BEZIT – 4. cvičení

Radek Janoštík

Univerzita Palackého v Olomouci

7. 3. 2024

Osobní certifikáty od CESNET

- V rámci sdružení CESNET máme možnost získat důvěryhodné osobní certifikáty
- Pomocí `https://pki.cesnet.cz/cs/tcs-personal.html` si projdeme žádostí a zřiďíme si osobní certifikát

Digitální podpis emailu

- Problém bývá s podporou klientů (podepisování i ověření
- Weboví klienti často nepodporují vůbec, případně jen ověření
- Je dobré mít na email plnohodnotnou aplikaci
  - MS Outlook
  - Thunderbird
- Ukázka podepsaného/šifrovaného emailu (Thunderbird)

Digitální podpis emailu

- Problém bývá s podporou klientů (podepisování i ověření
- Weboví klienti často nepodporují vůbec, případně jen ověření
- Je dobré mít na email plnohodnotnou aplikaci
  - MS Outlook
  - Thunderbird
- Ukázka podepsaného/šifrovaného emailu (Thunderbird)
- Ukázka podepsaných emailů ve webových klientech

Digitální podpis souborů

- Velmi rozšířeno ve státní správě (podpisy žádostí o dotace, podpisy starostů, . . .)
- Ne každý prohlížeč PDF dokáže ověřit a podepsat
  - Integrované čtečky v prohlížečích (většinou neumí)
  - Adobe Reader, Okular, LibreOffice, FoxitPDF reader (ano))
- Ukázka

Podpis jakýchkoliv souborů

- PDF i email mají standard pro podepisování – koncept *elektronické obálky*
- Princip pro digitální podpisy a šifrování můžeme využít pro jakékoliv soubory
- $\Rightarrow$ Distribuce podpisu a klíčů vlastní cestou

Podpis jakýchkoliv souborů

- PDF i email mají standard pro podepisování – koncept *elektronické obálky*
- Princip pro digitální podpisy a šifrování můžeme využít pro jakékoliv soubory
- $\Rightarrow$ Distribuce podpisu a klíčů vlastní cestou
- Velkým pomocníkem je knihovna OpenSSL
- Spočítáme kontrolní součet a podepíšeme jej:
  `openssl dgst -sha256 -sign private.pem -out ./sign.sha256 soubor.txt`
- Dostaneme binární soubor s podepsaným kontrolním součtem (převedeme do Base64)
  `openssl base64 -in sign.sha256 -out podpis`
- Soubor s podpisem můžeme distribuovat

OpenSSL – ověření podpisu

- Ověříme jednoduchým příkazem:

```
$ openssl dgst -sha256 -verify public.pem -signature sign.sha256 soubor.txt
Verified OK
```

- Víme, že soubor byl podepsán vlastníkem privátního klíče v takovém tvaru, ve kterém k nám dorazil

Úkol

- Obstarejte si podpisový certifikát/klíč (CESNET(Pro studenty nelze :-(), self-signed, . . .)
- Odešlete mi podepsaný a zašifrovaný email (S/MIME)
- Zkontrolujte podpis u podepsaných slidů, zjistěte podrobnosti o certifikátu
  - Slidy
- Podepište nějaké PDF vaším podpisem (BP, prázdné pdf, . . .) a pošlete mi jej emailem