TECHNOLÓGIA ELEKTRONICKÉHO PODPISU
TECHNOLOGY OF ELECTRONIC SIGNATURE

Ladislav Schwartz[1)], Dušan Trstenský[1)], Jaroslav Sádovský[2)]
[1)]Katedra telekomunikácii, Elektrotechnická fakulta, Žilinská univerzita, Veľký diel 010 26 Žilina, Slovensko
[2)]Department of Information Technology, Technical University of Vienna Wiedner Hauptstrasse 8-10, A-1040 Wien, Austria

Abstrakt Elektronický podpis používa pre svoje vygenerovanie elektronický odtlačok správy a asymetrický algoritmus šifrovania. Pri verifikácii správy na prijímacej strane musí byť zhodný elektronický odtlačok pôvodnej správy s odtlačkom prijatej správy. Elektronickým podpisom je zabezpečená autentizácia autora a integrita prenesených dát. Elektronickým podpisom je možné podpísať všetko, čo je v digitálnej forme.

Summary An electronic signature uses a hash of message and an asymetrical algorithm of encryption for its generation. During verification of message on receiver side the hash of original message must be identical with the hash of received message. Electronic message is secured autentization of author and integrity of transmission date. By electronic signature it is possible to sign everything what is in digital form.

1. ÚVOD

Elektronický podpis (EP), niekedy aj digitálny podpis (DP) je prostriedok k zaisteniu elektronickej autentizácie autora (podpisovateľa) a integrity podpisovaných dát [2, 4]. Jeho úlohou je preukázať, že dokument bol skutočne podpísaný osobou, o ktorej predpokladáme, že tento dokument podpísala a zároveň poskytnúť možnosť overenia, či počas prenosu nedošlo k modifikácii tohto dokumentu.
Elektronický podpis je podľa definície v norme ISO 9697 reťazec, ktorý slúži na ochranu integrity, autentizáciu a na autorizáciu elektronických dokumentov.
Elektronický podpis je kľúčovým prvkom seriózneho elektronického obchodu a ďalších elektronických služieb s prívlastkom "e-". Aby takýto podpis mal právnu váhu porovnateľnú s vlastnoručným podpisom, musí v súlade s § 40 ods. 4 Občianskeho zákonníka umožňovať zachytiť obsah právneho úkonu a určiť osobu, ktorá právny úkon elektronickými prostriedkami urobila.
Je to metóda pre bezpečnú komunikáciu, pomocou ktorej zisťujeme, či so správou alebo dátovým súborom nebolo manipulované a či bola zistená integrita. V spojení s certifikátom elektronický podpis potvrdzuje, že sa jedná o správu skutočne z predpokladaného zdroja.
Elektronický podpis v bežnom živote poskytuje dôkaz, že podpísaná osoba sa cíti byť obsahom dokumentu viazaná, že potvrdzuje svoj úmysel stotožniť sa s obsahom dokumentu, ktorý vystavil niekto iný, alebo že potvrdzuje autorstvo dokumentu a že preukazuje skutočnosť, že táto osoba bola prítomná na stanovenom mieste.
Dnes vieme podpísať všetko čo sa dá previesť do digitálnej formy a čo bolo kedysi nemysliteľné podpísať. Jedna sa napríklad o podpis programu, fotografie, plánu objektu, obsahu databázy a podobne.

2. PRINCÍP ELEKTRONICKÉHO PODPISU

V prípade elektronického podpisu je pre hash funkciu vstupnou informáciou podpisovaný dokument. Z celej rady jeho typických znakov je potom spočítaný hash. Podstatu fungovania elektronického podpisu tvorí implementácia určitej matematickej funkcie prostredníctvom špecializovaného programu, ktorého pripojením k určitému dokumentu dochádza k overeniu jeho pravosti.
Elektronické podpisovanie správy prebieha tak, že sa pomocou jednocestnej funkcie (hash funkcie) vytvorí tzv. digitálny odtlačok správy, ktorý je zašifrovaný tajným (súkromným) kľúčom a pridaný k tejto správe. Je to kryptografická charakteristika – Message Digest, ktorá charakterizuje spracovávaný dokument. Príjemca dešifruje získaný zašifrovaný odtlačok verejným kľúčom (obsiahnutým v certifikáte) a opäť pomocou hash funkcie vygeneruje z prijatej správy alebo dátového súboru nový odtlačok, pričom oba porovná a v prípade, že sú totožné, je elektronický podpis platný. Účinnosť podpisu závisí na kvalite jednocestnej hash funkcie a na účinnosti šifrovania tohto hash-a.
Hash-ovanie [1] je postup spracovania, ktorý využíva vlastnosti špeciálnych tried matematických funkcií nazvaných jednosmerné funkcie, alebo kryptografické hash-ovacie funkcie, ktoré umožňujú priradiť elektronickému informačnému reťazcu charakteristickú hodnotu tak, že výsledok spracovania je pre daný reťazec jednoznačnou hodnotou. Zároveň platí, že na základe znalosti charakteristickej hodnoty získanej spracovaním informačného reťazca hash-ovacou funkciou nie je možné zrekonštruovať pôvodný informačný reťazec. Je to teda matematická funkcia, ktorú je možné v jednom, priamom smere jednoducho spočítať, zatiaľ čo v opačnom smere (inverznom zobrazení) prebiehajú výpočty veľmi obtiažne.
Hash je v podstate miniatúrny odtlačok obsahu dokumentu. Výsledkom hash funkcie je 128 alebo 160 bitov dlhá sekvencia jednoznačne charakterizujúca vstupný blok dát.

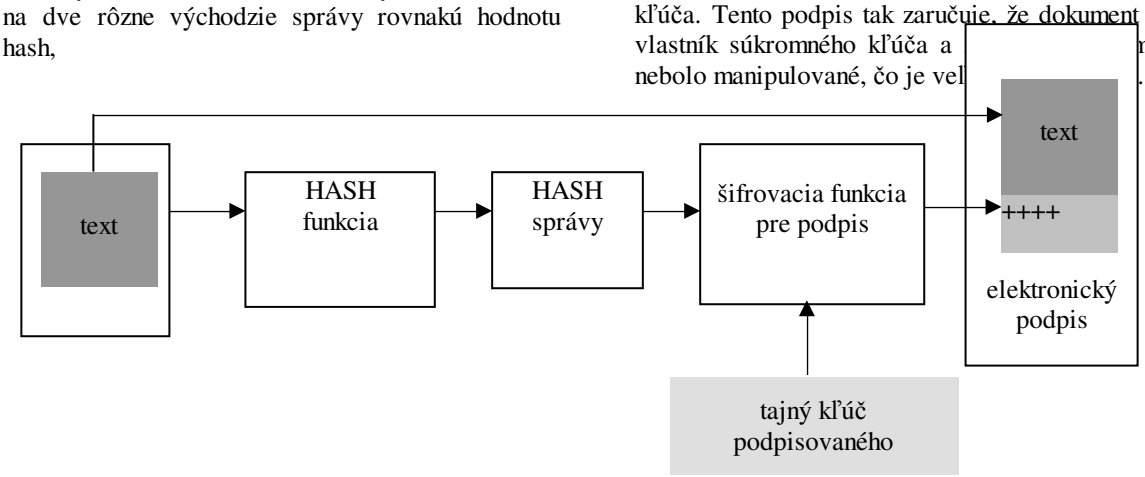
Aplikovaním hash-ovacieho algoritmu sa vyrieši aj otázka overiteľnosti integrity dokumentu - odtlačku, ktorého hodnota sa zmení v prípade akejkoľvek

modifikácie obsahu dokumentu. Šifrovaním tohto odtlačku tajnou časťou asymetrického šifrovacieho kľúča odosielateľa je zabezpečená identifikovateľnosť a nepopierateľnosť.

Základné požiadavky na hash funkcie sú:

- musí byť jednosmerná, teda je možné jednoducho vypočítať hash dokumentu, ale nesmie byť možné bežnými technickými prostriedkami z hodnoty hash odvodiť pôvodnú správu,
- musí byť nekolízna, teda nesmie byť možné dostať na dve rôzne východzie správy rovnakú hodnotu hash,
- musí byť fixná dĺžka výstupu, teda z dokumentu ľubovoľnej dĺžky je vygenerovaná sekvencia pevnej dĺžky, obvykle to je 128 alebo 160 bitov (napr. SHA-1).

Na počiatku elektronického podpisu sú vždy nejaké dáta v elektronickej podobe, ktoré chceme podpísať. Pomocou funkcie hash vypočítame hash správy. V tejto chvíli vstupuje do akcie tajný (súkromný) kľúč podpisovaného človeka. Špeciálny počítačový program pripojí k dátam podpis na základe hash-u a súkromného kľúča. Tento podpis tak zaručuje, že dokument podpísal vlastník súkromného kľúča a [illegible]ni dátami nebolo manipulované, čo je vel[illegible]. 1).



Obr. 1 Vygenerovanie elektronického podpisu
Fig. 1 Generation of electronic signature

V uvedenom prípade je dokument prenášaný v otvorenej forme, t.j. čitateľnej, čo je v prípade zachovania dôveryhodnosti tohto dokumentu neprípustné. Vtedy je vhodné tento dokument šifrovať vhodným symetrickým šifrovacím algoritmom, čo samozrejme prináša opäť ďalší problém spoľahlivého doručenia použitého šifrovacieho kľúča pre zašifrovanie dokumentu .

Namiesto rukopisu je použitý tajný kľúč. Algoritmus digitálneho podpisu DSA (Digital Signature Algorithm) s 1024 bitovým modulom p je nasledovný [3].

Parametre:

- verejný modul p, čo je 1024 bitové prvočíslo v rozsahu $2^{1023}<p<2^{1024}$,
- verejné 160 bitové prvočíslo q v rozsahu $2^{159}<q<2^{160}$, ktorá je deliteľom čísla $p-1$,
- verejné číslo g, ktoré vznikne voľbou prirodzeného čísla h ($1<h<p-1$) tak, že $g=h^{(p-1)/q} \bmod p>1$ (g je generátor cyklickej podgrupy rádu q v grupe čísiel 1 až $p-1$).

Kľúče:

- tajný 160 bitový kľúč x, t.j. číslo v rozsahu $0<x<q$,
- verejný 1024 bitový kľúč y taký, že $y=g^x \bmod p$.

Čísla p, q, g (napríklad pre účely certifikátov) označujeme ako parametre štandardu digitálneho podpisu DSS (Digital Signature Standard); sú verejné a môžu byť dokonca spoločné pre skupinu ľudí. Čísla y a x sú skutočné kľúče. Tajný kľúč má dĺžku len 160 bitov, čo je na rozdiel od iných asymetrických systémov veľmi malé číslo užitočné pre čipové karty.

Tiež sa tu používa 160 bitový parameter k ($0<k<q$), ktorý sa generuje pre každý podpis zvlášť. Musí byť generovaný náhodne a nesmie byť prezradený rovnako ako tajný kľúč x. Pri podpisovaní novej správy je generovaná nová hodnota k.

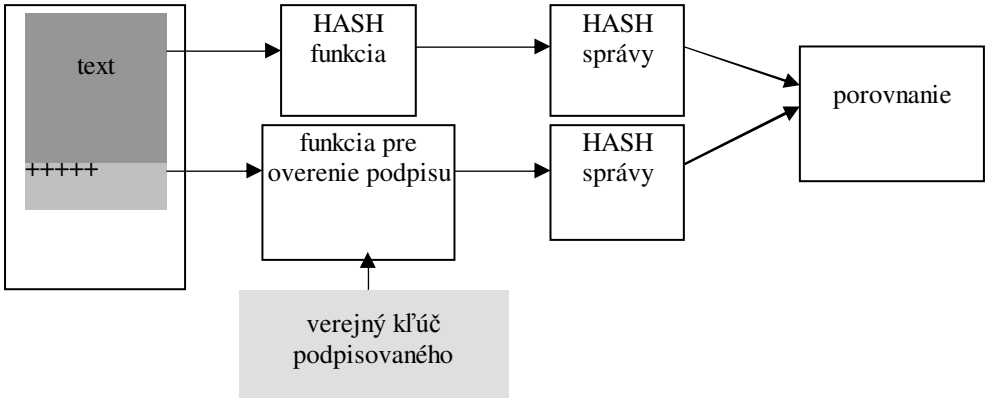
Správa M sa podpíše nasledovne. Najprv sa vytvorí hash-ovací kód $m=H(M)$ za použitia funkcie SHA-1. Potom sa vygeneruje číslo k a vypočíta sa dvojica čísiel (r, s), ktoré tvoria podpis:

$r=(g^k \bmod p) \bmod q$
$s=(k^{-1}(m+xr)) \bmod q$

Čísla s a r sa potom ako podpis pripoja ku správe M a takto tvoria celok – správa s pripojeným digitálnym podpisom. Úloha čísla k de facto spočíva v maskovaní tajného kľúča x (hodnota r v rovnici pre s) pri podpisovaní každej správy, a to vždy novým spôsobom. Overovateľ môže zistiť, že tajný kľúč x bol pri tvorbe (r, s) použitý, čím potvrdí platnosť podpisu, ale nemôže určiť hodnotu x ani hodnotu m.

Obdobným spôsobom prebieha i overenie elektronického podpisu na strane príjemcu[4]. Nestačí sa teda len uspokojiť s konštatovaním, že dáta sú elektronicky podpísané, ale je nutné overiť, či je podpis platný a či do prijatej správy nebolo zasahované niekde po ceste alebo ešte aj dodatočne po podpísaní.

Špeciálny program si informáciu rozdelí na dve časti. Jedna je podpísaná dátová časť a druhá je vlastný elektronický podpis. Postupne spočítava hash správy. Potom si spočíta hash z elektronického podpisu, pričom využije verejný kľúč podpísaného. Nasleduje porovnanie oboch hash-ov - dátového i podpisového a iba v prípade, že sú totožné, je zrejmé, že nedošlo k žiadnym úpravám zasielaných informácií a odosielateľ bol identifikovaný a overený obr. 2. Ak sa však objaví aj drobný nesúlad, znamená to, že niečo nie je v poriadku a príjemca je upozornený na neplatnosť elektronického podpisu. Nezáleží pritom na tom, kde, kto a ako správu modifikoval. Skutočnosťou zostáva len fakt, že elektronický podpis nie je platný.



Obr. 2 Verifikácia elektronického podpisu
Fig. 2 Verification of electronic signature

Zárukou originality a pôvodu dokumentu je potreba, aby príjemca elektronického dokumentu mohol získať verejnú časť šifrovacieho kľúča dôveryhodným spôsobom, t. j. spôsobom zaručujúcim, že táto časť kľúča patrí skutočne odosielajúcej strane. Na tento účel môžu komunikujúce strany využiť dve alternatívy:

- zabezpečiť dodanie verejného kľúča spoľahlivou cestou (osobné stretnutie, spoľahlivý kuriér a podobne),
- využiť tzv. certifikačnú autoritu, t.j. inštitúciu, ktorá potvrdí a zaručí, že daný verejný kľúč skutočne prináleží príslušnej strane. Keby sme hľadali podobnosť v bežnom živote, mohli by sme certifikačnú autoritu v určitom ponímaní prirovnať k notárskemu úradu. Táto alternatíva pritom rieši aj prípadné ďalšie riziko – možnosť, že došlo k odcudzeniu tajnej časti kľúča partnera, a tak sa za osobu považovanú za pôvodného majiteľa kľúča vydáva niekto cudzí.

Podpis sa overí nasledovne [3]. Príjemca správy M si vypočíta jej hash-ovaciu hodnotu $m=H(M)$ a ďalej z dôveryhodného zdroja musí získať parametre p, q, g a verejný kľúč y. Táto zdanlivo nevinná podmienka je kľúčová pre zistenie digitálnej identity signatára.
Príjemca skontroluje, že $0<r, s<q$ a vypočíta pomocné premenné:
$w=s^{-1} \bmod q$
$u_1=mw \bmod q$
$u_2=rw \bmod q$
$v=(g^{u1}y^{u2} \bmod p) \bmod q$
Ak je všetko v poriadku, musí byť $v=r$.
Šifrovanie a činnosti s ním spojené tvoria základnú časť technológie elektronického podpisu. Šifrovanie údajov zabezpečuje ich dôveryhodnosť a ochranu voči tretej strane. Je to proces, pri ktorom konkrétna kryptografická metóda transformuje otvorený text pomocou kryptografického algoritmu a šifrovacieho kľúča do šifrovaného textu. Pri tejto transformácii môžu byť použité:

- symetrické šifrovacie algoritmy,
- asymetrické šifrovacie algoritmy.

Pri symetrickom šifrovaní používajú obe strany ten istý tajný kľúč. Pri asymetrickom šifrovaní sa používajú nasledovné spôsoby:

- niekoľko k jednému (many-to-one), t.j. niekoľkí môžu používať verejný kľúč a len jeden má tajný kľúč, ktorým môže dešifrovať. Používa sa k šifrovaniu správ.
- jeden k niekoľkým (one-to-many), t.j. jeden má tajný kľúč a mnohí majú verejný kľúč, ktorým môžu dešifrovať. Tento spôsob sa používa práve pri elektronickom podpise.

3. ZÁVER

Na rozdiel od klasického podpisu je prakticky nemožné ho sfalšovať. Vďaka využitiu najmodernejších algoritmov pre zabezpečenie elektronického podpisu je čas potrebný na sfalšovanie rádovo 1,6 *1018 MIPS (Million Instruction Per Second) za rok, t.j. pokiaľ by bolo použitých desaťtisíc PC s výpočtovým výkonom 1000 MIPS, trval by výpočet 1011 rokov.

LITERATÚRA

[1] SCHWARTZ, L. – TRSTENSKÝ, D.: Elektronický otlačok správy. ADVANCES in Electrical and Electronic Engineering. ŽU v Žiline, Vol. 2/2003, ISSN 1336-1376
[2] KLÍMA, V.: Až nás podepíše počítač. CHIP 5/1999
[3] KLÍMA, V.: Podpis bez pera a papíru. CHIP 5/1999
[4] BAŠTEK, Z.: Elektronický podpis. Semestrálna práca 2003