Semnatura electronica si securitatea datelor în comertul electronic

Prof.dr. Ion IVAN, asist. Paul POCATILU, prep. Marius POPA, stud. Cristian TOMA
Catedra de Informatica Economica, A.S.E. Bucuresti

*In this paper are presented concepts and theories about electronic signature, secure communications, encrypting algorithms. Also it is expose the SSFTP Application – **S**ecure **S**ocket **F**ile **T**ransport **P**rotocol – and the principal rules and steps that have to be followed by the end-user and the developers of secure applications.*
***Key words**: electronic signature, encrypt procedures, e-commerce, security, RSA, PKI.*

1 Concepte generale despre securitatea tranzactiilor în e-commerce

Astazi, Internetul este folosit pentru a deservi o mare varietate de servicii care cer un grad ridicat de securitate, aplicatii cum ar fi e-commerce, e-banking, management financiar-bancar. Mai mult ca oricând, companiile realizeaza pe Web operatii folositoare afacerilor cum ar fi: folosirea resurselor în mod distribuit si concurent la distanta, cooperarea cu parteneri pentru realizarea de proiecte interactiv prin retea, vânzarea produselor prin Web, etc. Dezvoltarea retelelor necablate – wireless network – implica utilizatorii într-un mediu foarte dinamic si nomadic. Utilizatorii cer sa acceseze resursele «de acasa» în mod transparent si sigur din Internet Cafe-uri, aeroporturi, centre comerciale si alte companii. O solutie puternica la aceste cerinte, trebuie sa fie capabila sa satisfaca urmatoarele cerinte de securitate:

1. ***Confidentialitatea*** – protejeaza continutul tranzactiilor împotriva citirii neautorizate, de catre alte persoane decât receptorii specificati de emitator.
2. ***Autentificarea*** – permite receptorului unui mesaj sa determine în mod sigur identitatea expeditorului.
3. ***Integritatea datelor*** – în retea furnizeaza receptorului unei tranzactii siguranta ca mesajul primit este identic cu mesajul emis de expeditor.
4. ***Prevenirea nerecunoasterii tranzactiei de catre expeditor (Non-Repudierea)*** – garanteaza integritatea si originea tranzactiilor din punctul de vedere al expeditorului si nu a destinatarului. Se împiedica astfel ca expeditorul unei tranzactii electronice sa nege trimiterea ei.
5. ***Aplicarea selective a unor servicii*** – de multe ori este necesara acoperirea unor parti ale tranzactiilor, de exemplu cele continând numarul cartii de credit al unui client. Aceasta nu trebuie sa fie în clar vânzatorului, care poate abuza de utilizarea ei.

2. Semnatura electronica în comertul electronic

Sfârsitul acestui secol a fost dominat de revolutia informatica în Internet, considerata a fi a treia revolutie industriala. Elementul esential de schimbare consta în a înlocui hârtia si semnatura ologrfa cu noi servicii adaptate noii societati informationale. La ora actuala pentru semnatura electronica în tranzactiile din e-commerce sunt folosite sistemele criptografice cu chei publice.

2.1. Sistemele criptografice cu cheii publice folosite pentru semnatura electronica

Sistemele criptografice cu cheii publice inventate de Diffie si Hellman, de la Universitatea din Stanford, folosesc un principiu diferit de criptarea clasica: în loc de o singura cheie secreta, sunt folosite doua cheii diferite, una pentru criptare cealalta pentru decriptare. Una din cheii este secreta – cheie privata(PRIV) - si este cunoscuta numai de detinator. Cealalta cheie, denumita si cheie publica (PUB), este facuta publica si poate fi cunoscuta de oricine.
Ambele chei sunt de fapt siruri de biti, generate de un program capabil de acest

lucru. Cheia publica poate fi plasata pe orice server sau oriunde în lume, însa cea privata trebuie pastrata într-un loc sigur.
Pentru a asigura confidentialitatea, datele sunt criptate la trimitere cu cheia publica a receptorului. Datele pot fi decriptate doar de receptorul adevarat cu cheia sa privata.
Daca se doreste a se verifica autenticitatea unui document, datele trebuiesc procesate în urmatorul mod:

- documentul este criptat cu cheia privata a expeditorului, caree «semneaza în acest mod » ;
- documentul este trimis receptorului ;
- receptorul verifica « semnatura » decriptând documentul cu cheia publica a expeditorului;

O cheie criptografica este de fapt un sir de biti ce poate fi organizat sub forma de fisier. Cheia privata este stocata pe computerul personal, pe un disc portabil sau pe un card. Algoritmi de criptare cu cheie publica reclama o complexitate matematica mare, fiind bazati în general pe operatii complexe matematice în aritmetica numerelor întregi foarte mari.
Din urmatoarele motive semnatura digitala respecta toate conditiile ce trebuie îndeplinite în securitatea tranzactiilor: semnatura este autentica pentru ca este verificata doar de cheia publica a emitatorului; semnatura nu poate fi falsificata pentru ca doar emitatorul stie cheia secreta proprie; semnatura nu poate fi refolosita pentru ca depinde de continutul documentului care este criptat; semnatura nu poate fi "alterata" pentru ca orice încercare de a schimba continutul documentului face ca semnatura sa nu mai fie verificata de cheia publica a emitentului mesajului; semnatura este un element de non-repudiere pentru ca receptorul mesajului nu are nevoie de ajutorul emitentului pentru a verifica daca semnatura este adevarata.
În concluzie semnatura electronica reprezinta un atribut personal, fiind folosita pentru recunoastere a identitatii unei persoane în anumite operatii. Semnatura electronica rezolva problema identitatii persoanei si autenticitatii documentului mai bine decât semnatura ologrefa.

2.2. Algoritmii matematici folositi pentru semnatura electronica

În implementarile practice, algoritmii cu cheie publica sunt adesea ineficienti din punct de vedere al timpului de executie pentru a realiza semnatura digitala. Pentru a câstiga timp, în procesul de semnare digitala se foloseste o functie de dispersie (hash) ce ajuta la realizarea unui rezumat al documentului sau mesajului care trebuie transmis.
Principali pasi ce trebuiesc urmariti pentru a transmite un fisier în conditiile unor tranzactii sigure sunt: se executa un rezumat al documentului cu ajutorul unei functii hash; rezumatul este criptat cu cheia secreta a emitatorului care totodata realizeaza si semnatura digitala în acest mod; documentul împreuna cu semnatura sunt trimise la receptor; receptorul verifica semnatura în 3 pasi (se creeaza un nou rezumat al documentului primit, rezumatul semnat este decriptat cu cheia publica a emitatorului, iar cele doua rezumate sunt comparate si daca rezumatele se potrivesc atunci semnatura este cea adevarata).
În prezent se folosesc urmatorii algoritmi:

- pentru rezumat: MD2, MD4 si MD5 (Message Digest creat de Ronald Rivest), SHA (Secure Hash Algorithm, creat de US Standard Institute), NIST pentru semnatura standard DSA;
- pentru semnatura: RSA (creat de Rivest, Shamir si Adleman), El Gamal si DSA.

Unul din cele mai bune sisteme criptografice cu cheii publice este prezentat în continuare.

2.3. Algoritmul RSA

A fost creat de trei cercetatori de la Massachusetts Institute of Technology si este un standard de facto. Este folosit pe scara foarte larga ca un foarte bun sistem criptografic cu cheii publice. Algoritmul beneficiaza de mare apreciere în mediul guvernamental si comercial, fiind sustinut de mai

multe cercetari si studii din comunitatea academica.
RSA se bazeaza pe quasi-imposibilitatea de a factoriza numere foarte mari. Functiile de criptare/decriptare sunt exponentiale unde exponentul este cheia iar calculele se fac în inelul claselor de resturi modulo n.
Parametrii sistemului criptografic sunt:
1. **p** si **q** sunt 2 numere prime foarte mari (secrete, eventual cunoscute doar de proprietar).
2. modulul **n**, facut public, este obtinut ca produsul lui p si q, n = p*q
3. indicatorul Euler **f (n)**=(p-1)*(q-1), imposibil de determinat de un atacator, deoarece factorii primi ai numerelor n, p si q sunt necunoscuti
4. cheia secreta, **PRIV,** aleasa ca fiind un numar întreg foarte mare relativ prim cu f(n), preferabil din intervalul [max(p,q)+1, n-1].
5. cheia publica, **PUB,** un întreg calculat printr-o versiune a algoritmului lui Euclid, ca fiind invers modulo f(n). PUB = inv(PRIV, f(n)).
6. **M** documentul în format electronic.
7. **H(M)**, rezumatul – digest – documentului, calculat cu o functie de dispersie hash.

Spre deosebire de algoritmi DSA si El Gamal, care pot fi folositi doar pentru semnatura electronica, RSA poate fi folosit si pentru criptare/decriptare. Taria algoritmului consta în dificultatea de a factoriza n în p si q. Laboratoarele RSA sugereaza a se folosi numere prime foarte mari pe 128 sau 1024 biti, a caror factorizare se face în mai multi ani. Pasii pentru a transporta un fisier în conditii de securitate (specifici aplicatiei SSFTP si nu algoritmului RSA) sunt urmatorii:
1. se face rezumatul unui document cu ajutorul unei functii de dispersie hash;
2. rezumatul este criptat cu cheia privata a emitatorului;
3. rezultatul de la pasul 2 este criptat cu cheia publica a receptorului;
4. se executa criptarea documentului cu cheia publica a receptorului;
5. documentul criptat împreuna cu semnatura sunt transmise catre receptor;
6. receptorul primeste semnatura plus documentul criptat si-l decripteaza pe acesta din urma cu cheia sa privata;
7. rezultatului de la pasul 6 i se aplica functia de la pasul 1;
8. receptorul decripteaza semnatura cu cheia sa privata;
9. rezultatul de la pasul 8 este decriptat cu cheia publica a emitatorului;
10. rezultatul de la pasul 9 este comparat cu cel din pasul 7. Daca rezultatele se potrivesc atunci semnatura electronica va fi validata.

Sub diferitele forme de implementare, algoritmul RSA este cunoscut ca metoda cea mai sigura de criptare si autentificare disponibila. Aplicatia SSFTP este un exemplu practic de folosire si implementare a unui sistem criptografic RSA.

3. Aplicatia SSFTP

Sa consideram ca utilizatorul A doreste sa transmita într-un mod securizat un raport financiar stocat în format electronic într-un fisier. Pentru aceasta, SSFTP are doua parti: un element este clientul, iar celalalt element este serverul, care asteapta documente de la clienti si le stocheaza pe disc în vederea prelucrarii ulterioare (de exemplu B, o banca comerciala, asteapta niste formulare on-line de la clienti – serverul este concurent dezvoltat multifir de executie bazat pe conexiune orientata TCP). Interfata grafica serverului si interfata grafica utilizator a clientului este prezentata sunt redate la adresa http://www.ivan.ase.ro/RIE3-2002.htm. Serverul ruleaza pe o masina Linux Red Hat iar clientul pe o masina Windows XP. În continuare este descris protocolul aplicatiei SSFTP.
Programul citeste primul octet din rezumatul fisierului ce reprezinta raportul financiar (rezumat facut cu functia MD4). Fie valoarea lui 65 (caracterul 'A' în ASCII).

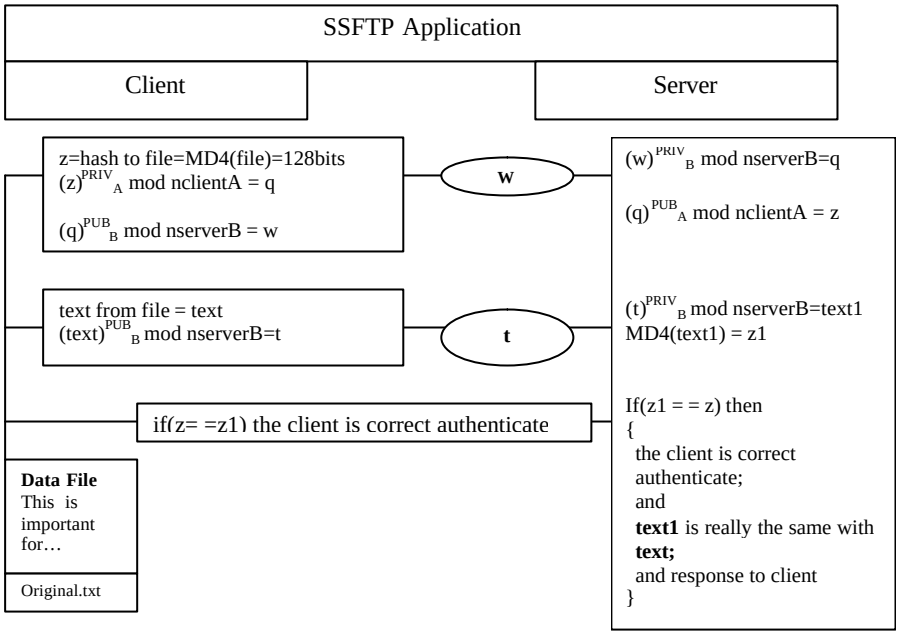

Fig. 1. Protocolul aplicatiei

Caracteristicile ***clientului*** (user A) sunt:

- n = 3233;
- Cheia publica: (71;3233)
- Cheia privata: (791;3233)

Caracteristicile ***serverului*** (user B) sunt:

- n = 1795382159;
- Cheia publica: (1366415437; 1795382159)
- Cheia privata: (1795373509; 1795382159)

Clientul si serverul fac urmatorii pasi pentru a comunica în conditii de securitate:

- litera A (octetul cu valoarea 65) este criptata cu cheia privata a userului A: $\mathbf{65^{791} \bmod 3233 = 2811}$
- rezultatul este criptat cu cheia publica a serverului: $\mathbf{2811^{1366415437} \bmod 1795382159 = 1776501223}$
- numarul **1776501223** nu poate fi transformat în 65 decât daca i se aplica succesiv cheia publica a clientului (a lui A) si apoi cheia privata a serverului (B): $\mathbf{1776501223^{1795373509} \bmod 1795382159 = 1783091602}$
- se aplica cheia publica a clientului A: $\mathbf{1783091602^{71} \bmod 3233 = 65}$
- se continua în acelasi mod pâna când se termina rezumatul mesajului (rezumatul are 16 octeti daca este realizat cu functia de dispersie MD2 sau MD4).

Mai exista o varianta prescurtata de protocol al aplicatiei pentru dispozitivele cu putere redusa de calcul. Aceasta varianta presupune ca mesajul sa fie o singura data criptat cu cheia privata a expeditorului si sa nu i se mai aplice cheia publica a serverului. Acest lucru implica o bresa în securitatea mesajului. Dupa ce se transmite rezumatul se transmite si fisierul criptat cu cheia publica a serverului. La receptionarea mesajului daca se autentifica corect expeditorul fisierul este apoi efectiv decriptat cu cheia secreta a serverului.

Una din problemele sistemului criptografic RSA implica urmatoarea specificatie: cheia serverului (modulul) trebuie sa fie mai mare decât orice cheie a unui client. Se impune ca pe viitor sa se reglementeze de exemplu un prag de 10^{99} pentru valoarea modului n, astfel încât oricine sa aiba doua perechi de chei publice si private, o pereche cu modulul mai mic de 10^{99} si alta cu modulul mai mare de 10^{99} .

4. Statistici privind aplicatia SSFTP

Aplicatia a fost testata pe diferite sisteme si a dat rezultate foarte bune. Pentru început se considera chei RSA pe 1024 de biti din tabelul urmator. Fisierele de test au fost generate automat iar pentru compresie si criptare au fost citite din fisier blocuri de informatie de 92 octeti pâna la sfârsitul fisierului. Programul foloseste o biblioteca special creata, denumita *XSySRSASecurityLib*. În biblioteca sunt functii pentru criptare, compresie, semnatura digitala, de dispersie si de generare de numere prime si chei RSA pe 128, 512, 1024 biti, folosind optim spatiul de disc si timpul la fiecare operatie.

Exponent public	Exponent privat	n modulus
10122152481535604773307125	68494860958402809174584951	10436881232962973548135140
17870109545739036822729947	97775181118575105187124509	80849412174447294844825067
51911700132387353638286217	35308920429552248725502181	43616661963228810103162045
80533455774231435014041885	72459160066149487486555601	59828341432767405139179399
59844223431367123746606365	71926585366846757489817533	69139388829086910741104755
81480472452041492224941418	17203104457538219784190993	73235467435389735104602504
08389043619397400968903537	03093668210754461818826380	51275535546742272997478389
62828123460170504889165002	11628452499623394707820645	53197086688999761031056110
99083918755619382533671093	65032989164362868734269112	12139888706661734811585000
13522537184063233476551918	27205505591326844879895754	55341205203793132603246299
90623023372763446233037858	16576736582944552766014449	39348702596272708063382428
3289780021053445085663 7	70749660950461137120 21	51924677019838598941961

Daca fisierul original este doar criptat, lungimea sa este dubla fata de lungimea celui original. Programul ofera si posibilitatea de a face compresie si criptare în acelasi timp. În acest caz lungimea fisierului criptat este de cinci ori mai mica decât lungimea celui original, iar timpul consumat pentru aceasta operatie este nesemnificativ. Orice client poate comunica cu orice cripto-sistem server care respecta protocolul implementat de aplicatie. Protocolul prevede sa fie transmise mai multe informatii de interes cum ar fi: numele si adresa de IP a cripto-sistemului server, metoda de compresie utilizata (ZIP, JAR, PKZIP), metoda de scriere/citire pe si de pe disc (serializare, scriere string octet cu octet, scriere string octet cu octet codat UTF8, lungimea si cheia publica a expeditorului si datele codificate). Pe viitor se urmareste integrarea aplicatiilor cu un server al Autoritatii de Certificare care sa ia în considerare PKCS (Public Key Cryptography Standards) elaborat de laboratoarele RSA. În urma testelor s-au înregistrat datele statistice, existente la adresa http://www.ivan.ase.ro/RIE3-2002.htm.

Din aceste serii statistice se observa ca lungimea fisierului original este 0.55 din cea a fisierului criptat si de aproximativ 5 ori mai mare decât cea a fisierului comprimat si criptat. În acest exemplu s-au folosit chei pe 1024 de biti si s-au criptat blocuri de câte 92 de biti din fisier. O concluzie se desprinde de aici ca lungimea fisierului criptat depinde si de lungimea cheilor folosite.

Se fac urmatoarele notatii:

F = fisierul original de date;
F' = fisierul de date criptat;
L(F) = lungimea fisierului F = x;
L(F') = lungimea fisierului criptat F' = y;
L(F') <> L(F) deci x<>y.

Din tabel rezulta ca x = 5.6699*y. Este evident ca exista o functie liniara care transforma pe x în y, $y = a*x + b$, unde:

$$a=\frac{\sum x\sum y - n\sum xy}{(\Sigma x)^2 - n\sum x^2} \text{ si } b=\frac{1}{n}(\sum y - a\sum x).$$

Din calcule rezulta a = 0.0334 si b = 2054.5714 iar coeficientul de corelatie este 0.9767. Acesta din urma arata ca exista o legatura foarte puternica între variabilele x si y. De asemenea este evidentiata cu acest coeficient si directia legaturii între x si y. Functia de regresie este:

$$y = 0.0334*x + 2054.5714$$

De exemplu un fisier cu lungimea de 10KB (x=10), în urma compresiei si criptarii va avea lungimea de 2.32KB.

Aplicatia SSFTP genereaza orice fel de cheii RSA si poate cripta si face compresie la orice tip de fisier (text, MS Word, Star Office, executabil, fisiere imagine, fisiere video – mpeg, avi etc.) fara pierdere de informatii si cu o performanta ridicata. Codul sursa al aplicatiei a fost scris în limbajele Java (JDK 1.3.1) si C/C++. SSFTP prezinta o mare scalabilitate si portabilitate pe aproape orice sistem de operare (UNIX/Linux, Windows, OS2, Symbian OS, Java OS) deoarece 90% din codul sursa este scris în Java.

5. Concluzii

Încrederea si viitorul comertului electronic în conditii ridicate de securitate depinde de

evolutia semnaturii electronice. Scalabilitatea si fiabilitatea aplicatiei SSFTP depinde de viteza de comunicare a implementarilor protocoalelor existente, de puterea motoarelor de baze de date, de securitatea conexiunilor fizice, etc.

De exemplu daca un client de la un telefon mobil doreste sa transmita un mesaj important pentru a realiza cumparaturi cu ajutorul aplicatiei SSFTP, atunci mesajul va avea urmatoarea ruta:

- Utilizatorul completeaza un formular (formularul este realizat în WML – Wireless Markup Language si este asemanator cu cele facute în HTML pe Web) cu cartea lui de credit si alte informatii importante.
- Înainte de a trimite informatia la serverul de Web bytecode-ul de pe telefon va trece prin Proxy Gateway, iar semnatura electronica se va realiza la end-user prin procedee specifice (WMLS – Wireless Markup Language Script are o librarie Crypto începând cu WAP 1.2.1 – Wireless Application Protocol).
- Informatia criptata si semnata ajunge la serverul de la supermarket unde este stocata într-o baza de date cu ajutorul unui server-script side.
- Clientul de SSFTP lanseaza la fiecare 20 secunde un fir de executie care citeste din baza de date si transmite informatia prin TCP/IP serverului de la banca.
- Dupa autentificarea primita de la serverul de la banca mesajul va urma aceeasi ruta dar înapoi: supermarket server, WAP Proxy Gateway, si în final la PDA sau telefonul mobil al utilizatorului.

Pentru o conexiune 100% sigura, SSFTP, în locul comunicatiei directe pe socket-uri poate folosi unele din cele mai noi tehnologii: CORBA, COM, DCOM sau .NET. Aceste tehnologii se bazeaza pe RPC (Remote Procedure Call).

Din aceste considerente, semnatura electronica este un mod de autentificare a continutului documentelor electronice si va avea un rol decisiv în tranzactiile specifice comertului electronic.

Bibliografie

[CALI00], Calin Vaduva, Programarea în Java, Editura Albastra, Cluj-Napoca 2001

[DENN82], Denning D.E, "Cryptography and Data Security", Editura Addison-Wesley, New York 1982

[DERE96], Derek Atkins, Paul Buis, Chris Hare, Robert Kelly, "Internet Security Professional Reference", Editura New Riders Publishing, Indianapolis 1996

[FLOR99], Florian Mircea Boian, "Programarea distribuita în Internet", Editura Albastra, Cluj-Napoca 1999

[HEWL01], Hewlett Packard Security references

[IRIN99], Irina Athanasiu, "O perspectiva pragmatica asupra limbajului Java", Editura Agora Press, Târgu Mures 1999.

[IVAN98], Ion Ivan, Daniel Vernis, "Compresia de date", Editura CISON, Bucuresti 1998.

[IVAN01], Ion Ivan, Paul Pocatilu, Cristian Toma, Alexandru Leau, "e3-com", Informatica Economica Nr. 3(19)/2001, Bucuresti 2001.

[IVSM98], Ion Smeureanu, Ion Ivan, Marian Dârdala, "Structuri si obiecte în C++", Editura CISON, Bucuresti 1998.

[TARD91], J.J. Tardo, K. Alagappan: "SPX: Global authentication using public key certificates", IEEE/ACM Transactions on Networking, May 1991.

[VICT94], Victor Valeriu-Patriciu, "Criptografia si securitatea retelelor de calculatoare cu aplicatii în C si Pascal", Editura Tehnica, Bucuresti 1994.

[VICT98], Victor Valeriu Patriciu, Bica Ion, Monica Ene-Pietroseanu, "Securitatea Informatica în UNIX si Internet", Editura Tehnica, Bucuresti 1998.

[VICT01], Victor Valeriu Patriciu, Bica Ion, Monica Ene-Pietroseanu, Calin Vaduva, "Securitatea comertului electronic", Editura BIC ALL, Bucuresti 2001.

[WONG97], C.K Wong, S.S. Lam: "Digital Signatures for Flows and Multicasts", IEEE/ACM Transactions on Networking, Oct 1998.