Certifikační autorita PostSignum

Pavel Plachý

CA PostSignum

- Poskytovaní komerčních certifikátů
- Poskytování kvalifikovaných certifikátů
- Poskytování kvalifikovaných časových razítek

Komerční certifikáty

- používají se pro bezpečné přihlášení do datové schránky

Osobní certifikáty – pro osobní přihlášení

Serverové certifikáty – pro přístup aplikací (spisových služeb)

Komerční certifikáty vydává Veřejná certifikační autorita (VCA)
Podrobnosti na **vca.postsignum.cz**

Kvalifikované certifikáty

- používají se pro podepisování elektronických dokumentů

Osobní certifikáty – pro vytvoření elektronického podpisu

Systémové certifikáty – pro vytvoření elektronické značky

Kvalifikované certifikáty vydává Kvalifikovaná certifikační autorita (QCA)
Podrobnosti na **qca.postsignum.cz**

Kvalifikovaná časová razítka

- s pomocí časových razítek lze u elektronických transakcí, formulářů, archivovaných dat, elektronických podpisů apod. prokázat jejich existenci v určitém čase
- časové razítko potvrzuje, že označená data existovala před uvedeným časovým okamžikem
- ve spojitosti s el. podpisem a el. značkou tvoří nezbytné minimum pro archivaci elektronických dokumentů

Kvalifikovaná časová razítka vydává Autorita časových razítek (TSA)

Podrobnosti na **www.postsignum.cz/tsa/**

Prodej certifikátů

Samostatný prodej certifikátů bez média

- Soukromý klíč je uložen v operačním systému
- ochrana heslem
- lze vytvořit kopii soukromého klíče

Prodej včetně média pro bezpečné uložení

- Soukromý klíč je uložen na médiu – USB tokenu, čipové kartě
- ochrana PINem
- nelze vytvořit kopii soukromého klíče

Bezpečný klíč k datové schránce

Obsah balíčku:

- Elektronický prostředek USB token iKey 4000
- Obslužný SW (instalační CD a licenční ujednání)
- Poukázky na bezplatný odběr osobních certifikátů

Bezpečný klíč k datové schránce

	USB token iKey 4000	Instalační CD	Licenční ujednání	Poukázka komerční certifikát	Poukázka kvalifikovaný certifikát
BK KOMPLET	✓	✓	✓	✓	✓
BK PODPISOVÝ	✓	✓	✓	✗	✓
BK PŘÍSTUPOVÝ	✓	✓	✓	✓	✗

Bezpečný klíč k datové schránce

Technická specifikace:

- Podpora hashovacích algoritmů SHA-1, SHA-2
- Podpora RSA klíčů 1024 i 2048 bitů
- Základní verze je pro OS MS Windows XP, Vista i Windows 7
- Speciální verze je určena pro OS LINUX a MacOS

Distribuce

- Prostřednictvím obchodníků České pošty
- Prostřednictvím přepážek Czech POINT České pošty
- Objednávkou na webových stránkách

- Detailní informace na **www.bezpecnyklic.cz**

Novinky v poskytovaných službách

Přechod na hashovací algoritmus SHA256 a RSA 2048

Spuštěny nové CA (označené číslem 2)

Původní s SHA1

Nové CA s SHA256

Novinky v poskytovaných službách

Zařazení kořenových certifikátů PostSignum mezi důvěryhodné CA

- rozděleno na tři etapy:

1. Microsoft
2. Mozilla, Adobe
3. Opera, Apple Safari

Novinky v poskytovaných službách

Postupná úprava webových stránek www.postsignum.cz

- nový online generátor klíčů a žádostí o certifikát
  - zjednodušení obsluhy
  - podpora Win 7

- nový způsob obnovy certifikátu
  - zjednodušení obsluhy

Děkuji za pozornost