Digitální podpis

Digitální podpis je kryptografický mechanismus, který slouží k ověření **autenticity** (původu) a **integrity** (neporušenosti) dat. Na rozdíl od naskenovaného vlastnoručního podpisu je digitální podpis neoddělitelně spojen s obsahem konkrétního dokumentu.

Základem digitálního podpisu je asymetrická kryptografie (veřejný a soukromý klíč) a hashovací funkce.

Jak funguje proces podepisování?

Proces se skládá ze dvou hlavních fází: vytvoření podpisu a jeho následné ověření.

1. Vytvoření podpisu (Odesílatel)

1. Z dokumentu se vytvoří jedinečný otisk (**Hash**).
2. Tento hash odesílatel zašifruje svým **soukromým klíčem**.
3. Výsledkem je digitální podpis, který se připojí k dokumentu.

2. Ověření podpisu (Příjemce)

1. Příjemce vypočítá vlastní hash z obdrženého dokumentu.
2. Pomocí **veřejného klíče** odesílatele dešifruje připojený podpis (získá původní hash).
3. Pokud se oba hashe shodují, je potvrzeno, že dokument nikdo nezměnil a podepsal ho skutečně majitel soukromého klíče.

Co digitální podpis zajišťuje?

- **Autenticita:** Máte jistotu, kdo dokument podepsal (pokud odesílatel neztratil svůj soukromý klíč).
- **Integrita:** Pokud by se v dokumentu změnil byť jen jeden znak (tečka, mezera), výsledný hash by byl zcela jiný a podpis by byl neplatný.
- **Nepopiratelnost:** Odesílatel nemůže tvrdit, že dokument nepodepsal, protože k vytvoření podpisu je zapotřebí jeho unikátní soukromý klíč.

Rozdíl: Digitální vs. Elektronický podpis

V běžné mluvě se tyto pojmy zaměňují, ale v právu a IT mají odlišný význam:

Typ	Popis
Elektronický podpis	Široký právní pojem. Může to být i jméno napsané v e-mailu nebo naskenovaný obrázek podpisu.

Typ	Popis
Digitální podpis	Konkrétní technické řešení založené na kryptografii, které naplňuje právní požadavky na elektronický podpis.

Využití v praxi

- **HTTPS certifikáty:** Každý webový certifikát je digitálně podepsán certifikační autoritou.
- **E-mail (S/MIME, PGP):** Zajišťuje, že e-mail skutečně poslal daný kolega a ne útočník.
- **Aktualizace softwaru:** Operační systém instaluje pouze ovladače a programy s platným podpisem vývojáře (např. Microsoft, Apple).
- **Elektronické dokumenty (PDF):** Oficiální komunikace s úřady nebo fakturace.

> **Důležité:** Bezpečnost digitálního podpisu stojí a padá na ochraně **soukromého klíče**. Pokud je klíč ukraden, útočník může podepisovat dokumenty jménem oběti. Proto se pro kritické podpisy používají čipové karty nebo USB tokeny.

— **Viz také:** Šifrování, Hashování, HTTPS/TLS, PKI (Public Key Infrastructure)