Popis služby centrálního úložiště certifikátů

Cíl dokumentu

Dokument popisuje službu sloužící ke správě certifikátů a vytváření kvalifikovaných digitálních podpisů dle Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 pro partnery rozvojového projektu “eIDAS 2019”. Popis obsahuje funkční vlastnosti, ale také obecné technické specifikace platné pro pilotní fázi do 31.12.2019.

Poskytované služby

V rámci pilotního provozu bude pro každého účastníka projektu k dispozici sada služeb pro správu osobních certifikátů v centrálním uložišti, vzdálené podepisování dokumentů a ověřování platnosti podpisů elektronických dokumentů. Konkrétněji:

- Správa kvalifikovaných certifikátů uživatelem
- Správa kvalifikovaných certifikátů zaměstnanců organizace
- Vytváření kvalifikovaných digitálních podpisů dokumentů a dat
- Ověření platnosti uznávaného a kvalifikovaného digitálního podpisu dokumentů

Popis rozhraní

- REST rozhraní přes protokol HTTPs, datové zprávy jsou v JSON
- Webové (uživatelské) rozhraní
    - Pro správu certifikátu uživatelem
        - Podání žádosti o nový certifikát
        - Prodloužení platnosti certifikátu
    - Pro správu certifikátů zaměstnanců
        - Schvalování žádostí o vydání certifikátu
        - Přehled vydaných certifikátů
    - Pro podepisování dokumentů
    - Pro ověření platnosti podpisu
- Aplikační (strojové) rozhraní
    - Pro správu certifikátů zaměstnanců
        - Schvalování žádostí o vydání certifikátu
        - Přehled vydaných certifikátů
    - Pro podepisování dokumentů
    - Pro ověření platnosti podpisu

Použité technologie

- HSM nShield provozované v zabezpečeném prostředí
- Kvalifikované certifikáty od PostSignum
- RemSig jako software pro správu certifikátů a vytváření digitálních podpisů
- Validátor digitálních podpisů dokumentů s vazbou na národní eIDAS bránu

Výkonové parametry

- HSM umožňuje 430 podpisů za vteřinu. Počet podpisů za jednotku času v systému RemSig závisí na vstupních parametrech (např. velikost podepisovaného dokumentu)
- Maximální počet certifikátů spravovaných systém RemSig je nejméně 1000 certifikátů pro každou VVŠ. Vyšší počet je po konzultaci možný.
- Dostupnost v pilotním provozu je garantována v pracovní době, tzn. 8:00 – 17:00 v pracovní dny. Reakce na výpadek je nejpozději následující pracovní den

Podpora implementace a straně VVŠ

V rámci pilotního provozu bude poskytnuta individuální podpora všem účastníkům projektu. Půjde především o:

- Kompletní dokumentaci k aplikačnímu rozhraní
- Testovací prostředí pro vývojáře informačních systémů
- Konzultace k připojení jednoho strojového rozhraní pro každou VVŠ v maximálním rozsahu 8 hodin

Vývojové a implementační práce na straně informačních systémů VVŠ není součástí této podpory, VVŠ si musí tyto práce zajistit u dodavatele informačního systému nebo jiným způsobem.

Produkční prostředí

Po ukončení pilotní fáze na konci roku 2019 bude převedeno do produkčního režimu, který bude mít tyto technické vlastnosti:

- 2x HSM geograficky oddělené (Praha, Brno), provozované v zabezpečeném prostředí
- 2x RemSig servery geograficky oddělené (Praha, Brno), provozované v zabezpečeném prostředí