Proiectarea unei aplicatii pentru comert electronic pe Internet

Prep. Carmen STANCIU
Catedra de Informatica Economica, A.S.E. Bucuresti

Numarul foarte mare de utilizatori conectati la Internet si numeroasele lor sfere de activitate, a dus la extinderea domenilor vietii economico-sociale în care Internetul îsi face prezenta, patrunzând astfel si în sfera economicului, sub forma comertului electronic.
***Cuvinte cheie**: comert electronic,Internet, protocoale de securitate.*

Comertul electronic este un domeniu în plina expansiune în toata lumea, datorita facilitatilor deosebite pe care le ofera partenerilor de afaceri si progreselor tehnologice ce-i fac posibila utilizarea.
Articolul prezinta elementele de pornire pentru realizarea unei aplicatii de comert electronic, si anume caracteristicile aplicatiei fiecarui partener ce participa la comertul electronic (cumparator, vânzator, intermediar), precum si fluxul de informatii dintre ei.
În vederea realizarii unei aplicatii pentru implementarea comertului electronic folosind ca platforma Internetul, trebuie sa tinem seama de modalitatile de plata existente.
Presupunem ca din totalitatea banilor electronici existenti, se utilizeaza carti de credit, pentru realizarea operatiei de vânzare-cumparare. Pentru ca aceasta aplicatie sa poata functiona corect, implica existenta a trei tipuri de parteneri: **vânzator**, **cumparator si intermediar** (aquirer gateway)**,** care asigura securitatea informatiilor cartii de credit pe Internet.
Din punct de vedere al securitatii, atacurile care apar asupra unui astfel de sistem sunt de doua tipuri: • **pasive**, care actioneaza asupra conexiunii dintre client si server si constau în *monitorizarea traficului*; • **active**, care actioneaza tot asupra conexiunii dintre client si server si constau în *modificarea traficului de retea* si cele care actioneaza *asupra serverului vânzatorului.*
Protectia împotriva acestor atacuri se realizeaza prin protocoale, astfel: • **protocol de transport sigur end-to-end**, pentru prevenirea atacurilor de modificare si ascultare ale retelei; • **protocol de plata electronica**, care se adreseaza atacurilor de la serverul vânzatorului (va fi discutat în continuare).
Un ***protocol electronic de plata*** este un protocol de comunicatie *între 3 sau 4 parti,* reprezentate *de vânzator, cumparator si poar-ta de plata - banca emitatoare-eventual si un furnizor de carti de credit*. Implicarea bancii emitatoare se realizeaza prin metode ce sunt bine fundamentate (atacurile prin Internet asupra bancii nu se discuta aici).
În figura 1 este prezentat schematic sistemul de plata dintre cei doi parteneri de afaceri, exemplul cuprinzând 4 parti.

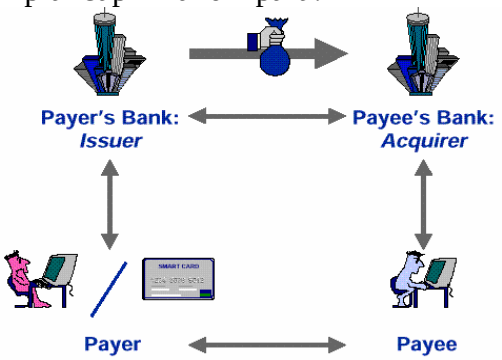


Fig. 1. Lista cerintelor de securitate

Pentru un sistem electronic pe Internet care utilizeaza carti de credit si debit, *Lista cerintelor de securitate* se împarte în doua categorii: • **securitatea canalului de transport** (conexiunii), care este asigurata de un protocol de nivel de trasport securizat; • **securitatea specifica platii**, care este asigurata de protocolul de plata electronica, care realizeaza: furnizarea semnaturii, non-repudi-erea, criptarea secundara (care consta în criptarea unor anumite câmpuri de date ce

vor fi decriptate de o terta parte); acest protocol asigura doua canale:între cumparator si vânzator; între vânzator si poarta de plata sau achizitie.
Presupunem ca protocolul suporta doar *micro tranzactii*, care sunt prea mici pentru ca ban-cile sa se ocupe de ele, ca transactii indivi-duale. Tranzactiile macro nu se discuta aici.
Totodata protocolul va fi proiectat pentru a utiliza serviciile furnizate de protocolul de transport securizat, deoarece:
• simplifica protocol de plata, datorita autentificarii node-to-node, confidentialitatii si integritatii datelor care sunt automat furnizate de nivelul transport;
• separa criptarea conexiunii, autentificarea si integritatea fata de protocolul de plata, furnizând astfel mai multa flexibilitate în implemntarile viitorului IPsec, sau unor mecanisme similare.
Deci, protocolul de plata electronica va fi privit din doua puncte de vedere:
• *al functiilor oferite nivelului inferior*, adica nivelului transport:
- **confidentialitate** - cele doua canalele de comunicatie între doua noduri (unul între cumparator-vânzator, altul între vânzator-intermediar) trebuie sa fie criptate;
- **autenticitate** - se prezinta sub doua forme: a) toti vânzatorii si intermediarii trebuie sa se autentifice reciproc, precum si catre cumpa-rator, autentificarea cumparatorului fiind op-tionala (se realizeaza prin *mecanisme de transport securizat); b)*suport pentru semna-tura digitala, pentru a demonstra originea si chitanta pentru non-repudiere, necesare în unele aplicatii; are nevoie de acces la câmpuri si valori ce trebuie sa fie semnate si apoi folosite în aplicatie;
- **integritatea datelor** - este mentinuta permanent, prin calculul unei chei de rezumat a mesajului; aceasta poate fi o parte a unui mecanism de securitate a canalului; se poate adauga un *extra nivel de integritate* a mesajului, aplicând fiecarui mesaj functii discrete pentru a determina atacurile de tipul "terminare târzie", si de a fi sigur ca mesajul a venit într-un recipient nealterat.
• *al serviciilor specifice de plata pe care trebuie sa le furnizeze partilor*:
- **confidentialitatea** numarului cartii de credit, PIN-ului, si a altor informatii ale cumparatorului; acestea sunt pastrate criptat chiar si fata de vânzatorul de la care are loc tranzactia;
- **confidentialitatea** unor informatii specifice intermediarilor, bancii emitatoare s.a.;
- **semnaturi digitale** - pentru diferitele mesaje care circula între diferitele parti, pentru a se verifica originea lor, diferita fata de autentificarea nodurilor.
În continuare se utilizeaza urmatoarele notatii:
• K{val} = valoarea criptata sub K, utilizând un algoritm simetric pentru cheie;
• PKx{key} = cheia criptata cu cheia publica PK utilizând un algoritm cu chei publice de catre x, unde x= {C (customer), M(merchant), A (acquirer)};
• E{val} = criptarea unei valori cu o cheie de criptare ce este obtinuta dintr-o criptare cu cheie publica a chitantei (recipient); se utilizeaza la anvelope digitale;
• H(val) = mesajul rezumat al valorii, utilizând un algoritm de rezumat al mesajului care este negociat de parti;
• Cx, CERTx = certificatul entitatii x;
• Sx(Val) = valoarea combinata cu semnatura digitala a entitatii x, utilizând cheia sa privata; semnatura poate fi verificata utilizând cheia publica PKx din certificatul Cx; daca entitatea x nu are o pereche de chei publica-privata, atunci se genereaza o "sem-natura de grad scazut", utilizând valoarea discreta a lui Val cu informatii din x, cum ar fi numarul cartii de credit, informatii perso-nale despre x (numar secret social, adresa, PIN).
Un sistem de plata electronic necesita elemente diferite pentru fiecare entitate implicata în tranzactie.

Aplicatia cumparator
Cumparatorul detine urmatoarele informatii:
• numar carte de credit, adresa stabila, PIN

pentru diferite conturi, alte informatii confidentiale pentru procesul de autentificare; • nume, adresa temporara; • optional, unul sau mai multe certificate digitale.
Cumparatorul are urmatoarele cerinte: • entitatile neautorizare nu trebuie sa aibe acces la tranzactie; • informatiile legate de cartea de credit pot fi optional ascunse fata de vânzator, pentru a preveni atacul asupra serverului vânzatorului de pe Internet, precum si de a preveni bonurile de plata neautorizate ale vânzatorului; • optional, facturile semnate de vânzator sau intermediar trebuie sa fie suportate, cumparatorul având astfel dovada tranzactiei; • prevenirea transactiilor neautorizate, incluzând transactiile în care raspund persoanele neautorizate.
Aplicatia cumparatorului trebuie sa implementeze: • toate functiile de navigare si cumparare; • generatoare de ordine de plata, informatii de plata (slips - payment information), semnaturi pentru tranzactii; • informatii aditionale necesare pentru a suporta tranzactii cu carti de credit: primirea preturilor si a informatiilor necesare de la vânzator, criptarea ID-ului tranzactiei cu numarul cartii de credit sau cu alta informatie financiara; acesta informatie poate sa fie accesibila intermediarului, doar utilizând cheia publica a intermediarului extrasa din certificatul digital; verificarea semnaturii de la vânzator si intermediar, pentru a fi sigur de autenticitatea lor; generarea semnaturii pe facturi si autorizarea mesajului, utilizând certificate publice sau informatii personale cu numarul cartii de credit.

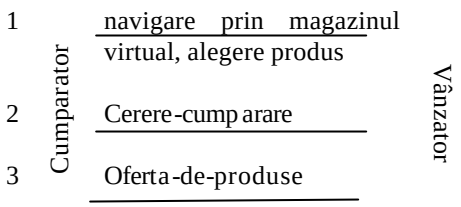
Aplicatia vânzator
Vânzatorul detine informatiile urmatoare: • MID (Merchant ID) asignat de catre intermediar fiecarui vânzator; acest MID poate fi global unic, sau unic unui specific intermediar, depinzând de implementare; • numele si adresa; • certificatul sau digital; •numele si informatii despre intermediarul sau, incluzând certificatul intermediarului si informatii despre cum sa comunice cu poarta intermediarului; •o baza de date cu toate tranzactiile deschise, cu corespondentele dintre TransactionID si AuthID, împreuna cu informatii despre cumparator;
Vânzatorul cere: • operatii eficiente si automate a autorizarii platilor; • semnatura de autorizare; • semnaturi optionale de la cumparator pentru a aproba tranzactiile si de a obtine dovada aprobarii.
Aplicatia vânzatorului furnizeaza toate functiile astfel încât cumparatorul sa obtina informatii despre produs si preturi, precum si: • generarea unui TransactionID pentru fiecare cerere a cumparatorului; acesta se genereaza secvential, se utilizeaza o singura data si se foloseste pentru a urmari cererea înainte de a fi autorizat de catre intermediar; • verificarea semnaturii intermediarului; • genereaza chitante pentru semnatura optiona-la a cumparatorului; • genereaza rezumate din informatiile cererilor pentru ca intermediarul sa verifice autenticitatea lor.

Aplicatia portii intermediare (acquirer)
Intermediarul detine urmatoarele informatii: • nume si adresa; • certificat digital; • nume si informatii, incluzând certificate, despre vânzator; acestea pot fi stocare criptat pe masina portii, într-o baza de date a vânzatorilor; • un tabel cu TransactionID deschise ale fiecarui vânzator, si eticheta AuthID corspunzatoare cu MID-ul vânzatorului.
Cerinte: • suport pentru diferite metode de management al tranzactiilor, incluzând: o singura data, cu repetare, cu transport partial; • autentificarea tranzactiilor ptin semnatura vânzatorilor.
Cerintele aplicatiei: • adaugarea unui set nou de produse necesare pentru finalizarea tranzactiilor financiare pe Internet; • primirea cererilor si a TransactionID cu informatiile finaciare ale cumparatorului si realizarea autorizarii cartii de credit; • translatarea mesajului standard al vânzatorului, într-un format utilizat în autorizarile din retea.

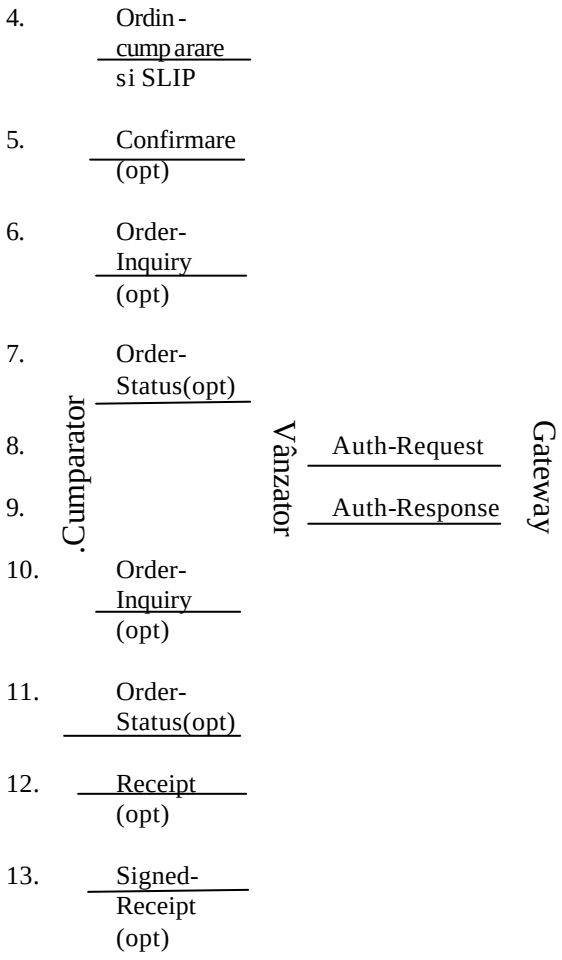
Protocolul de plata pentru comert electronic

În continuare sunt prezentate etapele pe care trebuie sa le urmeze un protocol de comert electronic si câteva elemente legate de fluxul mesajelor interschimbate.

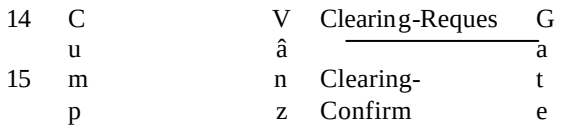
•*Definirea mesajului si a fluxului*

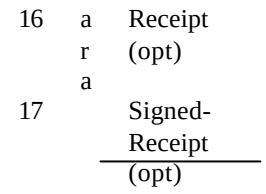


• *Grupul de autorizare*

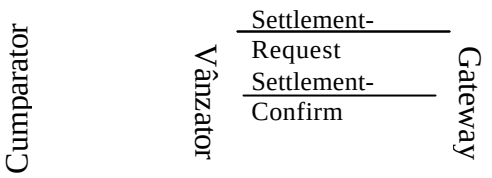


• *Grupul de Clearing*





• *Prelucrarea chitantelor si achitarea*



Bibliografie

1. CLARKE, R., Electronic Commerce Definitions, 1997;
2. COOPER, J.,Computer and Communication Security, McGray Hill, New York, 1989;
3. CURTICAPEAN, P., Sisteme informatice bancare, PC WORLD România, 11, 1997;
4. DARDAC, N.,Operatiuni bancare, Ed. Didactica si Pedagogica, Bucuresti,1996;
5. ELGAMAL.,T.,Commerce on the Internet, july 14, 1995;
6. HULME,M., s.a, Security in the Financial Service Sector, Electronic Banking&Finance, Elsevier Publishers, U.K., 1990;
7. IBM Zurich Research Lab, Secure Electronic Commerce, sept 29, 1997;
8. MASTER CART&VISA, SET - Formal Protocol Definition, may 31, 1997
9. MOISA,T., Securitatea datelor în Internet, Planeta Internet, octombrie,1997
10. PLANETA Internet, În cautarea punctului de vânzare ideal, iunie, 1997;
11. POPESCU, M., eBank- sistem bancar de plati electronice si informatii la distanta, PC WORLD România, 11, 1997.