cesnet

eIDAS

Michal Procházka

3. 9. 2024

Obsah

- Stručný úvod do problematiky elektronického podepisování eIDAS
- RemSig
- eIDAS služby CESNET
- Statistiky, ceník

Pojmy

- Kvalifikovaný certifikát
  - Certifikát vydaný kvalifikovaným poskytovatelem služeb vytvářejících důvěru a poskytující kvalifikované služby vytvářejících důvěru - PostSignum
- Typy elektronických podpisů
  - **Kvalifikovaný elektronický podpis osoby**
    - Založený na kvalifikovaném certifikátu s privátním klíčem generovaným na certifikovaném zařízení (QSCD - qualified signature creation device)
  - **Kvalifikovaná elektronická pečeť**
    - Založený na kvalifikovaném certifikátu s privátním klíčem generovaným na certifikovaném zařízení, určený pro systémy
- Kvalifikované časové razítko
  - Časové razítko vydané kvalifikovaným poskytovatelem služeb vytvářejících důvěru a poskytující kvalifikované služby vytvářejících důvěru

- Vše definováno nařízením eIDAS č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu

CESNET eIDAS služby

- Kvalifikovaný elektronický podpis/pečeť dokumentů a dat
  - Odkudkoliv
  - Kdykoliv
  - Ve velkém množství a rychle
  - Bez nutnosti mít hardwarové zařízení pro každého uživatele
- Kvalifikované i nekvalifikované časové razítko
  - K jakémukoliv dokumentu
- Validaci kvalifikovaných elektronických podpisů a pečetí
  - Příchozí elektronicky podepsaný dokument musí být validován

Cíl

- Podpora kvalifikovaného podpisu, pečetě a razítka ve všech agendách, službách a aplikacích z jednoho místa
- Minimalizace uživatelské interakce
  - Při získání certifikátu
  - Prodlužování certifikátu
  - Podpisu/pečetění
- Soulad s nařízením eIDAS č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu

RemSig

- Služba vyvíjená a používaná od roku 2015 na MUNI
- Systém pro správu certifikátů a privátních klíčů s možností vytváření vzdálených podpisů
- Poskytuje API pro integraci informačních systémů
- Napojena na CA PostSignum přes API

Formální spojení s PostSignum

Služby

- Dostupné přes API
  - Správa kvalifikovaných certifikátů
  - Kvalifikované podpisy
  - Kvalifikované pečetění
  - Kvalifikovaná časová razítka
  - Validace elektronických podpisů
- Dostupné přes RemSig GUI
  - Správa kvalifikovaných certifikátů
  - Kvalifikované podpisy
  - Kvalifikované pečetění
  - Kvalifikovaná časová razítka
  - Validace elektronických podpisů

Správa kvalifikovaných certifikátů

Správa kvalifikovaných certifikátů

- Kvalifikované certifikáty od PostSignum CA
  - Umístěné na certifikovaném zařízení (QSCD)
- Žádost i obnova certifikátu přes webové rozhraní RemSig nebo přes IS
- Podpora PUK
  - Vygenerované heslo, které lze použít k resetu hesla k certifikátu
- Deaktivace certifikátu

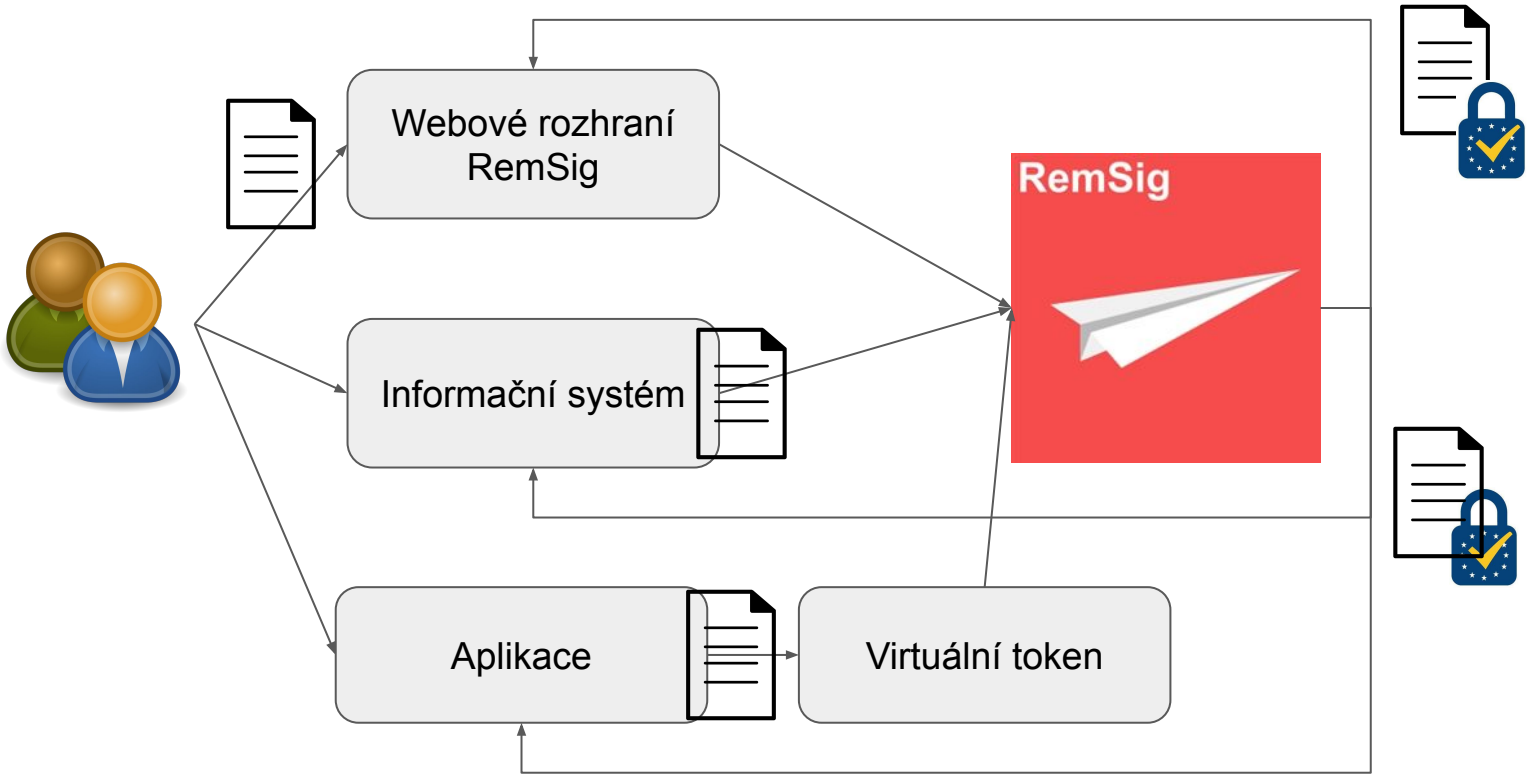
Kvalifikované podpisy

Kvalifikovaný podpis

- Kvalifikovaný certifikát umístěný na certifikovaném zařízení => **kvalifikovaný podpis**

- Formy podpisu
  - PDF
  - PKCS#1
  - PKCS#7

Schéma integrace



Podpis přes informační systém

- IS komunikuje s RemSig přes API
- Podpis PDF dokumentů a dat (PKCS#1, PKCS#7)
- Podpora dávkového podepisování
  - Asynchronní
- Podpora časových razítek
- Podpora umístění viditelného vodoznaku
- Heslo k certifikátu se zadává mimo IS

Virtuální token

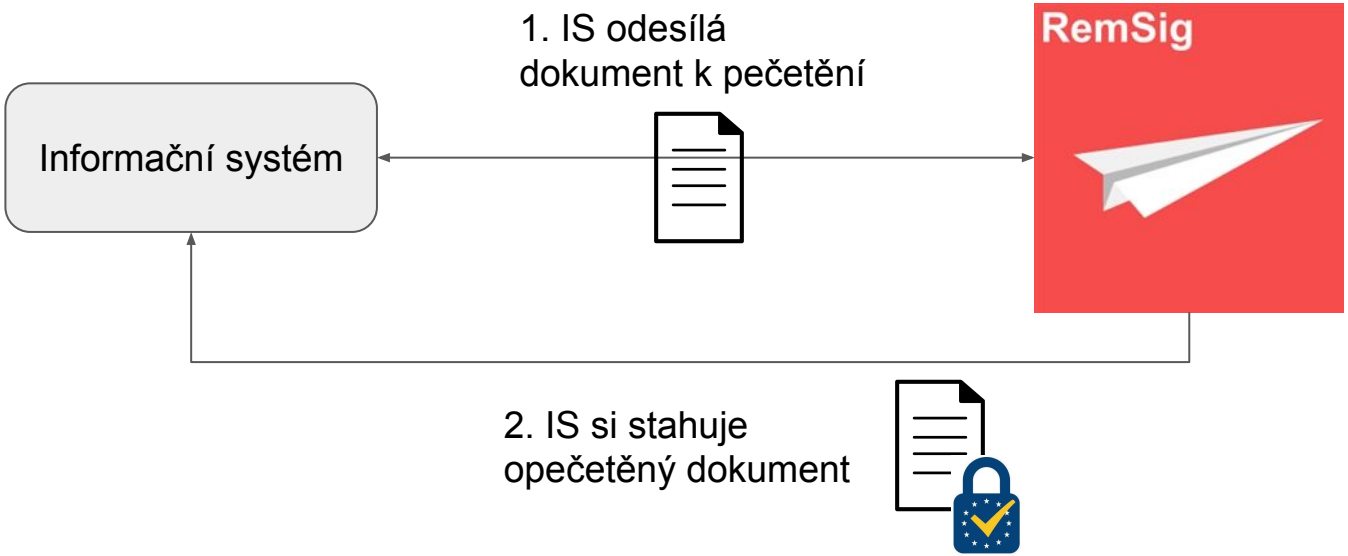
Podpis přes virtuální token

- Zpřístupnění certifikátu z RemSig v systémovém úložišti certifikátů Windows a MacOS
  - Virtuální token pro MacOS je samostatná zpoplatněná služba
- Automatická integrace do aplikací využívající systémové úložiště Windows a MacOS
  - Např. Adobe Acrobat, EZAK
- Výměna certifikátu probíhá pouze na jednom místě
- Lze podepisovat i ze zařízení, která nemají USB port
- Není nutné pořizovat, distribuovat a spravovat USB tokeny

Kvalifikované pečetě

Kvalifikované pečetě

- Určeno pro systémy, které automatizovaně pečetí dokumenty a data
- Kvalifikovaná pečeť je určena pro organizaci



Časová razítka

Časová razítka

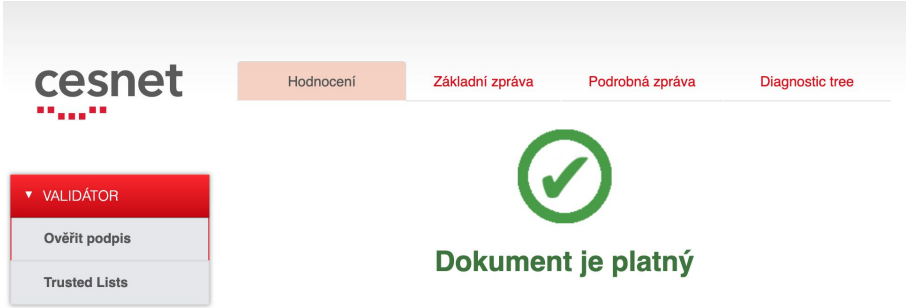
- Při podpisu přes API lze specifikovat, zda má být dokument opatřen časovým razítkem

- Dva režimy pro výběr časového razítka
  - Časová razítka v rámci eIDAS služeb CESNET
    - Kvalifikované časové razítko od PostSignum
    - Nekvalifikované od CESNET TSA
  - Vlastní poskytovatel časových razítek
    - Při žádosti o podpis se vloží identifikace poskytovatele a přístupové údaje
    - Přístupová data jsou po použití zahozena

Validace digitálních podpisů

Validace digitálních podpisů

- Kontrola, zda je podpis na dokumentu validní
  - Různé druhy politik



- Možnosti validace
  - Přes webové rozhraní
  - API - přes rozhraní informačního systému

- Dostupný na https://validator.eidas.cesnet.cz
- Metodický návod pro ověřování platnosti uznávaných podpisů a pečetí (MVČR)
  - https://www.mvcr.cz/soubor/metodicky-navod-pro-overovani-platnosti-uznavanych-podpisu-a-peceti.aspx

Validace digitálních podpisů

- Výsledek validace dokumentu
  - Dokument je platný
  - Dokument obsahuje části, které jednoznačně nepotvrzují platnost
  - Dokument je neplatný
  - Dokument není podepsaný

- Prezentace výsledku ve 4. úrovních
  - Ano/Ne
  - Jednoduchý report - čitelný běžným uživatelem
  - Detailní report - popisující proces validace
  - Diagnostic Tree - detailní report v podobě XML

Typy podpisů

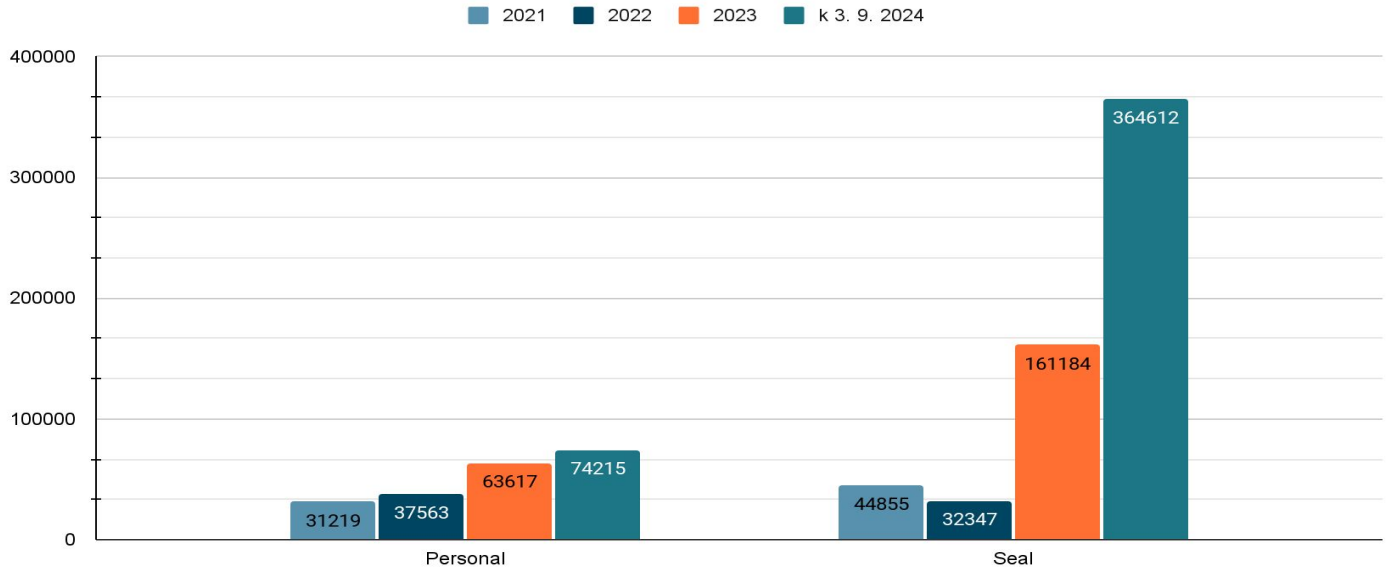
Typy podpisů

- Formáty
  - **PAdES** - PDF
  - XAdES - XML
  - CAdES - binární data
- Úrovně podpisu
  - **B-B**
    - Základní podpis
  - **B-T Level**
    - Podpis + časové razítko
  - **B-LT Level**
    - Podpis + časové razítko + validační informace k certifikátu
  - B-LTA Level
    - Podpis + časové razítko + validační informace k certifikátu + časové razítko na validační informace

Statistiky

Statistiky

- 17 připojených institucí
- 760 platných kvalifikovaných certifikátů z 1134 celkově
- 17 platných kvalifikovaných pečetí z 48 celkově



Zvýhodněné ceny od PostSignum

Zvýhodněné ceny od PostSignum

	Cena bez DPH
Kvalifikovaný certifikát pro el. podpis (platnost 1 rok)	212,73 Kč
Kvalifikovaný certifikát pro el. podpis (platnost 3 roky)	531,82 Kč
Kvalifikovaný certifikát pro el. pečeť (platnost 1 rok)	419,01 Kč
Kvalifikovaný certifikát pro el. pečeť (platnost 3 roky)	1 047,52 Kč

Dodatečná sleva při zřízení vlastní registrační autority.

Odkazy

Více informací na https://eidas.cesnet.cz

Dotazy směřovat na eidas@cesnet.cz

RemSig: https://remsig.cesnet.cz

Validátor: https://validator.eidas.cesnet.cz