Česká pošta, s.p.

Certifikační autorita PostSignum

6. 12. 2012

Ing. Miroslav Trávníček

Česká pošta

Služby certifikační autority

- **Kvalifikované certifikáty –** komunikace s úřady státní správy
- **Komerční certifikáty –** bezpečný způsob autentizace
- **Kvalifikovaná časová razítka –** prokázání existence dokumentu v určitém čase
- **Prodej HW zařízení na uložení certifikátů –** TOKEN + certifikát = Bezpečný klíč
- **Prodej SW pro vytváření el. podpisů a přidání časového razítka** (PDF Signer, VerisignIT)

Typy certifikátů

- CA PostSignum vydává dva typy certifikátů:
  - **kvalifikované (QCA)**
    - jsou vydávány v souladu se zákonem 227/2000 Sb.
    - ze zákona lze kvalifikovaný certifikát využít pouze pro vytvoření elektronického podpisu, není určen pro šifrování a autentizaci
    - slouží především pro komunikaci s orgány veřejné moci
  - **komerční (VCA)**
    - vydávání komerčních certifikátů není upraveno zákonem
    - slouží k autentizaci (přihlašování certifikátem např. do datové schránky) a šifrování (nejčastěji se jedná o šifrování e-mailů nebo komunikace na webových stránkách – HTTPS), ale lze s ním vytvářet i elektronický podpis např. při komunikaci v rámci firmy

Typy certifikátů

- Typy certifikátů lze rozdělit ještě dle toho, koho certifikát identifikuje:
  - **osobní (QCA i VCA)**
    - identifikují konkrétní osobu
  - **systémové (pouze QCA)**
    - identifikují firmu a dají se přirovnat k razítku, jsou používány nejčastěji v rámci automatických systémů (ePodatelny ...)
  - **serverové (pouze VCA)**
    - Identifikují např. server a používají se nejčastěji k zabezpečení webových stránek HTTPS nebo pro vzájemnou bezpečnou komunikaci systémů

Všechny vydávané certifikáty mají shodně **platnost 365 dní**.

Postup zřízení certifikátu

- Uzavření smlouvy
- Vygenerování elektronické žádosti o certifikát
- Návštěva pobočky České pošty
- Vydání certifikátu
- Instalace certifikátu
- Používání certifikátu
- Obnova certifikátu
- Zneplatnění certifikátu (seznam zneplatněných certifikátů)

(informace jsou žadateli zasílány na e-mailovou adresu)

Uzavření smlouvy

- Uzavření smlouvy – na kterékoliv pobočce ČP se službou CzP
- Náležitosti smlouvy – podepsaná statutárním zástupcem firmy
  – doklad o IČ
  – seznam Pověřených osob

- **Pověřená osoba** – má oprávnění komunikovat s CA
  – předkládá seznamy žadatelů
  – má oprávnění zneplatnit certifikát žadateli

- Platba za vydané certifikáty se provádí fakturou (fakturační období je dekádní), platí se za každý vydaný certifikát.

Vydání certifikátu na pobočce ČP

- Žádost o **prvotní certifikát** musí doručit žadatel **osobně** na pobočku ČP, aby mohla být ověřena jeho totožnost. Po ověření totožnosti je certifikát vydán.
- Co vzít s sebou na pobočku?
  - Doklad totožnosti
  - Vygenerovanou elektronickou žádost
    - Při generování žádosti vzniká privátní a veřejný klíč.
  - Případně vyplněné formuláře
- Po vydání certifikátu následuje instalace certifikátu

Vydání následného certifikátu

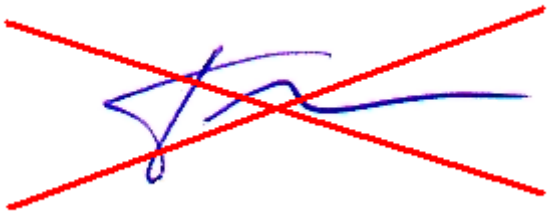
- Žádost o **následný certifikát** může být zaslána elektronicky (e-mailem, pomocí webové aplikace) na elektronickou podatelnu.
- Již není nutná návštěva pobočky ČP.
- Jak je ověřena totožnost žadatele?
  - Totožnost je ověřena na základě elektronického podpisu.
- Za jak dlouho je vydán certifikát?
  - V případě osobního certifikátu, který je obnoven pomocí webové aplikace, je vydání realizováno v řádu minut.

Pojmy – certifikát

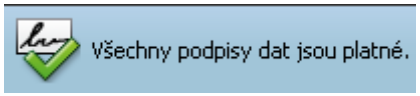
- **Co je certifikát a k čemu slouží?**
  - Certifikát je soubor dat (jakési potvrzení), které vydává certifikační autorita jako důvěryhodný orgán, kterému důvěřují komunikující strany.
  - Certifikát dokládá totožnost osoby, která vlastní odpovídající privátní klíč.
  - Certifikát slouží k vytváření elektronického podpisu nebo jeho ověření.
- **Jaké může certifikát obsahovat údaje?**
  - Certifikát obsahuje údaje, které si zvolil žadatel (pověřená osoba).
  - Mimo osobních údajů o žadateli a firmě obsahuje také veřejný klíč, údaje o vydávající certifikační autoritě, dobu platnosti, IKMPSV a další údaje…
- **Zveřejnění certifikátu, je to bezpečné?**
  - Ano, certifikát obsahuje pouze veřejný klíč a není tedy možné jeho zneužití. Privátní klíč zůstává vždy v držení vlastníka certifikátu a ani CA s ním nepřichází do styku.

Pojmy – elektronický podpis

- **Co je elektronický podpis a jak ho poznám?**



  - **PDF**
  - **Outlook**
  - **Mozilla**



- Jsou to data, která jsou pevně svázána s podepsanou zprávou.
- **Zajišťuje:**
  - Integritu – při změně zprávy dojde k poškození el. podpisu
  - Identifikaci – jednoznačně určuje osobu, která el. podpis vytvořila
  - Nepopiratelnost – podepisující osoba nemůže popřít vytvoření el. podpisu
- Vytváří se pomocí certifikátu (privátního klíče).

Portál CS OTE

- Komerční certifikát (přihlášení umožněno i kvalifikovaným)
- Certifikát musí obsahovat IČ
- Počet zastupujících firem = počet certifikátů
- Registrace pomocí PDF formuláře

Praktická ukázka

- Vygenerování elektronické žádosti na WWW
- Instalace certifikátu
- Obnova certifikátu před jeho vypršením
- Použití certifikátu
  - Elektronický podpis PDF, e-mailu
  - Přihlášení do webové aplikace

Děkuji za pozornost

Více informací o certifikační autoritě PostSignum naleznete na:

www.postsignum.cz