Michal Chňoupek
770419/0186

V Praze dne 6.1.2000

Digitální podpis

IZI213

Dnes se elektronické dopisy podepisují běžně pouze textovým řetězcem, který nezaručuje, že dopis pochází od člověka, který je uveden na konci dopisu. Dokonce ani naskenování podpisu do počítačové podoby nezaručuje pravost elektronického dokumentu, neboť se jedná pouze o přidaný obrázek do dopisu, který může být kopírován a dále zneužit.

Problém vyřeší nasazení digitálních podpisů. Digitální podpis je složitý zašifrovaný číselný kód, který je pro každého uživatele ojedinělý a který je právně ověřitelný. K podepisování dokumentů slouží privátní klíč a ke čtení slouží klíče veřejné. Používají se tedy tzv.asymetrické šifry

Hlavní výhoda digitálního podpisu spočívá v tom, že mnoho lidí se nedokáže dvakrát stejně podepsat a má tak například problémy v bance při výběru z účtu. Navíc digitální podpis je velice jednoduše a rychle ověřitelný. Další nespornou výhodou je to, že signatář může odesílat libovolný elektronický dokument či přistupovat k nejdůvěrnějším datům, aniž by se musel bát zneužití těchto dat.

Na rozdíl od elektronického podpisu, který je "pouhým podpisem", je účelem zaručeného (bezpečného) elektronického podpisu zajistit, že zprávu podepsala opravdu oprávněná osoba. Vychází z principu existence "ověřovatele informací", který ověřuje vztah mezi zaručeným elektronickým podpisem a oprávněnou osobou. Pravděpodobně nejsoučasnější variantou realizující zaručený elektronický podpis je podpis digitální, vycházející z principu existence dvou klíčů vygenerovaných majitelem podpisu: soukromého a veřejného.

Jaké jsou hlavní cíle a zásady bezpečnosti elektronické komunikace

Obvykle si lidé slučují pojem bezpečnost se šifrováním, resp. s nerozluštitelností důvěrných elektronických dat. Ve skutečnosti je problém poněkud, ale ne příliš, složitější. Zpravidla cíle zabezpečení dat při jejich výměně a použití rozdělujeme na tři zásady:

- **Zásada důvěrnosti**, která vyjadřuje potřebu uložit data tak, aby jejich obsah mohl přečíst jen ten, komu jsou určena
- **Zásada neomítnutelnosti odpovědnosti** vyjadřuje neméně důležitou potřebu možnosti dokázat, kdo je autorem zprávy
- **Zásada integrity** má na starosti, aby data došla nejen úplná, ale též prokazatelně nezměněná

Pokud budou elektronické zprávy všechny tři zásady respektovat, pak je jejich bezpečnost stoprocentně zaručena.

Symetrické šifrování

Symetrické šifrování je metoda, při které je otevřený text zašifrován s pomocí jistého klíče a může být obnoven jen se znalosti tohoto klíče. Symetrické šifrovací algoritmy se vyvíjejí doslova tisíce let. Většina moderních algoritmů je založena na matematické teorii čísel. Při symetrickém šifrování si musí autor a příjemce nějakým bezpečným způsobem vyměnit klíč. Samotné symetrické šifrování nemůže nikdy problém předání klíče vyřešit.

Rozhodujícím kriteriem síly symetrické šifry je délka klíče. Zpráva totiž musí odolat tzv. útoku hrubou silou, který předpokládá prostě vyzkoušení všech možných klíčů. Délka se uvádí v počtu bitů binárního čísla. Má-li tedy šifra sílu 4 bity, je 2^4=16 možných klíčů. Je zřejmé, že tato síla neobstojí. Přestože přidáním jediného bitu se počet klíčů (a tedy šifrovací síla) zdvojnásobí, jsou 40tibitové klíče používané např. v prohlížečích firem Netscape a Microsoft určených pro vývoz z USA dnes poměrně snadno rozluštitelné. Americký standard, šifra DES s 56 bity, kterou kdysi na zakázku americké vlády vyvinula firma IBM, se dnes také otřásá v základech. V současné době asi nejčastěji používané 128mibitové klíče zaručují odolnost proti útokům hrubou silou minimálně na několik let dopředu.

Asymetrické šifrování

Teprve v 70. letech 20. století byl navržen první asymetrický šifrovací algoritmus. Jeho princip je jednoduchý: zpráva se zašifruje jedním klíčem, rozšifrovat se však musí jiným klíčem. Navíc ze znalosti prvního klíče nelze zjistit druhý. První klíč může být tedy dán ve známost komukoli (tzv. veřejný klíč nebo veřejná část klíče), zatímco druhý si uchovává vlastník v tajnosti (soukromý klíč nebo soukromá část klíče). Mezi nejznámější asymetrické šifry patří RSA, Diffie-Hellman a DSS.

Délka klíče asymetrické šifry má trochu jiný význam. Asymetrické šifry jsou většinou založeny na nějakých speciálních číslech (např. prvočíslech). Při útoku hrubou silou tedy stačí zkoumat jen tato speciální čísla. Dnes se běžně pracuje s délkou klíče 1024 bitů, avšak pro dlouhodobější použití je lépe zvolit 2048 bitů nebo více.

Kouzlo asymetrických šifer spočívá v tom, že to, co bylo zašifrováno jedním z klíčů privátní/veřejný, lze rozšifrovat jedině druhým klíčem z dané dvojice. Tedy zašifruji-li něco svým klíčem privátním, rozšifruje to někdo pouze, má-li můj klíč veřejný. A obráceně.

Jaké jsou privátní a veřejné klíče

Privátní a veřejný klíč tvoří vždy nerozlučnou dvojici. Logicky patří totiž jeden k druhému. Jeden lze vypočítat jednoznačně z hodnoty druhého. Problém je ale v tom, že zatímco veřejný je možno z privátního vypočítat snadno a rychle, obráceně je to prakticky nemožné. Ne proto, že by nebylo známo jak, ale proto, že výpočet by byl natolik náročný na kapacitu počítače, že výsledek by nebylo možné získat ani v horizontu let. Privátní klíč si každý musí chránit jako oko v hlavě, ale klíč veřejný by měl naopak zveřejnit.

Zašifrování dokumentu privátním klíčem a následné dešifrování klíčem veřejným za účelem ověření, kdo svým privátním klíčem dokument zašifroval, se nazývá metodou elektronického podpisu.

Použití privátního a veřejného klíče

Je dokument zašifrován privátním klíčem, pak ho lze přečíst jen po dešifrování klíčem veřejným téhož autora. Tím nelze obsah dokumentu utajit, ale pouze ověřit, kdo jej zašifroval a kdo je také jeho autorem. Pokud chceme obsah dokumentu zabezpečit před neoprávněným přístupem, pak postupujeme obráceně: dokument zašifrujeme. Tím zajistíme, že dokument lze rozšifrovat jen privátním klíčem příjemce. Obě metody lze kombinovat. Nejdříve dokument elektronicky podepíšeme, tedy zašifrujeme naším privátním klíčem, potom zašifrujeme veřejným klíčem příjemce. Tak je zajištěno nejen utajení před všemi nepovolanými, ale i prokazatelnost autorství a autenticity.

K digitálnímu podpisu

Zpráva, která má být podepsána, je transformována pomocí signatářova soukromého klíče do posloupnosti znaků (tj. řady písmen a číslic) připojené k vlastní zprávě jako její digitální podpis. Kdokoliv, kdo má k dispozici signatářův veřejný klíč, může si jeho aplikováním na připojený digitální podpis ověřit, zda skutečně je autorem zprávy signatář a zda zpráva nebyla po odeslání změněna. Digitální podpis lze tedy vymezit tak, že jde o funkci odeslané zprávy a tajné informace, která je známa pouze majiteli soukromého klíče a lze jej ověřit pomocí všeobecně známého veřejného klíče.

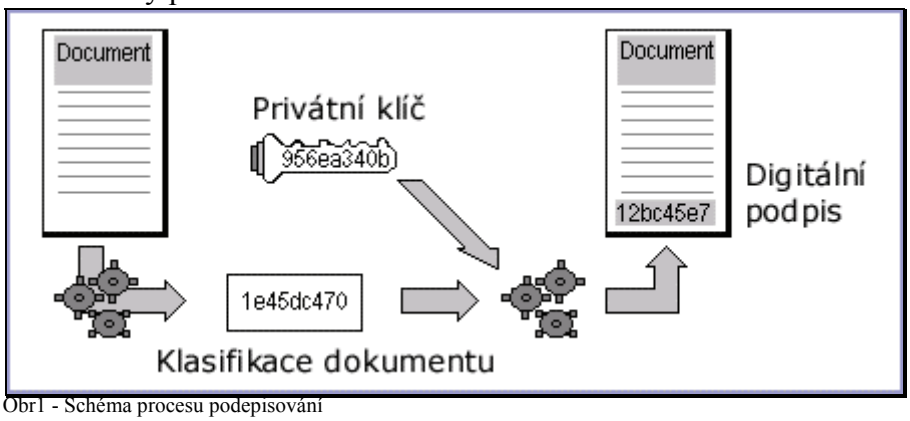
Problémem je způsob, jak ověřit pravost zveřejněných veřejných klíčů. K tomu slouží digitální či elektronický certifikát. Digitální certifikát obsahuje:

- osobní údaje držitele
- veřejný ověřovací kód držitele
- údaje o Certifikační autoritě
- digitální podpis Certifikační autority.

Jde se o uživatelův veřejný klíč a další údaje popisující držitele certifikátu (jméno, bydliště, fotografie apod.) To vše je zašifrováno privátním klíčem, jehož veřejný klíč je znám a dostupný z nezaměnitelných zdrojů..

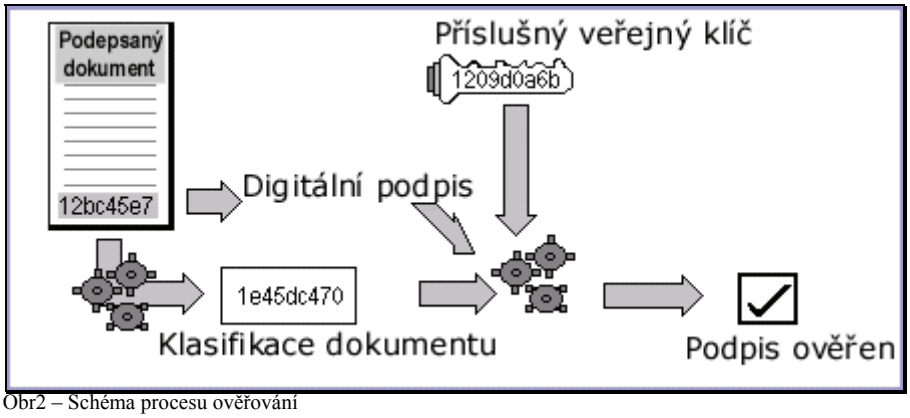
Držitelem a vydavatelem privátního klíče je tzv. Certifikační autorita instituce (popřípadě útvar, který tyto certifikáty neboli elektronické občanské průkazy vydává). Každý může požádat Certifikační autoritu o digitální certifikát.

Proces podepisování:
Nejdříve se zpřístupní privátní klíč, poté se vytvoří krátká číselná klasifikace dokumentu a nakonec se kombinací klasifikace dokumentu a privátního kódu autora vytvoří unikátní soubor čísel, digitální podpis, který se přičlení k dokumentu . Důležité je, že funkci procesu podepisování lze zajistit automaticky počítačem.



Obr1 - Schéma procesu podepisování

Proces ověření:
Odvozením z digitálního podpisu příjemce zpětně generuje číslo vyjadřující klasifikaci dokumentu Číslo klasifikace dokumentu se kombinuje s digitálním podpisem i veřejným klíčem a ověřuje se správnost podpisu. Správnost postupu lze zajistit pouze příslušným veřejným klíčem. Pokud ověřovací mechanizmus selže, není autorem dokumentu osoba, která se za autora vydává nebo byl po podpisu dokument změněn. I funkce procesu ověřování lze zajistit automaticky počítačem.



Obr2 – Schéma procesu ověřování

Použité informační zdroje:
www.pgp.cz
www.netzurnal.cz