

Semnături digitale în sistemele de plăti din comerțul electronic

Prof.dr.Victor-Valeriu PATRICIU,
Catedra de Calculatoare, Academia Tehnică Militară, București

Lucrarea analizează câteva din aplicațiile criptografiei computaționale în dimensiul comerțului electronic. Este evidențiat suportul hard și soft pentru sistemele electronice de plăti și se prezintă variante practice de folosire a paradigmelor semnăturii digitale în autentificarea tranzacțiilor financiare bazate pe cartele inteligente.

Cuvinte cheie: sisteme electronice de plăti, banii electronici, cartelă inteligeantă (smartcard), semnătură digitală, sisteme cu chei secrete, sisteme cu chei publice, criptografie computațională.

1. Introducere

Comerțul electronic tradițional se referă la utilizarea în rețele cu valoare adăugată a unor aplicații de tipul transferului electronic de documente(EDI), comunicații fax, coduri de bare, transferul de fișiere și poștă electronică. Extraordinara dezvoltare a interconectivității calculatoarelor în Internet, în toate segmentele societății, a condus la o tendință tot mai evidentă a companiilor de a folosi aceste rețele în aria unui nou tip de comerț, *comerțul electronic în Internet*, care să apeleze, pe lângă vechile servicii amintite și la altele noi, cum ar fi cele create în jurul lui World-Wide Web, companii și holdinguri virtuale sau o piață a învățământului pe Internet. Însă acest nou tip de comerț a stimulat cererea pentru noi metode adecvate de plată. În cadrul noului concept denumit sugestiv “*satul global*” (*Global Village*), dezvoltarea unor activități comerciale între participanți situati la mari distanțe geografice unii de alții nu poate fi concepută fără folosirea unor *sisteme electronice de plăti (EPS-Electronic Payment Systems)*. Aceste noi mijloace de plată permit transferarea comodă, sigură și foarte rapidă a banilor între partenerii de afaceri. De asemenea înlătuirea monedelor

și bancnotelor, actualele forme tradiționale de numerar, prin ceea ce denumim *bani electronici*, conduce, pe lângă reducerea costurilor de emisie și menținere în circulație a numerarului și la o sporire a flexibilității și securității sistemelor de plăti.

2. Banii în comerțul electronic

Sistemele electronice de plăti trebuie să atingă nivele foarte ridicate de securitate, viteză, caracter privat și confidențial, descentralizare și internaționalizare și să fie unanim acceptate atât de consumatori cât și de comercianți sau afaceriști. Vom analiza 3 astfel de *metode de plată electronică*: transferul electronic de fonduri (EFT-Electronic Fund Transfer), banii electronici (digi cash) și tehnologia numită Ecash.

- **Transferul electronic de fonduri**

Sistemele de cecuri electronice au fost folosite încă din anii '80; ele utilizează structura de bănci existente și elimină cecurile de hârtie. Transferul electronic de fonduri folosește sisteme de cecuri electronice, prezentând

o serie de avantaje în raport cu cecurile de hârtie:

- timpul foarte rapid de efectuare a plășilor;
- reducerea costurilor privind hârtia folosită;
- confirmarea instantanee a solvabilitășii plășitorului;
- flexibilitatea și marea varietate de implementare, de la tranzacșii mici folosind retelele de automate de bani (ATM - Automatic Teller Machine) la marile retele internașionale de clearing, cum ar fi CHIPS (Clearing House Interbank Payments System), format din peste 120 de bănci din întreaga lume. De exemplu, CHIPS efectuează zilnic în jur de 200.000 de tranzacșii cu o valoare însumată de 1,2 miliarde dolari SUA.

O slăbiciune evidentă a acestui sistem de cecuri electronice o constituie caracterul privat și confidenșialitatea plășilor. În plus, băncile sunt obligate, prin reglementările în vigoare, să poată documenta în detaliu fiecare transfer.

• Banii electronici

Banii electronici (numiști și *digi cash*) reprezintă echivalentul electronic al banilor reali. Ei prezintă câteva caracteristici esenșiale:

- anonimitatea plășilor, ceea ce conduce la imposibilitatea identificării cumpăraștorului;
- lichiditatea, ceea ce presupune că acești bani electronici sunt unanimi acceptaști de către toate firmele comerciale care sunt conectate la Internet;
- superioritatea în raport cu banii reali, care sunt costisitor de fabricat și de întreținut; de asemenea securitatea și imposibilitatea falsificării sau pierderii sunt alte atuuri ale banilor electronici.

Banii electronici pot lua diferite forme cum ar fi:

-Cartele. care permit de la plășile cele mai simple ale convorbirilor telefonice, până la plășile oricărora cumpărașturi într-un magazin. Aceste cartele au evoluat către ceea ce numim acum *smartcard-*

uri, cu facilităști multiple de plată (cum ar fi cunoscutul MasterCard) realizate după standardul convenit de consorșiu EMV (Europay, Master Card și Visa) și bazate pe protocoale criptografice puternice cu chei publice.

-Sisteme electronice pure, utilizabile în tranzacșii Internet, unde cumpăraștorul și vânzătorul sunt 2 calculatoare fizice interconectate prin reteea. Transmiterea banilor electronici de la cumpăraștor la vânzător este protejată prin cifrare atât cu criptosisteme convenișionale cât și cu chei publice.

• Ecash

Tehnologia Ecash reprezintă un exemplu de sistem electronic de plăști, care folosește poșta electronică. Ea a fost dezvoltată în Olanda, de către DigiCash Co. din Amsterdam, fiind implementată de către bănci din SUA (Mark Twain Bank of Missouri) și din Finlanda. Este prima solușie totalmente software pentru plășile electronice.

Tranzacșii se desfășoară între cumpăraștor și vânzător care trebuie să aibă conturi la aceiași bancă. Cumpăraștorii trebuie să înștițeze banca că doresc să transfere bani din conturile lor obișnuite în așa numitul cont Ecash Mint. În orice moment, cumpăraștorul poate interacșiona de la distanșă, prin calculatorul său și folosind un client software, cu contul Mint și poate retrage fonduri de aici pe hard-discul calculatorului său. Formatul acestor fonduri este electronic, suite de zero și unu, protejate criptografic. Ca urmare hard-discul cumpăraștorului devine un veritabil "portofel electronic". Apoi se pot executa plăști între persoane individuale sau către firme, prin intermediul acestor Ecash.

Ecash are un caracter privat: deși banca ține o evidenșă a fiecărei retrag-

geri Ecash și a fiecărui depozit Mint, este imposibil ca banca să stabilească utilizarea ulterioară a Ecash. Această proprietate se datorează folosirii unor criptosisteme cu chei publice RSA, cu o lungime a cheii de 768 biți. Pe lângă anonimitatea plășilor, Ecash asigură și nerepudierea, adică acea proprietate care permite rezolvarea neambiguă a oricărora dispute între cumpărător și vânzător privind recunoașterea plășilor. De asemenea, prin verificare în baza de date a băncii, este împiedicată orice dublă cheltuire a Ecash.

În sinteză, un **sistem electronic de plăști** poate fi definit ca ansamblul de tranzacții cerute de :

- conversia banilor numerar (cash sau din cont) în bani electronici și invers;
- transferul banilor electronici între utilizatorii care folosesc sistemul.

3. Dispozitive utilizate în sistemele electronice de plăști

Interacțiunea reală (fizică) într-un sistem electronic de plăști constă în tranzacții care se desfășoară între anumite **dispozitive** care implementează entitășile impliate în sistem.

(1) **Portofelul electronic (Electronic Wallet)** este cel care implementează purtătorul de bani electronici. El este folosit de către cumpărător pentru stocarea de bani electronici. Structura sa hardware este dependentă de protocolele criptografice care implementează tranzacții EPS, fiind mai frecvente următoarele configurașii fundamentale:

- Structură de tip Personal Computer, în care utilizatorul are acces complet la resursele hard și soft ale dispozitivului. Arhitectura, tipică pentru un PC cu resurse limitate de tip **calculator de buzunar (hand-held computer)**, cuprinde: unitate centrală în jurul unui microprocesor pe 8 biți, memorie RAM între 256 bytes și 2 kbytes, 8-10 kbytes EPROM, 2-10 kbytes EEPROM, dintre care zona care conține cheile secrete ale dispozitivului trebuie să aibă restricșii de acces.

Interfașa cu utilizatorul este formată dintr-o tastatură și un display. Conectarea la punctele de acces ale EPS se face de obicei printr-o legătură serială în infraroșu. Acest tip de structură dezavantajează băncile, neliniștite de controlul total al utilizatorului asupra resurselor dispozitivului de plată.

- Structură de tip sensibilă la deschidere (temper-proof resistant), numită **cartelă inteligentă (smart-card)**. Aceasta se prezintă sub forma unui chip incorporat într-o cartelă de plastic și cuprinde: un microprocesor de 8 biți, memorie RAM de 256 bytes, 8 kbytes EPROM; 8 kbytes EEPROM. Comunicașia cu punctul de acces se face prin contact direct cu cititorul de cartelă. Utilizatorul nu are acces la resursele hard și soft, fapt ce avantajează băncile. Securitatea unor astfel de dispozitive se bazează pe presupunerile criptografice făcute asupra protocolelor precum și pe imposibilitatea deschiderii smartcard-ului și a efectuării unui "reverse-engineering" asupra software-ului său.

- **Structură de tip portofel electronic cu observator (electronic wallet with guardian)** care cumulează avantajele structurilor anterioare, ajungând la un compromis între interesele băncii și ale posesorului. Arhitectura dispozitivului cuprinde 2 microcalculatoare care comunică pe timpul desfășurării tranzacșii. Primul microcalculator, al utilizatorului, numit și portmoneu, are sarcina să comunice cu punctul de acces al EPS. El este de fapt de forma unui calculator de buzunar cu tastatură și display. Cel de-al doilea microcalculator, numit și observator sau prin abuz de limbaj smartcard, servește interesele băncii. El este introdus în interiorul primului calculator. În timp ce calculatorul utilizatorului permite să se controleze corectitudinea trans-

zactiilor, calculatorul observator previne dubla cheltuire a banilor electronici, avizând fiecare tranzacție făcută de primul calculator.

(2) *Punctul de vânzare(POS-Point of Sale)* implementează *registratorul de casă*, care reprezintă acea entitate care stochează temporar la vânzător bani electronici. Dispozitivul este realizat din punct de vedere tehnic ca o structură de tip PC, având ca interfețe atât o legătură serială în infraroșu cât și un cititor de smartcard.

(3) *Distribuitorul de bani electronici (Electronic Money Dispenser)* este dispozitivul prin care se încarcă bani electronici în portofelul electronic al cumpărătorilor. Dintre soluțiile tehnice folosite pentru implementarea sa amintim:

- *Distribuitor cont-bani electronici*, soluție care permite incrementarea valoării din portofel pe baza retragerii unei sume de bani reali din contul deschis de cumpărător. Distribuitorul este prevăzut cu o legătură serială în infraroșu sau pentru cititor de smartcard. Distribuitorul este conectat în rețea cu calculatoare care deservesc diferite bănci emitente de bani electronici.

- *Distribuitor carte de credit-bani electronici*, soluție care permite incrementarea valorii din portofel pe baza creditării cumpărătorului de către o casă de credit. Distribuitorul este prevăzut cu un dispozitiv de citire în care se introduc cartelele de credit (magnetice) ale cumpărătorilor. De asemenea mai există un canal infraroșu și de smartcard pentru conectarea portofelului. În acest caz distribuitorul nu trebuie să fie conectat în rețea cu calculatoarele băncilor.

- *Distribuitor numerar-bani electronici*, soluție care permite incrementarea valorii portofelului pe baza colectării de la cumpărător a unei sume cash.

4. Conceptul de semnătură digitală

Semnătura digitală reprezintă un mijloc de autentificare atât a emițătorului cât și a mesajului propriu-zis. Printre numeroasele ei aplicații, semnătura digitală stă și la baza securității cartelor inteligente. Spre deosebire de semnătura olografă, care identifică doar emițătorul, semnătura digitală furnizează și mijloace de asigurare asupra integrității conținutului mesajului electronic recepționat. Semnătura digitală reprezintă o mică cantitate de date memorate pe mediul electronic și care se transmite odată cu mesajul. Ea este produsă prin anumite calcule făcute de către emițător, pe baza unei chei și a conținutului mesajului. Acest proces se numește *funcția de semnare*. La recepție, printr-o *funcție de verificare*, se face un alt set de calcule asură semnături și mesajului, constatăndu-se sau nu valabilitatea semnăturii.

Există în aceste calcule niște parametri -numiți *chei*- care diferă de la o semnătură la alta și care sunt specifici celui care produce semnătura.

Producerea semnăturilor digitale se poate baza atât pe criptosisteme simetrice cât și pe cele cu chei publice.

- *Metodele de semnătură digitală cu sisteme cu chei secrete (simetrice)* folosesc aceeași cheie atât la semnare cât și la verificare. Figura 1 ilustrează acest proces. În cadrul funcției de semnare, mesajul M este cifrat folosind cheia secretă drept parametru. La verificare, folosind aceeași cheie secretă și mesajul în clar, se dă verdictul de valid sau invalid asupra semnături digitale recepționate. Dezavantajul acestei metode constă în necesitatea stabilirii și distribuției prealabile a cheii secrete între emițător și receptor.

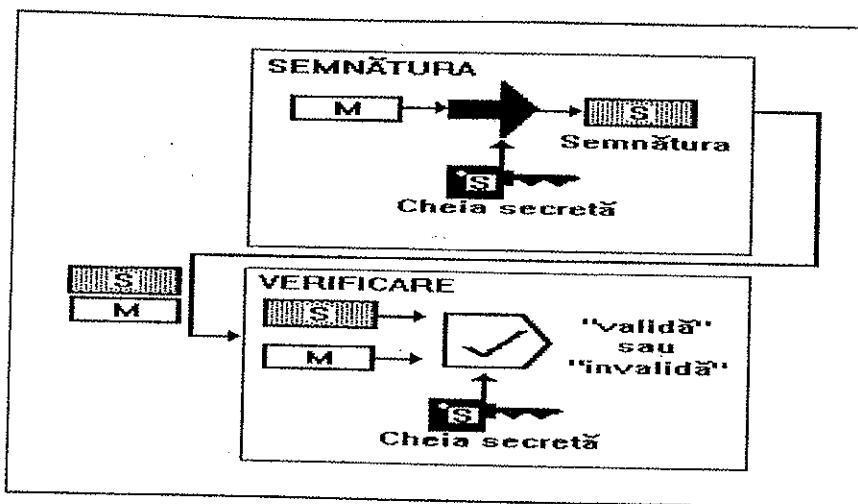


Figura 1 Semnătură digitală cu sisteme simetrice

- *Metodele de semnătură digitală cu chei publice (asimetrice)*, ilustrate în figura 2, folosesc la semnare cheia secretă a emițătorului iar la verificare cheia publică a acestuia. Ca urmare, o semnătură poate fi produsă doar de

către emițătorul autentic, singurul care cunoaște cheia secretă, dar poate fi verificată de orice persoană care cunoaște cheia publică a emițătorului.

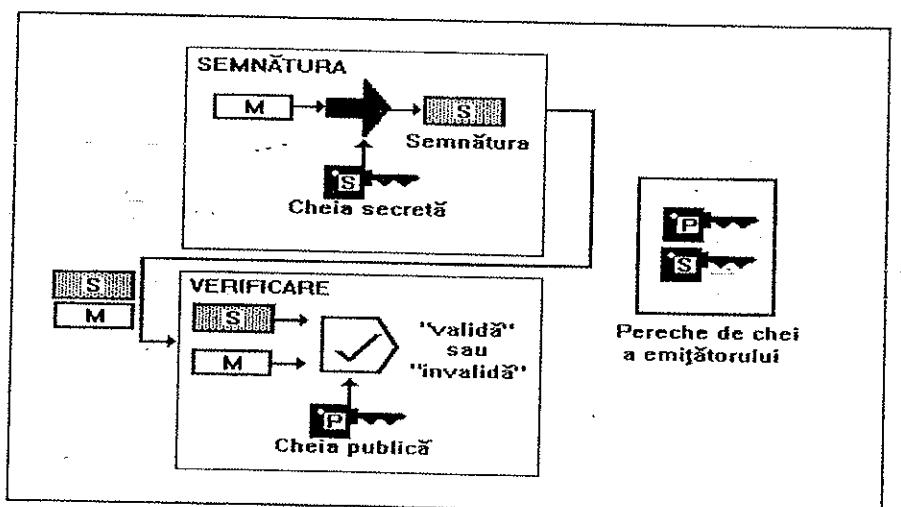


Figura 2 Semnătură digitală cu chei publice

5. Producerea semnăturilor digitale la cartele inteligente

În cazul *sistemelor de plăti electronice*, semnăturile digitale sunt realizate după o procedură puțin diferită. În primul rând, dacă s-ar folosi sistem criptografic simetric, ar exista un risc al desconspirării cheii secrete de verificare care este memorată în echipamentul vânzătorului. De aceea, acest echipament trebuie protejat cu un modul de protecție a cheii, care să poată fi controlat doar de

către furnizorul echipamentului. Se preferă sistemele cu chei publice, care trebuie să memoreze la terminal doar cheia publică. Însă aceste sisteme creează probleme în EPS, deoarece cer un volum de calcule destul de mare, care se fac lent pe un dispozitiv cu putere de calcul redusă, cum este cartela intelligentă. În plus, cartela intelligentă expune riscului desconspirării cheii secrete pe care o are memorată.

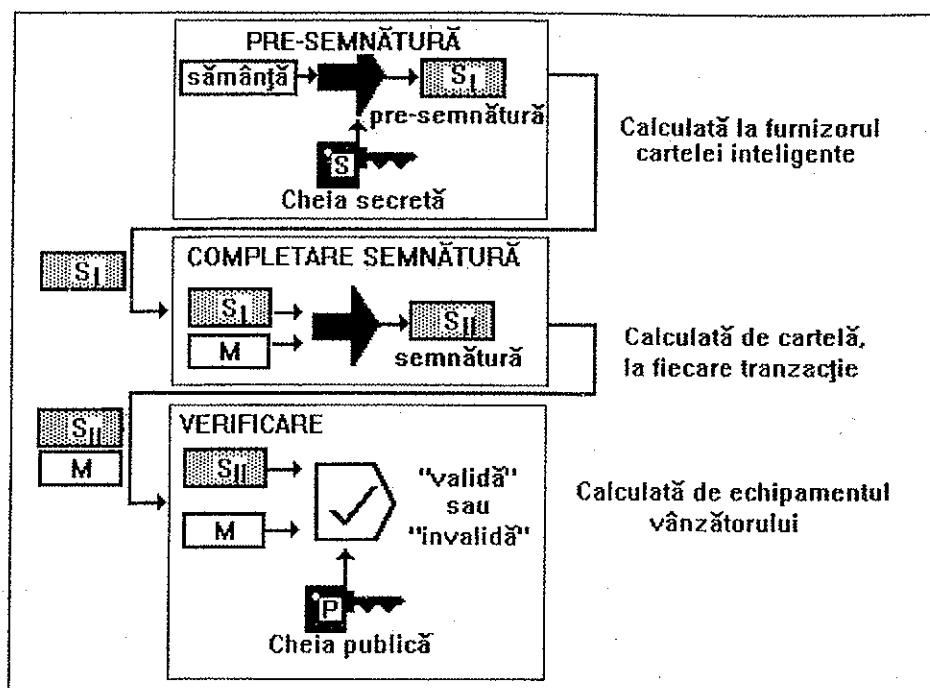


Figura 3 Semnătură digitală prin conceptul de transport al semnăturii

De aceea, *funcția de semnare* - numită aici *transportul semnăturii* - este împărțită în 2 subfaze (vezi figura 3):

-prima -*presemnătura*, partea intensivă a creării semnăturii, are loc o singură dată, în afara cartelei inteligente; rezultatul acestei faze, specific pentru cartelă și proprietarul ei, este *transportat* apoi și memorat în cartela intelligentă;

-a doua -*completarea semnăturii*, care cere resurse modeste, se face în cartela intelligentă și este dependentă de mesajul semnat.

Verificarea semnăturii se face în mod obișnuit, într-o singură fază.

6. Utilizarea semnăturilor digitale la cartelele inteligente

Folosirea conceptului de *transport al semnăturii* în cazul EPS este explicată în figura 4. Furnizorul cartelei inteligente, de obicei banca, crează pre-semnătura specifică unei persoane, printr-un proces off-line.

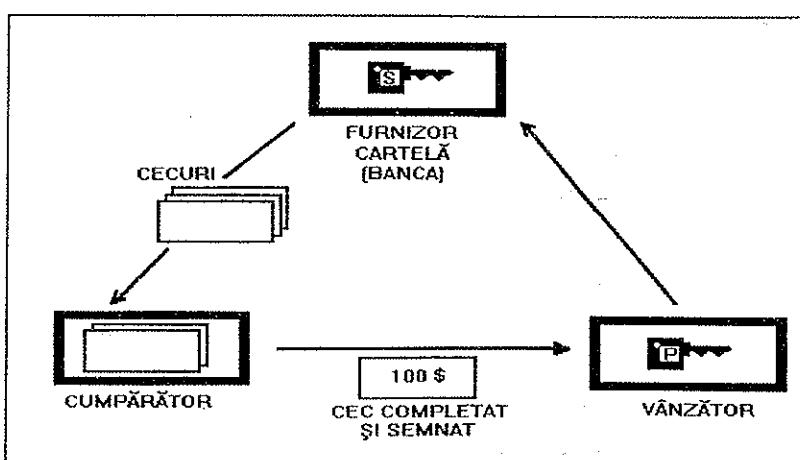


Figura 4 Utilizarea conceptul de transport al semnăturii cu chei publice la cecuri

Este ca și când banca ar da persoanei niște *cecuri electronice în alb*. Pentru crearea lor, banca folosește cheia sa secretă și apoi le memorează pe cartelă.

În timpul unei tranzacții de plată, cartela transformă cecul într-unul completat cu valoarea plății. Apoi vânzătorul, la terminalul său, verifică

semnătura cecului cu cheia publică a băncii, cheie care este memorată pe terminalul.

Firma DigiCash a dezvoltat o tehnică de compactare prin care se pot memora în memoria nevolatilă a cartelei (1K EEPROM) sute sau chiar mii de cecuri. O altă variantă de folosire a sistemelor cu chei publice în cartelele inteligente, preconizată pentru viitorul imediat, este bazată pe conceptului de *transport de monedă* (figura 5). În cadrul cartelei există un *contor balanță*, care poate fi incrementat de către bancă. Atunci când

cumpărătorul face o plată pe baza cartelei, va semna suma (monedele) cu cheia secretă existentă pe cartelă. Deoarece cartela deține 2 informații sensitive, valoarea balanței și cheia secretă, ea trebuie să fie rezistentă la deschidere. Vânzătorul, prin terminalul existent în magazin, va verifica autenticitatea monedelor, folosind cheia publică. Mai sigure, sistemele de plăti bazate pe transportul de monedă electronică au un mare viitor.

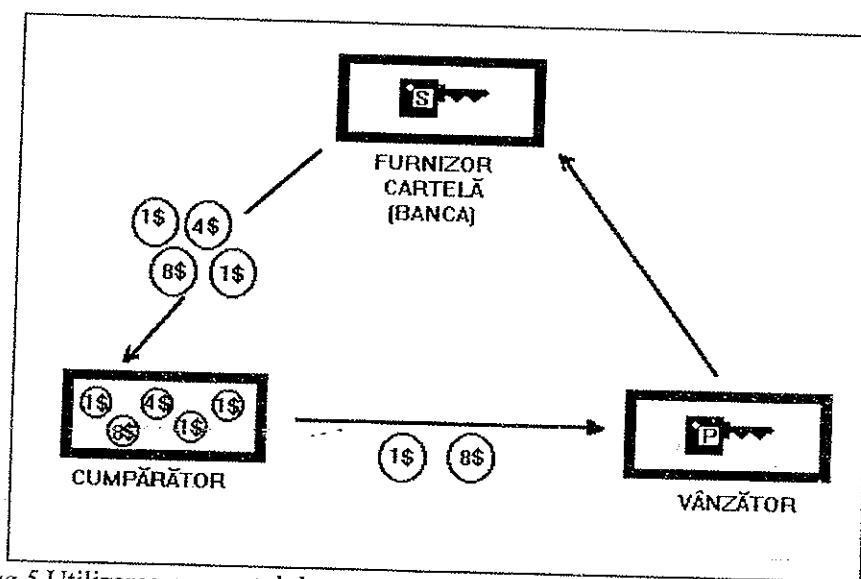


Figura 5 Utilizarea conceptului de transport al semnăturii cu chei publice la monede

În concluzie, am prezentat doar o singură aplicație a criptografiei computaționale în asigurarea securității sistemelor de plăti electronice: *semnătura digitală*. Alte utilizări privesc confidențialitatea, integritatea și autentificarea fișierelor, documentelor, poștei electronice, transmisiilor fax sau a aplicațiilor EDI.

Bibliografie

1. Cheswick William, Bellovin Steven, "Firewalls and Internet Security", Addison Wesley Professional Computing Series, 1994;
2. Denning D.E., "Encryption Policy and Market Trends", RSA Data Security Conference, 1997;
3. Farrow Rik - "UNIX System Security", Addison Wesley, 1991;
4. Garfinkel S., Spafford G., "Practical

UNIX & Internet Security", O'Reilly & Associates, 1996;

5. Holbrook P., Reznolds J., "Site Security Handbook", RFC 1244;

6. Jennifer S. Pieprzyk J., "Cryptography: An Introduction to Computer Security", Prent. Hall, 1989;

7. Karila Arto, "Open Systems Security - an Architectural Framework", Helsinki, 1991

8. Muftic S., "Security Mechanisms For Computer Networks", Proj. Rep. CEC COST-11, 1990;

9. Patriciu, V.V., "Criptografia și securitatea retelelor de calculatoare", Ed Tehnica, București, 1993;

10. Radu, Cristian, "Criptografia în sisteme electronice de plăti", Teză de doctorat, U.P.București;

11. RSA Data Security, Inc., "The Keys to Privacy and Authentication", Products Catalog, Redwood City, USA, 1996.