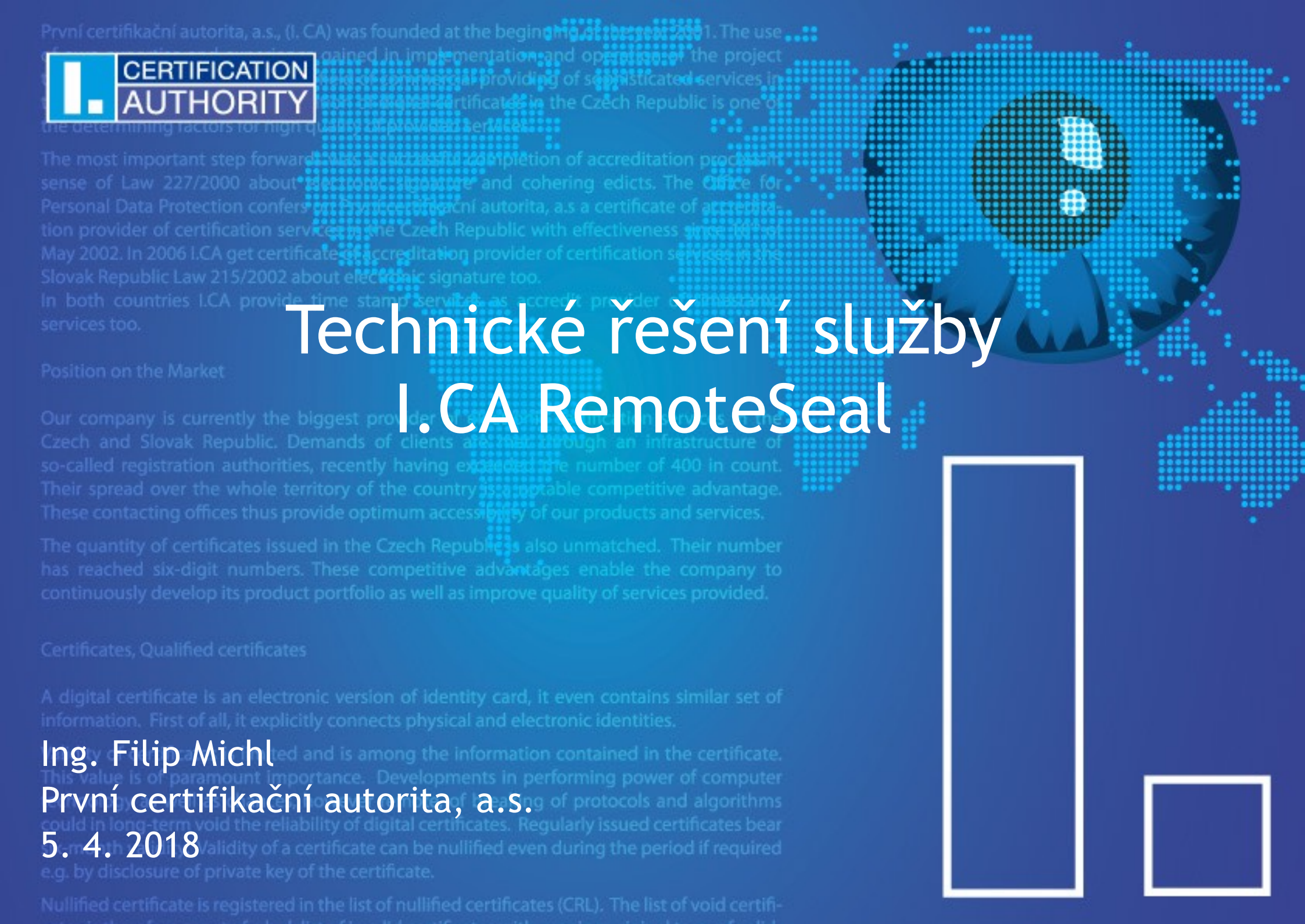


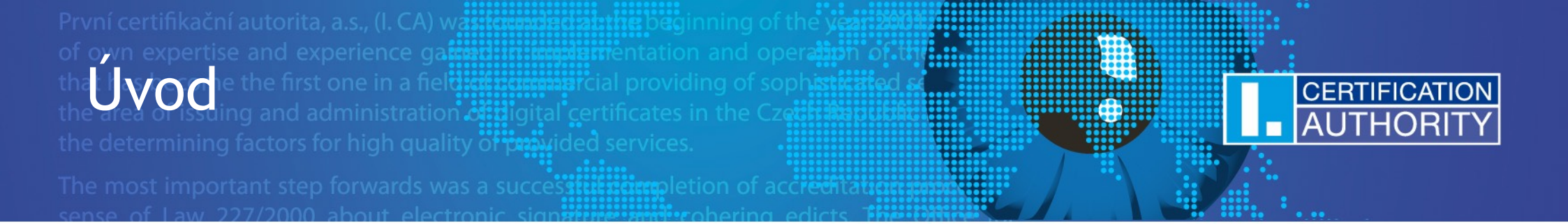
Technické řešení služby I.CA RemoteSeal

Ing. Filip Michl
První certifikační autorita, a.s.
5. 4. 2018

Agenda

- Úvod
- ARX CoSign vs. DocuSign Signature Appliance
- Architektura
- Zřízení služby
- Aktivace služby
- Klientská komponenta
- Proces opečetění dat
- Automatické prodloužení služby
- Webové rozhraní
- Bezpečnost

Úvod



- I.CA RemoteSeal – služba pro vzdálené vytváření **Kvalifikovaných elektronických pečetí**

- Nejvyšší možná forma elektronické pečetě, vyžadující:
  - Kvalifikovaný certifikát pro elektronické pečetě (QcStatement 6.2)
  - Privátní klíč vygenerovaný a uchovávaný v certifikovaném QSealCD zařízení.
  - Zajištění bezpečného způsobu autentizace uživatele vůči QSealCD zařízení za účelem použití privátního klíče.

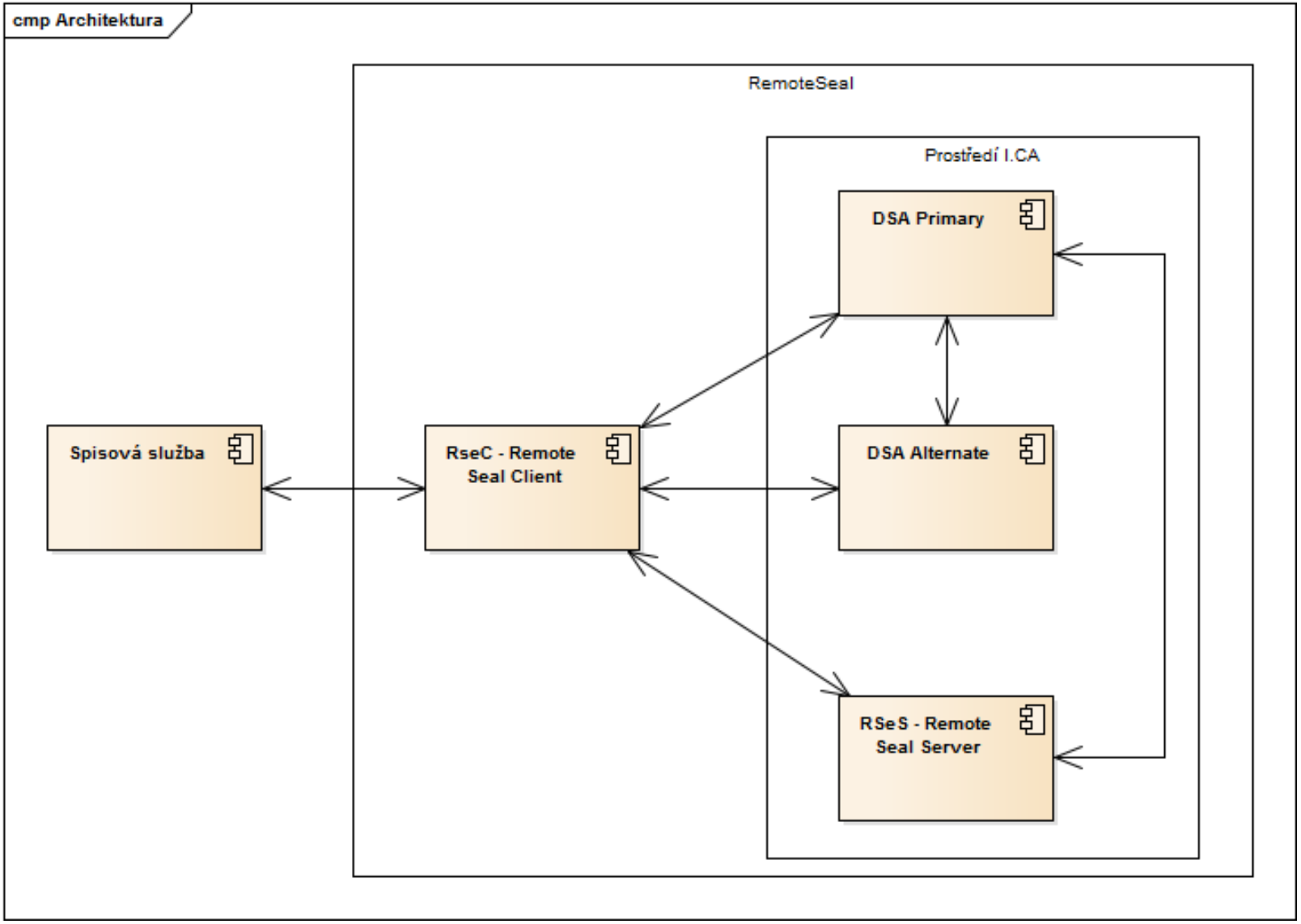
DocuSign Signature Appliance alias ARX CoSign

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

DocuSign Signature Appliance alias ARX CoSign

- Zařízení certifikováno jako QSealCD
  - viz https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds
- Certifikace (resp. specifikovaný Security Target) umožňuje využít zařízení jako HSM modul pro vytváření kvalifikované pečeti na dálku pouze při splnění podmínky:
  - Zařízení musí být provozováno Kvalifikovaným poskytovatelem služeb vytvářejících důvěru.
- Zařízení generuje, uchovává a používá privátní klíče takovým způsobem, že je nelze v otevřené podobě exportovat.
- Zařízení poskytuje REST API over HTTPS pro realizaci pečetění a potřebný management.
- Dvojici zařízení je možné provozovat v režimu High Availability.
- Zařízení je certifikováno dle Common Criteria for Information Technology Security Evaluation, version 3.1 revision 4 s úrovní záruk EAL4+

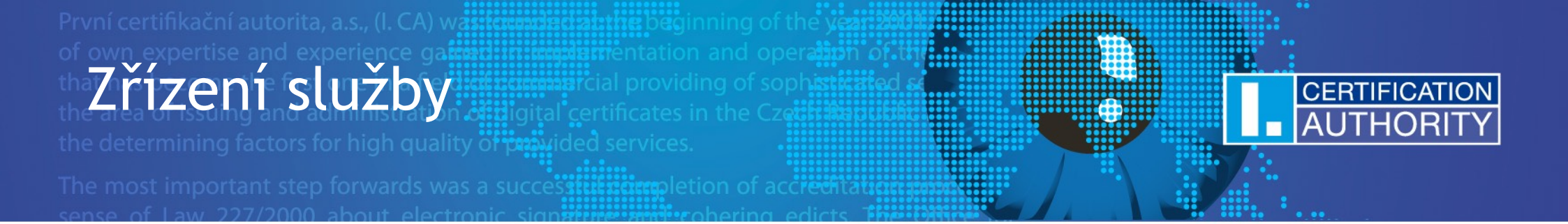
Architektura



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.

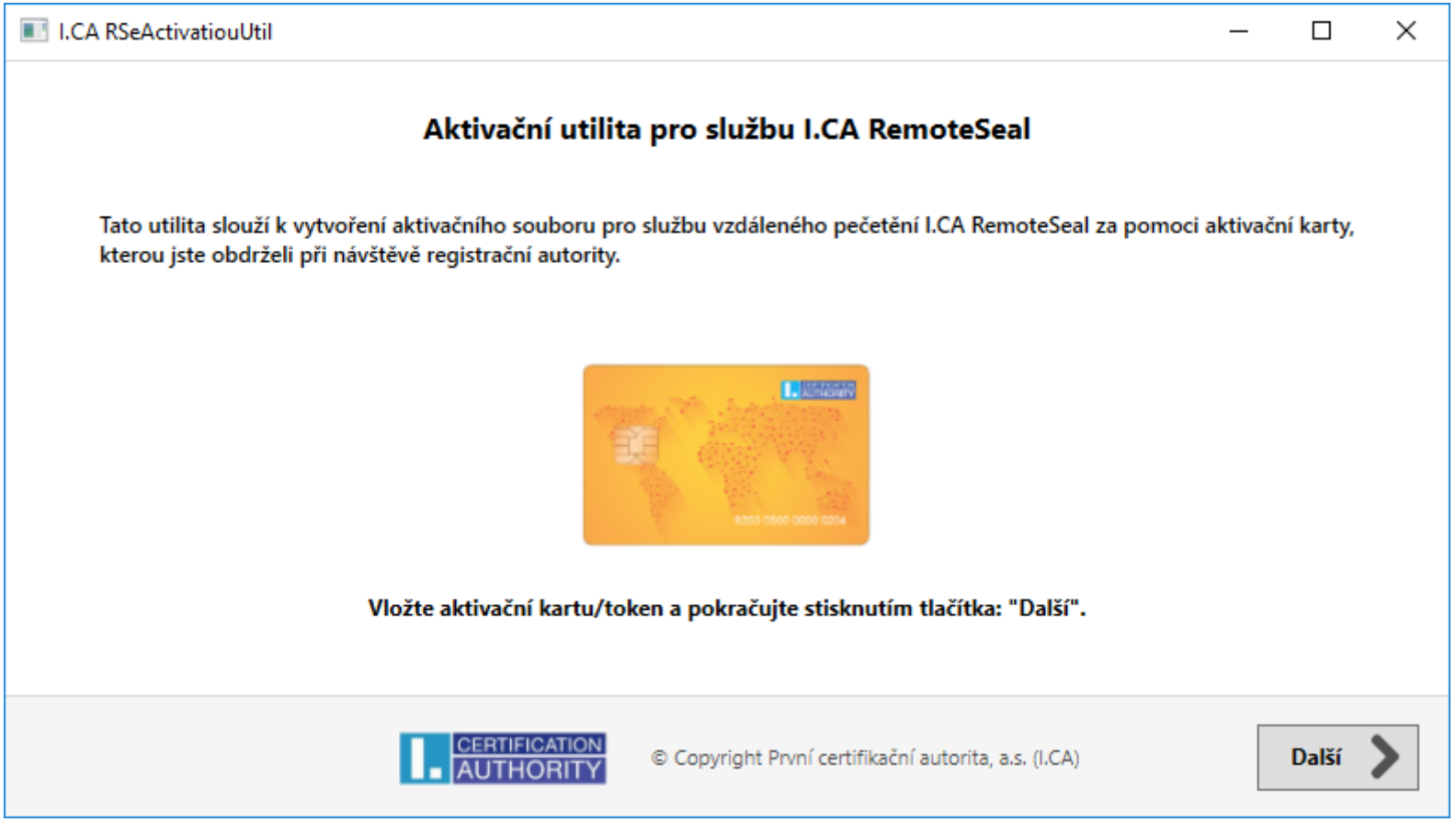
Zřízení služby



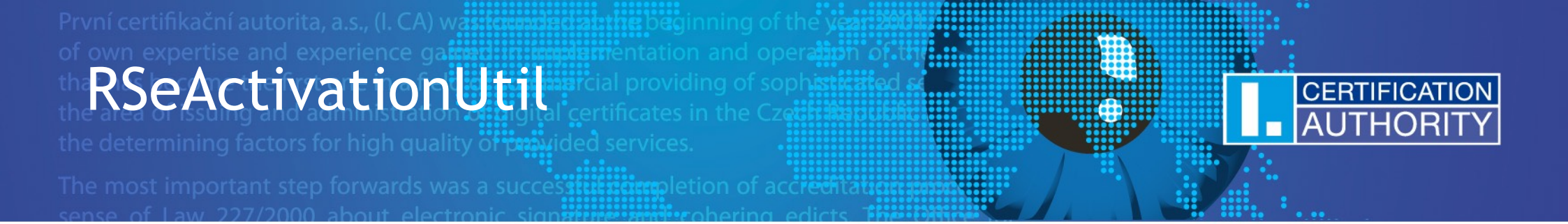
- Probíhá návštěvou oprávněné osoby klienta na Registrační autoritě (RA).
- Před návštěvou RA není potřeba generovat žádnou žádost.
- Oprávněná osoba si odnáší aktivační kartu, na které je:
  - Prvotní autentizační certifikát včetně privátního klíče
  - Pečetící certifikát (pouze veřejná část klíče)
- V tuto chvíli je aktivační karta resp. privátní klíč autentizačního certifikátu jediná možnost, jak dešifrovat autentizační údaje k DSA.

Aktivace RemoteSeal Clienta

- Oprávněná osoba spustí dodávanou utilitu RSeActivationUtil



RSeActivationUtil

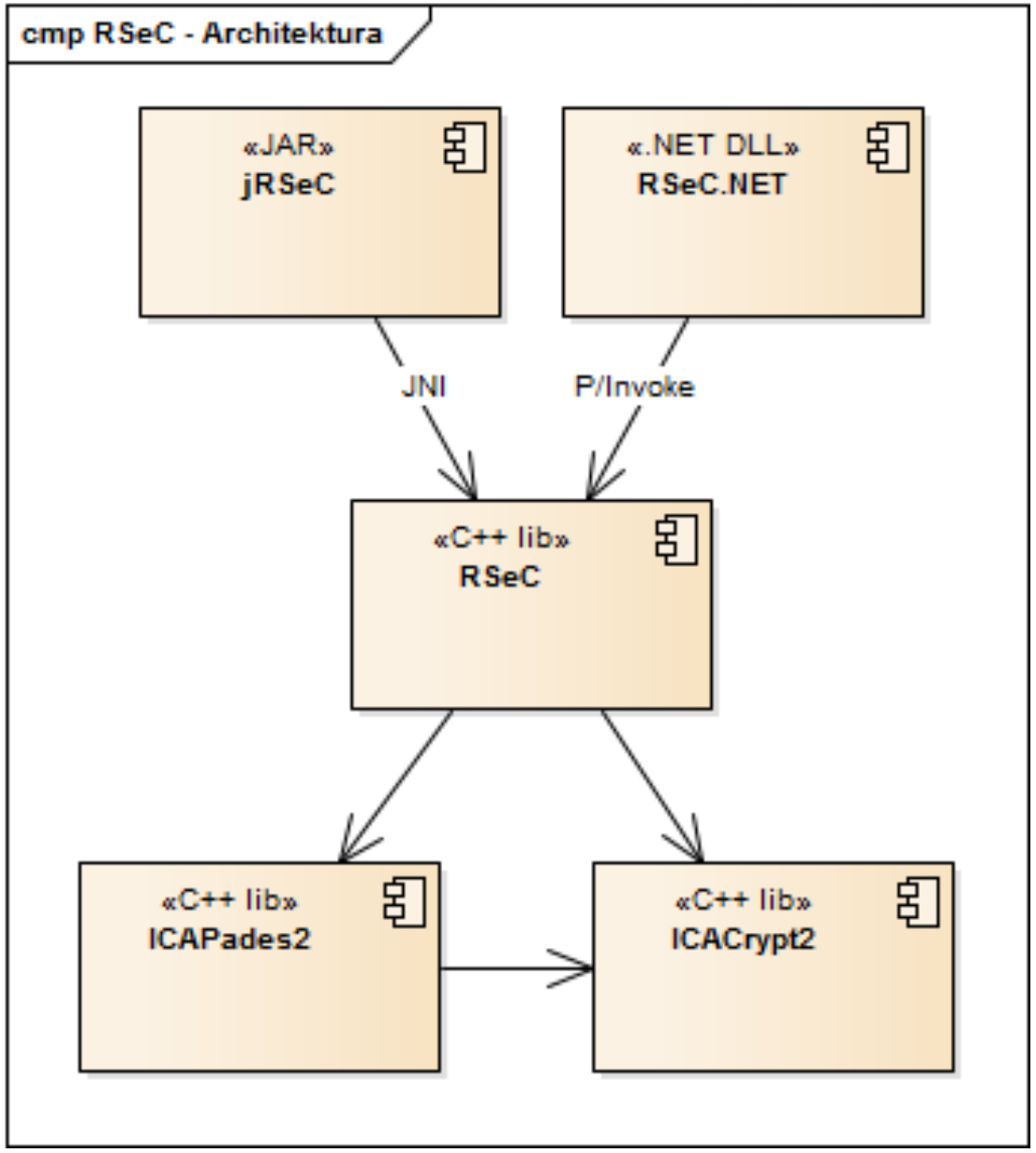


- Po vložení aktivační karty a stisku tlačítka „Další“ utilita:
  - Naváže oboustranně autentizovaný HTTPS kanál s RemoteSeal serverem.
  - Automaticky vytvoří a odešle ke zpracování žádost o vydání následného certifikátu k prvotnímu autentizačnímu certifikátu.
  - Po vydání následného certifikátu je tento automaticky získán z CA.
  - Provede přešifrování kryptogramu autentizačních údajů k DSA uloženého na RSeS, kvůli zajištění přístupu i pomocí následného certifikátu.
  - Následný certifikát včetně privátního klíče vyexportuje utilita do aktivačního souboru. Obsah aktivačního souboru je šifrován tak, že jej není možné použít jinak než v RSeC.
- Uživatel tento aktivační soubor následně načte do aplikace volající RSeC (typicky do spisové služby).

RSeActivationUtil – technické parametry

- Jednoduchá Windows GUI utilita.
- Nemusí být spouštěna na stejném PC, na kterém je provozován RSeC.
- Vyžaduje: .NET 4.0

RSeC - Architektura



- 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.

RSeC – 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

- Podepisovaná data (business obsah) nikdy neopouští volající systém (komponentu RSeC)!

Proces opečetění dat

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

Spisová služba

Opečetěný dokument

klient

I.CA

I.CA RemoteSeal

Proces opečetění dat

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

Spisová služba

RSeC

Příprava podpisu, výpočet hashe

Rozšifrování autentizačních údajů

Opečetěný dokument

Žádost o opečetění

Získání aktuálního pečetícího certifikátu

Kryptogram autentizačních údajů

Autentizace, hash k opečetění

Kryptogram hashe

Získání časového razítka

klient

I.CA

TSA

Ověření žádosti, založení pečetící transakce

Ověření autentizace, opečetění hashe privátním klíčem

I.CA RemoteSeal RSeS + DSA

Automatické prodloužení služby

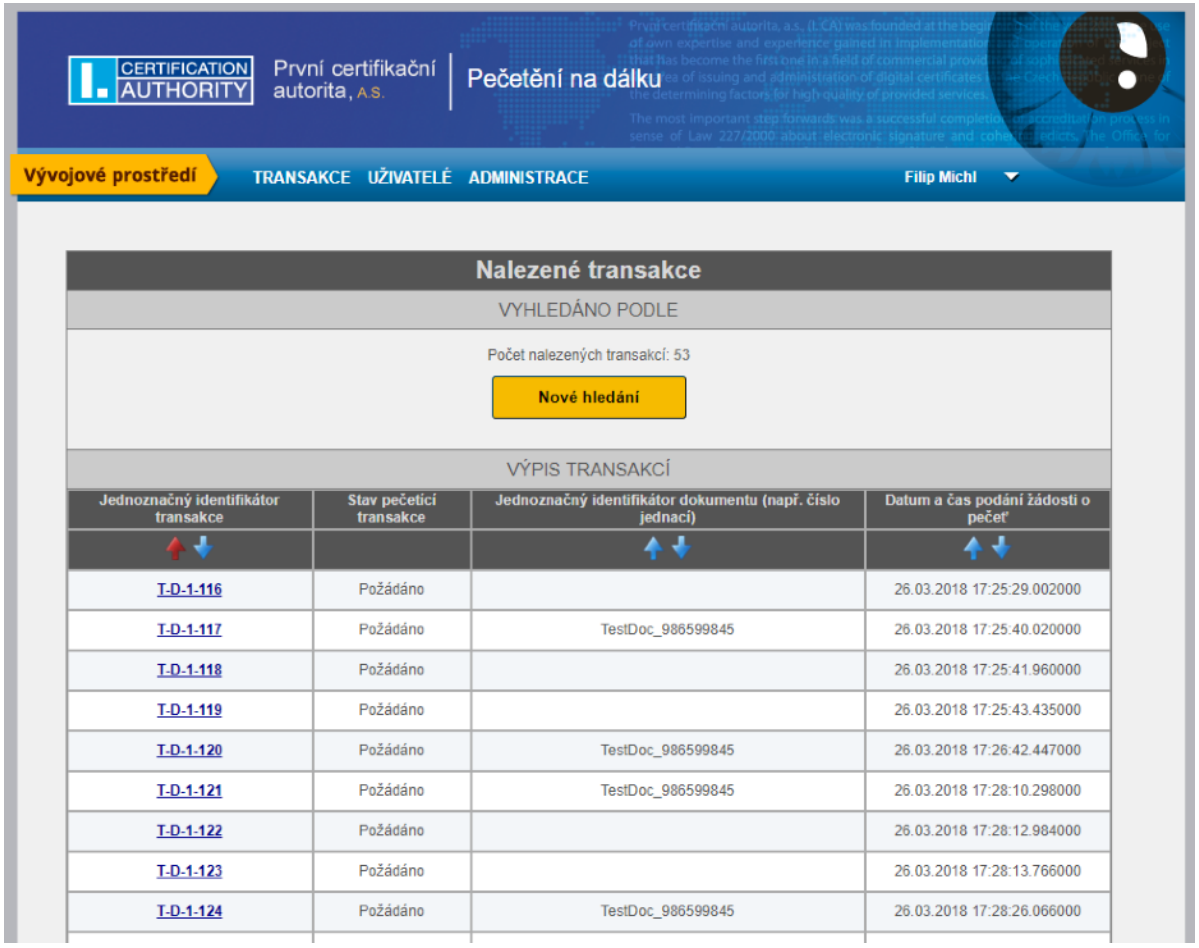
- RSeC disponuje funkcionalitou automatické obnovy autentizačního certifikátu.
- Před koncem platnosti autentizačního certifikátu je automaticky vytvořena žádost o následný certifikát, která je odeslána na I.CA.
- V rámci odeslání žádosti je veřejný klíč zaregistrován na RSeS a dojde k přešifrování autentizačních dat k DSA pro umožnění přístupu pomocí následného certifikátu.
- Po vydání následného autentizačního certifikátu je tento stažen a automaticky se začne využívat pro autentizaci k RSeS.
- Celý tento proces se děje zcela automatizovaně a transparentně vůči volající aplikaci a probíhá jako součást operace opečetění dat.
- Z hlediska volající aplikace stačí zajistit, aby došlo cca 1x za 14 dní k opečetění libovolného dokumentu.

Automatické vydání následného pečetícího certifikátu

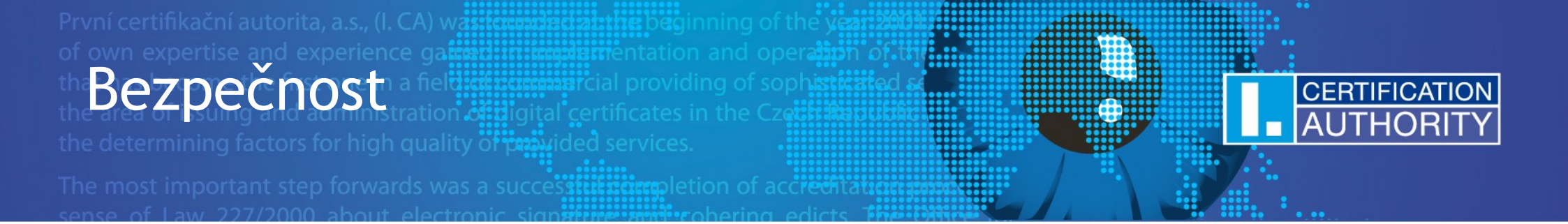
- Před koncem platnosti pečetícího certifikátu dojde prostřednictvím RSeC k vygenerování nového klíčového páru v DSA a vygenerování a opečetění žádosti o následný certifikát původním pečetícím certifikátem.
- Tato žádost je zpracována v I.CA standardní cestou.
- Po vydání certifikátu provede RSeC registraci certifikátu do DSA a RSeS a tento se tímto okamžikem začne automaticky používat pro vytváření kvalifikovaných elektronických pečetí.
- Tento proces je plně automatický a z volající aplikace transparentní.
- Z hlediska volající aplikace stačí zajistit, aby došlo cca 1x za 14 dní k opečetění libovolného dokumentu

Webové uživatelské rozhraní

- Webové uživatelské rozhraní umožňuje oprávněné osobě klienta:
  - Procházet a prohledávat seznam provedených opečetění
  - Hledat např.: dle data, hashe dokumentu nebo čísla jednacího
  - Prohlížet detailní informace zda a kdy a jakým certifikátem byl daný dokument opečetěn.

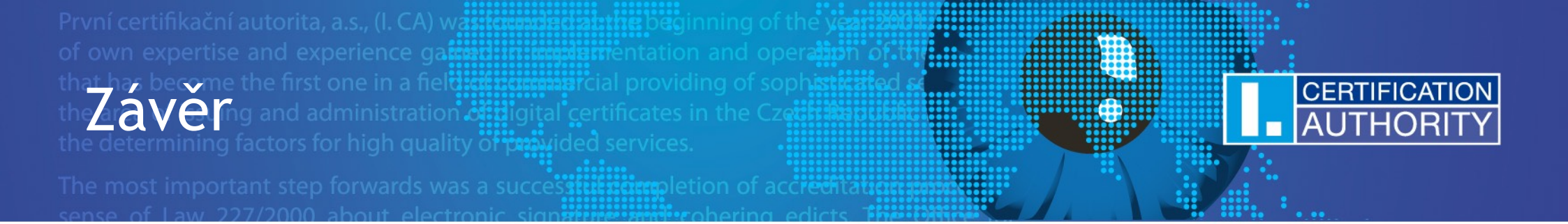


Bezpečnost



- DSA je včetně svého řešení autentizace certifikováno jako řešení pro vytváření Kvalifikované elektronické pečetě.
- Přesto I.CA RemoteSeal přidává další bezpečnostní prvky:
  - Zamezení potenciální možnosti zkopírování autentizačních údajů do DSA mezi návštěvou RA a aktivací služby díky bezpečné aktivační čipové kartě.
  - Zakládání transakcí na RSeS prostřednictvím oboustranně autentizovaného HTTPS kanálu pro zpřístupnění zašifrovaným autentizačních dat k DSA.
  - Runtime kontrola integrity klientské komponenty RSeC (i RSeActivationUtil).
  - Zabezpečení komunikačního kanálu RSeC-DSA pomocí techniky Certificate Pinning.
  - Kontrola integrity konfigurace RSeC proti neoprávněným změnám.
  - Možnost zpětné kontroly seznamu opečetěných dokumentů.

Závěr



Děkuji za pozornost.

Ing. Filip Michl
michl@ica.cz