ASPECTE GENERALE ALE SEMNĂTURILOR DIGITALE

Cristian Marinescu

cristian.marinescu@omicron.at
Universitatea Politehnica Bucureşti

Abstract: Informaţia este bunul cel mai de preţ în era comunicaţiilor şi a calculatoarelor, reprezentând cunoaşterea la un nivel foarte avansat. În forma sa digitală, ea a modificat radical modul de lucru al oamenilor, dar mai ales percepţia societăţii asupra însăşi informaţiei. Securitatea semnăturilor digitale este un domeniu complex, care face în prezent obiectul unor intense cercetări ştiinţifice. Articolul de faţă face o catalogare a diverselor metode de a realiza semnături digitale şi o analiză succintă a problemelor cu care se confruntă utilizatorul acestora.

Cuvinte cheie: securitate, semnături digitale.

Abstract: Information is one of the most important goods in the computer and communications era. In its digital form it has changed the way people work, but especially how society perceives information itself. The security of digital signatures is a complex domain and is currently the focus of scientific research. The present article presents different categories of digital signatures, analyzing the problems which the user encounters when using digital signatures.

Keywords: digital signatures, security.

1. Introducere

Tehnologia informaţiei s-a dezvoltat în ultimele decenii cu o viteză nemaiîntâlnită, depăşind posibilităţile societăţii umane de a accepta schimbările majore, petrecute în ultimul timp. Semnăturile digitale pun la dispoziţia utilizatorului posibilitatea de a înlocui în practică semnăturile olografe (scrise de mână). Sunt necesare tehnologii standardizate la scară internaţională pentru a asigura o interoperabilitate ridicată, o recunoaştere naţională, dar şi internaţională, dar mai ales un nivel de securitate ridicat, fără de care semnăturile digitale nu pot atinge acest scop.

Bazele teoretice ale semnăturilor digitale au fost puse cu aproape trei decenii în urmă, dar utilizarea şi implementarea acestora a luat amploare în urmă cu câţiva ani. Acest fenomen se datorează faptului că legislaţia în domeniul semnăturilor electronice a fost adoptată relativ recent, impulsionând cercetările din acest domeniu. S-a creat astfel cadrul necesar utilizării la scară largă a semnăturilor digitale [2].

Datorită necesităţii de a transmite la distanţă documente semnate în format electronic, apare tot mai imperios necesitatea de a realiza protocoale sigure, ce pun tehnici digitale la dispoziţie, şi care rezolvă problemele enumerate anterior. Pentru a obţine totodată valabilitatea documentelor electronice în faţa legii, sunt necesare semnături electronice, care să fie echivalente din punct de vedere legal cu semnăturile olografe. Acestea trebuie să aibă aceleaşi proprietăţi cu semnăturile olografe, iar momentul de timp la care semnătura a fost realizată să fie cunoscut [7].

Semnăturile olografe reprezintă o tehnică veche, creată datorită necesităţii societăţii umane de a încheia înţelegeri, acorduri sau contracte pe care semnatarii să le respecte, şi totodată pentru a conferi documentelor un caracter individual sau de nereprodus. Semnăturile sunt, în general, ataşate unor documente (scrisori, contracte, operaţii bancare) pe acelaşi mediu de stocare şi transmisie (în cazul de faţă hârtia). Ele sunt utilizate pentru a exprima acordul semnatarului cu conţinutul unui document, originea datelor sau reprezintă modalitatea de a împiedica modificări ulterioare ale datelor în cauză. Semnăturile olografe au caracter de unicat prin faptul că sunt create de către oameni, fiind totodată uşor de recunoscut, dar greu de reprodus [7]. Prin apariţia tehnologiilor moderne, semnăturile olografe s-au demodat, dar anumite proprietăţi şi avantaje ale acestora au fost recunoscute ca fiind foarte importante pentru realizarea semnăturilor digitale. Documentele în format electronic se diferenţiază într-un mod evident de documentele clasice, redactate pe hârtie. Nu există diferenţe între original şi copie [9], datele putând fi modificate, duplicate, transmise şi stocate într-un număr nelimitat, fără posibilitatea de a constata ceea ce s-a întâmplat cu datele.

Lipsa unor originale digitale este o trăsătură ce deosebeşte în mod fundamental metodele vechi de a păstra documentele pe hârtie, de metodele electronice. Datorită proprietăţilor ce le caracterizează, documentele electronice se confruntă cu următoarele aspecte:

- datele codificate în format binar nu prezintă individualitate [5];
- documentele electronice pot fi uşor copiate, multiplicate şi modificate, fără posibilitatea de a detecta eventualele modificări [8];
- semnătura electronică nu este conectată fizic la documentul semnat [4];
- din conţinutul datelor sau al semnăturii nu rezultă neapărat momentul de timp la care a fost creat documentul sau semnătura [6].

Semnăturile electronice sunt considerate echivalentul semnăturilor olografe în lumea digitală, reprezentând o modalitate de a semna datele în format electronic. Ca urmare, documentul împreună cu semnătura electronică digitală pot fi stocate, transmise sau replicate în format electronic. Datorită acestor proprietăți, semnăturile digitale au o largă utilizare în crearea și păstrarea actelor în format digital [7]. La o analiză atentă a cerințelor pe care trebuie să le îndeplinească orice fel de semnături electronice pentru a înlocui în practică semnăturile olografe, se poate însă observa că singura tehnologie capabilă să pună la dispoziție o soluție viabilă sunt semnăturile digitale [7].

Deși semnăturile digitale preiau toate proprietățile semnăturilor olografe, ele se deosebesc de acestea prin însăși natura lor. Producerea semnăturilor olografe constă dintr-un proces fizic, intrinsec producătorului, care prin caracterul său unic îl identifică pe semnatar fără a permite ulterior posibilitatea de a nega efectuarea semnăturii. Spre deosebire de aceasta, semnătura digitală este produsă de către o unitate electronică sau de către un calculator. Rolul semnatarului se rezumă la a pune la dispoziția sistemului niște date de intrare (cheie privată sau parolă), identificarea realizându-se în baza cunoașterii acestei informații secrete [12].

O altă deosebire o reprezintă faptul că, în timp ce o semnătură olografă este identică (sau cel puțin asemănătoare) pentru orice document, semnăturile digitale diferă între ele în funcție de conținutul documentului semnat. Cu alte cuvinte, falsificatorul are din punct de vedere teoretic șansa să producă o semnătură falsă pe un document scris de mână, dacă are posibilitatea de a studia îndeajuns semnătura originală, și de a o copia de pe un document pe altul. Prin comparație, atacatorul unei semnături digitale are posibilitatea de a apela la puterea de calcul a unei întregi rețele de calculatoare pentru a încerca falsificarea acesteia [10].

Există însă și deosebiri fundamentale între semnăturile clasice și cele digitale:

- semnăturile digitale sunt, de obicei, atașate documentului inițial, spre deosebire de cele olografe care fac parte integrantă din document (hârtia – mediul de stocare și transmisie – este considerată în acest caz o parte a documentului);
- verificarea acestora este diferită, semnătura olografă fiind comparată cu un specimen de semnătură (o modalitate relativ nesigură și subiectivă), în timp ce o semnătură digitală este verificată pe baza cheii publice și a algoritmului utilizat la producerea semnăturii;
- spre deosebire de cazul semnăturilor olografe, copiile realizate după o semnătură digitală sunt identice, având practic aceeași valoare ca și originalul (prima semnătură generată); de fapt, în aceste condiții, este impropriu a se vorbi despre un original în format electronic în sensul clasic al cuvântului.

2. Servicii oferite de semnăturile digitale

Aplicațiile semnăturilor digitale variază în funcție de necesitățile domeniului de utilizare. De cele mai multe ori, semnăturile digitale sunt utilizate concomitent cu certificatele digitale cu cheie publică. Acestea reprezintă o legătură digitală între o pereche de chei și o identitate. Dintre serviciile de securitate, realizate cu ajutorul semnăturilor digitale, enumerăm [11], [1]:

- **identificarea și autentificarea:** entitatea ce trebuie autentificată sau identificată semnează o provocare cu ajutorul cheii sale private; verificatorul semnăturii poate fi sigur de *identitatea* celui cu care schimbă mesaje în baza a trei condiții ce se presupun îndeplinite: 1. cheia privată este cunoscută doar proprietarului său; 2. există o singură cheie privată, care corespunde cheii publice din certificatul digital. 3. certificatul face legătura nemijlocită între identitatea proprietarului și cheia sa publică; presupunând aceste condiții îndeplinite, verificarea semnăturii digitale va duce implicit la *cunoașterea* entității ce a efectuat-o;
- **integritatea datelor:** este obținută prin verificarea cu succes a semnăturii digitale, operație ce duce la concluzia că datele nu au fost modificate ulterior procesului de semnare; semnătura digitală reprezintă un *sigiliu de protecție*, care este imposibil de realizat fără cunoașterea cheii private;
- **nerepudierea datelor:** presupunând că posesorul certificatului este singurul care cunoaște cheia privată, verificarea semnăturii realizate asupra unor date duce la concluzia că posesorul certificatului este emitentul datelor, distribuitorul acestora sau a fost de acord cu semnarea lor în forma respectivă; datorită faptului că semnătura a fost realizată cu cheia privată corespunzătoare, semnatarul nu poate repudia semnătura o dată ce aceasta a fost efectuată; ca și în cazurile precedente, și aici se presupune că este imposibilă realizarea unei semnături false asupra unor date fără a cunoaște cheia privată;
- **declarația de acord:** este realizată cu ajutorul presupunerii că semnatarul a semnat documentul fiind de acord cu conținutul semantic al documentului;

- **încunoştinţarea:** este obţinută de asemenea cu ajutorul presupunerii că semnatarul unui document a luat la cunoştinţă conţinutul semantic al datelor semnate.

3. Metode de clasificare a semnăturilor digitale

Necesitatea introducerii semnăturilor digitale a apărut o dată cu răspândirea la scară tot mai largă a documentelor în format electronic. Conceptul ce stă la baza semnăturilor digitale îl reprezintă algoritmii asimetrici (cu cheie publică). Mesajul ce trebuie semnat este prelucrat cu ajutorul unei funcţii hash, apoi rezultatul este semnat utilizând cheia privată a semnatarului; verificarea semnăturii digitale este realizată prin intermediul cheii publice. În funcţie de scopurile urmărite şi domeniile de aplicaţie, au fost create diverse tipuri de semnături digitale. Acestea pot fi clasificate, în funcţie de numărul de părţi implicate în procesul de semnare, în funcţie de algoritmii utilizaţi sau în funcţie de modul în care este transportat mesajul semnat.

Din punct de vedere al numărului de părţi implicate în procesul de semnare, întâlnim două categorii [11]:

- semnături digitale directe; părţile implicate în procesul de comunicare (sursa şi destinatarul) negociază direct, semnătura digitală fiind realizată prin criptarea întregului mesaj sau a unui rezumat (message digest) cu ajutorul cheii private a sursei; punctul sensibil al acestei abordări îl reprezintă securitatea cheii private; pe de o parte, o cheie privată compromisă poate fi utilizată pentru a genera semnături digitale false, pe de altă parte, semnatarul poate nega efectuarea unei semnături, susţinând faptul că această cheie privată a fost compromisă, şi nu el este cel care a efectuat semnătura; pentru a preîntâmpina aceste două situaţii, se poate determina momentul de timp în care a fost efectuată semnătura digitală; acest lucru este posibil prin introducerea unei ştampile electronice de timp, însă aceasta, pe lângă faptul că aduce în schemă o terţă parte, complicând mecanismul de realizare a semnăturii, nu rezolvă din păcate nici una din cele două probleme prezentate; există în continuare suspiciunea repudierii unei semnături valabile de către un semnatar nesincer, iar în caz contrar, sunt greu de stabilit condiţiile când, dacă şi în ce fel a fost compromisă cheia privată; este greu de imaginat că posesorul cheii va putea raporta compromiterea acesteia în cazul în care nu îşi va da seama când şi în ce fel i-a fost compromisă cheia;
- semnături digitale realizate cu participarea unui arbitru: acestea implică utilizarea unei terţe părţi în care atât sursa, cât şi destinatarul au încredere; arbitrul joacă rolul unui Trusted Third Party (TTP), această schemă încercând practic să rezolve deficienţele apărute la semnăturile digitale directe; mesajul este semnat de către sursă, transmis apoi arbitrului pentru verificare, acesta confirmând încă o dată destinatarului autenticitatea semnăturii; există variante în care mesajul original rămâne ascuns arbitrului şi variante în care acesta este la vedere; în ambele cazuri, poate fi utilizată atât criptografia cu chei simetrice (caz în care apar şi probleme datorate faptului că arbitrul are câte o cheie comună împreună cu fiecare dintre părţi), cât şi criptografia cu chei publice, care este de obicei preferată; deşi această schemă are avantajul de a elimina unele dintre problemele algoritmilor simetrici, lasă totuşi nerezolvată problema compromiterii cheii semnatarului; varianta cea mai sigură implică o dublă semnare/criptare cu un algoritm cu cheie publică atât din partea sursei, cât şi din partea arbitrului, ceea ce duce însă la o vizibilă încetinire a întregului proces.

O altă metodă de clasificare a semnăturilor digitale se poate realiza ţinând cont de informaţia transportată de mesajul criptat. Astfel întâlnim două clase în funcţie de informaţia necesară pentru realizarea operaţiei de verificare [11]:

- semnături digitale cu apendice: acestea necesită mesajul original ca parametru de intrare al algoritmului de verificare;
- semnături digitale cu recuperarea mesajului: nu necesită mesajul original pentru efectuarea operaţiei de verificare, acesta fiind reconstituit din semnătura propriu-zisă.

Aceste categorii de semnături pot fi subîmpărţite din punct de vedere al funcţiei de redundanţă $R : M \to M_S$, unde M este spaţiul mesajelor, iar M_S este mulţimea tuturor mesajelor semnate. Dacă funcţia de redundanţă îndeplineşte condiţia $|R| > 1$, atunci semnăturile digitale sunt considerate a fi aleatoare, în caz contrar ele sunt deterministe. Acestea din urmă se împart la rândul lor în semnături de unică folosinţă (one-time) şi în semnături cu folosinţă multiplă [13].

O altă modalitate de catalogare a semnăturilor digitale este în funcţie de domeniul de utilizare prezentată. Aici întâlnim două categorii de semnături [8]:

- semnături cu funcţionalitate clasică, acestea fiind preponderent utilizate pentru realizarea unor semnături ce prezintă caracteristicile clasice ale semnăturilor în general (de exemplu, semnături

realizate cu algoritmi precum RSA, DSA etc.);

- semnături cu funcționalitate extinsă, la această categorie putem enumera semnături ce prezintă caracteristici noi, ce conferă o funcționalitate extinsă (de exemplu, semnături de unică folosință, semnături de grup, semnături oarbe etc.).

4. Metode de atac îndreptate împotriva semnăturilor digitale

La fel ca semnăturile olografe, şi semnăturile digitale pot fi atacate în încercarea de a produce semnături false. Metodele de atac diferă, însă, în acest caz fiind interesantă aflarea unei semnături identice cu cea generată de semnatar, şi nu a unei copii asemănătoare ca la semnăturile olografe. Scopul atacatorului este de a falsifica semnăturile digitale, cu alte cuvinte, de a produce semnături ce vor fi acceptate ca fiind generate de către un alt semnatar. În funcție de gradul de compromitere, putem întâlni următoarele categorii [11]:

- compromitere totală: atacatorul reuşeşte calcularea cheii private sau găseşte o metodă viabilă de a produce semnături echivalente pentru orice mesaj;
- compromitere selectivă: atacatorul are posibilitatea de a crea semnături digitale pentru un mesaj sau pentru o clasă de mesaje particulare, fără posibilitatea de a avea acces la semnături produse de semnatarul legitim;
- compromitere existențială: atacatorul este capabil de a falsifica cel puțin o semnătură, fără a deține practic controlul, dar având acces la un număr de semnături produse de semnatarul legitim.

Toate aceste categorii de atacuri pot fi catalogate în funcție de metoda abordării. Astfel întâlnim în practică două tipuri de atacuri [11]:

- atacuri bazate doar pe cunoaşterea cheii publice, atacatorul neavând la dispoziție semnături digitale autentice;
- atacuri bazate pe mesaje semnate, în acest caz atacatorul având la dispoziție pentru analiză un număr de semnături digitale produse de semnatarul legitim; aceste tipuri de atac pot fi subîmpărțite la rândul lor în:
  - atacuri bazate pe un număr de mesaje cunoscute: se cunosc semnăturile digitale pentru o mulțime de mesaje care nu pot fi alese de către atacator;
  - atacuri bazate pe un număr de mesaje selectate: în acest caz, se pot alege o serie de mesaje pentru care se poate obține semnătura digitală, dar fără a avea posibilitatea de a analiza semnăturile pentru a adapta procesul de alegere al mesajelor;
  - atacuri pe bază de oracol: atacatorul are posibilitatea de a alege mesajele, de a obține semnăturile corespunzătoare şi de a analiza semnăturile pentru a adapta mecanismul de alegere al acestora, folosind semnatarul legitim pe post de oracol.

Acest din urmă atac este şi cel mai periculos, obținerea unui număr suficient de mare de semnături digitale putând duce la aflarea cheii private sau a unui model de generare a semnăturilor false. Trebuie remarcat faptul că, deşi acest atac este relativ dificil de realizat în practică, o schemă bună de semnături digitale trebuie să preîntâmpine şi acest tip de atac. În funcție de posibilitățile pe care le are atacatorul, schema trebuie să asigure un nivel de securitate corespunzător pentru a face cât mai dificilă falsificarea semnăturilor digitale. În situația în care atacatorul nu are posibilitatea de a realiza decât un atac cu scopul unei compromiteri selective în baza cunoaşterii cheii publice, este suficient ca schema să împiedice atacul bazat pe mesajele selective. Dacă falsificatorul are posibilitatea de a realiza un atac asupra mesajelor, atunci schema trebuie să prevină şi compromiterea existențială. În cazul în care se utilizează de exemplu o funcție hash, aceasta trebuie să fie fixată, fără a oferi posibilitatea de a înlocui o funcție puternică printr-una mai slabă şi de a realiza un atac selectiv. În general, pentru a atinge un grad ridicat de securitate, se recomandă semnarea unui hash, şi nu a mesajului. Alte exemple de atacuri îndreptate împotriva unor scheme de semnături digitale pot fi întâlnite în [3].

5. Aspecte practice ale semnăturilor digitale

Semnăturile digitale sunt utilizate, de obicei, în contextul semnării unui document sau a unor date stocate într-un anumit format (de cele mai multe ori într-un fişier). O analiză a legăturilor şi complicațiilor ce apar în cazul semnăturilor multiple sau a semnăturilor pe documente multiple poate reliefa cazurile complexe de utilizare a semnăturilor digitale. Luând în considerare cazurile tipice, se poate observa că, în funcție de aplicație, sunt necesare două tipuri de semnături: semnături independente şi contrasemnături [4].

Semnăturile independente (Figura 1) nu depind unele de altele, fiind realizate în paralel pe acelaşi document, chiar dacă acestea sunt realizate la momente diferite de timp, ele au o pondere egală deoarece cronologia în care acestea au fost realizate nu prea contează. În cazul contrasemnăturilor, ordinea realizării acestora contează, ele ținând cont nu numai de documentul original, dar şi de semnăturile deja

existente. Termenul de contrasemnătură reunește semnăturile parțiale (încorporate) și semnăturile totale. Semnăturile olografe nu prezintă această diferențiere, ea apare doar datorită stocării în format electronic.

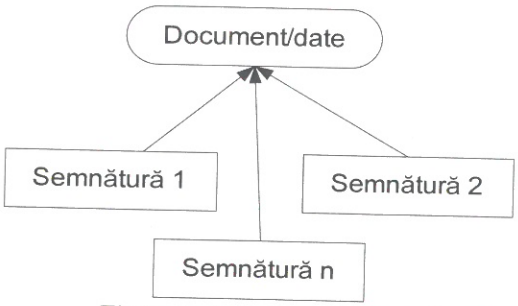

Figura 1. Semnătura independentă

În cazul semnăturilor parțiale, prima se efectuează asupra întregului document, iar fiecare din semnăturile care se adaugă se realizează asupra semnăturii precedente (Figura **2**). Spre deosebire de semnăturile parțiale, semnăturile totale se realizează întotdeauna pe întregul ansamblu existent, ce constă din documentul original plus semnăturile deja efectuate (Figura **3**). În baza acestor tipuri de semnături, se pot construi semnături oricât de complexe [4].

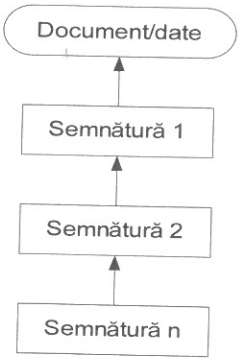

Figura 2. Semnătura parțială

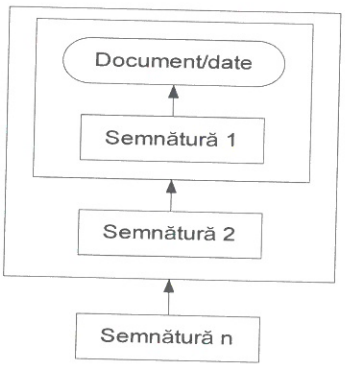

Figura 3. Semnătura totală

După realizarea semnăturii digitale apare problema stocării acesteia și a modalității cum se păstrează legătura la documentul semnat. Deși această problemă pare lipsită de importanță, lipsa de standardizare în această direcție a avut ca efect imposibilitatea de a utiliza cu succes semnăturile digitale, ducând la apariția unor soluții particulare ce nu au reușit să se impună. În practică, distingem trei categorii, în funcție de relația dintre semnătură și documentul semnat [4]:

- semnături ce încorporează datele semnate, acestea incluzând datele semnate (Figura 4);
- semnături încorporate, acestea fiind stocate în interiorul documentului (Figura 5);
- semnături detașate, ce sunt stocate separat de documentul semnat (Figura 6).

Pentru a realiza arhivarea unor semnături realizate asupra unor documente, acestea trebuie stocate împreună cu datele semnate într-un anumit format. Totodată, trebuie garantat faptul că documentul semnat nu va mai fi modificat – deziderat greu de realizat dacă luăm în considerare un exemplu practic de genul unui fișier Word: acesta este modificat ori de câte ori este deschis cu ajutorul aplicației, fiind automat transformat și formatat. Totodată, deschiderea acestuia cu o altă versiune a aplicației duce nemijlocit la adaptarea fișierului la un nou format. În ambele cazuri, rezultă o modificare a datelor, care face practic imposibilă utilizarea unei semnături digitale. Tot aici, trebuie menționată și necesitatea de a semna întotdeauna documentul în forma în care este afișat pe ecran de către aplicație, și nu cum este el stocat într-un fișier – ceea ce se numește *What You See Is What You Sign*. O altă problemă o reprezintă și necesitatea de a semna documente întregi, doar bucăți dintr-un document, sau mai multe documente dintr-o dată, în funcție de ceea ce dorește utilizatorul. Până în prezent, aceste probleme au fost prea puțin abordate de formatele de fișiere aflate în circulație, neexistând la ora actuală soluții viabile în acest sens.

În momentul de față, cele mai utilizate formate electronice pentru stocarea semnăturilor digitale cât și a documentelor semnate sunt: XMLdsig, Cryptographic Message Syntax (CMS) și Portable Document Format (PDFv1.3). Cu toate că oferă suport pentru semnăturile digitale, nici unul din aceste nu îndeplinește toate condițiile enunțate anterior. Se impune de aceea începerea unui proces de standardizare, care să ia în considerare toate cazurile prezentate, și care să aibă ca rezultat un format de fișier flexibil

care să răspundă necesităților întâlnite în practică.

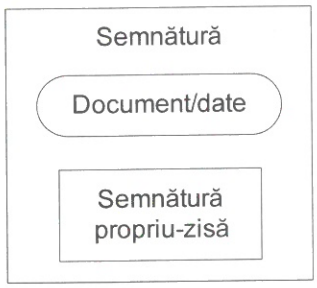

Figura 4. Semnătura ce încorporează datele semnate

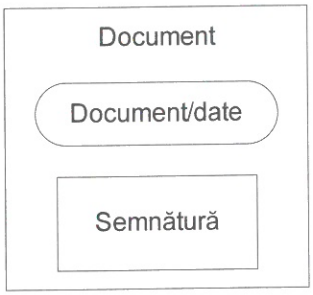

Figura 5. Semnătura încorporată în document

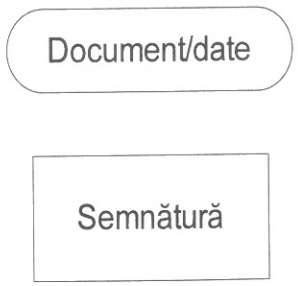

Figura 6. Semnătura detaşată de date/document

6. Concluzii

Tehnologia informației a parcurs în ultima perioadă o dezvoltare razantă, semnăturile digitale constituind un domeniu complex al acesteia. Bazele semnăturilor digitale au fost puse cu ani în urmă, dar securitatea semnăturilor digitale reprezintă în prezent obiectul unor intense cercetări științifice.

Semnăturile digitale se confruntă atât cu probleme de securitate, cât şi cu diverse probleme practice. Este necesară o analiză aprofundată a acestor probleme, pentru a găsi şi impune soluții sigure. Deşi cadrul legislativ a fost creat, acesta fiind practic primul pas în recunoaşterea semnăturilor digitale ca echivalent al semnăturilor olografe, problemele tehnologice împiedică încă în acest moment o utilizare a acestora la scară foarte largă. Problemele întâlnite în practică impun începerea unui proces de standardizare, care să aibă ca rezultat un format de fişier potrivit pentru stocarea semnăturilor digitale împreună cu datele de semnat.

Bibliografie

1. **ATREYA, M., B. HAMMOND, S. PAINE, P. STARETT, S. WU**: Digital Signatures, RSA Press, Berkley, USA, 2002.
2. **BROWN, P. W.**: Digital Signatures: Are They Legal for Electronic Commerce? IEEE Communications Magazine, vol. 32, nr. 9, 1994, pp. 76-80.
3. **HOWGRAVE-GRAHAM, N. A., N.P. SMART**: Lattice Attacks on Digital Signature Schemes, Designs, Codes and Cryptography, vol. 23, no. 3, 2001.
4. **LIOY, A., G. RAMUNNO**: Multiple Electronic Signatures on Multiple Documents, ICETE'04: Int. Conf. on E-Business and Telecommunication Networks, Setubal, Portugal, 2004, pp. 24-34.
5. **LIPMAA, H.**: Secure and Efficient Time-Stamping Systems, Dissertation, Tartu, 1999.
6. **MARINESCU, C., N. ȚĂPUȘ**: A Survey of the Problems of Time-Stamping or Why It Is Necessary to Have Another Time-Stamping Scheme, Proceedings of the IASTED Conference on Software Engineering 2007, SE2007, Austria, 2007.
7. **MARINESCU, C.**: O analiză a legislației din domeniul semnăturilor electronice şi a ştampilelor de timp, Revista Română de Informatică şi Automatică, vol. 17, nr. 4, 2007.
8. **MARINESCU, C.**: Semnarea electronică a datelor, Teză de doctorat, Facultatea de Automatică şi Calculatoare, Universitatea Politehnica Bucureşti, România, 2008.
9. **MAURER, U.**: Intrinsic Limitations of Digital Signatures and How to Cope With Them, Lecture Notes in Computer Science, vol. 2851, Proceedings of 6th International Conference on Information Security – ISC'03, Springer-Verlag, 2003, pp. 180-192.
10. **MENEZES, A., P. VAN OORSCHOT, S. VANSTONE**: Handbook of Applied Cryptography, CRC Press, 1996.
11. **MITCHELL, J., F. PIPER, P. WILD**: Digital Signatures, in Contemporary Cryptology, IEEE Press, NY, USA, 1992.
12. **SCHNEIER, B.**: Applied Cryptography – Protocols, Algorithms and Source Code in C, John Wiley & Sons, 1996.
13. **STINSON, D. R.**: Cryptography. Theory and Practice, Chapman & Hall/CRC, 2002.