cesnet

NOVÉ SLUŽBY CESNET PRO eIDAS

Jiří Bořík
CESNET

konference e-infrastruktury CESNET 2019
Praha

CESNET a eIDAS

- Nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách … je v platnosti
- V akademickém prostředí se přímo dotýká především VVŠ, v rámci jejich role Orgánu veřejné moci
- Východiska
  - Dlouhodobá diskuze o eIDAS na klubu ředitelů a dalších platformách
  - Plánované výstupy některých projektů v rámci CRP 2018
  - Výzva digitalizace v září 2018
  - Zkušenosti MU s provozem úložiště osobních certifikátů
  - Dlouhodobé zkušenosti CESNET s provozem PKI infrastruktury
  - Získání ISMS certifikace v roce 2018
- Pro rok 2019 zahájen společný projekt CESNETu a univerzit pro přípravu vybraných eIDAS služeb, především:
  - Centrální úložiště kvalifikovaných certifikátů
  - Podpisová aplikace s možností napojení na IS VVŠ
  - Validace podpisů na elektronických dokumentech
  - Ostatní související služby

FÁZE PROJEKTU

- **Přípravná fáze (do ledna 2019)**
  - Technické konzultace s partnery
  - Právní analýza dopadů eIDAS na VVŠ
- **Realizační fáze (2019)**
  - Centrální úložiště kvalifikovaných certifikátů
  - Validace podpisů na elektronických dokumentech
  - Vazba nejprve na CA PostSignum
  - Podpora napojení IS univerzit na centralizované služby
- **Další rozvoj (2020 a dále)**
  - Stabilizace provozu hlavních služeb, (výkon, redundance)
  - Další partneři (ostatní CA a případně další kvalifikované služby)
  - Varianty služeb (vyhrazená HSM, vlastní instance SW…)
  - Další vlastní certifikované služby (časová razítka?)

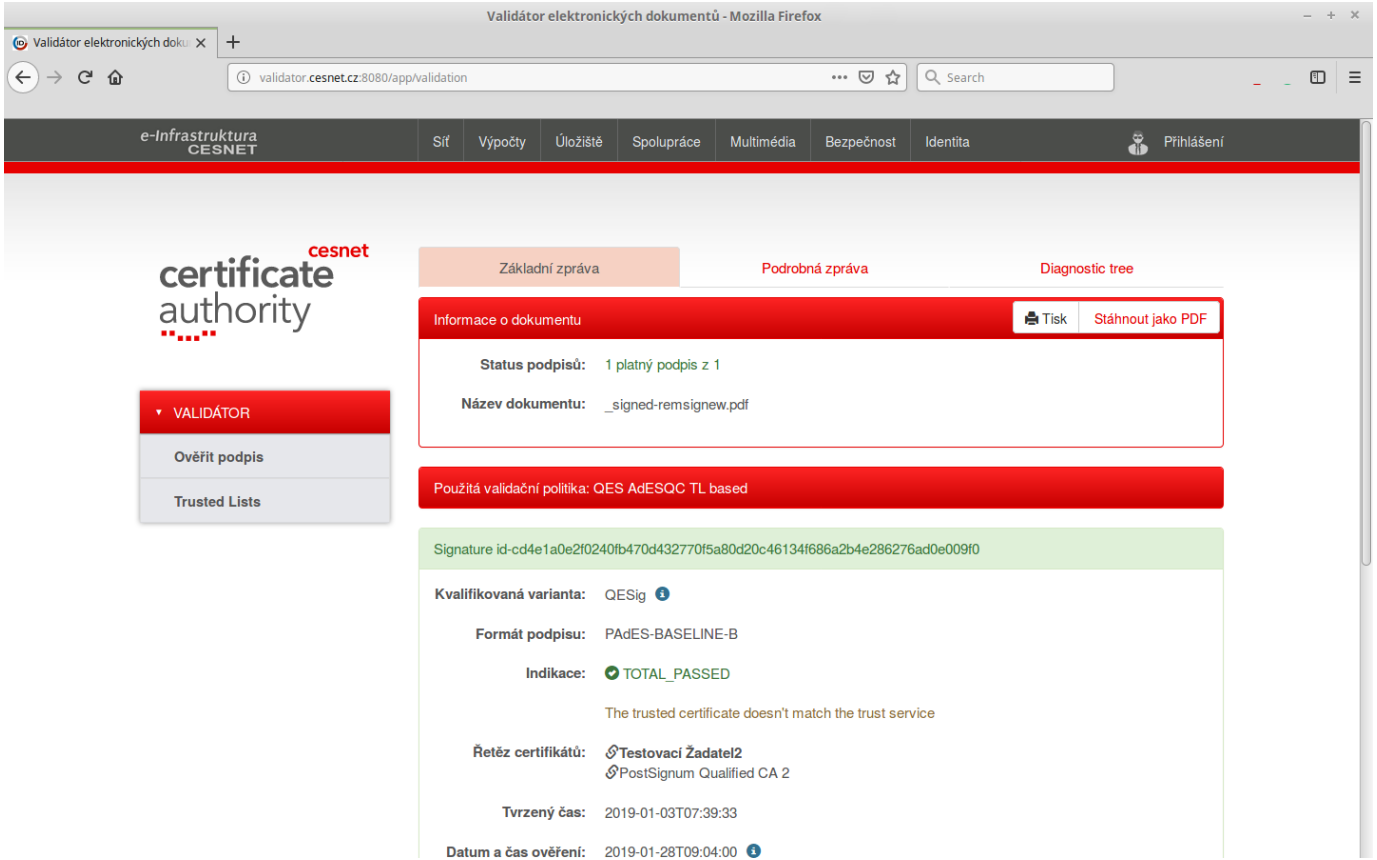
CENTRÁLNÍ PODPISOVÁ SLUŽBA

- **Úložiště certifikátů**
  - Certifikované HSM, QSCD - Qualified Signature Creation Device
- **Bezpečná a dostupná infrastruktura**
  - Geografické rozmístění Praha-Brno,
  - Fyzická bezpečnost zařízení
- **Modul pro řízení certifikátů**
  - Životní cyklus certifikátu (žádost, vystavení, revokace)
  - Uživatelské i admin rozhraní
- **Podpisový modul**
  - Vazba na centrální QSCD
  - Rozhraní pro podepisování
    - Podpis pomocí web aplikace
    - API pro informační systémy
    - Lokální API (virtuální čipová karta) Windows, MacOS
- **Podrobnosti v následující prezentaci**

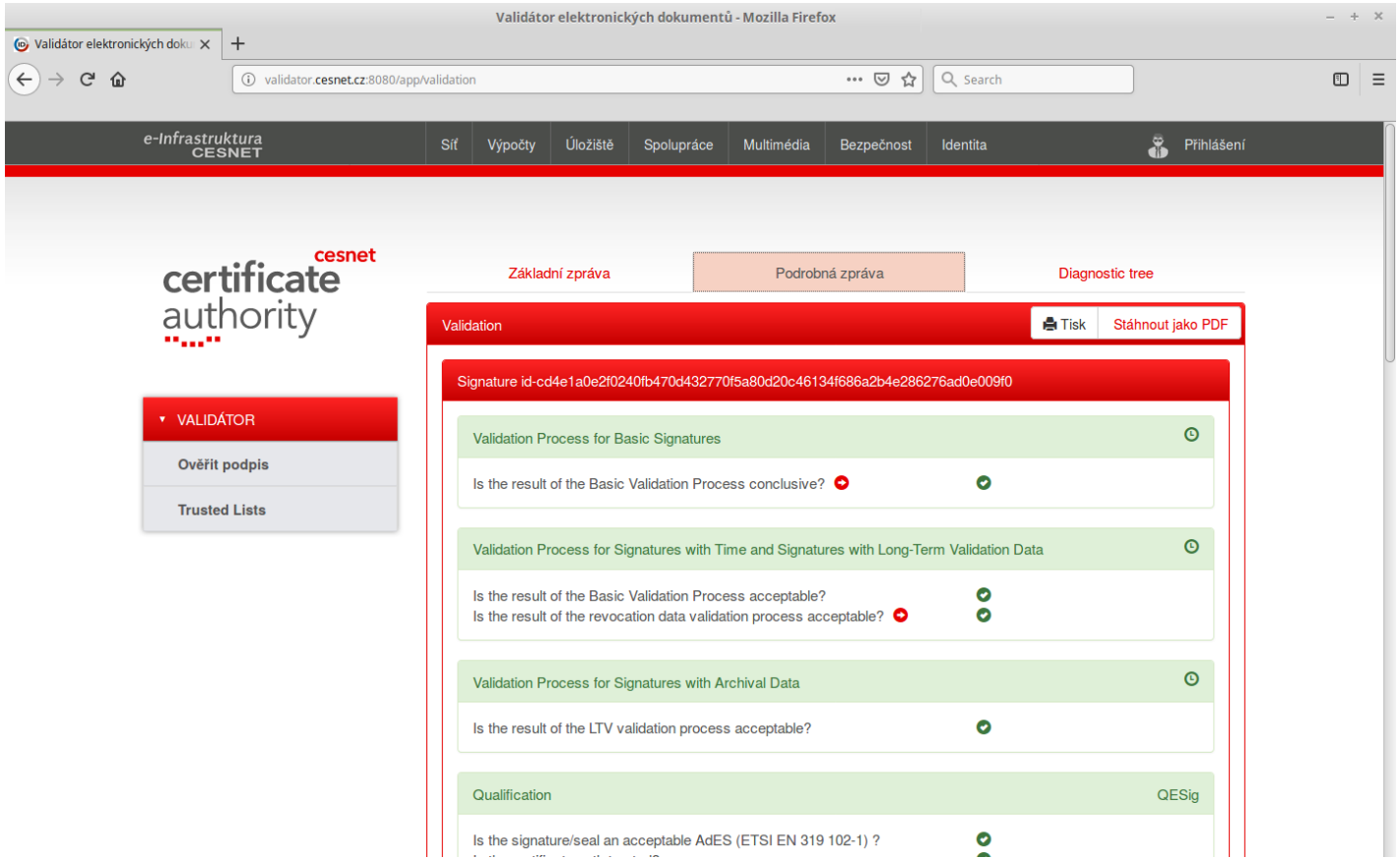
VALIDÁTOR PODPISŮ

- **Vychází z knihovny** Digital Signature Services (DSS)
  - Open source knihovna https://github.com/esig/dss pro vytváření a validaci elektronického podpisu v souladu s nařízení eIDAS
  - K dispozici demo aplikace na stránkách https://ec.europa.eu
  - Nejde o hotovou aplikaci: *„To minimize the risk of market distortion, DSS is provided as an open-source library and not as a ready-to-use tool… The CEF eSignature DSS service is intended for Service Providers active in the implementation of e-signature solutions. "*
- **Validační aplikace vyvíjená CESNETem**
  - Částečná lokalizace (menu, protokol, první vrstva validace)
  - Opakovaný test v čase např. t+24hod
  - Protokol o provedené validaci
  - Validace TCS a CESNET certifikátů
  - Uživatelské i strojové API

VALIDÁTOR PODPISŮ – PŘEHLED



VALIDÁTOR PODPISŮ - DETAIL



DALŠÍ PODPORA

- Rámcová smlouva pro nákup kvalifikovaných certifikátů a dalších produktů kvalifikovaných CA
  - Orientace na všechny hlavní dodavatele
  - Kontinuita služeb univerzity (návazné certifikáty)
- Nový web dokumentace – https://eidas.cesnet.cz (od 1.3.2019)
  - Veřejná část
    - Odkazy na relevantní zdroje
    - Obecné návody a postupy
  - Sekce pro členy
    - Návody pro připojení k novým službám CESNET
    - Analýza dopadů eIDAS na VVŠ

cesnet

DĚKUJI ZA POZORNOST

MÁTE NĚJAKÉ DOTAZY?