**Digitální podpisy**

Základní myšlenkou elektronického podpisu je obdoba klasického podpisu, jež má zaručit jednoznačnou identifikaci osoby v prostředí digitálního světa. Požaduje se, aby tento podpis byl jedinečný vzhledem k podepisovanému dokumentu a především kýmkoliv nezfalšovatelný. Díky těmto vlastnostem se stává digitální dokument podepsaný digitálním podpisem rovnocenným dokumentu podepsanému rukou.

"Digitální podpis je ve své podstatě číslo vypočítané v závislosti na podepisovaných datech a nelze jej tudíž zkopírovat na jiný dokument."

Jedná se v podstatě o informaci vztahující se k určitému dokumentu vyjádřenou velkým číslem. Tato informace nemá na obsah podepisovaného dokumentu žádný vliv. Vzhledem k tomu, že se vytváří na základě obsahu daného dokumentu, je na něm závislá a tedy nepřenosná na jakýkoliv jiný dokument. Samotné generování elektronického podpisu je založeno na kryptografické transformaci z dokumentu a soukromém klíči podepisujícího subjektu.

Od elektronického podpisu se vyžadují tyto vlastnosti:

1. Jednoznačná identifikace původce podpisu - příjemce ví, kdo dokument poslal.
2. Zajištění integrity zprávy - příjemce má jistotu, že dokument došel kompletní a nebyl během přenosu pozměněn.
3. Zaručení nepopiratelnosti - odesílatel nemůže popřít, že daný dokument opravdu odeslal.
4. Podpis nelze napodobit ani zneužít pro jiný dokument.

Od použití elektronického podpisu se tedy očekává, že zaručí nepopíratelné ověření identity odesílatele a zabezpečí integritu zasílaného dokumentu během přenosu.

## Typy elektronického podpisu

Při využívání datových služeb prostřednictvím internetu se setkáváme se dvěma odlišnými pojmy - "obyčejný" elektronický podpis a "zaručený" elektronický podpis.

### Obyčejný elektronický podpis

U tohoto typu se jedná o obyčejný vlastnoruční podpis převedený do digitální podoby (naskenovaný). Takovýto typ podpisu je využíván především jako předloha pro porovnání s vlastnoručním podpisem na dokumentu. Využívá se jak v prostředí bankovnictví, tak při různých dalších kontrolách, kde je nutné ověřit identitu podpisu.

Nedostatkem tohoto porovnání vlastnoručního podpisu a zdigitalizovaného podpisu je především v tom, že se jedná o čistě vizuální srovnání. Je zřejmé, že ne pokaždé se jedinci podaří podepsat stejným způsobem, ať už z jakéhokoliv důvodu. Nelze také vždy očekávat, že osoba, která porovnává oba podpisy, bude natolik schopná odlišit drobné nesrovnalosti aktuálního podpisu v porovnání s předlohou. Zde se jednoznačně ukazuje, že je tento způsob ověřování identity nespolehlivý. Pravý opak se očekává od využití zaručeného elektronického podpisu.

### Zaručený elektronický podpis

Jedná se o elektronický podpis, který je vytvořen za využití kryptografie (šifrování). Tento druh podpisu je vymezen v Zákoně číslo 227/2000 Sb., o elektronickém podpisu následující definicí:"Zaručeným elektronickým podpisem se rozumí elektronický podpis, který splňuje následující požadavky:

1. je jednoznačně spojen s podepisující osobou,
2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat."

## Princip fungování elektronického podpisu

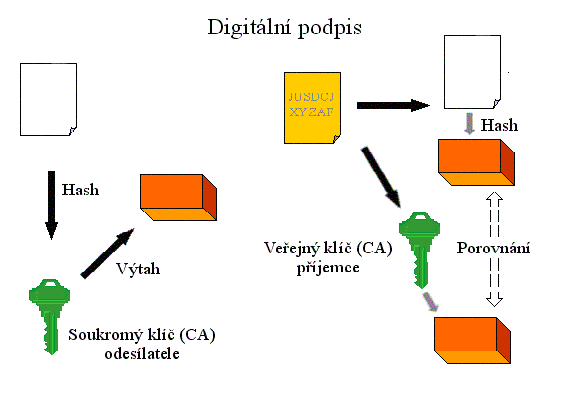
Samotné vytváření elektronického podpisu je složeno z několika kroků. Vzhledem k tomu, že elektronický podpis je velmi velké číslo (např. 1024 nebo 2048 bitů) vztahující se k jednomu konkrétnímu dokumentu, je nutné zajistit, aby jeho vygenerování proběhlo v přijatelném čase. K tomuto účelu se využívají tzv. hašovací funkce (hash function).

### Hašovací funkce

Pro urychlení vytvoření elektronického podpisu se většinou nešifruje soukromým klíčem celý dokument, ale obsah dokumentu je převeden pomocí jednosměrné hašovací funkce (např. MD5) na menší celek.

Princip využití hašování při tvorbě elektronického podpisu lze popsat následovně:

1. Odesílatel provede hash dokumentu s pomocí svého soukromého klíče.
2. Vzniklý hash přiloží k dokumentu, zašifruje ho veřejným klíčem příjemce a odešle.
3. Příjemce rozšifruje dokument svým soukromým klíčem.
4. Veřejným klíčem odesílatele provede hash rozšifrovaného dokumentu a porovná ho.
5. Pokud jsou oba otisky shodné, je zaručené, že dokument nebyl změněn. Pokud se však odlišují, je nutné provést celý přenos dokumentu znovu.



#### Podepisování dokumentu

Zašifrovaný a podepsaný dokument je zaslán příjemci. Příjemce ověří prostřednictvím veřejného klíče pravost podpisu odesílatele a integritu zprávy.

Z tohoto principu vyplývá, že odesílatel bude generovat elektronický podpis pro každý dokument sám za využití speciálního programu a svého soukromého klíče následujícím způsobem:

1. Odesílatel získá počítačový program pro vytváření a ověřování elektronického podpisu.
2. Programem vygeneruje dvojici soukromého a veřejného klíče.
3. Veřejný klíč předloží poskytovateli certifikačních služeb (CA - certifikační autorita), přičemž musí prokázat svou totožnost.
4. Certifikační autorita mu vystaví certifikát, který zaručuje, že veřejný klíč náleží právě této osobě.
5. Pomocí svého soukromého klíče může odesílatel vytvářet elektronický podpis pro jednotlivé dokumenty a příjemci si mohou pomocí jeho veřejného klíče ověřit pravost tohoto podpisu.

### Ověření pravosti podpisu

Pravost elektronického podpisu se ověřuje pomocí veřejného klíče. Tento klíč, který tvoří se soukromým klíčem neodmyslitelnou dvojici, slouží výhradně pro ověřování a nikoliv pro generování elektronického podpisu. Z toho vyplývá, že veřejný klíč je v případě elektronického podpisu podpisovým vzorem. Je možné publikovat veřejný klíč, neboť z něj nelze zatím žádným přijatelným způsobem odvodit klíč soukromý.

Ověření podpisu je opět prováděno počítačovým programem. Výstupem této operace je buď přijmutí alternativy, že podpis v dokumentu patří odesílateli a obsah nebyl během transakce změněn, nebo naopak její zamítnutí.

Veřejný klíč může příjemce získat přímo od odesílatele. Často bývá také zveřejněn (např. na internetu) i s údaji, komu patří. Aby si byl příjemce jist, že daný veřejný klíč patří odpovídajícímu odesílateli, je zapotřebí, aby jeho pravost někdo zaručil. Tato záruka je poskytována prostřednictvím tzv. certifikátu, který uděluje certifikační autorita.

**Použitá literatura:**

BERÁNEK, Marek. *Elektronický podpis* [online]. [cit. 2013-02-03]. Dostupné z: <http://kryptologie.uhk.cz/54.htm>

PINKAVA, Jaroslav. Základy kryptografie I. [online]. [cit. 2013-02-03]. Dostupné z: <http://crypto-world.info/pinkava/uvod/bulletin1.pdf>

PINKAVA, Jaroslav. Základy kryptografie II. [online]. [cit. 2013-02-03]. Dostupné z: <http://crypto-world.info/pinkava/uvod/bulletin2.pdf>