Digitální podpis

Digitální podpis není pouhý naskenovaný obrázek vlastnoručního podpisu. Je to matematický kód, který je pevně spojen s obsahem dokumentu a identitou odesílatele. Pokud se v podepsaném dokumentu změní byť jen jedno písmenko, podpis se stane neplatným.

Jak digitální podpis funguje?

Digitální podpis využívá kombinaci dvou technologií: hashování a asymetrického šifrování (RSA).

Proces vytvoření podpisu (Odesílatel):

```
1. **Hashování:** Z celého dokumentu se vytvoří unikátní otisk – tzv. [[hashovani|hash]]. Je to krátký řetězec znaků, který reprezentuje obsah dokumentu.
2. **Šifrování:** Odesílatel zašifruje tento hash svým **soukromým klíčem**. Tím vznikne samotný digitální podpis.
3. **Odeslání:** Dokument se pošle příjemci spolu s tímto podpisem.
```

Proces ověření (Příjemce):

```
1. **Dešifrování:** Příjemce vezme digitální podpis a dešifruje ho pomocí **veřejného klíče** odesílatele. Tím získá původní hash.
2. **Nové hashování:** Příjemce sám vytvoří nový hash z doručeného dokumentu.
3. **Porovnání:** Pokud se oba hashe shodují, je jasné, že dokument podepsal skutečně majitel klíče a že dokument nebyl po cestě změněn.
```

Tři pilíře digitálního podpisu

- **Autenticita:** Máme jistotu, kdo dokument podepsal (protože nikdo jiný nemá přístup k soukromému klíči odesílatele).
- **Integrita:** Máme jistotu, že dokument nebyl od okamžiku podpisu změněn (změna dat by vedla k jinému hashi).
- **Nepopiratelnost:** Autor nemůže později tvrdit, že dokument nepodepsal, protože k vytvoření podpisu byl nutný jeho unikátní soukromý klíč.

Elektronický vs. Digitální podpis

V běžné řeči se tyto pojmy pletou, ale právně a technicky je v nich rozdíl:

Typ	Popis	Právní váha
Elektronický podpis	Široký pojem – může to být i vaše jméno v e-mailu nebo scan podpisu.	Nízká, snadno zpochybnitelná.
Digitální podpis	Konkrétní kryptografická metoda (hash + RSA).	Vysoká, technicky prokazatelná.
Kvalifikovaný elektronický podpis	Digitální podpis založený na certifikátu od autority (např. PostSignum).	Nejvyšší, úroveň úředně ověřeného podpisu.

Praktické využití

- **E-mailová komunikace (S/MIME, PGP):** Podepisování zpráv pro ověření odesílatele.
- **Softwarové aktualizace:** Operační systém instaluje pouze ovladače, které jsou digitálně podepsány výrobcem (např. Microsoftem).
- **E-government:** Komunikace s úřady přes datové schránky nebo podepisování PDF dokumentů.
- **Kryptoměny:** Každá transakce v síti Bitcoin je digitálně podepsána majitelem peněženky.

Role Certifikačních autorit (CA)

Aby příjemce věděl, že veřejný klíč skutečně patří dané osobě, vstupuje do hry **Certifikační autorita**. Ta vydá tzv. **Digitální certifikát**, který funguje jako digitální občanský průkaz, v němž autorita potvrzuje: „Tento veřejný klíč patří panu Novákovi.“

Související pojmy: RSA, Hashování, Kryptografie, Certifikační autorita (CA), SSL/TLS, Integrity, Autentizace.