Úložiště certifikátů pro vzdálené podepisování

Plány a první výsledky společného projektu VVŠ v roce 2019

Daniel Kouřil, Michal Procházka, Jiří Bořík, Jan Chvojka, Erik Horváth

cesnet

MUNI

Motivace

- Kvalifikovaný podpis
  - Kvalifikovaný certifikát
    - Vydaný akreditovanou CA
  - Kvalifikovaný prostředek pro podepisování
    - (QSCD - Qualified Signature Creation Device)
    - Certifikované čipové karty nebo „Hardware Security Module“
- Podpora podepisování v organizaci
  - Podpora CA, kontrola životního cyklu certifikátu
  - Použití QSCD

Čipové karty jako QSCD

- Nové fyzické zařízení
  - Pořízení, výměna, rušení HW řešení
  - Náklady na provoz a uživatelskou podporu
- Přijetí technologie uživateli
  - Uživatelská přívětivost
  - Správné používání zařízení
  - Kompatibilita se zařízeními
- Zapojení podepisování do existujících „workflow“
  - Často portálová řešení pro oběh dokumentů
  - Zapojení lokálních úložišť je složité
- Podpora mobilních zařízení
  - HW úložiště nelze připojit

Podepisování jako služba

- Centralizované řešení pro správu certifikátů a soukromých klíčů
  - Správa certifikátů
  - Úložiště podepisovacích dat
  - Provádění kryptografických operací s podepisovacími daty
- Soukromý klíč chráněn pomocí kvalifikovaných prostředků
- Dostupné jako služba
- Uživatelsky přímočaré workflow pro podpisy
  - informační systém pošle dokument k podpisu
  - Uživatel autorizuje přístup k soukromému klíči (PIN)
  - Aplikace provede podepsání, příp. naformátování výsledku
  - Výstup vrátí zpět do informačního systému

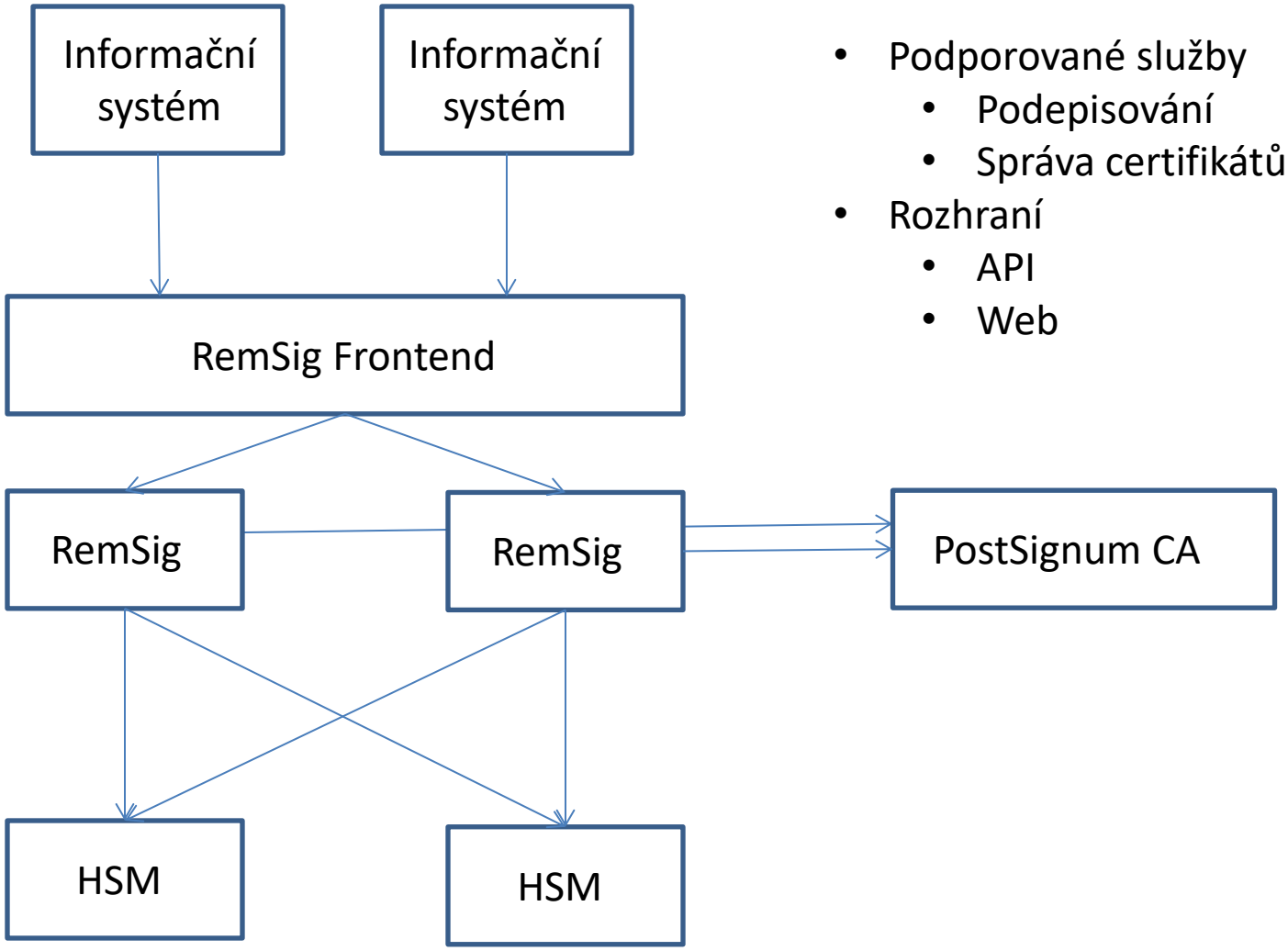
Zkušenosti s úložištěm

- RemSig na Masarykově univerzitě
  - V produkčním provozu od 2015
  - Napojení na administrativní agendu INET
    - ČNB, ČSSZ, interní agenda, pracovní výkazy
    - PDF dokumenty
  - Pouze pro uznávané elektronické podpisy
    - Ochrana klíčů pouze v softwarových úložištích

Společné úložiště osobních kvalifikovaných certifikátů

- Projekt v rámci výzvy digitalizace 2018 a eIDAS
- Vytvoření infrastruktury v souladu s eIDAS
  - Společné certifikované úložiště podepisovacích dat (nad HSM)
  - Podpisová aplikace dostupná přes API
  - Ověřování podpisů,
  - Správa certifikátů
- Provoz bude zajišťovat CESNET pro své členy

Architektura



- Podporované služby
  - Podepisování
  - Správa certifikátů
- Rozhraní
  - API
  - Web

Aktuální stav

- Rozšíření aplikace RemSig
  - Podpora HSM, podpora formátů podpisů dle eIDAS
- Zajištění certifikátů pro kvalifikovaný podpis
  - Zprovoznění HSM, smlouvy s PostSignum CA o vystavování certifikátů
- Ověřovací provoz od počátku 2019 na MU
  - Převedení stávajících certifikátů
  - Podepisování některých agend kvalifikovaným podpisem

Plán 2019

- Cílem je pilotní nasazení celého řešení a jeho ověření
  - Podepisování formou služby, pomocí kvalifikovaných certifikátů CA PostSignum
  - Aplikace pro řízení životního cyklu osobních certifikátů
  - Dostupné API
- Webová aplikace pro podpis dokumentů
- Integrace s vybranými univerzitními informační systémy
  - Spolupráce s MU a ZČU, další dle aktuálního stavu
- Právní stanovisko dokládajícího soulad navrženého řešení s nařízením eIDAS

Integrace do informačních systémů

- Požadované služby
  - Podepisování
  - Správa certifikátů
- Míra integrace
  - Zapojení do procesů (API)
  - Využití externích aplikací
  - Podpora newebových aplikací
    - PKCS11, Windows CSP, …
- Testovací prostředí k dispozici cca od května
- Aktivity na straně koncových systémů nejsou součástí projektu

Shrnutí

- Centralizované řešení pro kvalifikované podpisy
  - Uživatelsky přívětivé řešení
  - Využívající certifikované prvky pro soukromé klíče
- Plánováno jako služba sdružení CESNET
- Integrace pomocí API nebo vyhrazených aplikací
- Pilot, ověření a zhodnocení během 2019
- https://eidas.cesnet.cz/