27. Elektronický podpis (popis, použité funkce, získání, použití, omezení), certifikáty, zabezpečení dat před zneužitím a před ztrátou. Definujte a uveďte příklad využití redundace dat

- označení specifických dat, které v počítači nahrazují vlastnoruční podpis, ověřený podpis
- slouží k ověření totožnosti odesílatele v anonymním světe
- ověření el. podpisu zahrnuje kromě matematických operací i přenos důvery z důvěryhodné třetí strany na tvůrce podpisu a následně na důvěryhodnost elektricky podepsaného dokumentu
    - Digitální certifikát
    - Síť důvěry

Vlastnosti elektronického podpisu

- **Autenticita**
    - lze ověřit identitu subjektu, kterému patří el. podpis pomocí přenosu důvery
- **Integrita**
    - lze prokázat, že od vytvoření el. podpisu nedošlo k žádné změně v podepsaném dokumentu, že není dokument poškozen
- **Nepopirnatelnost**
    - autor nemůže tvrdit, že el. podpis k dokumentu nevytvořil
- **Časové ukotvení**
    - el. podpis může obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu
    - časové razítko vydává důvěryhodná třetí strana

Využití elektronického podpisu

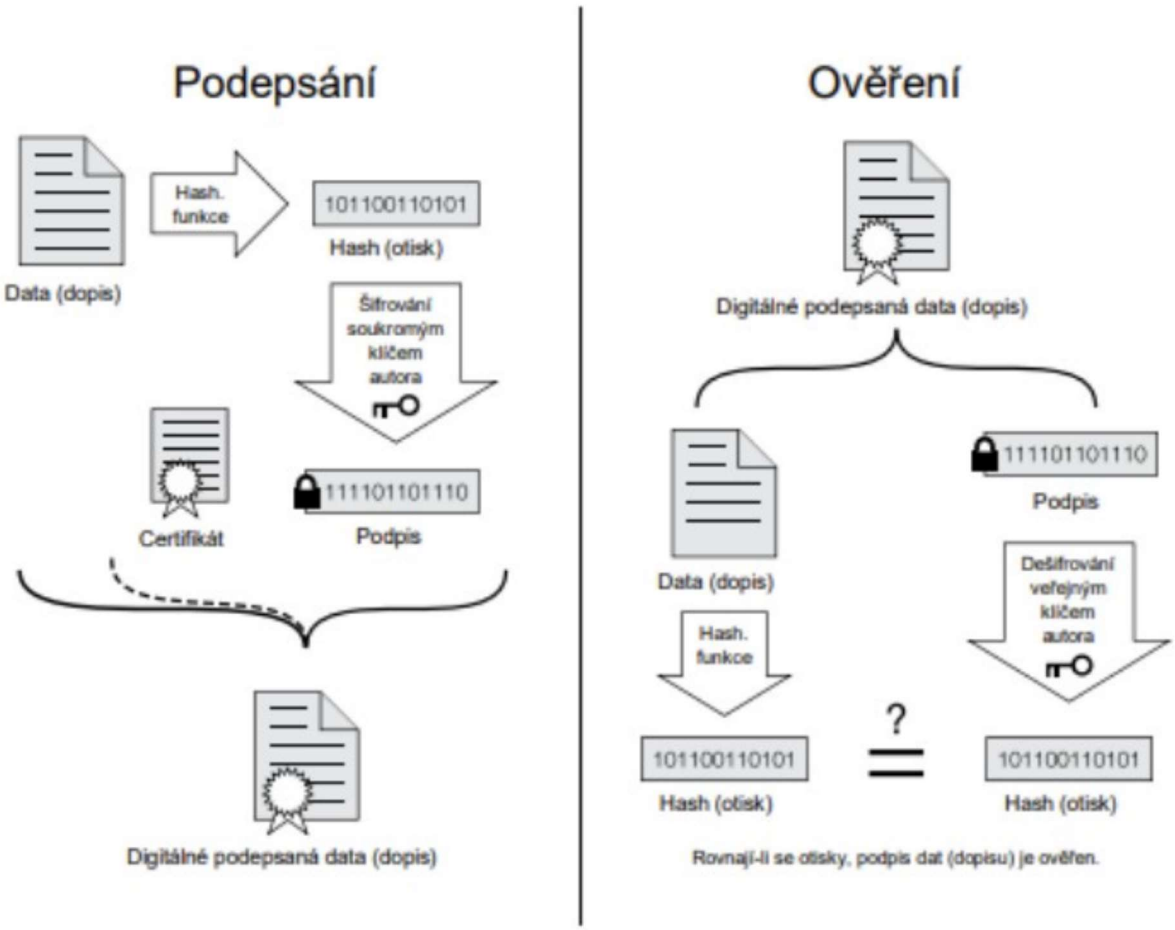
- datová schránka
- podepisování faktur
- žádosti o dotace, soc. dávky
- komunikace se státní správou

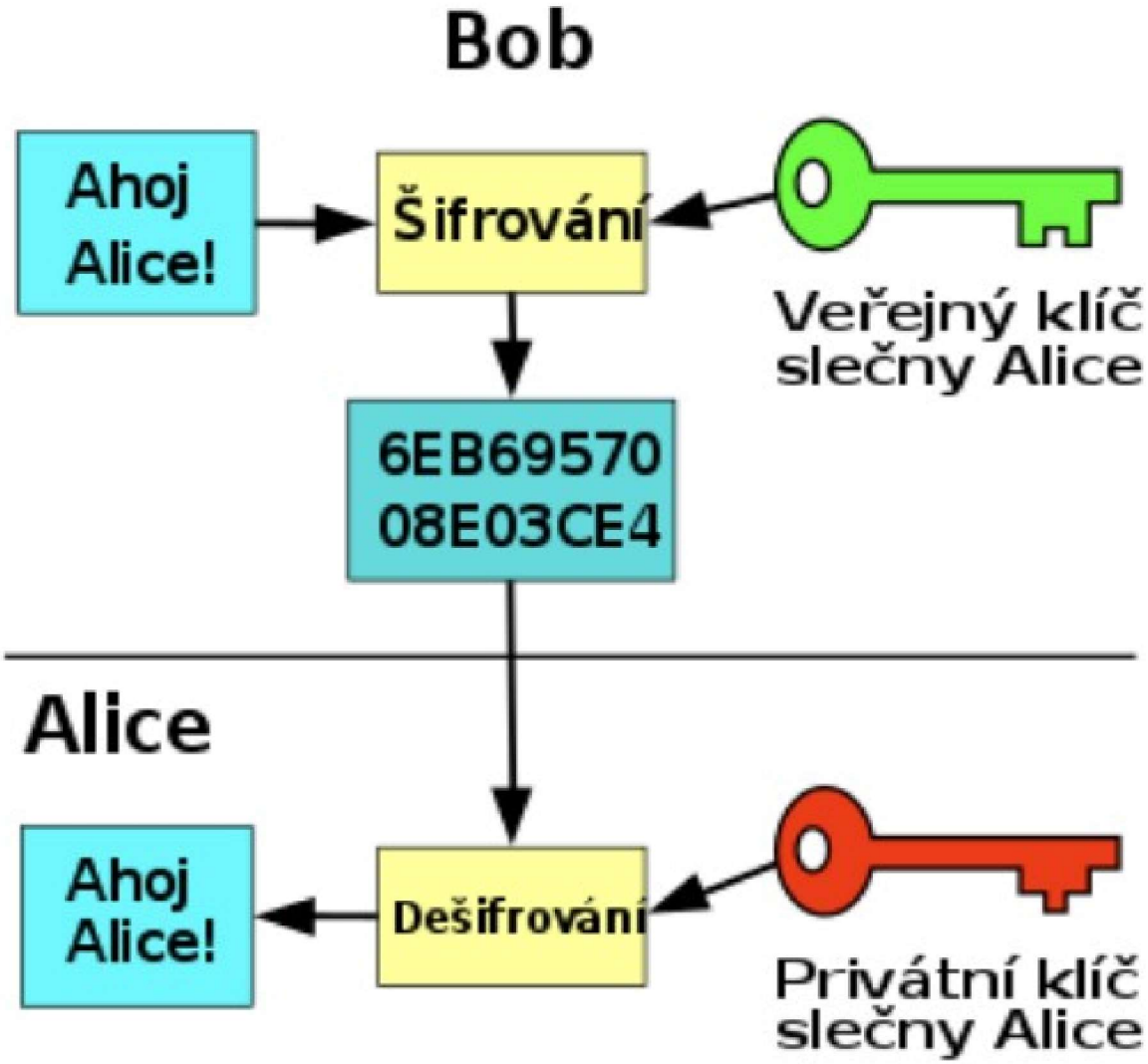
Postup získání elektronického podpisu

1) vygenerování žádosti na PC a žádost odešleme
2) uložení např. na flash disk
3) CzechPoint či jiná cerifikovaná autorita
4) ověření totožnosti (občanský průkaz)
5) přehrání ověřeného klíče do PC
6) pravidelné obnovování (každý rok)

HASH funkce

- asymetrická a jednosměrná funkce
- stejný výstup dat jak vstup (otisk)
- z hashe je možné rekonstruovat původní text zprávy
- v praxi lze identifikovat právě jednu zprávu





Ochrana dat před ztrátou

- zálohování (zrcadlení disku)
- distrubuované báze dat (data uložena na více místech)
- centralizované báze dat (data uložene na jednom zabezpečeném místě)

Ochrana dat před zneužitím

- zničení
- BP firmy
- hesla
- biometrické prvky

Redundance dat

- nadbytečnost dat, přenášení více symbolů než u optimálního kódu
- někdy je schálně (zabezpečující kódy)
- maximální redundance - 100 % (opakování celé zprávy)

Datová schránka

- každá právnická osoba a dobrovolně zapojená fyzická osoba má svou vlastní datovou schránku
- el. úložiště zřízené státem roku 2009
- zabezpečená šifrofacím protokolem SSC
- možnost přihlášení (jméno, heslo, SMS)
- **Využití:**
  - zabezpečení odesílání digitalizované pošty
  - k nepopiratelnosti původu
  - nepopiratelnost celistvosti
  - nepopiratelnost doručení