Semnatura digitala vs. Biometrie

Prep. Giani GRADINARU
Catedra Analiza Statistica si Evaluare, A.S.E. Bucuresti

Internetul este vulnerabil la atacuri care ar putea compromite serios integritatea tranzactiilor comerciale sau financiare si violarea corespondentei electronice. Semnatura digitala nu ne poate oferi siguranta deplina atunci când apelam la o retea de calculatoare pentru a comunica, lucra si interactiona. Se pare ca biometria în interactiune cu tehnologia informatiei ar putea oferi cele mai sigure modalitati de identificare electronica. Articolul trateaza avantajele si dezavantajele semnaturii digitale, precum si principalele elemente pe care le ofera biometria în acest sens.
***Cuvinte cheie**: biometrie[1], scaner, digital, electronic, securizare, identificare.*

Lumea în care traim experimenteaza o schimbare profunda de ansamblu, în urma aplicarii în practica a rezultatelor eforturilor de cercetare-dezvoltare depuse în diverse colturi ale lumii. Tehnologiile avansate usureaza munca oamenilor, le modifica modul de a petrece timpul liber si le faciliteaza contactele. Cresterea numarului de utilizatori ai Internetului conduce la crearea unei comunitati internationale, distrugând barierele impuse de spatiu.

Internetul a fost creat ca un mediu deschis. Punctul sau forte, protocolul de comunicatie TCP/IP, reprezinta cea mai mare slabiciune a lui. Prin urmare, Internetul este vulnerabil la atacuri care ar putea compromite serios integritatea tranzactiilor comerciale sau financiare sau chiar violarea corespondentei electronice. Aceste atacuri ar putea consta în:

- spionarea traficului pe anumite site-uri;
- spargerea unor parole;
- modificarea unor baze de date;
- trecerea drept o alta persoana ;
- negarea participarii la o tranzactie dupa ce aceasta a fost deja încheiata.

Folosirea metodelor electronice de efectuare si înregistrare a tranzactiilor financiare si comerciale capata, în ultima vreme, o amploare deosebita. Majoritatea statelor au gasit domenii în care comertul electronic devine din ce în ce mai eficient, concomitent cu cresterea beneficiilor pentru consumatori.

Într-o tranzactie comerciala pe Internet, vânzatorii si cumparatorii doresc sa stie urmatoarele:

- Cine este celalalt – sunt ambele parti autentice? Pot fi verificate identitatile lor?
- Tranzactia va fi înregistrata în asa fel încât nici una din parti sa nu poata pretinde ca ea nu a avut loc?
- Informatiile cu valoare financiara sau personala ce au fost schimbate sunt la adapost de orice alte priviri indiscrete?

În mediul comercial actual, stabilirea cadrului pentru autenticitatea informatiei cere familiarizarea cu concepte atât din aria legalitatii, cât si din cea a securizarii retelelor. Din punctul de vedere al securizarii informatiei, semnatura digitala reprezinta rezultatul aplicarii unor procese tehnice specifice. Din punct de vedere legal, semnatura capata valente sporite. Sa trecem în revista câteva dintre atributele semnaturii.

- *Autenticitatea semnatarului* – o semnatura trebuie sa indice cine este cel ce semneaza documentul, mesajul sau înre-

[1] Vezi articolul *"Internetul, instrument de eficientizare a mixului de marketing"*, autori Dana Colibaba, Giani Gradinaru, aparut în Revista de Informatica Economica, nr. 3/2000.

gistrarea si trebuie sa fie dificil de reprodus de o alta persoana neautorizata.

- *Autenticitatea documentului* – documentul poarta amprenta celui ce îl semneaza. Autenticitatea semnatarului si a documentului sunt instrumente folosite pentru excluderea impostorilor si sunt elemente esentiale a ceea ce, în terminologia securizarii informatiei, este numita nonrecunoastere. Nonrecunoasterea furnizeaza siguranta originii si transportului datelor si protejeaza expeditorul împotriva refuzului de receptare a datelor si destinatarul împotriva receptarii unor date false pe care expeditorul, de fapt, nu le-a trimis.
- *Act de confirmare* – lasarea semnaturii trebuie sa fie un act de confirmare care sa serveasca protocolului, sa fie o aprobare ca tranzactia se realizeaza în termeni legali.
- *Eficienta* - semnatura trebiue sa reprezinte cea mai mare asigurare atât a autenticitatii semnatarului cât si a autenticitatii do-cumentului.

Tehnicile de codificare reprezinta cheia siguran-tei comertului electronic. Ele asigura atât autenticitatea, cât si transmiterea securizata a informatiei între parteneri. Codificarea se bazeaza pe un algoritm matematic care transforma datele într-o secventa aparent fara înteles pentru oricine, în afara des-tinatarului precis al mesajului, care detine cheia decodificarii sale. Pentru a asigura au-tenticitatea, partile ce folosesc comertul electronic pot apela la serviciile unei **Terte Parti de Încredere** (TPI). Aceasta va genera si distribui niste elemente de identificare, asa cum bancile folosesc numarul de identificare personal (PIN) pentru a verifica cartile de credit.

În continuare ne propunem sa analizam câteva aspecte ale semnaturii digitale, apoi, ca un contraargument la acestea, sa descoperim ce ne poate oferi biometria în domeniul securizarii fluxurilor de informatii.

Semnatura digitala înmagazineaza o cheie particulara unica de identificare a expeditorului la mesajul corect. Oricine detine o cheie publica de utilizare poate verifica inte-gritatea semnaturii. Deoarece semnatura foloseste textul original ca o intrare în algoritm, orice abatere a procesului de codificare-decodificare duce la imposibilitatea recunoasterii semnaturii, aratând ca mesajul a fost alterat în tranzit sau ca semnatura a fost falsificata prin copierea ei de la un alt mesaj. O semnatura digitala copiata de pe un alt mesaj are o sansa foarte mica de a-si transfera cu succes autenticitatea. Totusi, semnatura digitala, ca instrument de iden-tificare are limitele ei. De exemplu, daca o persoana **A** foloseste cheia sa privata de semnare a mesajului, o alta persoana **B** poate verifica daca într-adevar persoana A a trimis acel mesaj numai daca cunoaste cheia publica a persoanei **A**. Pentru a fi sigura de autenticitatea cheii publice, persoana **B** are nevoie de serviciile unei **Terte Persoane de Încredere**, deoarece, în caz contrar, poate interveni un intrus care, folosindu-se de cheia publica a persoanei **A** sa trimita persoanei **B** un mesaj în numele primei persoane. Cât timp intrusul detine o cheie privata corespunzatoare cheii publice, el poate trimite mesaje persoanei **B** iar verificarea pe care persoana **B** o face asupra semnaturii de pe mesajul falsificat va duce la confirmarea autenticitatii mesajului, chiar daca, de fapt, acesta nu provine de la persoana **A**. În schimb, daca persoana **B** are acces la cheia publica reala a persoanei **A** printr-o **Terta Persoana de Încredere** si o foloseste pentru verificarea mesajului expediat de intrus, ve-rificarea va esua dovedind falsul.

Utilizarea semnaturii digitale implica, în mod curent doua procese, unul care-l priveste pe semnatar si altul pe cel ce primeste mesajul.

- **Crearea semnaturii digitale** utilizeaza rezultatul descompus al combinatiei unice dintre continutul semnaturii si cheia privata.

Din cele relatate constatam ca semnatura digiatala nu ne poate oferi siguranta deplina atunci când apelam la o retea de calculatoare pentru a comunica, lucra si interactiona. Studiile si cercetarile din ultima vreme lanseaza tot mai mult pro-

vocarea biometriei ca o oportunitate la securizarea informatiilor.
Biometria ofera alternativa identificarii la o retea prin masurile corpului uman, iar aceast mod de identificare are avantajul ca, atributele trupului nu pot fi uitate, pierdute sau transferate în mod facil de la o persoana la alta si, mai mult, sunt foarte greu de falsificat.

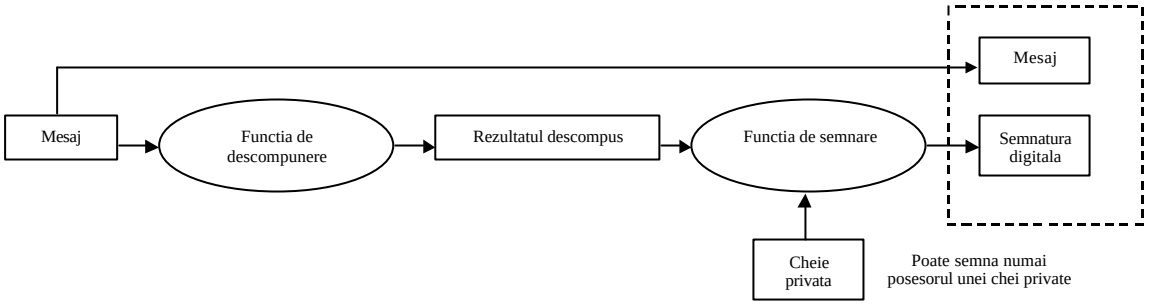

Fig. 1 - Crearea semnaturii digitale

Sursa: adaptare dupa Ghidul semnaturii electronice, Infrastructura legala a autoritatilor de certificare si securizarea comertului electronic, Information Security Committee Electronic Commerce and Information Technology Division Section of Science and Technology American Bar Association

- **Verificarea semnaturii digitale** este procesul de potrivire a semnaturii digitale pe baza referintelor privind continutul original si a cheii publice, în felul acesta determinându-se daca semnatura digitala a fost creata de detinatorul cheii private care sa corespunda referintelor cheii publice (figura 2).

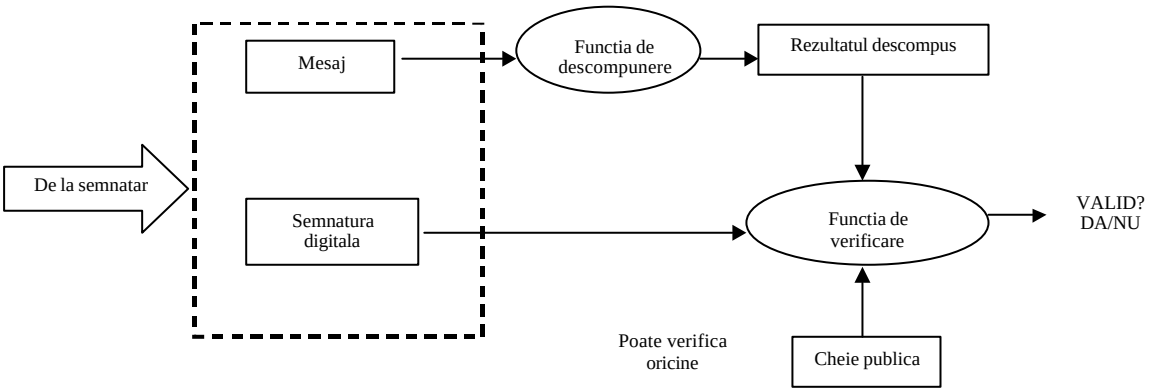

Fig. 2 - Verificarea semnaturii digitale

Sursa: adaptare dupa Ghidul semnaturii electronice, Infrastructura legala a autoritatilor de certificare si securizarea comertului electronic, Information Security Committee Electronic Commerce and Information Technology Division Section of Science and Technology American Bar Association.

Biometria ofera mai multe modalitati de folosire a elementelor ei. Se spune ca ideea dateaza de la vechii egipteni, când înregistrarile trasaturilor distinctive si masurile trupului erau folosite pentru a se asigura ca oamenii erau cei ce se pretindeau a fi. Calculatoarele moderne, bazate pe sisteme biometrice, sunt folosite pentru doua functii de baza. O functie de identificare a persoanei, prin care identificarea subiec-

tului se realizeaza prin compararea masurilor biometrice cu cele înregistrate în baza de date printr-o relatie de tipul "unu la mai multi". A doua functie este cea de verificare – este persoana respectiva cea ce se pretinde a fi? – verificare ce se realizeaza printr-o relatie de tipul "unu la unu".
Amprentele sunt cel mai des folosite ca ele-mente biometrice. Sistemele electronice moderne transforma caracteristicile conventionale ale amprentelor în coduri numerice. Acestea sunt corelate, cu un extraordinar grad de acuratete, cu informatiile înmagazinate în baza de date. Din cauza deselor apelari la help-urile de reamintire a parolelor, companiile tehnologice promoveaza folosirea pe scara cât mai larga a amprentelor ca modalitate de conectare la retelele de calculatoare. În plus, prin folosirea amprentelor, ca element de identificare, se elimina frauda electronica.
Un alt mijloc biometric, cu o popularitate în continua crestere, este geometria mâinii. Identificarea prin geometria mâinii implica scanarea formei, marimii unei parti, a întregii mâini sau a anumitor caracteristici (lungimea degetului). Sistemul de geometrie a mâinii este deja folosit la controlul accesului si verificarea identitatii la unele aeroporturi, birouri, fabrici, scoli, spitale, centrale nucleare si cladiri guvernamentale. El se foloseste si în sistemele de pontaj pentru a se evita frauda provocata de card-urile de intrare/iesire din unitate, card-uri ce puteau fi introduse si de alti colegi.
Alt mijloc biometric este sistemul de scanare a ochilor. Scanarea fibrelor, ridurilor, petelor de pe iris folosind o camera video ofera suficiente informatii pentru identificarea oricui. Desi tehnologia este privita ca fiind cea mai verosimila biomasurare, ea este totusi destul de costisitoare. Scanerele de iris au fost testate deja de bancile din Marea Britanie, Japonia si SUA ca un mod de identifica utilizatorii bancomatelor.
Un alt mijloc de masurare biologica este recunoasterea faciala, tehnologie care a câstigat teren, în ultima vreme, ca urmare a scaderii preturilor calculatoarelor. Sistemul functioneaza analizând o imagine video sau o fotografie si identificând pozitiile câtorva puncte nodale pe fata persoanei. Acestea, mai ales cele dintre frunte si buza de sus sunt neafectate de expresie sau par facial.
Recunoasterea faciala este utilizata, în special, pentru verificarea identitatii. Recunoasterea faciala, fata de alte mijloace de ma-surare biometrica, poate opera "pasiv", fara ca oamenii sa realizeze ca sunt scanati. Ea poate ajuta la prinderea teroristilor din aeroporturi, la arestarea huliganilor microbisti sau a trisorilor din cazinouri.
O alta forma de masurare biologica, care nu necesita un echipament costisitor este recunoasterea vocii, sistem care functioneaza prin analiza caracteristicilor fundamentale ale vocii. Desi aceasta tehnologie este ieftina, ea este mai putin valabila în cazurile în care se dispune de doar cateva secunde de convorbire înregistrata. Cota de piata a acestui mod de recunoastere a scazut în ultimul timp în favoarea recunoasterii faciale.
O semnatura de mâna poate fi, de asemenea, un mijloc de masurare biometrica. Creionul electronic devine din ce în ce mai popular iar abilitatile hardware de capturare a semnaturii se fac din ce în ce mai vizibile.
Exista o multime de alte tehnologii de masurare biologica, cum sunt: recunoasterea mirosului trupului, temperatura faciala si rezonanta acustica a capului. Bineînteles ca fiecare are propriile ei avantaje, dar sunt fie prea scumpe fie impracticabile si nu se comercializeaza.
Biometria va creste sigur în importanta atât pentru guverne cât si pentru companii. Adoptarea la scara larga într-un interval de timp scurt nu este probabila. Consumatorii vor avea retineri în a adopta tehnologia daca vor trebui sa plateasca în plus pentru ea iar beneficiile nu vor fi pe masura.
Deja calculatoarele au devenit parte integranta a vietii noastre de zi cu zi iar majoritatea tranzactiilor, de la semnarea contrac-telor pâna la efectuarea cumpara-

turilor si la completarea formularelor pentru recuperarea taxelor se realizeza digital, astfel încât se creeaza cadrul propice pentru ca firmele de biometrie sa spere ca produsele lor vor fi curând omniprezente si indispensabile.

Bibliografie

1. "The Economist" - colectia 2000
2. www.port4.com
3. www.abanet.org
4. www.nese.dni.us
5. www.ilpf.org
6. www.webcom.com/legaled/ETAForum