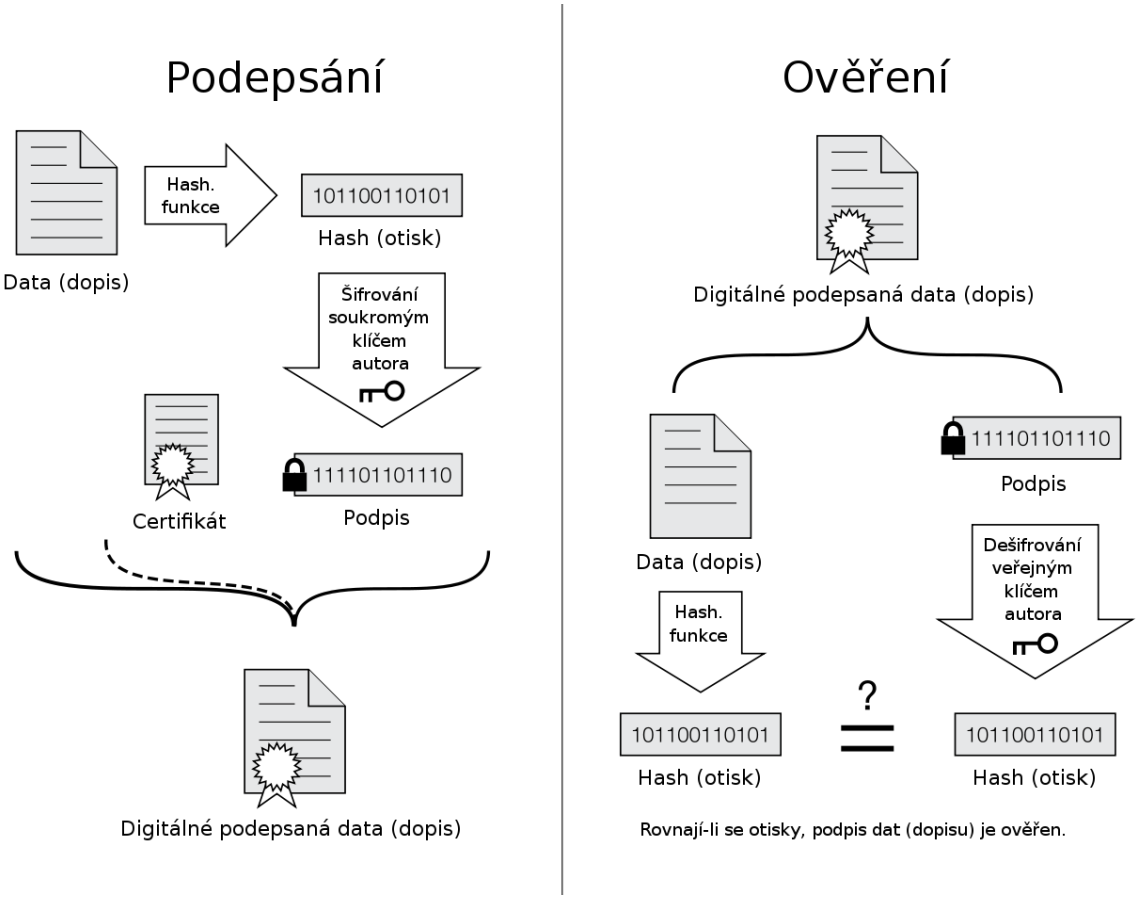
Elektronický podpis

- Nahrazuje vlastnoruční ověřený podpis
- Je připojen k datové zprávě
- Je logicky spojen se zprávou
- Je vytvořen pro konkrétní data
- Přenos důvěry z důvěryhodné třetí strany na tvůrce podpisu
- Využívá digitální certifikát

Vlastnosti elektronického podpisu

- Autenticita
  - Lze ověřit identitu
- Integrita
  - Zpráva nebyla změněna
- Nepopiratelnost
  - Autor nemůže tvrdit, že dokument nevytvořil
- Časové ukotvení
  - Prokazuje datum a čas podepsání

Princip funkce



Získání elektronického podpisu

Elektronický podpis v současnosti vydávají v České republice 3 poskytovatelé: Česká pošta, eIdentity, První certifikační autorita

Certifikáty

- Jsou vydávány certifikační autoritou
- Je to digitálně podepsaný veřejný klíč (v asymetrické kryptografii)
- Využití k identifikaci protistrany
- Obsahuje
    - Serial Number – (certifikáty mají pro lepší identifikaci vlastní sériové číslo, není to však nutnost)
    - Subject – identifikační údaje majitele certifikátu
    - Signature Algorithm – algoritmus použitý k vytvoření podpisu
    - Signature – digitální podpis veřejného klíče vytvořený certifikační autoritou
    - Issuer – identifikační údaje vydavatele certifikátu
    - Valid-From – datum počátku platnosti certifikátu
    - Valid-To – datum konce platnosti certifikátu; nejběžnější doba platnosti je jeden rok
    - Key-Usage – účel veřejného klíče (šifrování, ověřování podpisů nebo obojí)

Zabezpečení dat před zneužitím a před ztrátou

- Před ztrátou
    - Zálohování
    - Distribuované BD (vs. Centralizované BD)
    - Cloudy
- Před zneužitím
    - Zničení (skartace, spalovna)
    - Autorizovaný přístup: bezpečnostní politika firmy
    - Hesla
    - Biometrie (otisky prstů, snímání sítnice)

Redundance dat

- Redundance = míra nadbytečnosti
- Přenášení více symbolů, než v optimálním kódu
- Redundance je často plánovaná (zabezpečující kódy)
- Maximální redundance je 100 % - opakování celé zprávy
- Příklad: paritní bit, koncový součet

Hammingova vzdálenost

- P (rho) – udává počet míst, ve kterých se budou 2 sousední slova vzájemně lišit
- P = 1 – bez redundance
- P = 2 – lze detekovat chyby
- P ≥ 3 – lze chyby opravit

Přenosový kanál

$$C = B \log_2 \left(1 + \frac{S}{N}\right) \ [bps]$$

- C – kapacita
- B – šířka

- S – znak
- N – počet permutací dané abecedy

Kanálové zabezpečovací kódy

- Detekční
  - Parita
- Korekční
  - Konvoluční – SLO
    - Binární
    - Nebinární
  - Blokové – KLO
    - Nelineární
    - Lineární
      - Cyklické
      - Necyklické

Příklady

- ARQ – detekční, automatic repeat request, když zpráva dojde chybná, příjemce si o ní zažádá znovu
- BCH – lineární polynomiální korekční kód, cyklické samoopravné kódy, využito v QR
- Parita – detekční kód lichého počtu chyb
- CRC – cyclic redundancy check, kontrolní součet
- Hash – redundantní
  - jakékoli množství vstupních dat vytváří stejně dlouhý otisk
  - malá změna vstupních dat vytvoří velkou změnu otisku
  - z hashe je prakticky nemožné rekonstruovat původní zprávu
  - v praxi je velmi nepravděpodobné, že různým zprávám bude odpovídat stejný hash