Elektronická identifikácia, elektronický podpis a bezpečnosť informačných systémov

Pavel Horovčák [1]

The electronic identification, signature and security of information systems

The contribution deals with the actual methods and technologies of information and communication systems security. It introduces the overview of electronic identification elements such as static password, dynamic password and single sign-on. Into this category belong also biometric and dynamic characteristics of verified person. Widespread is authentication based on identification elements ownership, such as various cards and authentication calculators. In the next part is specified a definition and characterization of electronic signature, its basic functions and certificate categories. Practical utilization of electronic signature consists of electronic signature acquirement, signature of outgoing email message, receiving of electronic signature and verification of electronic signature. The use of electronic signature is continuously growing and in connection with legislation development it exercises in all resorts.

Key words: *electronic identification, information system, electronic signature, internet, authentication.*

Úvod

Bezpečnosť informačných systémov (IS) je v súčasnosti podporovaná celým spektrom moderných bezpečnostných technológií. Patrí medzi ne napríklad technika firewallu, rôzne metódy šifrovania, elektronický podpis a iné.Významné miesto medzi nimi má technika autentifikácie, ktorej úlohou je zabezpečiť vierohodné overenie totožnosti používateľa. Toto overenie môže byť vykonané troma spôsobmi [1]:

– na základe znalostí používateľa,
– na základe charakteristiky overovanej osoby (biometrika)
– na základe vlastníctva rôznych identifikačných prvkov.

V prípade použitia kombinácie týchto spôsobov hovoríme o tzv. silnej autentifikácii, ktorá je v súčasnosti už tiež využívaná v praxi (napríklad vo vzťahu klient – banka pri výbere peňazí z bankomatu, či klient mobilnej siete, ktorý má SIM (Subscriber Identification Module) kartu a pozná jej PIN (Personal Identification Number).

Prehľad elektronických identifikačných prvkov

Autentifikácia na základe **znalostí** je najstaršia a doteraz najbežnejšia technika, založená na znalosti **statického hesla**. Ochrana heslom je priamo integrovaná do operačného systému či inej aplikácie a teda dodatočné cenové náklady nie sú potrebné. Súčasne je tu však fakt, že je to najmenej zabezpečená služba z rôznych dôvodov – počnúc možnosťou uhádnutia hesla a končiac priamo zoznamom hesiel pri monitore počítača, k čomu vedie v súčasnosti používanie viacerých služieb, chránených heslami. Bezpečnejšie riešenie je použitie **dynamického hesla**, vygenerovaného jednorázovo pre konkrétnu komunikáciu. Perspektívnym sa javí stratégia **jediného prihlásenia** (single sign-on), ktorá bude odstraňovať nereálnosť mnohých prihlasovacích mien a hesiel pri zabezpečení e-obchodu, ako z hľadiska používateľa, tak z hľadiska administrácie.

Autentifikácia na základe **charakteristiky** overovanej osoby zahŕňa rad starších aj celkom nových metód [2]. Najstaršou technikou je **snímanie odtlačkov prstov** na báze elektrických, optických, ultrazvukových, tepelných a tlakových snímačov. Najnovšie ultrazvukové snímače sú však veľmi drahé. Snímanie odtlačkov je založené na princípe jedinečnosti odtlačkov každého človeka. Nevýhodou je možnosť "oklamania" snímača kópiou odtlačku na návleku. Ďalšie dve metódy využívajú jedinečnosť očnej sietnice a očnej dúhovky človeka. Metóda založená na **očnej sietnici** (retina) je veľmi náročná z hľadiska snímania. Snímanie **očnej dúhovky** (iris) pomocou kamery je podstatne jednoduchšie, a preto perspektívnejšie, aj keď je tiež dosť drahé. Iná metodika je založená na **rozpoznávaní tváre**, ktorá využíva programovo simulované neurónové siete a prvky umelej inteligencie. Systém tak dostáva možnosť "naučiť sa" podobu jednotlivých osôb a potom ju porovnávať so snímaným obrazom. Iným známym princípom je **rozpoznávanie hlasu**, ktorého spoľahlivosť je o niečo menšia ako u iných techník a môže klesať pri rôznych drobných ochoreniach či okolitom hluku. Jej výhodou je nízka cena a nenáročnosť snímania, nevýhodou nižšia presnosť. Technika **dynamiky písania** na klávesnici pri zadávaní mena a hesla skúma a vyhodnocuje časy stláčania jednotlivých klávesov. Tým možno zabrániť prístupu do systému pri odcudzení hesla. Riešenie je programové, pomerne jednoduché a zvyšuje bezpečnosť prístupu pomocou hesla.

[1] *Ing. Pavel Horovčák, CSc*., Katedra informatizácie a riadenia procesov F BERG Technickej univerzity v Košiciach, 042 00 Košice, ul. Boženy Němcovej 3 (Recenzované 18.7.2002)

Autentifikácia na základe **vlastníctva** rôznych identifikačných prvkov zahŕňa magnetické karty, čipové inteligentné karty a bezkontaktné čipové karty, ako aj autentifikačné kalkulátory. **Magnetické snímacie karty** sú najstarším predstaviteľom tohto druhu autentifikácie. Rozsah ich použitia je veľký, od dochádzkových, kopírovacích alebo objednávacích systémov až po platobné karty, pritom ale ich bezpečnosť nie je vysoká, lebo nie je technický problém urobiť kópiu magnetického prúžku. **Čipové** (mikročipové) **inteligentné karty** (smart cards) obsahujú mikroprocesor, ktorý môže zabezpečovať rôzne služby, počnúc autentifikáciou, cez ochranu údajov až po šifrovanie. Umožňujú podporu silnej autentifikácie používateľa (dvojfaktorovú autentifikáciu), bezpečné uloženie digitálnych certifikátov, či súkromného kľúča, a tým aj určenie zodpovednosti používateľa za vykonanie elektronickej transakcie. Tieto karty môžu integrovať aj ďalšie funkcie, ako napríklad vstup do objektov, firemná identifikácia, stravovanie, stratégia jediného prihlásenia, mobilné uchovanie certifikátov a ďalšie, preto rozsah ich použitia neustále narastá. Sem patria aj karty SIM. Pri kúpe SIM karty dostane zákazník pridelené telefónne číslo a zapečatený PIN a PUK (Personal Unlocking Key) kód. V karte je zabudovaný mikroprocesorový čip s telefónnym číslom zákazníka a s ďalšími informáciami súvisiacimi s predplatným jeho služieb. **Bezkontaktné čipové karty** sú založené na prenose identifikačného čísla z karty do snímača na základe indukcie. Ich použitie je tiež veľmi široké – od informačných technológií cez finančné služby až po hromadnú dopravu. Z pohľadu zvýšenia bezpečnosti sa možno stretnúť tiež s kombináciou oboch týchto princípov na jednej karte, ktorá potom obsahuje nezávislú bezkontaktnú identifikačnú časť a súčasne výkonný mikroprocesor. **Autentifikačný kalkulátor** sa tiež nazýva elektronický kľúč a je jedným z najlepších prostriedkov silnej autentifikácie. Jeho úlohou je zabezpečenie dvoch hlavných bezpečnostných funkcií. Prvou je výpočet dynamického alebo jednorázového hesla (OTP – One-Time Password) pre overenie totožnosti používateľa pristupujúceho k vzdialenému systému. Druhou funkciou je výpočet elektronického podpisu (MAC – Message Authentication Code) na zabezpečenie elektronickej transakcie a integrity jej obsahu.

Autentifikácia môže v **budúcnosti** využívať rôzne kombinácie dnešných techník, napríklad podkožnú implantáciu bezkontaktného čipu s pamäťou. Tu však vystupujú do popredia predovšetkým morálne a etické problémy. Fantázii sa medze nekladú, a preto sú dnes na svete úvahy o vytvorení syntetickej látky – nositeľky informácií, podobne ako DNA. Iné úvahy smerujú k snímaniu mozgových vĺn človeka a ich vyhodnoteniu.

Elektronický podpis – čo to je ?

Definícia elektronického podpisu podľa smernice Európskeho parlamentu [4] hovorí, že elektronický podpis predstavuje dáta v elektronickej forme, ktoré sú pripojené alebo logicky súvisia s inými elektronickými dátami a ktoré slúžia ako metóda autentifikácie (overenia pravosti).

Občiansky zákonník v § 40 ustanovuje, že každý písomný právny úkon je platný, ak je podpísaný konajúcou osobou. Písomná forma je zachovaná, ak je právny úkon urobený telegraficky, ďalekopisom alebo elektronickými prostriedkami, ktoré umožňujú zachytenie obsahu právneho úkonu a určenie osoby, ktorá právny úkon urobila [5].

Primárne použitie elektronického podpisu je v oblasti elektronickej pošty. Príjemcovi elektronickej pošty správa elektronicky podpísaná **zabezpečí** bezpečnú identifikáciu odosielateľa, **autentifikáciu** – overenie skutočnej identity autora (tieto dve vlastnosti sú prakticky rovnaké), **integritu správy** – zaručuje neporušenosť správy na ceste od odosielateľa k príjemcovi a **nepopierateľnosť** – odosielateľ nemôže poprieť autorstvo správy.

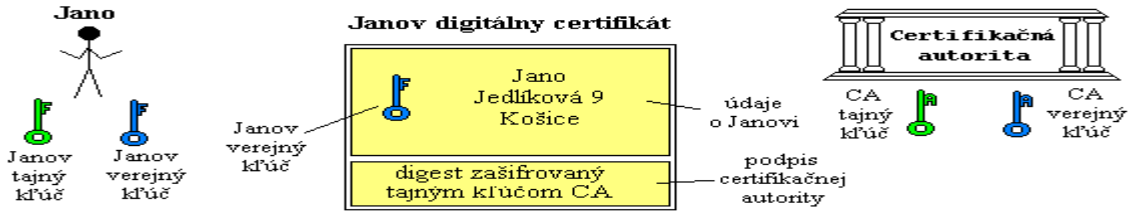
Elektronický podpis (tiež digitálny podpis) je technicky založený na využití dvojice **kľúčov** (**tajný a verejný**) pre asymetrické šifrovanie správy. Medzi tajným a verejným kľúčom je matematický vzťah a platí, že z verejného kľúča nie je možné dostupnými technickými prostriedkami odvodiť kľúč tajný. Verejný kľúč je preto možné publikovať bez nebezpečenstva prezradenia tajného kľúča. Elektronicky podpísanú správu môže čítať každý, ale je isté, že ju vytvoril práve odosielateľ a že nebola po ceste zmenená. K podpísanej správe sa pripojí kontrolný súčet, tzv. message digest, zašifrovaný tajným kľúčom odosielateľa. Príjemca ho pomocou verejného kľúča dekóduje a porovná ho s vypočítaným kontrolným súčtom. Ak sa zhodujú, správu odoslal majiteľ tajného kľúča a po ceste nebola zmenená.

Ak má každá strana komunikácie svoju dvojicu kľúčov, môže odosielateľ správu zašifrovať (verejným kľúčom príjemcu) aj digitálne podpísať (svojim tajným kľúčom), čím je táto dokonale chránená (lepšie ako klasické dokumenty bez ochrany proti zmene). Príjemca má zaručené, že:

- správu si po ceste nikto tretí neprečítal (šifrovanie),
- správu odoslal skutočne ten, kto je podpísaný (podpis),
- správa nebola po ceste zmenená (digest) .

Elektronický podpis je na rozdiel od podpisu vlastnoručného stále iný. Presnejšie, je iný pre každý podpísaný dokument. Ručný podpis je pri elektronickom podpise nahradený procesom spojenia dvoch čísel zložitými matematickými operáciami. Výsledok je pripojený k podpisovanému dokumentu a prenášaný ako celok, pr.e-mailom.
Digitálny certifikát zabezpečuje väzbu verejného kľúča na konkrétnu osobu a je digitálne podpísaný treťou dôveryhodnou stranou, ktorej verejný kľúč je známy. Táto dôveryhodná strana sa nazýva certifikačná autorita

(CA) a je to všeobecne známa inštitúcia, ktorá vydáva digitálny certifikát po overení totožnosti certifikovaného. Postup certifikácie je znázornený na obr. 1. Digitálny certifikát je teda verejný kľúč spojený s údajmi o jeho vlastníkovi, podpísaný certifikačnou autoritou (spojené spolu s message digest zašifrovaným tajným kľúčom certifikačnej autority). Verejné kľúče niektorých svetových certifikačných autorít sú súčasťou bežných poštových klientov (Netscape Communicator aj MS Outlook). Verejný kľúč inej, menej rozšírenej certifikačnej autority je do poštového klienta potrebné zaviesť ručne (obyčajne je dostupný na www stránke certifikačnej autority). Pojmy digitálny certifikát a elektronický podpis sa často (v zmysle vyššie uvedeného nie celkom správne) zamieňajú.



Elektronický podpis prakticky

Rozdelenie certifikátov. Podľa účelu sa certifikáty delia na **osobné** certifikáty (pre koncových používateľov, ktorí používajú bezpečnú poštu a ako klienti pristupujú protokolom HTTPS na WWW server), na certifikáty **pre server** (certifikáty WWW serverov, na ktoré sa pristupuje protokolom HTTPS, certifikáty adresárových serverov pracujúce s protokolom SecureLDAP) a na certifikáty **certifikačnej autority** (CA) (treba sa uistiť o jeho pravosti, hoci aj telefonicky). Platnosť osobného certifikátu je zvyčajne 1 rok (tab. 1), certifikátu CA 10 rokov (obr. 2).

Current status: Certificate is valid.

This certificate belongs to:	**This certificate was issued by:**
Pavel Horovcak	CA FRI-ZU
Pavel.Horovcak@tuke.sk	emil@utcpd.sk
F BERG TU Kosice	FRI-ZU Prievidza
Technicka univerzita	Zilinska univerzita
Kosice	Zilina
Slovakia	Slovakia
SK	SK

Serial Number:
64
This certificate is valid from May 29 13:27:54 2001 GMT until May 29 13:27:54 2002 GMT.
Certificate Fingerprint:
MD5: A9:11:F3:F6:08:14:DF:C6:C5:FC:55:24:D7:B0:21:0A
SHA-1: 7E:0F:67:9E:20:2C:CC:AA:86:91:8C:50:79:18:74:D6:26:B7:72:C6

Tab.1 Ukážka osobného certifikátu. Tab.1 Example of personal certificate.

Kroky, potrebné na získanie osobného certifikátu sú nasledovné:

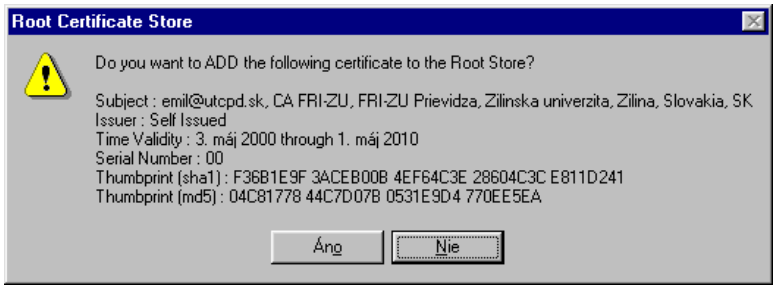
Získanie elektronického podpisu [7]. Túto službu už v súčasnosti poskytuje niekoľko organizácií, najmä pre účely osvety a prípravy na "ostré" využívanie elektronického podpisu v praxi. Jednou z nich je aj Žilinská univerzita[8], presnejšie jej certifikačná autorita. Prvým krokom pre získanie elektronického podpisu je vyplnenie formulára žiadosti o vydanie osobného certifikátu s identifikáciou žiadateľa, jeho vytlačenie a odoslanie. Prijatie je potvrdené e-mailom, na ktorý treba dať Reply. Následne sa vygeneruje súkromný a verejný kľúč. Súkromný si uloží žiadateľ do databázy svojho prehliadača, verejný ide na podpis CA. Tam žiadateľ prinesie vytlačený formulár žiadosti spolu s osobnými dokladmi (občiansky preukaz, pas), čím sa overí jeho totožnosť a CA potvrdí podpisom pravosť verejného kľúča a umiestni ho na svojej stránke, čím umožní ďalším záujemcom získanie uvedeného verejného kľúča. Adresu tejto stránky je vhodné uvádzať aj v e-mailovej komunikácii, aby si nový príjemca správy mohol daný verejný kľúč „stiahnuť" a uložiť do databázy svojho prehliadača.

Použitie elektronického podpisu. Odosielateľ správy potrebuje vhodné programové vybavenie – poštového klienta – ktoré vie realizovať operáciu podpisu. To dnes vedia všetky bežné aplikácie (MS Outlook, Netscape, Pegas, atď.). Ďalej potrebuje mať súkromný kľúč, ktorým "prebehne" podpisovanú správu, vytvorí jej kontrolný súčet (hash), aj s údajmi o odosielateľovi. Vykonanie podpisu správy je voliteľné – dôležité správy sa podpisujú, ostatné prípadne nie. Túto činnosť poštový klient vykonáva automaticky.

Príjem elektronického podpisu. Príjemca správy potrebuje mať verejný kľúč odosielateľa, ktorým môže overiť elektronický podpis odosielateľa. Tento verejný kľúč môže získať priamo od odosielateľa alebo od certi-

fikačnej autority, ktorá ho odosielateľovi pridelila. Týmto verejným kľúčom príjemca "prebehne" prijatú správu a vytvorí jej kontrolný súčet. Ak sú obidva súčty rovnaké, správa je v poriadku, inak nie.

Overenie elektronického podpisu. Príjemca potrebuje do svojho poštového klienta pridať certifikát certifikačnej autority, ktorá vydala osobný certifikát odosielateľa. Z www stránky treba tento certifikát „stiahnuť" (prípadne uložiť na disk), prezrieť a nainštalovať. Je zrejmé, že jeden používateľ môže dostávať podpísané správy certifikované viacerými certifikačnými autoritami, čím si môže vytvoriť databázu certifikátov. Pokiaľ nie je takýto certifikát nainštalovaný, je elektronický podpis správy pokladaný za neplatný. V tejto situácii je potrebné buď vykonať už spomínanú inštaláciu certifikátu certifikačnej autority alebo možno zvoliť vyslovené dôverovanie alebo nedôverovanie danému certifikátu.



Obr.2 Certifikát certifikačnej autority.
Fig.2 Certificate of certification authority.

Oblasti využitia elektronického podpisu

Nasadenie a využívanie elektronických podpisov je predmetom blízkej budúcnosti. Hlavné oblasti použitia sú orientované na elektronické aplikácie, ktoré akceptujú elektronické podpisy. Niektoré oblasti fungujú už v súčasnosti. V prvom rade je to oblasť finančných služieb a elektronického bankovníctva, kde sú v súčasnosti zúčastnené všetky významné bankové inštitúcie. Ďalšou významnou oblasťou je elektronický obchod, ktorý sa v súčasnosti rozvíja tak v oblasti B2B (business to business) ako aj B2C (business to customer). Elektronický podpis má nezastupiteľné miesto pri využívaní najrozšírenejšej internetovej služby – e-mailu, pričom všetky poštové klientske aplikácie majú technológiu certifikátov už dlhší čas implementovanú. Významnú úlohu majú tiež serverové certifikáty, ktoré umožňujú overovanie medziserverovej komunikácie a používajú sa tiež pri vkladaní citlivých údajov na server. Podmieňujú tiež šifrovanie prenášaných údajov medzi klientom a serverom na báze protokolu SSL (Secure Socket Layer), pri ktorom sa využíva kombinácia symetrického a asymetrického šifrovania. Postupne sa dá očakávať prenikanie a využívanie elektronického podpisu do ďalších oblastí štátnej správy, ako napríklad správa daní a poplatkov, správny poriadok, občiansky súdny poriadok, zdravotníctvo, poisťovníctvo. Bude to závisieť jednak na postupe legislatívneho procesu v jednotlivých oblastiach, jednak na postupe prijímania vykonávacích predpisov k Zákonu o elektronickom podpise a v neposlednom rade aj na cenovej politike jednotlivých certifikačných autorít.

Na Slovensku Zákon o elektronickom podpise má číslo 215/2002 Z.z. (Zbierky zákonov). Je účinný od 1.5.2002, okrem niektorých paragrafov, ktoré nadobúdajú účinnosť 1.9.2002.

Záver

Bezpečnosť informačných a komunikačných systémov a ďalších aplikovaných systémov (finančné, bankové, registračné a iné) je založená na využití štyroch bezpečnostných prvkov: **autentifikácia**, **šifrovanie**, **elektronický podpis** a **archív**. Podrobný rozbor týchto atribútov z hľadiska ich aplikácie v oblasti bezpečnosti elektronického bankovníctva v praxi na Slovensku je predmetom článku [3]. Súčasný stav vedomia používateľov a dokonca nezriedka aj tvorcov rôznych informačných systémov v oblasti ich bezpečnosti je veľmi nízky a preto je potrebné snažiť sa všetkými formami a prostriedkami o jeho zvýšenie. Mimoriadne aktuálnou sa stáva táto problematika najmä s nástupom a rozširovaním rôznych ICT (informačných a komunikačných technológií), kedy sa rôzne citlivé, dôležité, či dokonca tajné údaje a informácie musia rôznymi spôsobmi prenášať na diaľku a stávajú sa tak predmetom útokov nepovolaných osôb (či programov).

Literatúra

[1] Váša, J.: Autentifikace pro bezpečnost. *Connect! 2/2002, str.12.*
[2] Sobotka R.: Přehled elektronických identifikačních prvků. *Connect! 2/2002, str.13 – 15.*
[3] Rexa R., Fapšo R., Schreiber R.: Bezpečnosť elektronického bankovníctva v praxi. *PC Revue 6/2001.*
[4] Rexa R.: Od praktických skúseností k návrhu zákona o elektronickom podpise. *PC Revue 10/2001.*
[5] Občiansky zákonník č. 40/1964 Zb.
[6] Piškula M.: Elektronický podpis. *Právní magazín. http://www.zastudena.cz 21.8.2001.*
[7] Kršák, E.: Elektronický podpis. *In: Zborník prednášok na medzinárodnú konferenciu Systémová integrácia 2001, SSSI Žilina 2001, str. 185 – 194, ISBN 80-7100-880-X.*
[8] https://cert.utc.sk/ca.