Elektronický podpis. Ide skutočne o podpis?
Alebo el. podpis očami bežného človeka.

Väčšinu ľudí spočiatku zaujíma len to, čo k elektronickému podpisu potrebujú, ako el. podpis vytvoria a kam sa el. podpis uloží. No neskôr chcú poznať trochu viac o spôsoboch, akým el. podpis vzniká a načo si treba dávať pozor pri el. podpisovaní.

K el. podpisovaniu potrebujete 2 veci:

1. váš súkromný kľúč, ktorý je uložený v čipovej karte podobnej bankomatovej karte alebo môžete mať váš súkromný kľúč uložený v súbore napríklad na diskete,
2. program, ktorý vytvorí elektronický podpis.

Ak chcete niečo el. podpísať, napríklad dokument uložený v počítačovom súbore, tak potom do programu zadáte názov súboru, v ktorom je dokument uložený a HESLO na sprístupnenie vášho súkromného kľúča.

Program vygeneruje z dokumentu uloženého v súbore a pomocou vášho súkromného kľúča el. podpis, ktorý sa uloží do nového súboru. Nakoniec môžete tieto dva súbory (podpísaný dokument a el. podpis) odoslať niekomu, kto bude chcieť overiť váš podpis.

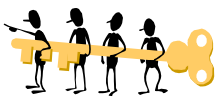
Ten, kto overuje váš podpis zadá pri overovaní do programu názov súboru, v ktorom je uložený overovaný dokument a zadá do programu názov súboru s el. podpisom. Program si potom načíta potrebné údaje zo súboru s el. podpisom a porovná ich s overovaným dokumentom. Ak je všetko v poriadku, program vypíše dátum a čas podpísania a údaje identifikujúce podpisovateľa, ak boli súčasťou súboru s el. podpisom.

Ak vás zaujímajú aj jednotlivé postupy pri el. podpise, v ďalšej časti sa ich budem snažiť priblížiť v obraznej forme nevyžadujúcej znalosti z informatiky alebo matematiky.

V tejto časti článku sa budem snažiť vysvetliť problematiku el. podpisu trochu netradične, pomocou bežných, pre každého známych vecí, ktoré obrazne nahradia matematické algoritmy.

Základom bude krabička so zámkou a dva rôzne kľúče od zámky. Do zámky budú pasovať len tieto dva kľúče a iné kľúče nebudú pasovať. Ďalej zámka na krabičke bude mať takú vlastnosť, že ak krabičku zamknete s jedným kľúčom, tak potom sa bude dať odomknúť len pomocou druhého kľúča. To znamená, že kľúčom, ktorým ste krabičku zamkli už krabičku otvoriť nemôžete a na otvorenie krabičky musíte potom použiť len druhý kľúč.

- Kľúč, ktorým budete krabičku zamkýnať nazvime **súkromný kľúč** a budete ho vlastniť **len vy**.
- Druhý kľúč, ktorým sa bude dať potom krabička odomknúť, nazvime **verejný kľúč** a urobme z neho veľké množstvo kópií, ktoré budú **verejne dostupné**.



A teraz budete chcieť poslať, napríklad svojej priateľke, pekný prsteň a chcete, aby vedela, že je určite len od vás.

1. Najprv si urobíte z prsteňa obrázok (fotku).
2. Obrázok vložíte do krabičky, ktorú zamknete vaším súkromným kľúčom.
3. Prsteň aj s krabičkou pošlete vašej priateľke.

Po doručení prsteňa a krabičky sa priateľka pokúsi otvoriť krabičku s verejným kľúčom. Je možné, že priateľka má viac priateľov a teda viac verejných kľúčov. Ale jedine s vašim verejným kľúčom, ktorý ste jej nedávno ***osobne*** dali, sa je krabičku podarí otvoriť. Po otvorení krabičky s obrázkom porovná obrázok a prsteň. A ak sa rovnajú, je si istá, že ste jej prsteň poslali jedine vy.

Zamknutú krabičku s obrázkom nazývame **digitálny podpis**. Podstata digitálneho podpisu spočíva v tom, že každý si môže digitálny podpis prezrieť, ale nemôže na ňom nič zmeniť. Podpis môže vytvoriť (vložiť obrázok do škatuľky a zamknúť ho so súkromným kľúčom) len vlastník súkromného kľúča. Druhou dobrou vlastnosťou digitálneho podpisu je, že pri kontrole porovnáme obrázok z krabičky odomknutý verejným kľúčom s tým, z čoho sa obrázok pri podpisovaní vytvoril, a teda overíme nezmodifikovanie (nesfalšovanie) napríklad podpísaného dokumentu.

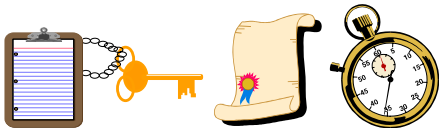
Ak by ste našli nejakú zamknutú krabičku a potom od nej neznámy verejný kľúč, nevedeli by ste, kto ju zamkol (kto vlastní súkromný kľúč). Až po otvorení krabičky a porovnaní obrázku z krabičky s vecami, pri ktorých bola krabička priložená, sa môžete presvedčiť že nik tieto veci nezmenil. Ak obrázok z krabičky je rovnaký ako priložené veci, je to dôkaz, že nik tieto veci nesfalšoval a sú teda také, ako keď ich neznámy vlastník súkromného kľúča digitálne podpísal (zamkol obrázok v krabičke so svojím súkromným kľúčom).

Aby každý, kto kontroluje váš digitálny podpis vaším verejným kľúčom vedel, že kľúč patrí vám a teda aby si mohol byť istý, že ste to podpisovali vy, pripojíte k vášmu verejnému kľúču prívesok s kartičkou, na ktorej sú informácie o vašom mene a ďalšie vaše identifikačné údaje.

A tu vzniká nebezpečenstvo, lebo ak niekto iný pripojí vašu kartičku k jeho verejnému kľúču a podpíše niečo, o čom vy neviete. Ale keďže na jeho verejnom kľúči je vaša kartička, budú si lúdia kontrolujúci podpis s podstrčeným verejným kľúčom myslieť, na základe informácií na kartičke, že ste to podpisovali vy.

Aby sa zabránilo takémuto zneužitiu, môžete si dať podpísať verejne dôveryhodnej osobe váš verejný kľúč spolu s vašimi identifikačnými údajmi, ktoré máte na kartičke pripojenej k vášmu kľúču. Verejne dôveryhodná osoba pridá k vašim údajom na kartičke údaje o sebe, ako podpisovateľovi, ďalej pridá čas podpísania a dobu, do kedy bude jeho podpis vášho verejného kľúča platný. Nakoniec digitálne podpíše kartičku spolu s vaším verejným kľúčom (vytvorí obrázok z vášho kľúča a kartičky, ktorý zamkne do krabičky svojím súkromným kľúčom).

Takéto spojenie identifikačných údajov s vaším verejným kľúčom, pomocou digitálneho podpisu dôveryhodnej osoby, nazývame **certifikát**. Dôveryhodná osoba môže byť napríklad úradník, ktorého poveril touto činnosťou Národný bezpečnostný úrad alebo iná osoba, ktorej verejný kľúč v certifikáte je verejne dostupný a všetci dôverujú údajom, ktoré táto osoba podpisuje. Všeobecne sa takáto osoba nazýva **certifikačná autorita (CA)**.



Ak do údajov, ktoré digitálne podpisujete (vytvárate z nich obrázok, ktorý zamknete do krabičky vaším súkromným kľúčom) pridáte ďalšie informácie, napríklad informácie o vašom verejnom kľúči, vašom certifikáte, čase podpísania alebo type podpisovaných údajov, vytvoríte tak **elektronický podpis**.

Pri kontrole elektronického podpisu odomknete krabičku verejným kľúčom z certifikátu, ktorý je napríklad priložený k elektronickému podpisu a skontrolujete či sa obrázok z krabičky zhoduje s podpísanými údajmi. Potom prekontrolujete nesfalšovanie certifikátu (pomocou digitálneho podpisu certifikátu s verejným kľúčom certifikačnej autority, ktorá certifikát vydala) a nakoniec sa opýtate certifikačnej autority, či ňou vydaný certifikát je stále platný. Overenie, že certifikát je stále platný, čiže nie je v zozname certifikátov, ktorých platnosť bola odvolaná v certifikačnej autorite, je dôležité. Napríklad ak by vám zlodej ukradol súkromný kľúč a pomocou neho by zlodej podpisoval údaje pod vaším menom, oznámite certifikačnej autorite, aby zaradila váš certifikát do **zoznamu odvolaných (zneplatnených) certifikátov** (certificate revocation list **CRL**). Od času, kedy bol váš certifikát zaradený do zoznamu odvolaných certifikátov, budú vaše podpisy neplatné a teda zlodej nebude môcť zneužiť váš súkromný kľúč.

A teraz prejdem k reálnemu popisu častí, z ktorých sa skladá elektronický podpis počítačom spracovateľných údajov. Táto časť je už určená pre trochu matematicky zdatnejších čitateľov.

Obrázok podpisovaných údajov nám nahradil hašovaciu funkciu. **Hašovacia funkcia** zabezpečí transformáciu informácie obsiahnutej v podpisovanom dokumente do informácie uloženej v konštantne veľkom bloku jednotiek a núl. Najčastejšie sa používajú hašovacie funkcie SHA-1, ktorej blok má veľkosť 160 bitov a MD5, ktorej výsledok má veľkosť 128 bitov. Ak si predstavíme obsah dátového súboru ako jedno veľmi veľké číslo, čiže súbor obsahuje jednu informáciu, potom nám z toho vyplýva, že bežný súbor o veľkosti 60kBytov (60*1024*8 bitov) môže obsahovať 2^{491520} rôznych informácií. Zatiaľ čo haš SHA-1 "len" 2^{160} rôznych informácií. Z toho nám vyplýva, že ku každej z $(2^{491520} - 2^{160})$ rôznej informácií uloženej v 60kBytovom súbore môžeme nájsť aspoň jednu

takú, ktorá bude mať rovnaký haš. Ale 2^{160} je dostatočne veľké číslo na to, aby sme dúfali, že dva rôzne dokumenty nebudú mať rovnaký haš.

Krabička s dvoma kľúčmi nám nahradila **asymetrický šifrovací algoritmus** napríklad **RSA**.

Súkromný a verejný kľúč je dvojica veľkých čísel, ktoré sú vygenerované tak, aby bežne dostupnými prostriedkami neumožnili nájdenie tretieho čísla, s ktorým by sa dalo previesť rovnakú operáciu ako s týmito dvoma číslami. Alebo zo znalosti jedného čísla si odvodiť druhé číslo.

Zamknutie obrázku v krabičke súkromným kľúčom nám nahradilo asymetrické **zašifrovanie** hašu podpisovaného dokumentu so súkromným kľúčom.

Odomknutie krabičky s verejným kľúčom nám nahradilo asymetrické **odšifrovanie** hašu s verejným kľúčom.

Dúfam, že tento netradičný spôsob priblíženia problematiky elektronického podpisu vám pomohol zorientovať sa v nových pojmoch a umožnil osvojiť si základné princípy pri elektronickom podpise.

Ing. Peter Rybár
pr@mailbox.sk
http://elpi.host.sk/