění dat



Spisová  
služba

Dokument k opečetění, parametry požadovaného opečetění, číslo  
jednací, aktivační soubor



Opečetěný dokument

klient

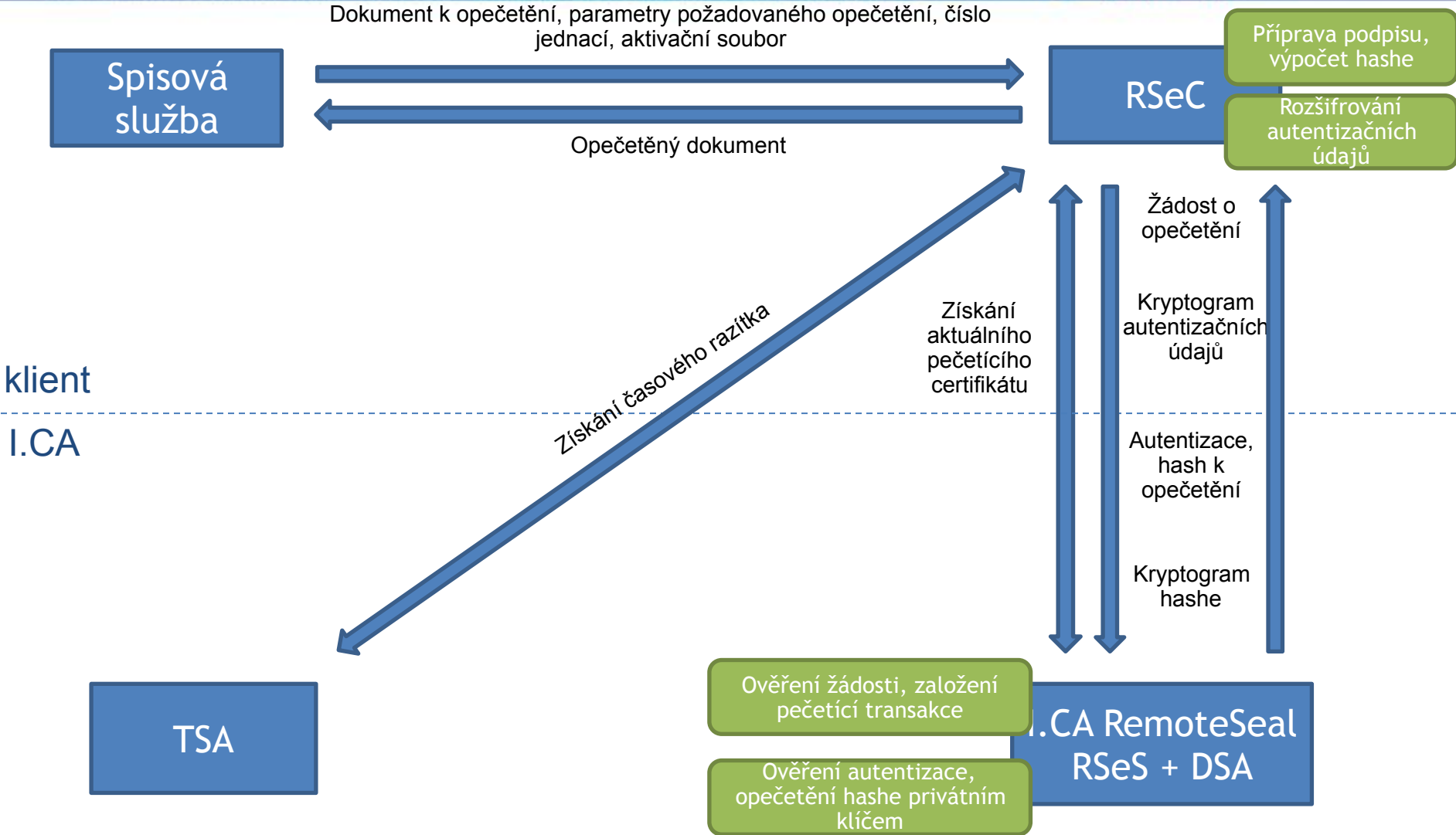
I.CA

I.CA RemoteSeal

# Proces opečetění dat



První certifikační autorita, a.s. (I.CA) was established at the beginning of the year 2000. It is a company of own expertise and experience gained in the implementation and operation of information systems in the area of issuing and administration of digital certificates. In the Czech Republic, the determining factors for high quality of provided services. The most important step forwards was a successful completion of accreditation process in the year 2001. In the year 2002, the act of Law 237/2002 about electronic signatures was published. It is the first step towards the implementation of the act of Law 237/2002 about electronic signatures and creating e-signatures.





# I.CA RemoteSeal



- Zřízení služby
- Aktivace RemoteSeal klienta
- Automatické prodloužení služby = vydání následného kvalifikovaného certifikátu pro elektronickou pečeť i autentizačního certifikátu

**Pro klienty, jež měli problém s přístupností přes proxy soustavu do Internetu, byla služba rozšířena o variantu I.CA RSeProxy.**

Komponenta RSeProxy je jednou z klientských komponent k systému RemoteSeal, jedná se o SOAP webovou službu určenou k nasazení na Windows Server v prostředí klienta, přičemž koncová aplikace, jež požaduje pečetění, komunikuje přes SOAP přímo s RSeProxy, které pak interně komunikuje se službou RemoteSeal na straně I.CA pro vytvoření kvalifikované elektronické pečeti a popř. přidání časového razítka.

V klientském prostředí tedy běží služba I.CA RSeProxy, která poskytuje do vnitřní sítě webové rozhraní. Všechny počítače využívající službu pečetění komunikují pouze s touto službou a přístupy do Internetu tudíž nepotřebují. Přístup do I.CA má povolen pouze ten server, na kterém služba RSeProxy, běží. Aktivační soubor se nachází také na Windows serveru.

# Testovací aplikace



## Součástí klienta RSeC je testovací

TestApp RSeC.NET

Input:

ActivationFile:  Browse...  as byte[]

File to sealed:  Browse...

Options:

Signature type:  CAES  PAdES  XAdES

Hash algorithm: sha256 Document ID (optional):   Add TimeStamp

Signature options - PAdES:

Visible signature Location:  Reason:

Visible signature options:

Type: TextOnly Document page: 1

Description:

Dimension [ mm ]:

X:  Y:

Width:  Height:

Background image:  Browse...  as byte[]

Signature image:  Browse...  as byte[]

Seal document

# Obchodní model



Jde o kombinaci paušálního poplatku a jednotkové ceny za jedno opečetění v množstevních pásmech (obdobně časovým razítkům). Při nulovém odběru pečetí není paušální poplatek hrazen.

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

Je také možné dodat HSM modul (či koupí klient) do prostředí klienta, avšak v módu „black box“ se správou kvalifikovaného poskytovatele.

# Produkční prostředí



Služba I.CA RemoteSeal je poskytována:

1. na základě přímého smluvního vztahu I.CA a klienta
2. prostřednictvím dodavatelů spisových služeb
  1. Gordic spol. s r.o. 27 klientů
  2. VERA, spol. s r.o. 9 klientů
  3. PilsCom, s.r.o. 11 klientů

Služba je v produkčním prostředí využívána více než 100 klienty.

Prvním klientem bylo Ministerstvo průmyslu a obchodu pro RŽP.

Počet odebraných pečetí/časových razítek je cca 100 - 250 tis. /  
měsíc

# Závěr

První certifikační autorita, a.s. (ICA) was founded at the beginning of the year 2005. It has a long history of expertise and experience gained in the implementation and operation of ICA, which is the first one in a field of official providing of sophisticated services in the area of issuing and administration of digital certificates in the Czech Republic. The determining factors for high quality of provided services.

The most important step forwards was a successful completion of accreditation process of law 237/2001 about electronic signatures and related acts. The first



Děkuji za pozornost.

Roman Kučera

[kucera@ica.cz](mailto:kucera@ica.cz)

[remoteseal@ica.cz](mailto:remoteseal@ica.cz)

[www.ica.cz/remote-seal](http://www.ica.cz/remote-seal)