

## **Capitolul 6.**

### **Comerțul electronic, eComerț**

#### **Cuprins capitol 6.**

(Figuri 6-1/cap6.2., 6-2/cap6.3.,6-3/cap6.5.2.,6-4/cap6.5.2.,6-5/cap6.5.2.,6-6/cap6.6)

- 6.1. O clasificare a comerțului electronic
- 6.2. Schema de principiu a comerțului electronic
- 6.3. Elementele componente ale comerțului electronic
- 6.4. Riscurile, fraudele și disputele în comerțul electronic
- 6.5. Securitatea comerțului electronic
  - 6.5.1. Securitatea telecomunicațiilor – protocoalele SSL și TLS
  - 6.5.2. Securitatea tranzacțiilor de plată – protocoalele 3-D Secure, SecureCode, și SET
- 6.6. Anatomia unei tranzacții de eComerț care folosește protocolul 3-D Secure
- 6.7. Exemple de eComerț actual. Piețe electronice, licitații, furnizori de servicii de plată prin Internet
  - 6.7.1. Comerțul electronic între consumatori și companii, sau comerțul electronic cu amănuntul (B2C)
  - 6.7.2. Piețe electronice, licitații electronice
  - 6.7.3. Furnizori de servicii de plată prin Internet
- 6.8. Comerțul electronic în România
  - Note și bibliografie

Reputata revistă englezească *The Economist* a publicat în mai 2004 un raport special destinat comerțului electronic din care vom cita câteva afirmații semnificative: „eComerțul nu numai că a devenit ceva uriaș, în sine, dar a crescut într-un asemenea mod încât va schimba felul în care se fac afacerile, cu sau fără Internet”; „nici o companie nu își mai poate permite să ignore Internetul”; „competiția pe Internet este feroce.... transparența prețurilor e o regulă .... consumatorii au acces la un volum fără precedent de informații asupra produselor.... comportamentul consumatorilor se schimbă, ei folosesc Internetul pentru a lua decizii privind cumpărăturile pe care le fac și în afara Internetului”; „răspândirea conexiunilor rapide la Internet a constituit un factor cheie în creșterea eComerțului”; „... îngrijorarea referitoare la fraude reprezintă cel mai mare pericol pentru comerțul pe Internet”; „companiile de software, proiectanții de situri și furnizorii de servicii care au contribuit la constituirea Internetului trebuie de urgență să-l facă un loc mai sigur pentru desfășurarea afacerilor” (1).

Comerțul electronic, eComerțul, apărut prin 1994, este comerțul care se desfășoară prin mijloace electronice, adică prin calculatoare și sisteme de telecomunicații. Cea mai mare parte a acestui comerț desfășurat între cumpărători – persoane și comercianți - companii se desfășoară prin rețeaua publică a Internetului, și de aceea a spune eComerț echivalează cu a spune comerț pe Internet, sau comerț în timp real (online), dar acest comerț poate avea loc și prin rețele de telecomunicații care nu sunt publice ci aparțin unor sisteme private de plăți și transfer de fonduri. O altă definiție, mai largă, descrie eComerțul ca fiind constituit din toate plățile în care datele tranzacției (plătitor, destinatar, sumă, etc) sunt transmise electronic, plătitorul și plătitul sunt implicați direct în tranzacție, iar toate informațiile necesare autorizării plății sunt schimbate între cele două părți, electronic (2).

În 2002 existau aproximativ 170 de milioane de utilizatori de Internet în Europa, și cam același număr în America de Nord. Numărul de servere sigure (SSL), capabile de a găzdui situri (website) de comercianți era de circa 185.000.

În România, în anul 2003, numărul de utilizatori de Internet reprezenta circa 24% din populație, numărul de calculatoare personale era de circa 2,1 milioane, iar numărul de furnizori de servicii de Internet (ISP) era de 400 (3).

Aceste cifre indică existența unei infrastructuri impresionante și de neignorată, capabile să ofere toate serviciile necesare dezvoltării eComerțului, inclusiv în România.

Simplu spus eComerțul este un comerț rapid, care se desfășoară în timp real, și comod, iar cumpărătorii și comercianții au drept piață, prin Internet, întreaga lume, magazinele fiind deschise „24 din 24”. Cel mai mare pericol al acestui tip de comerț este riscul de fraudă. Ultimele tehnologii însă, ca de exemplu protocolul de autentificare 3-D Secure adoptat de Visa și MasterCard, diminuează substanțial acest risc, iar eComerțul este în prezent într-o dezvoltare puternică, inclusiv în România.

Instrumentele de plată în comerțul electronic sunt cardurile bancare, cecurile electronice, scrisorile de credit electronice, ordinele de transfer electronice, și, în general, orice instrument bancar de inițiere a unei plăți care poate fi pus sub formă electronică și pentru care există un sistem de procesare.

Pentru desfășurarea în bune condiții de securitate comerțul electronic trebuie să îndeplinească o serie de cerințe: asigurarea confidențialității și integrității datelor pe timpul păstrării și transmiterii lor; autentificarea tranzacțiilor (individualizarea fiecărei tranzacții); asigurarea independenței de natura punctului de acces la Internet (device independence), astfel ca cumpărăturile să se poată face de la un calculator personal, de la un asistent personal digital (PDA), telefon, etc; asigurarea interoperabilității care permite plăți globale, transfrontaliere; asigurarea unei complete evidențe contabile care poate servi în caz de dispute, fraude, probleme legale, etc.

În acest capitol vom face o clasificare a tipurilor de eComerț, urmată de o prezentare a principiilor și elementelor constitutive ale comerțului electronic, o descriere a anatomiei unei tranzacții de eComerț prin Internet în care plata este inițiată prin carduri, o prezentare a riscurilor și a metodelor de asigurare a securității, după care vom face o scurtă prezentare a unor sisteme existente de eComerț, bazate pe Internet, inclusiv în România.

## **6.1. O clasificare a comerțului electronic**

Comerțul electronic poate fi împărțit în două categorii mari: comerțul între persoane și companii (B2C, business-to-consumers, companii-consumatori), numit și comerțul electronic cu amănuntul, și comerțul între companii (B2B, business-to-business).

Comerțul electronic cu amănuntul are loc între consumatorii (persoane fizice) care dispun de un calculator personal cuplat la Internet și comercianții care își expun produsele pe un sit, prin care persoanele văd și aleg produsele expuse pe sit, după care inițiază plata produselor cumpărate cu un card bancar de plată. Acest tip de eComerț derulează cel mai mare număr de tranzacții, dar valoarea totală anuală a acestuia este totuși neesențială în raport cu valoarea tranzacțiilor din comerțul electronic dintre companii.

Comerțul electronic dintre companii constă în mod majoritar din comerțul dintre companiile care se aprovizionează (procurement) și cele care sunt furnizori de produse (suppliers). Furnizorii își expun marfa pe Internet iar companiile care achiziționează aleg și emit o comandă (order) electronică de achiziționare (plata fiind, de regulă, realizată ulterior electronic, sau ne-electronic, prin mijloacele bancare existente). În 2001, în SUA, valoarea acestui comerț a depășit 31 de trilioane de dolari, dar doar sub 1% din tranzacțiile de plată au fost inițiate prin carduri de plată, vasta majoritate a plăților fiind inițiate prin cec și transfer de fonduri prin casele automatizate de transfer/decontări (ACH, Automated Clearing House) (4).

Comerțul electronic se poate desfășura în întregime în timp real (on-line), caz în care atât autorizarea tranzacției de plată, cât și decontarea interbancară, au loc în timp real. Sau se poate desfășura doar parțial în timp real (autorizarea în secunde, iar decontarea a 2-a zi, cum este cazul în care plata se face prin carduri de plată naționale sau internaționale), în care doar autorizarea de plată cu card se obține în timp real, iar decontarea interbancară se face ulterior prin sistemul de carduri, sau prin intermediul serviciilor bancare obișnuite care pot fi, sau nu, electronice, sau în cazul în care decontarea este amânată până în momentul în care comerciantul prezintă documentul prin care cumpărătorul certifică faptul că a primit marfa comandată. Livrarea mărfii de către comerciant poate avea și ea loc în timp real, ca în cazul descărcării (download) imediat după autorizare, de pe Internet a unor astfel de produse cum ar fi muzică, imagini sau software, sau poate avea loc la câteva zile după acceptarea comenzii. Este important ca autorizarea tranzacției să aibă loc în timp real pentru ca cumpărătorul să perceapă efectiv că, în câteva secunde, a făcut o cumpărătură.

O formă foarte răspândită de eComerț între consumatori și comercianții cu sit pe Internet este aceea în care comerciantul folosește situl său doar ca pe un „catalog” de prezentare a produselor (descriere, preț, condiții de plată și livrare, etc), iar cumpărătorul alege, și dă o comandă de cumpărare, însoțită de identificarea și adresa sa, fără însă a și plăti. Comerciantul îi va confirma primirea comenzii și va

livra marfa la domiciliu, moment în care va fi și plătit (de regulă cu numerar sau prin ramburs, dar și cu cec sau cu card, dacă operatorul care livrează marfa dispune de un terminal de plată POS mobil). În acest caz comanda este electronică și în timp real, iar livrarea și plata se desfășoară ulterior, de regulă în câteva zile (modelul de plată „pizza delivery”).

O altă formă de comerț electronic are loc în cadrul așa numitelor licitații electronice (electronic auctions) care au loc pe Internet, cumpărătorii și vânzătorii fiind persoane sau companii. Vânzătorii își expun pe un sit specializat produsele pe care doresc să le vândă, însoțite de un preț minim la care sunt dispuși să îl vândă, iar cumpărătorii conectați la acel sit oferă prețurile pe care sunt dispuși să le plătească. Vânzătorul va alege cumpărătorul care a oferit cel mai mult și va intra în contact direct cu acesta pentru a perfecta ulterior vânzarea și detaliile de realizare a acesteia, pe cale electronică, sau altfel.

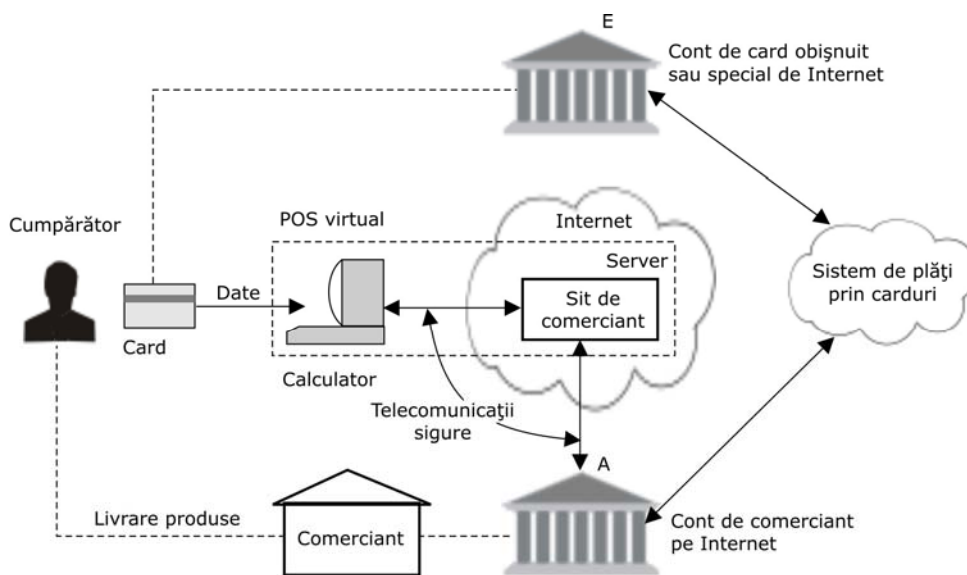
Comerțul electronic se poate realiza direct între cele două părți – cumpărătorul și comerciantul, sau se poate realiza prin intermediul unor companii specializate care furnizează servicii de plată prin Internet (PSP, Payment Service Provider). În acest caz situl comerciantului va fi cuplat (de regulă tot prin Internet) la situl furnizorului de servicii de plată, iar acesta va prelua, în numele comerciantului și băncii acestuia, procesarea electronică a tranzacției de plată cu card a cumpărătorului (va obține autorizarea tranzacției și va furniza comerciantului datele tranzacției astfel ca acceptatorul acestuia să obțină decontarea de la emitent).

Marea majoritate a comerțului electronic care are loc prin Internet sau prin rețelele private de telecomunicații este un comerț domestic în care cumpărătorul și comerciantul au aceeași monedă, moneda țării. În cazul în care plata se face prin carduri internaționale, iar emitentul cardului și acceptatorul comerciantului sunt, ambii, membri ai aceluiași sistem internațional de carduri (cum ar fi Visa, MasterCard sau JCB), atunci comerțul se poate desfășura și transfrontalier, moneda cumpărătorului putând fi diferită de moneda comerciantului. În cazul acestui comerț transfrontalier dificultatea constă în mecanismele de livrare a mărfii și în problemele de legislație legate de reglementările bancare și de rezolvare a eventualelor dispute care pot apare în actul de comerț.

Comerțul electronic se poate desfășura sub multe forme, cu toate sau numai unele dintre etapele actului de comerț desfășurându-se electronic (prezentarea și alegerea produselor, lansarea comenzii, autorizarea plății, livrarea, decontarea finală). Clasificarea prezentată mai sus, fără a fi exhaustivă, a urmărit în esență introducerea ideilor principale care stau la baza acestui tip de comerț.

## **6.2. Schema de principiu a comerțului electronic**

În acest capitol vom prezenta schema de principiu a comerțului electronic desfășurat pe Internet între cumpărători, sau consumatori (persoane fizice), și comercianți, în care plata cumpărăturilor se face prin card bancar de plată, cardul fiind național sau internațional.



**Figura 6-1. Schema de principiu a comerțului electronic prin Internet, cu plata prin carduri**

În figura 6.1 se prezintă schema generală de principiu în care apar principalele elemente ale comerțului electronic – un sit de comerciant aflat pe un server de găzduire, cumpărătorul cu calculatorul său personal cuplat software printr-un navigator (browser) la Internet, băncile emitentă și acceptatoare a cardului cu care se face plata, și sistemul de carduri (național sau internațional) din care fac ambele parte. Dreptunghiul figurat punctat și cuprinzând calculatorul personal, legătura prin Internet, și situl comerciantului este echivalent, din punctul de vedere al acceptatorului comerciantului, cu un terminal de plată cu card, adică reprezintă un POS virtual (VPOS, Virtual POS; a nu se confunda cu situația în care datele de card sunt introduse de la un calculator personal al unui comerciant în vederea obținerii unei autorizări prin Internet, caz care poartă deasemenea numele de POS virtual). Schema este similară în cazul plății prin cec electronic, ordin de plată electronic, etc – se înlocuiește doar cardul cu cecul, și sistemul de plăți prin carduri cu cel de plăți prin cecuri, etc.

O cumpărătură pe Internet se desfășoară, în principiu, astfel. Cumpărătorul accesează situl unui comerciant prin intermediul navigatorului din calculatorul său (de exemplu MS Internet Explorer) căruia îi furnizează adresa comerciantului (de exemplu [www.comerciant.ro](http://www.comerciant.ro)). Odată ajuns pe paginile magazinului virtual al comerciantului, va cerceta produsele prezentate și va selecta unul sau mai multe produse pe care le va pune apoi în coșul, sau căruciorul, virtual de cumpărături (shopping cart). Rolul coșului este de a aduna toate cumpărăturile și de a afișa totalul de plată, astfel încât în momentul plății să se ceară o singură autorizare pe totalul de plată și nu câte una pentru fiecare produs. Apoi programul specializat al sitului comerciantului îl va invita pe cumpărător să-și introducă într-un formular (HTML form) pe care i-l afișează, datele de identitate – nume, adresă de email, adresă de facturare (billing address) și adresă de livrare (shipping address), precum și datele de plată – tip de card, număr de card, dată de expirare. După ce cumpărătorul își citește datele de pe card și le introduce manual de la tastatură în formularul afișat, va apăsa un buton special al formularului (inscripționat, de exemplu, cu "Cumpără") a cărei apăsare echivalează cu generarea unei comenzi ferme de cumpărare și, în același timp, cu acceptarea totalului de plată, și a regulilor și condițiilor de plată și de livrare a produselor pe care comerciantul le-a afișat pe sit, iar cumpărătorul este obligat să le cunoască. Programul specializat al sitului va adăuga automat la datele cumpărătorului o altă serie de date care descriu plata (sumă, monedă, numărul de identificare a tranzacției) și identitatea comerciantului, și va forma din toate acestea un mesaj pe care îl va transmite la sistemul de management de carduri, SMC, al acceptatorului comerciantului prin legătura de telecomunicații dintre serverul care găzduiește situl, și acceptator. SMC-ul acceptatorului se află acum, în principiu, în starea în care a primit un mesaj cu o cerere de autorizare de la unul din terminalele sale de plată POS instalat la unul din comerțanții săi. Mai departe autorizarea tranzacției se desfășoară ca în cazul unei tranzacții ce are loc la un POS dintr-un magazin real, adică acceptatorul emite prin sistemul de carduri o cerere de autorizare către emitentul cardului, de la care primește apoi un răspuns de autorizare. Răspunsul este trimis de acceptator la serverul care găzduiește situl comerciantului său, iar programul special din sit afișează pe ecranul cumpărătorului o pagină cu un raport prin care îi confirmă (sau infirmă) acestuia efectuarea cumpărăturii, angajamentul implicit al comerciantului de a-i livra produsele și condițiile de livrare. Raportul afișat poate fi tipărit de cumpărător și este echivalent cu o chitanță de plată. După un număr de zile produsele expediate de comerciant ajung la cumpărător, iar în momentul livrării la

adresa de livrare care a fost indicată, cumpărătorul va accepta livrarea mărfii prin semnarea unui document de recepție. Acest document va ajunge înapoi la comerciant și va putea servi în eventualele rezolvări de dispute. Acceptatorul va putea credita imediat după autorizare contul comerciantului său, după care introduce tranzacția în fișierul său de tranzacții pe care îl va trimite la emitent în vederea decontării interbancare.

Din momentul în care cumpărătorul a apăsă pe butonul "Cumpără" din formularul afișat, trimițându-și datele de card și ordinul de cumpărare, și până în momentul în care programul special din situl comerciantului îi afișează raportul de răspuns cu confirmarea efectuării cumpărăturii, timpul scurs este, de regulă, de circa 5-10 secunde. Acest timp de răspuns se compune, în mare, din partea de circa 2-4 secunde petrecută de tranzacție în sistemul de carduri și din partea de 3-5 secunde petrecută în Internet (serverul sitului comerciantului, telecomunicații cu protocol sigur SSL sau TLS). În cazul utilizării unor protocoale de autentificare a deținătorului de card, cum ar fi protocolul 3-D Secure, se mai adaugă un interval de până la 10-15 secunde necesare autentificării cumpărătorului, cardului și comerciantului.

Tranzacția de plată descrisă este o tranzacție cu card de tipul "cardul-nu-este-prezent", adică nici cumpărătorul și nici cardul nu se află în fața comerciantului atunci când se face plata, ceea ce conduce la un risc asumat de comerciant (și de acceptator) mai mare decât în cazul unei plăți de tip "cardul-este-prezent" care are loc într-un magazin real. Ca urmare măsurile de securitate luate în cazul eComerțului prin Internet sunt mai puternice și mai cuprinzătoare. Iată, pe scurt, în cele ce urmează, care sunt măsurile uzuale de securitate.

Legăturile de telecomunicații dintre calculatorul personal al cumpărătorului și serverul care găzduiește situl comerciantului, precum și acelea dintre acest server și SMC-ul acceptatorului comerciantului, trebuie să fie legături sigure care să asigure confidențialitatea datelor comunicate și să garanteze autenticitatea celor două părți de la capetele transmisiei. Aceste telecomunicații se implementează printr-un protocol special numit SSL (Secure Socket Layer protocol) sau prin succesorul acestuia, numit TLS (Transport Layer Security protocol), ambele asigurând criptarea (simetrică) a mesajelor și autentificarea ambelor părți. Legătura între serverul de găzduire și SMC-ul acceptatorului se poate face și direct, printr-o linie închiriată care nu e publică (cum ar fi în cazul Internetului), mai ales în cazul în care acceptatorul are mai multe situri de comerciant (un portal) pe un același server, securitatea și viteza transmisiunilor trebuind să fie astfel mult sporită.



Cardul cu care cumpărătorul face cumpărături pe Internet poate fi un card obișnuit al sistemului de carduri sau un card special destinat plății prin Internet, care asigură cumpărătorului o siguranță sporită. Astfel de carduri speciale pot avea, de exemplu, o limită maximă a sumei din cont, o perioadă de expirare foarte scurtă, sau pot fi carduri virtuale ce sunt folosite de regulă numai pentru o singură cumpărătură, după care sunt reîncărcate cu suma necesară următoarei cumpărături.

Autentificarea părților implicate într-o tranzacție de comerț electronic este probabil cea mai importantă măsură de asigurare a securității tranzacțiilor. Părțile implicate sunt deținătorii de carduri, emitenții cardurilor, comercianții și eventual porțile de acces (gateway) de la Internet la sistemul de plată cu carduri. În prezent există trei astfel de protocoale de autentificare utilizate în eComerț: protocolul SET (Secure Electronic Transactions), protocolul 3-D Secure (Three-Domains Secure) și protocolul SecureCode (ultimele două fiind asemănătoare și aparținând, respectiv, lui Visa și lui MasterCard). Vom reveni asupra acestor protocoale.

Comerciantul va încheia cu acceptatorul său de plăți cu carduri prin Internet, un contract special de comerciant pe Internet, cu condiții și prevederi speciale, specifice acestui tip de comerț. Comisionul pe care comerciantul îl va plăti acceptatorului per fiecare tranzacție de eComerț este de regulă mai mare decât în cazul comerțului real, de exemplu de 3-10% din valoarea tranzacției, față de circa 1-3% în cazul comerțului real. Contractul cu acceptatorul va prevedea de asemeni modul de desfășurare a disputelor ce pot apare între cumpărător și comerciant, cu indicarea clară a responsabilităților acceptatorului și celor ale comerciantului, în cazul fraudelor sau a altor excepții.

### **6.3. Elementele componente ale comerțului electronic**

Vom face aici o scurtă descriere a principalelor elemente conceptuale componente ale comerțului electronic, iar în capitolele următoare vom detalia elementele mai importante legate de riscuri, fraude și securitate. Nu toate elementele componente se află în toate sistemele de eComerț.

Principalele elemente componente ale unei activități de comerț electronic desfășurat prin Internet sunt următoarele:

a) comerciantul, acceptatorul său și situl (website) comerciantului pe Internet;

- b) cumpărătorul plătitor cu card, calculatorul său personal, portofelul său electronic și emitentul cardului;
- c) telecomunicațiile sigure între cumpărător și sit, și între sit și acceptatorul comerciantului;
- d) aplicația de eComerț a acceptatorului, distribuită, cu un modul client în situl comerciantului și un modul server în SMC-ul acceptatorului, și poarta de acces la Internet (gateway);
- e) serverul din Internet care asigură găzduirea siturilor de comerciant și legăturile cu SMC-urile acceptatorilor (sau ale procesatorilor independenți adoptați de aceștia);
- f) riscurile, fraudele și disputele;
- g) protocoalele de autentificare care asigură securitatea sporită a tranzacției;
- h) costul tranzacțiilor și microplățile;
- i) piețele electronice, licitațiile.

**a) Comerciantul, acceptatorul său și situl pe Internet al comerciantului**

Comerciantul care dorește să vândă prin Internet și să accepte plăți prin carduri, trebuie mai întâi să-și găsească o bancă acceptatoare care să-i ofere un contract special de cont de comerciant pe Internet. Acest acceptator va trebui să dispună de un sistem de management de carduri, SMC, capabil de a procesa tranzacții de eComerț, sau să externalizeze această procesare către un procesator independent specializat.

Contractul de comerciant pe Internet, care se încheie între comerciant și banca acceptatoare care oferă serviciile de eComerț, este un contract cu clauze speciale destinate a acoperi riscurile mai mari ale acestui tip de comerț, pe care și le asumă acceptatorul. De regulă acceptatorul va verifica bine comerciantul și credibilitatea lui înainte de a-l admite. Unele din riscurile mari ale acceptatorului sunt acelea ca comerciantul să nu livreze marfa plătită (cu tranzacția autorizată), caz în care cumpărătorul va cere banii înapoi de la acceptator prin intermediul emitentului său, sau acela că, după livrarea mărfii, cumpărătorul să nu recunoască că a făcut tranzacția sau că tranzacția a fost făcută fraudulos (cazul tipic de "I did not do it" – "nu am făcut-o" ) și să ceară iar banii înapoi. Pentru acoperirea acestor riscuri mărite acceptatorul poate cere un comision mai mare per fiecare tranzacție, clauze asigurătorii, etc.

Comerciantul va apela apoi la un furnizor de servicii de Internet (ISP, Internet Service Provider) căruia îi va cere să-i găzduiască (hosting) un sit (website) propriu de comerț, numit magazin virtual, și să-i furnizeze o adresă de Internet de forma, de

exemplu, [www.numecomerciant.com](http://www.numecomerciant.com). Comerciantul își poate proiecta el însuși propriul sit, poate apela la serviciile unor companii specializate, sau poate recurge la oferta acceptatorului de a-i crea magazinul și de a-i pune într-un portal de eComerț al acceptatorului, alături de magazinele virtuale ale altor comercianți ai săi.

Situl comerciantului se compune de regulă dintr-o pagină de intrare cu rol de prezentare generală a comerciantului și a magazinului, și dintr-un set de pagini cu prezentarea produselor (descriere, preț). O serie de pagini vor informa cumpărătorii asupra condițiilor de plată și de livrare a produselor cumpărate, și vor descrie responsabilitățile comerciantului și cumpărătorului în toate situațiile, normale sau de excepție, precum și avertizarea legală că dacă apasă butonul "Cumpără", care dă comanda de cumpărare, atunci acceptă implicit toate condițiile comerciantului și toate responsabilitățile care îi revin, așa cum sunt afișate pe sit. Aproape întotdeauna situl va conține și o pagină (cu programul aferent) care reprezintă coșul, sau căruciorul, virtual al cumpărătorului (shopping cart). Cumpărătorul selectează pe rând produsele dorite și le trimite în coș, iar coșul va însuma toate cheltuielile și va indica cumpărătorului doar un total final de plată. Există multe variante de programe care implementează un coș virtual, unele dintre acestea fiind disponibile gratuit pe Internet. La sfârșitul cumpărăturilor, cumpărătorul va examina conținutul coșului și totalul de plată și dacă e mulțumit va apăsa un buton prin care declară că e gata de plată. Un astfel de buton inscripționat de exemplu cu "Doriți să plătiți acum?", va trimite pe ecranul calculatorului cumpărătorului un formular (form) de plată, invitând cumpărătorul să introducă datele sale de identificare și ale instrumentului său de plată.

După introducerea în formular a datelor, cumpărătorul apasă butonul de generare a comenzii către comerciant, inscripționat de exemplu cu "Cumpără", iar acesta va determina expedierea datelor comenzii (produsele selectate, datele de card ale cumpărătorului, datele privind livrarea, datele comerciantului și altele) din sit către SMC-ul acceptatorului, prin intermediul programului său care rezidează în sit și care reprezintă modulul client de eComerț al acceptatorului. După ce acceptatorul va primi răspuns de la emitent la cererea de autorizare a plății, programul său de eComerț, adică modulul server de eComerț din SMC-ul său, va expedia răspunsul către sit, iar modulul client din sit va afișa cumpărătorului un raport final care îi indică efectuarea, sau neefectuarea, cumpărăturii, și acceptarea sau neacceptarea plății. Este posibil ca modulul client din sit să emita și un mesaj de poștă electronică (email) către calculatorul cumpărătorului pentru a-i confirma cumpărătura și pentru

a-i aminti eventual și condițiile de livrare a produselor cumpărate (adresă și data de livrare, de exemplu).

Întrucât toate tranzacțiile de eComerț trec prin SMC-ul acceptatorului, modulul server de eComerț al acestuia va genera periodic, de exemplu o dată pe zi, câte un fișier de comenzi (order file) pentru fiecare din comercianții săi pe Internet. Fișierul de comenzi primit de un comerciant îi indică acestuia toate livrările ferme și cu plata acceptată, pe care trebuie să le facă către toți cumpărătorii săi. Comerciantul poate dispune și de o bază de date de comenzi chiar pe sit, iar modulul client de eComerț poate furniza toate datele unei comenzi acceptate pentru a fi înscrise, comandă cu comandă, în această bază de date, caz în care nu mai este necesar fișierul descris anterior. Comerciantul va efectua livrările pe bază de document de recepție semnat de cumpărător și va păstra aceste documente. Acceptatorul face decontarea interbancară cu emitenții cardurilor care au făcut cumpărăturile și poate credita contul comerciantului imediat după autorizare, cerând documentul de recepție doar în cazurile de dispută.

### ***b) Cumpărătorul plătitor cu card, emitentul cardului, calculatorul personal al cumpărătorului și portofelul electronic, ePortofel***

Cumpărătorii pe Internet pot folosi pentru plată orice card (cu bandă magnetică sau cu cip) emis cu permisiunea sau cu scopul de a fi folosit în acest fel de plată. Ținând seama de riscurile plăților pe Internet emitenții pot emite carduri speciale care urmăresc, în caz de fraudă, micșorarea pe cât posibil a efectelor acesteia.

Există mai multe categorii de astfel de carduri cu risc redus pe Internet – carduri înregistrate de emitent pentru a fi folosite cu un protocol de autentificare (cum este 3-D Secure), carduri cu parametri care reduc riscul, și carduri, sau conturi, virtuale.

Cardurile înregistrate cu un protocol ca 3-D Secure sau SET oferă maxima siguranță. Visa și MasterCard, și în curând și JCB, oferă posibilitatea înregistrării cardurilor lor de debit sau de credit în sistemul protocolului 3-D Secure (promovat de Visa și agreat și de celelalte două). Vom reveni asupra acestui protocol și a semnificației înregistrării (enrollment) unui card.

Cardurile cu risc redus în plățile pe Internet au parametri stabiliți la emitere în așa fel încât în caz de fraudă, pierderea să fie cât mai mică. Uzual se pune o limită maximă de mică valoare pe suma care poate exista în cont în orice moment (de

exemplu maxim 100 euro), iar data de expirare a validității cardului se stabilește ca fiind apropiată de data emiterii. Pot fi micșorați și parametrii care stabilesc valoarea maximă admisă pentru o cumpărătură (de exemplu 50 euro) sau numărul maxim de tranzacții pe Internet, pe zi (de exemplu maxim 2 tranzacții pe zi). Emitentul va decide parametrii de risc și va emite un produs adresat în mod special plății pe Internet.

O protecție bună se asigură prin cardurile virtuale, emise de fapt ca un cont virtual (virtual account) a cărui descriere (nume, număr de cont, dată de expirare, monedă, etc) e înmănată deținătorului sub forma de informație tipizată pe un formular, sau sub forma unui card obișnuit de plastic, dar care nu are bandă magnetică (nu poate fi folosit în lumea reală). Contul cardului virtual e încărcat de cumpărător cu puțin timp înaintea efectuării cumpărăturii cu o valoare apropiată de valoarea la care se va face cumpărarea. Contul va fi reîncărcat înaintea următoarei cumpărături (de pe un alt card, dintr-un cont de debit, de la ATM sau POS, sau prin serviciile bancare electronice – prin Internet sau prin telefonie mobilă). Astfel de carduri, în România, sunt de exemplu cardul virtual Virtuon (cu sigla Visa, fără PIN și fără bandă magnetică) emis de BCR, și cardul Taifun Virtual (cu sigla MasterCard) emis de Banc Post (5).

O altă metodă de a reduce șansele de a capta datele unui card în vederea unei folosiri frauduloase este aceea de a genera pseudo-numere de card. Emitentul va emite astfel de carduri și va stabili în interiorul SMC-ului său o perioadă de valabilitate foarte scurtă, de la o jumătate de oră până la maxim câteva luni, după care numărul de card va dispărea definitiv din evidența SMC-ului, iar cumpărătorul va putea cere apoi emiterea unui alt astfel de card, pentru o altă cumpărătură. Cardul poate avea aparența unui card de credit dar în sistemul emitentului va putea fi pus în corespondență cu un cont de debit (care dă o mai mare siguranță emitentului).

Calculatorul personal al consumatorului trebuie să fie legat fizic la Internet (dial-up, cablu, rețea) și să dispună de un navigator (browser) capabil de a asigura legături sigure (https:) adică care folosesc protocoalele SSL sau TLS. La calculator ar putea fi legat, dar aceasta nu este un lucru frecvent, și un cititor de carduri cu bandă magnetică care ar prelua datele de pe cardul de plată, sau un cititor de carduri cu cip care ar prelua din cip datele secrete (cuvinte de control, chei, certificate) ale consumatorului, necesare eventual în cazul autentificării sale în cadrul protocoalelor de securitate, sau ar putea fi legate alte dispozitive speciale de autentificare (token).

Cumpărăturile pe Internet pot fi mult ușurate prin conceptul de portofel electronic, ePortofel (eWallet). Un portofel electronic este un program rezident în

calculatorul cumpărătorului care conține toate datele de plată ale cumpărătorului, adică datele de identitate (nume, adrese, diverse) și datele de card de plată, și este inițializat de cumpărător o singură dată cu toate aceste date. Apoi, în momentul completării formularului care îi apare pe ecran ca urmare a efectuării cumpărării, datele din ePortofel sunt trecute automat (un simplu clic) în formular. Acest ePortofel poate rezida în condiții de securitate și în serverele pentru situri de comercianți sau în servere specializate, putând fi astfel disponibil și din alte puncte de acces la Internet, nu numai de pe calculatorul personal al cumpărătorului. Portofelul poate păstra și chitanțele tranzacțiilor efectuate, colectând datele din pagina cu raportul de încheiere a tranzacției. Pentru completarea automată a formularului comerciantului cu datele din ePortofel, portofelul și formularul trebuie să fie compatibile (adică să aparțină aceluiași sistem).

### ***c) Telecomunicații sigure***

Datele care circulă între calculatorul cumpărătorului și SMC-ul acceptatorului, trecând prin serverul de găzduire a sitului comerciantului, trebuie să rămână permanent secrete, nealterate și să provină de la o sursă (cumpărător, comerciant/server, acceptator) autentică.

Aceasta se asigură prin protocoale sigure de transmisiuni cum sunt SSL (Secure Sockets Layer), succesorul său similar TLS (Transport Layer Security), PCT (Private Communication Technology), și altele. Cel mai utilizat protocol sigur în eComerț este SSL, urmat de TLS care se bazează pe el și îi aduce unele îmbunătățiri. Caracteristic acestor protocoale este faptul că la fiecare operațiune de cuplare se generează o nouă cheie de criptare și se face o nouă autentificare (cel puțin a serverului de găzduire a sitului comerciantului). Vom reveni asupra protocolului SSL.

Dacă legătura între acceptator și serverul de găzduire se asigură printr-o linie închiriată, care este mai sigură decât cea publică prin Internet, poate fi suficient un protocol mai simplu de telecomunicații, care să asigure doar o criptare a mesajelor (eventual și un cod MAC pentru verificarea integrității), fără autentificarea capetelor transmisiei. Dacă legătura se face prin Internet, se poate folosi și protocolul VPN (Virtual Private Network) care, asemeni SSL-ului, asigură criptarea și integritatea mesajelor, precum și autentificarea părților.

### ***d) Aplicația de eComerț a acceptatorului – modulul client și modulul server de eComerț, poarta de acces la Internet***

Banca acceptatoare care oferă clienților săi comercianți serviciul de comerț electronic prin Internet cu plată prin card trebuie să dispună de un SMC capabil de procesare a tranzacțiilor generate în cadrul acestei forme de comerț. Această funcționalitate a SMC-ului acceptatorului se asigură printr-o aplicație (set de programe) compusă din două părți, sau module – un modul aflat în SMC și numit modulul server de eComerț, și un modul aflat în situl fiecărui comerciant din serverul de găzduire numit modulul client de eComerț. Între cele două module funcționează legătura sigură de telecomunicații care se stabilește între acceptator și server. În cazul plății cu carduri aparținând marilor sisteme de carduri mesajele care circulă prin această legătură sunt în formatul ISO 8583. Rolul fundamental al aplicației de eComerț a acceptatorului este de a dialoga cu cumpărătorul și de a transforma tranzacția de eComerț în așa fel încât să producă o tranzacție echivalentă cu una obișnuită, din lumea reală, produsă de un card la un terminal de plată POS, care să fie procesată de sistemul existent de plăți prin carduri, cu extensiile necesare (6).

Un acceptator are de regulă mai multe situri de comercianți aflate pe același server de găzduire, sau pe servere diferite. Fiecare sit de comerciant dispune de un modul client de comerț electronic care apelează la unicul modul server de comerț electronic din SMC-ul acceptatorului. Eventual fiecare server de găzduire dispune de un singur modul client, care e folosit de toate siturile de comercianți care aparțin aceluiași acceptator.

Logic vorbind sistemul acceptatorului dispune de o interfață cu Internetul prin intermediul căreia se face tot schimbul de informații cu serverele de comercianți. Această interfață are numele de poartă de plată (payment gateway), sau poartă de access (gateway), cuprinde protocoalele de transmisiuni și modulul server de eComerț al acceptatorului, făcând legătura între Internet și sistemul de plăți prin carduri, trecând prin SMC-ul acceptatorului.

Rolul modulului client este de a asigura interfața cu navigatorul cumpărătorilor, adică de a transmite datele primite de la cumpărători la modulul server din SMC-ul acceptatorului, de a primi răspunsul de la acesta, și de a-l trimite înapoi la navigatorul cumpărătorilor. Modulul client va adăuga datelor cumpărătorului și identitatea comerciantului (Merchant ID). În esență, la momentul plății, modulul client va afișa un formular (HTTP form) pe ecranul cumpărătorului în care acesta își va introduce datele secrete ale cardului cu care plătește, după care va forma cu aceste date (plus încă altele) un mesaj pe care îl va expedia, cu titlu de cerere de autorizare, către modulul server. La primirea răspunsului de la modulul server va genera pe ecranul cumpărătorului o pagină-raport cu informațiile care îi confirmă

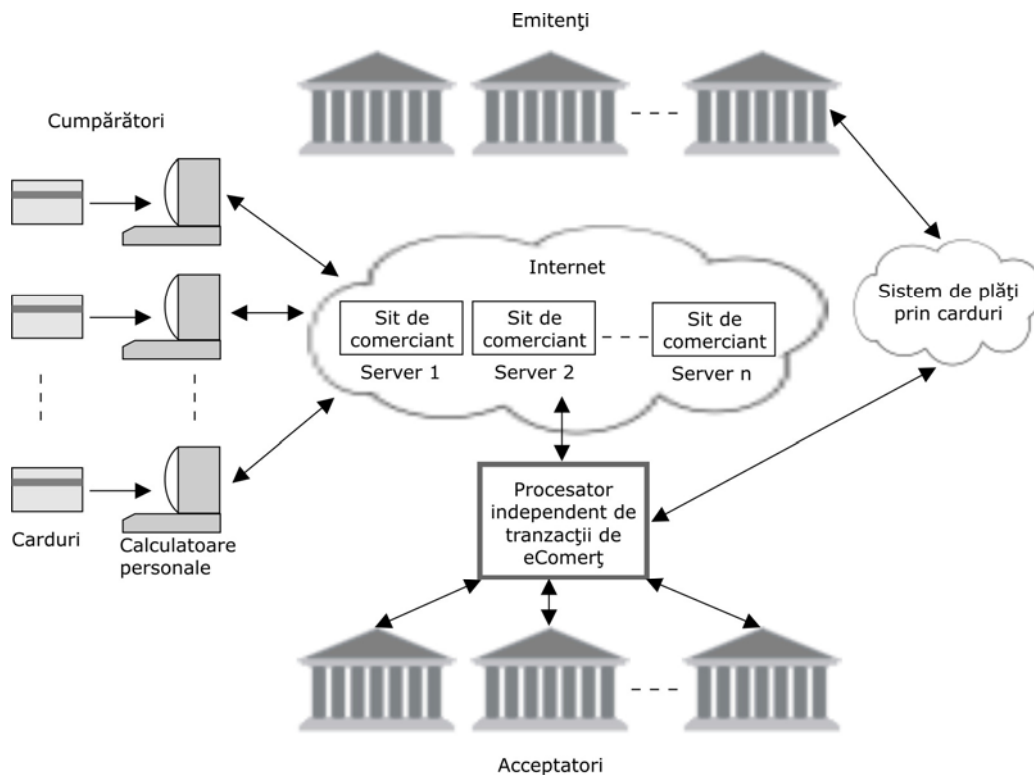
acestui a efectua plătii și datele operației de cumpărare. Va putea eventual trimite cumpărătorului și un mesaj electronic (email) de confirmare a operației. Desigur, va păstra într-un fișier o înregistrare a tuturor mesajelor transmise și recepționate.

Rolul modului server este de a primi tranzacțiile de eComerț cu cererile de autorizare de la toate modulele client, de a le transforma în tranzacții ale sistemului adăugând și identitatea acceptatorului și, după autorizare, de a le trimite modului client de la care a venit cererea de autorizare.

În cazul folosirii protocoalelor de autentificare speciale, cum sunt 3-D Secure și SET, ambele module, client și server, vor dispune de funcționalitățile suplimentare cerute de aceste protocoale, principiile rămânând aceleași.

Acceptatorul care nu dispune de un SMC propriu capabil să ofere serviciile de eComerț poate apela la serviciile unui procesator independent de tranzacții cu carduri, care are această facilitate. În acest caz legăturile cu serverele de găzduire ale siturilor comercianților și cu sistemul de plăți prin carduri sunt asigurate de procesatorul independent, iar acceptatorul păstrează doar o singură legătură (de regulă printr-o linie închiriată) cu procesatorul. Această modalitate este prezentată în figura 6.2. În România un astfel de procesator independent este compania PayNet ([www.paynet.ro](http://www.paynet.ro)), iar procesatorul Romcard ([www.romcard.ro](http://www.romcard.ro)), care aparține unor bănci mari, oferă deja pentru băncile proprietare, și pentru alte bănci, un serviciu de comerț electronic complet și certificat bazat pe protocolul 3-D Secure, sub siglele Visa și MasterCard (a se vedea și capitolul 12.2).





**Figura 6-2. Schema de principiu a comerțului electronic prin Internet în care acceptatorii folosesc un procesor independent**

### **e) Serverul de găzduire a siturilor de comercianți**

Serverul de găzduire a siturilor de comercianți aparține unui furnizor de servicii de Internet (ISP, Internet Service Provider) cu obișnuitele servicii de găzduire pagini HTML (sau XML), de poștă electronică, și de legături de telecomunicații cu acceptatorii potențiali. Acceptatorii pot dispune de propriul server de găzduire pentru comercianții lor, sau indică acestora serverele cu care lucrează.

Un astfel de server poate găzdui multe situri de comercianți, fiecare cu numele lui de Internet, și de la mai mulți acceptatori. Pentru fiecare acceptator va exista probabil câte un tip diferit de modul client de eComerț, care se află în situl (fișierul de pagini) comercianților aceluși acceptator. Serverul va avea legături de telecomunicații cu fiecare acceptator în parte.

Calitățile cele mai importante ale serverului de găzduire trebuie să fie siguranța de funcționare (un grad de disponibilitate mai mare de 99,5% este strict necesar), viteza de procesare și de telecomunicații, și capacitatea mare de stocare de situri.

Serverul trebuie de asemenea să aparțină unei companii în care toate părțile implicate au o mare încredere, adică să fie autentificat de o Autoritate de Certificare

admisă de toți (cum ar fi de exemplu compania americană VeriSign, care este un furnizor global de certificate de autenticitate pentru servere).

### **f) Riscurile, fraudele și disputele**

Riscurile de fraudă în comerțul electronic prin Internet sunt generate pe de o parte de rețeaua de telecomunicații publice, inerent nesigură, a Internetului și pe de altă parte de faptul că tranzacția se face în situația "cardul-nu-este-prezent" în fața comerciantului în momentul cumpărării. Vom defini riscul ca posibilitatea apariției unor pierderi sau unor daune. Pierderile pot fi financiare sau de confidențialitate.

Telecomunicațiile publice nesigure, accesibile oricui și tuturor, oferă șansa unei interceptări frauduloase a mesajelor, din care se pot extrage date secrete (de card, de identitate) care ar putea fi ulterior folosite în mod fraudulos, în dauna deținătorului de card cumpărător, sau a comerciantului.

Faptul că deținătorul și cardul nu sunt prezenți în fața comerciantului oferă șansa prezentării la plată a unui card fraudulos, sau a unui cumpărător cu identitate frauduloasă (card and cardholder impersonation).

Cazurile frecvente de fraudă în care comerciantul acceptă plata dar nu livrează marfa, sau în care cumpărătorul primește marfa comandată și plătită după care declară că nu el a făcut tranzacția și reclamă banii înapoi, conduc la dispute ale căror proceduri de rezolvare costă toate părțile implicate.

Pierderile directe și indirecte datorate fraudelor vor fi suportate de comerciant (acceptator), de emitentul cardului, de deținătorul de card, și chiar de sistemul de plăți prin carduri în ansamblu în cazul în care un cumpărător nemulțumit renunță la cardurile sistemului și trece la cardurile altui sistem.

S-a apreciat că în 2003 fraudele din eComerț au generat pierderi financiare de circa 1,8 miliarde dolari, 1 din 6 cumpărători cu card a fost, sub o formă sau alta, victima unei fraude financiare, și 1 din 12 cumpărători și-au văzut identitatea furată. Frauda pe Internet este de circa 17 ori mai mare decât cea care are loc în magazinele reale, tranzacțiile frauduloase de comerț electronic reprezentând circa 1% din total, față de numai circa 0.06% tranzacții frauduloase care au loc în magazinele reale (7). Alte surse indică cifre mai mici pentru aceste fraude.

### **g) Protocoalele de autentificare care asigură o securitate sporită a tranzacțiilor – 3-D Secure, SecureCode, SET**

După o rapidă dezvoltare a eComerțului la sfârșitul deceniului 90, fraudă crescuse la un nivel considerat inacceptabil, iar răspândirea comerțului electronic a

regresat. Această situație a determinat creșterea preocupărilor pentru securitate și astfel au apărut, printre altele, protocoalele de securitate sporită specifice eComerțului, și anume mai întâi complexul protocol SET susținut de Visa și MasterCard, apoi protocoalele Verified by Visa bazat pe 3-D Secure al lui Visa și SecureCode al lui MasterCard, ultimele două similare ca concepție, dar mai simple și mai ușor de implementat decât SET. În prezent protocolul de autentificare 3-D Secure pare să se impună ca cea mai bună soluție fiind susținut de Visa (care l-a inventat), de MasterCard și de JCB. De remarcat că în România, din 2004, mai multe bănci mari (BCR, Raiffeisen Bank, și Banca Tiriac) acceptă comercianți pe Internet și emit carduri sub sigla Visa și MasterCard care pot fi folosite pentru comerțul electronic cu protocolul 3-D Secure, procesatorul acestor bănci fiind compania Romcard. Vom reveni asupra acestor protocoale.

#### ***h) Costul tranzacțiilor, microplățile***

Efectuarea oricărei tranzacții de eComerț propune costuri pentru toate părțile implicate. Costul unei tranzacții de eComerț are în general o parte fixă de 0,1-0,5 dolari SUA și o parte variabilă ce poate fi mai mare de 5% din sumă (2). Cei care suportă în final aceste costuri sunt cumpărătorii și comercianții. Comercianții rezolvă de regulă problema ridicând acoperitor prețul produselor vândute. Cumpărătorul "simte" costul pe care trebuie să-l plătească pentru o tranzacție pe Internet raportat la valoarea produsului cumpărat, deși costul în sine al tranzacției nu depinde de această valoare. Astfel încât în cazul cumpărării unor produse sau servicii de mică valoare, costul tranzacției de cumpărare poate apărea ca prea mare, eventual inacceptabil. Internetul este un loc predilect pentru punerea în vânzare a produselor și serviciilor de mică valoare cum ar fi software cvasi-gratuit, melodii, imagini, informații diverse, pentru care costul poate fi de câțiva dolari sau chiar câțiva cenți. În acest caz avem de a face cu microplăți (micro payments). Limita pentru definirea unei microplăți e pusă convențional la 10, sau, după alte surse, la 25 dolari SUA, plățile inferioare acestei limite fiind considerate microplăți (2). Se definesc chiar nanoplățile, ca fiind plățile a căror valoare este sub 1 dolar SUA. Pentru micro- și nanoplăți pe Internet există metode adecvate de plată care fac costul tranzacției foarte mic. Una din aceste metode este folosirea ePortomoneelor (ePurse) ca mijloc de plată pe Internet, iar alta este plata prin transferul direct de fonduri între conturi (account-based transfer), conturile cumpărătorilor și comercianților aflându-se la aceeași entitate (dispare operația de decontare), cum e cazul sistemelor de plată PayPal și PayDirect.

### ***i) Piețe electronice, licitații***

Comerțul electronic poate fi organizat și după modelul piețelor reale – mai mulți comercianți își prezintă produsele și serviciile în cadrul aceluiași sit, cumpărătorii pot cerceta mai multe magazine virtuale, pot compara prețurile și pot participa la vânzările de produse prin licitație organizate de diverși vânzători, sau pot cumpăra la prețurile fixe afișate.

Cumpărătorii și vânzătorii pot fi persoane fizice sau companii, în orice combinație – persoane cu persoane (P2P), persoane cu companii (B2C), sau companii cu companii (B2B). Administrația centrală (guvernul) și cea locală (guvernul local), în postură de companie, participă frecvent la achiziția de produse și servicii de la furnizori, prin licitație (B2G).

În cadrul unei licitații vânzătorul afișează produsul, un preț minim de pornire, și o durată a licitației, iar cumpărătorii declară prețul maxim pe care sunt dispuși să-l ofere, putând să modifice acest preț pe durata licitației întrucât pot vedea în orice moment prețul cel mai mare oferit curent. Vânzătorul alege, la sfârșitul perioadei de licitație, prețul cel mai mare și intră în contact direct cu cumpărătorul care l-a oferit, pentru a perfecta vânzarea, stabilind modul de plată și condițiile de livrare. Plata se poate face prin mijloacele electronice oferite de piața electronică sau prin mijloacele tradiționale existente între băncile celor doi.

O piață electronică, procedura de licitație și mijloacele de plată sunt implementate prin aplicațiile specifice ale companiei care deține situl, sau portalul, ce reprezintă piața electronică.

## **6.4. Riscurile, fraudele și disputele în comerțul electronic**

Așa cum am arătat, riscul de fraudă în comerțul electronic e datorat, în principu, caracterului public al rețelei de telecomunicații a Internetului și faptului că nici deținătorul de card, și nici cardul, nu sunt prezenți în fața comerciantului în momentul efectuării tranzacției de cumpărare.

În multe țări, conform legislației naționale, răspunderea pentru o tranzacție frauduloasă revine comerciantului (reprezentat de acceptatorul său) sau emitentului cardului. Din acest motiv deținătorul de card e puternic încurajat, știind că nu va

pierde bani în cazul unei fraude, atâta vreme cât își respectă propriile obligații (față de emitent și față de comerciant și regulile acestora) (8).

Vom prezenta pe scurt în cele ce urmează care sunt tipurile mai importante de pericole de fraudă care ar putea apare în acest tip de comerț (9).

Un agent fraudulos care cunoaște domeniul, pe care îl vom numi fraudator, poate intercepta mesajele transmise și poate extrage datele cardului. Mai târziu fraudatorul poate efectua o tranzacție introducând în comandă datele de card astfel obținute. Acest tip de fraudă poate fi eliminat numai printr-o procedură de autentificare a deținătorului de card (prin PIN sau printr-o parolă, sau expresie, de control). Deținătorul legal al cardului va nega, evident, că a făcut tranzacția și se va declanșa o dispută a cărei rezolvare presupune costuri.

Fraudatorul poate modifica o comandă de cumpărare, schimbând, de exemplu, lista de cumpărături sau cantitatea acestora, astfel încât comerciantul va livra produsele greșit, iar cumpărătorul va refuza recepționarea acestora și va cere banii înapoi. Comerciantul își va putea pierde clienții.

Fraudatorul poate modifica paginile din situl comerciantului cu scopul de a dezinforma cumpărătorii care se vor îndrepta astfel spre alt comerciant.

Fraudatorul poate fi chiar comerciantul dacă va utiliza datele de card primite în cursul unei plăți (în cazul în care are acces la aceste date) pentru a efectua el însuși tranzacții în locul deținătorului de card legitim. Aceasta reprezintă una din cele mai mari temeri ale cumpărătorilor pe Internet, care ar prefera să știe că datele lor de card nu se păstrează în situl comerciantului.

Fraudatorul poate să creeze un fals sit de comerciant, care arată ca un magazin virtual legitim, dar care nu e legat de nici o bancă acceptatoare sau sistem de plăți. El va capta astfel toate datele de card pe care cumpărătorii păcăliți le vor furniza când vor face o cumpărătură.

Un deținător legitim al unui card legitim poate deveni un fraudator dacă, după ce a efectuat o cumpărătură și a primit produsele, neagă că a făcut tranzacția și încearcă să obțină banii înapoi.

Fraudatorii pot de asemenea să încerce să facă nefolosibil un sit de comerciant, generând un număr foarte mare de tranzacții cu date de card inventate, tranzacții care vor fi respinse, dar situl va fi practic nefolosibil de către cumpărătorii legitimi, fiind supraîncărcat cu respingerea tranzacțiilor invalide.

Ca urmare a diverselor forme de fraudă un deținător de card care e cumpărător pe Internet poate contesta, sau disputa, sub diverse motive, fie toată tranzacția, fie doar aspecte ale acesteia. Cumpărătorul se va adresa cu o plângere

către emitentul cardului său, iar acesta va începe o procedură de rezolvare a disputei, conform regulilor sistemului de carduri și împreună cu acceptatorul care reprezintă comerciantul, în scopul returnării banilor, total sau parțial (chargeback, returnare plată). Motivele cele mai frecvente invocate de cumpărător sunt "nu am făcut tranzacția", "nu doresc ceea ce am primit" și "nu am primit ceea ce am cumpărat". Rezolvarea acestor dispute implică costuri suplimentare relativ mari pentru emitent și pentru acceptator, și, în mod frecvent, pierderile mai mari sunt suferite de comerciant.

## **6.5. Securitatea comerțului electronic**

Măsurile speciale de securitate în cazul comerțului electronic prin Internet, în care plățile se fac cu carduri, sunt concentrate, în principal, în două direcții – asigurarea securității telecomunicațiilor, și asigurarea securității tranzacțiilor prin procedee mai puternice de autentificare, în principal a deținătorului de card. Prima direcție încearcă să rezolve problema riscurilor generate de caracterul public al transmisiunilor prin rețeaua Internetului, iar a doua pe aceea a riscurilor generate de o situație în care "cardul-nu-este-prezent" (similară cu cazul comenzilor date prin telefon sau poștă).

Alte măsuri de securitate sunt luate la nivelul legislației și al reglementărilor bancare și ale sistemelor de carduri, iar altele urmăresc comportamentul cumpărătorilor (memorând o istorie a tranzacțiilor) și depistarea unui profil al cumpărătorului, sau comerciantului, potențial fraudulos căruia mai apoi i se vor interzice tranzacțiile. Unii emitenți pot utiliza chiar rețele neuronale care pot identifica un fel anume, susceptibil de a fi fraudulos, de a face cumpărăturile – de exemplu efectuarea unui mare număr de cumpărături într-un interval scurt de timp (câteva ore) de pe multe situri de comerciant, caz în care cumpărătorul va fi imediat contactat pentru verificare.

### **6.5.1. Securitatea telecomunicațiilor – protocoalele SSL și TLS**

În prezent securitatea telecomunicației între calculatorul personal al cumpărătorului și serverul de găzduire al sitului comerciantului, precum și aceea dintre acest server și procesorul acceptatorului se asigură prin protocolul SSL, sau prin succesorul său TLS.

Ambele protocoale asigură toate elementele fundamentale ale unei transmisiuni sigure – criptarea mesajelor care asigură confidențialitatea, verificarea integrității conținutului mesajelor, și autentificarea entităților de la ambele capete ale transmisiunii.

Protocolul SSL (Secure Sockets Layer), ajuns astăzi la versiunea 3.0, a fost proiectat de compania americană Netscape Communications în 1995 și s-a răspândit în toată lumea fiind instalat în toate navigatoarele importante (Internet Explorer și Netscape) și în toate serverele de găzduire de situri, devenind un standard de facto al securității telecomunicațiilor pe Internet. Iată pe scurt modul său de funcționare.

În momentul în care un navigator adresează un server în regim de securitate (adrese începând cu https:), acesta va trimite navigatorului propriul său certificat de autenticitate, eliberat de o Autoritate de Certificare (care respectă standardul X.509) cunoscută și acceptată (cum ar fi VeriSign Inc.), criptat și semnat de aceasta cu cheia sa secretă și conținând identitatea serverului și cheia publică a serverului. Opțional, și navigatorul poate trimite certificatul său către server. Navigatorul va decripta certificatul serverului (cu cheia publică, pe care o cunoaște, a Autorității de Certificare) și va obține cheia publică a serverului, apoi va genera o cheie secretă valabilă numai pentru cuplarea în curs (la fiecare legătură cu serverul se va genera o nouă cheie). Această cheie de criptare a mesajelor (de 40 sau 128 de biți) este la rândul ei criptată cu cheia publică a serverului, căruia îi este apoi expediată. În acest fel ambele capete ale transmisiei dispun acum de o cheie secretă de criptare mesaje, cu care își criptează mesajele pe care încep să și le trimită. Această cheie de criptare mesaje se folosește și la aplicarea unui cod MAC (Message Authentication Code) care permite verificarea integrității mesajelor schimbate.

Protocolul TLS (Transport Layer Security) a fost elaborat de IETF (Internet Engineering Task Force), organizația de standardizare a Internetului, pe baza SSL 3.0 și reprezintă o îmbunătățire a acestuia în mai multe privințe. Este de așteptat să se substituie treptat protocolului SSL (10).

### **6.5.2. Securitatea tranzacțiilor de plată – protocoalele 3-D Secure, SecureCode și SET**

O creștere substanțială a securității tranzacțiilor de plată se poate obține prin folosirea unor protocoale de autentificare al căror rol este să autentifice actorii principali ai tranzacției ce are loc pe Internet – deținătorul de card și cardul lui, comerciantul și acceptatorul lui, și poarta de acces (gateway) din Internet către sistemul de plăți prin carduri. Aceasta autentificare se face fie prin certificate de autenticitate care necesită un sistem de chei publice (PKI, Public Key Infrastructure), fie prin alte metode, mai simple. Esențială este autentificarea deținătorului de card deoarece aici se află sursa majorității fraudelor.

Trei astfel de protocoale sunt astăzi în folosință – protocolul SET proiectat în 1996 de Visa, MasterCard, IBM și alții, protocolul 3-D Secure proiectat de Visa, și protocolul SecureCode proiectat de MasterCard, ultimele două în 2001. Cel care asigură securitatea maximă, întrucât autentifică pe toți actorii tranzacției, este protocolul SET. Acesta este însă un protocol complicat, scump și greu de implementat, motiv pentru care nu este răspândit, pare amenințat cu dispariția și nu vom insista asupra lui. Dintre celelalte două, care sunt mai simple și mai ușor de implementat, protocolul 3-D Secure tinde să devină un standard de facto fiind acceptat și de MasterCard și de JCB.

Protocolul de autentificare 3-D Secure este prezentat de Visa sub marca "Verified by Visa" (VbV), această marcă fiind prezentă pe siturile comercianților ai căror acceptatori au aderat la protocol. MasterCard oferă însă sub marca proprie de "SecureCode" un număr de trei protocoale de autentificare distincte, la alegere pentru acceptatori – protocolul SPA/UCAF (primul care a purtat marca), protocolul CAP derivat din primul, și implementarea proprie a protocolului 3-D Secure.

Spre deosebire de SET, protocoalele 3-D Secure și SPA/UCAF nu mai impun certificate de autenticitate pentru toate părțile, ceea ce reprezintă o mare simplificare. Autentificarea deținătorului de card se face în timpul tranzacției de către emitentul acestuia numai pe baza numelui și a unui cuvânt de control (password) sau PIN (sau prin alte metode, la alegerea emitentului), certificatul de autenticitate al cumpărătorului nemaifiind strict necesar.

În cele ce urmează vom face o scurtă prezentare a celor trei protocoale, punând un accent ceva mai mare pe 3-D Secure, după care vom face o scurtă comparație între protocoalele 3-D Secure și SecureCode (SPA/UCAF).

### **a) Protocolul SET**



Acest protocol (11) folosește certificate de autenticitate și generează diverse chei pentru deținătorul de card, pentru comerciant și pentru poarta de acces (gateway) la sistemul de plăți prin carduri. Poarta de acces se află la nivelul acceptatorului care are legatura cu sistemul de plăți prin carduri și reprezintă punctul de acces din Internet în acceptator și mai departe în sistemul de carduri.

Certificatele de autenticitate sunt generate de Autorități de Certificare diferite, aflate într-o ierarhie, la vârful căreia se află o autoritate rădăcină care aparține consorțiului SET, numit SETCo. Această rădăcină va certifica Autoritățile de Certificare ale sistemelor de carduri (Visa, MasterCard) care, la rândul lor, vor certifica emitenții și acceptatorii.

Fiecare emitent va fi apoi Autoritatea de Certificare pentru deținătorii lui de carduri, și cardurile lor, iar fiecare acceptator va fi Autoritatea de Certificare pentru comercianți și porțile lor de acces (de la serverul de găzduire la acceptator).

În prima fază a tranzacției părțile se autentifică între ele – deținătorul de card cu comerciantul (opțional), deținătorul de card cu poarta de acces (opțional), comerciantul cu deținătorul de card (obligatoriu), și comerciantul cu poarta de acces (obligatoriu).

În a doua și ultima fază are loc autorizarea tranzacției în care, în maniera deja descrisă, datele cardului ajung la acceptator care formulează o cerere de autorizare către emitent, al cărui răspuns îl trimite apoi către calculatorul deținătorului de card trecând prin poarta de acces și serverul de găzduire a sitului comerciantului.

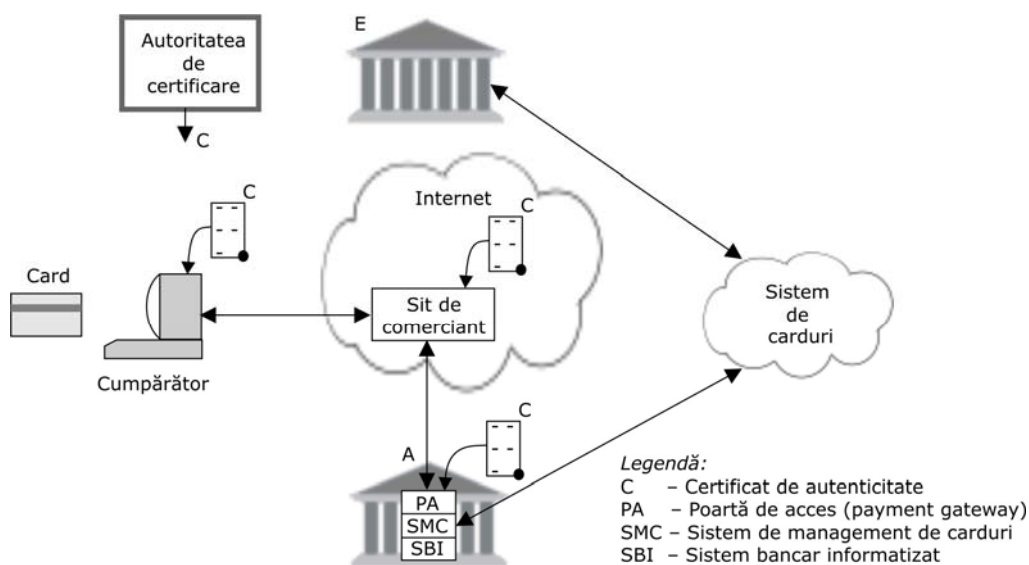


Figura 6-3. Protocolul SET

În figura 6.3 se prezintă schema de principiu a protocolului SET. O variantă simplificată a acestui protocol, numită 3-D SET (server based), care nu mai păstrează certificatul cumpărătorului în calculatorul lui personal (făcând astfel posibilă cumpărarea și de la alte puncte de acces la Internet), nu s-a bucurat nici ea de succes, rămânând în continuare complicată și scumpă.

### **b) Protocolul 3-D Secure**

Ca urmare a răspândirii reduse a protocolului SET, un protocol foarte sigur dar complex și scump, Visa introduce în 2001 propriul protocol numit 3-D Secure, mai simplu și mai ușor de implementat, bazat pe un model de sistem de securitate care cuprinde trei domenii (12). Scopul celor trei domenii este acela de a defini clar responsabilitățile părților implicate în tranzacție. Cele trei domenii sunt Domeniul Emitentului, care cuprinde deținătorii de card și emitenții cardurilor lor; Domeniul Acceptatorului, care cuprinde comercianții și acceptatorii lor; și Domeniul de Interoperabilitate, care asigură comunicarea între emitenți, acceptatori și sistemul Visa. Protocolul asigură autentificarea numărului de card, a deținătorului de card, și a comerciantului, la fiecare tranzacție.

În modelul celor trei domenii, 3-D, la tranzacția de plată autentificată participă direct emitentul cardului și comerciantul. În momentul în care cumpărătorul inițiază plata, comerciantul (modulul de 3-D Secure din situl lui) va cere mai întâi autentificarea numărului cardului iar apoi va cere emitentului să-i autentifice deținătorul de card. După ce va primi autentificarea semnată, va urma autorizarea normală a plății (trimite la emitent, prin sistem, o cerere de autorizare, etc). Comerciantul va începe deci întotdeauna prin a cere emitentului să-i autentifice mai întâi cardul și deținătorul de card.

Deținătorul de card trebuie să se înregistreze (enrollment) în sistem la emitentul său și să-și declare cel puțin un nume și o parolă prin care emitentul poate să-l autentifice în momentul tranzacției, trimițând apoi aceasta autentificare comerciantului. Protocolul lasă libertatea emitentului de a alege și alte metode de autentificare a deținătorului de card care să arate, în momentul efectuării tranzacției, că este deținătorul legitim al cardului cu care se face plata. Emitentul poate astfel cere deținătorului de card să dispună de un certificat propriu de autenticitate, să folosească un card inteligent (printr-un cititor cuplat la calculatorul personal) ca depozitar sigur al identității, sau să folosească metodele de autentificare din serviciile

bancare electronice (eBanking) proprii. Uzual însă deținătorul de card e autentificat de emitent doar prin nume și parolă.

După ce îl autentifică, emitentul va genera un răspuns semnat electronic (un certificat de autentificare a deținătorului de card) pe care îl trimite comerciantului pentru a-i confirma autenticitatea deținătorului de card, iar comerciantul va putea trece la faza de autorizare normală a tranzacției.

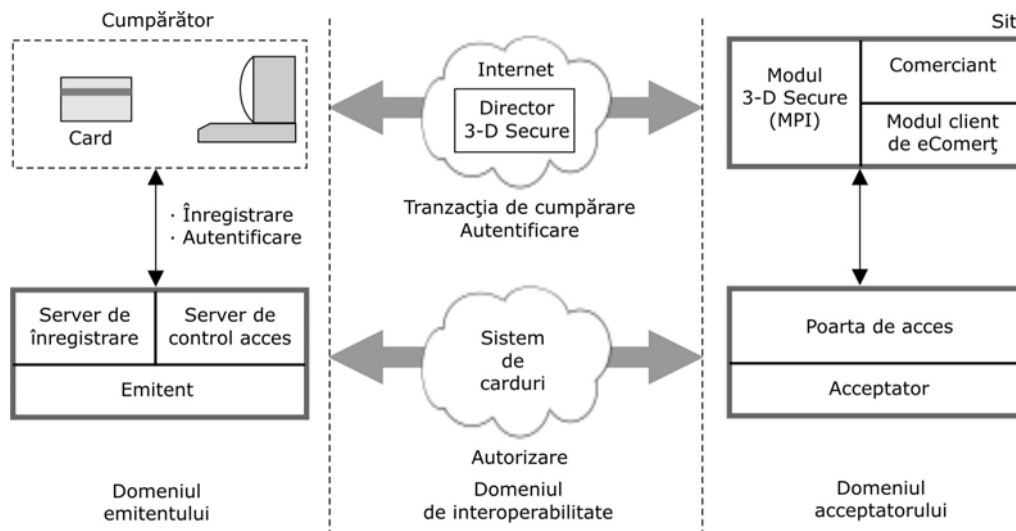
Deținătorul de card este liber să-și instaleze și un portofel electronic, ePortofel (eWallet), care va conține informațiile de identitate (nume, adresă, parolă, etc) și cele de card (tip card, număr card, dată de expirare) și care îi poate servi la automatizarea procesului de completare a formularului de plată (form filling) și la păstrarea chitanțelor pentru tranzacțiile efectuate.

Emitentul dispune de un serviciu de înregistrare în sistemul 3-D Secure a cardurilor și deținătorilor de card (înregistrarea se poate face și prin Internet) păstrând într-un server de înregistrare (Enrollment Server) numerele de card, numele și parola deținătorilor participanți. Emitentul mai dispune și de un server de control al accesului (ACS, Access Control Server) care are rolul de a primi cererile de autentificare a cumpărătorului venite de la comercianți, de a face autentificarea acestuia verificând numărul de card, numele și parola (sau o altă metodă), și de a trimite răspunsul semnat înapoi la comerciant.

În domeniul de interoperabilitate Visa (sau MasterCard, care a aderat la sistem) dispune de un Director (Directory Service) care este un server central pe Internet (ce dispune de un certificat de autenticitate) în care se păstrează numerele de card ale tuturor cardurilor înregistrate în sistemul 3-D Secure (înscrise de emitenți) precum și adresele de Internet (URL) ale serverelor de control al accesului (ACS) ale emitenților cardurilor înregistrate. În acest Director se păstrează și o arhivă a tuturor autentificărilor date de emitenți, pentru a servi rezolvării unor eventuale dispute.

În domeniul acceptatorului, acceptatorii trebuie să dispună de o poartă de acces (payment gateway) la sistemul de plată prin carduri Visa/MasterCard, iar comercianții lor trebuie să-și instaleze, pe lângă (sau în locul, dacă îi preia funcțiile) modulul client de eComerț, și un modul de 3-D Secure care poartă numele standard de MPI (Merchant Plug-In module), adică modul de comerciant 3-D Secure instalat în sit. Acest modul de comerciant 3-D Secure va genera cereri de autentificare a cardului și a cumpărătorului către emitent, prin intermediul Directorului, iar după primirea răspunsului va trimite cererea de autorizare a tranzacției către poarta de acces a acceptatorului (prin intermediul modulului client de eComerț) care, la rândul

lui, o va trimite mai departe în sistemul de carduri prin acceptator. În cursul acestei operații modulul MPI al comerciantului se va autentifica față de Director printr-un certificat de autenticitate sau, mai simplu, printr-un password, iar Directorul va face același lucru față de comerciant. În felul acesta are loc, la fiecare tranzacție, și o autentificare a comerciantului. După primirea răspunsului de autorizare, modulul comerciantului va trimite cumpărătorului o pagină cu un raport asupra efectuării tranzacției. În cazul în care tranzacția este inițiată de un card care nu este înregistrat în sistemul 3-D Secure, comerciantul va putea sări peste etapa de autentificare a cumpărătorului și va trece direct la autorizare, sau va respinge tranzacția, după cum a ales acceptatorul.



**Figura 6-4. Schema de principiu a domeniilor protocolului 3-D Secure**

Figura 6.4 prezintă schema de principiu a domeniilor protocolului 3-D Secure. Mesajele privind autentificarea circulă între Domeniile emitentului și acceptatorului în cadrul Domeniului de interoperabilitate, și au loc prin Internet. Mesajele prin care se face autentificarea deținătorului de card circulă între acesta și emitentul său, în cadrul Domeniului emitentului. Mesajele prin care se cere autorizarea tranzacției și se face procesarea plății circulă între comerciant și acceptatorul său, în cadrul Domeniului acceptatorului, iar aceleași mesaje dar care se schimbă între acceptator și emitent în vederea realizării autorizării și procesării plății, circulă în cadrul Domeniului de interoperabilitate prin sistemul de carduri (VisaNet, BankNet). Legăturile prin Internet sunt legături sigure, efectuate prin protocolul SSL, în care fiecare entitate server dispune de un certificat de autenticitate iar mesajele sunt criptate. În capitolul 6.6 vom prezenta anatomia unei tranzacții de eComerț care folosește protocolul 3-D Secure. Comerciantul nu are acces la datele cardului de

plată, care nu sunt stocate pe situl său, și poate vedea numai verdictul final de autentificare dat de emitent – autentificat sau neautentificat.

Protocolul 3-D Secure verifică esențialmente autenticitatea cardului și a deținătorului de card și dă astfel comerciantului încrederea că va fi plătit după ce va livra produsele comandate. Protocolul poate fi folosit în principiu și pe alte canale de plată – telefoane mobile, asistenți digitali personali (PDA) sau televiziunea digitală prin cablu.

Visa estimează că introducerea protocolului va diminua cu până la 80% numărul de tranzacții disputate. Pentru a încuraja răspândirea protocolului în rândurile membrilor săi, Visa a stabilit, pentru regiunea CEMEA în care se află și România, termenul de aprilie 2003 ca un moment dincolo de care răspunderea (până la acea dată împărțită între emitent și acceptator, în funcție de circumstanțe) în cazul unei pierderi datorate unei fraude în comerțul electronic va reveni acelei părți care nu a implementat protocolul (liability shift). În SUA până în 2004 protocolul a fost deja adoptat de 80% din bănci, iar în Europa de peste 100 de bănci și peste 10.000 de comercianți.

### **c) Protocolul SecureCode**

Sub denumirea de SecureCode, MasterCard oferă membrilor săi trei protocoale de autentificare a deținătorului de card – protocolul SPA/UCAF, protocolul CAP care este o variantă a primului, și protocolul 3-D Secure în versiunea MasterCard.

Asemeni lui Visa și tot în 2001, MasterCard anunță protocolul SPA (Secure Payment Application) bazat pe utilizarea unui mecanism de transport de date prin rețeaua sa (BankNet), denumit UCAF (Universal Cardholder Authentication Field) care transportă un așa numit "semn de autentificare" (authentication token) utilizat pentru a indica autentificarea deținătorului de card care a făcut tranzacția, motiv pentru care este numit SPA/UCAF. Protocolul CAP (Chip Card Authentication Program) este o variantă a SPA pentru plata cu carduri inteligente și presupune de regulă cuplarea la calculator a unui cititor de astfel de carduri. MasterCard adoptă apoi în 2002 protocolul 3-D Secure într-o variantă proprie și îl prezintă tot sub denumirea generică de SecureCode. Acceptatorii MasterCard au libertatea de a-și alege tipul dorit de protocol.

În cele ce urmează vom face o scurtă prezentare a protocolului SPA/UCAF (13). Protocolul cere participarea directă a emitentului care autentifică cumpărătorul și a comerciantului care dispune de un modul client de eComert specific SPA, și impune ca fiecare cumpărător deținător de card să-și instaleze în calculatorul său un

portofel electronic care îi va servi la autentificare și la efectuarea plății. Acest program (numit și "SPA applet") are atât funcția de ePortofel care deține datele de identificare și de card de plată, cât și aceea de a interacționa cu comerciantul și cu emitentul cardului.

Emitentul dispune de un server de ePortofel (wallet server, sau SPA server) și distribuie cumpărătorilor care se înregistrează câte un ePortofel pe care aceștia și-l instalează apoi în calculatorul lor personal. În momentul înregistrării (enrollment) cumpărătorul își va defini și o parolă, sau un PIN, după care va fi autentificat ulterior. Când va începe tranzacția, ePortofelul se va activa și va cere deținătorului de card să se autentifice printr-un formular (se cere parola) după care se va conecta la emitent pentru a-i trimite aceste date și a-i cere o dovadă a autentificării. Serverul emitentului va verifica datele introduse cu cele păstrate la momentul înregistrării în sistem și va genera un mesaj cu un "semn de autentificare" (authentication token) pe care îl va întoarce ePortofelului. Acest semn de autentificare poartă numele de AAV (Accountholder Authentication Value), valoarea de autentificare a deținătorului de cont de card, și arată, în esență, dacă parola introdusă este corectă, caz în care deținătorul de card este declarat autentic.

Comercianții au un modul client de eComerț, specific protocolului, care le este furnizat de acceptatorul participant la sistem. Acest modul interacționează cu cumpărătorii și cu ePortofelele lor, precum și cu poarta de acces (unde e modulul server de eComerț) a acceptatorului. Când cumpărătorul va declanșa cumpărătura, comerciantul va adauga la datele tranzacției și semnul de autentificare (ce se va păstra în câmpul UCAF din structura mesajelor care circulă prin rețeaua BankNet a MasterCard), și va trimite totul către acceptator. Acesta va trimite mai departe cererea de autorizare a tranzacției și semnul de autentificare, prin rețea la emitent. Emitentul va compara semnul de autentificare primit cu cel pe care l-a generat anterior în momentul autentificării cumpărătorului și dacă acestea coincid, trece la procedura de autorizare, ca urmare a căreia înapoiază acceptatorului un răspuns la cererea de autorizare.

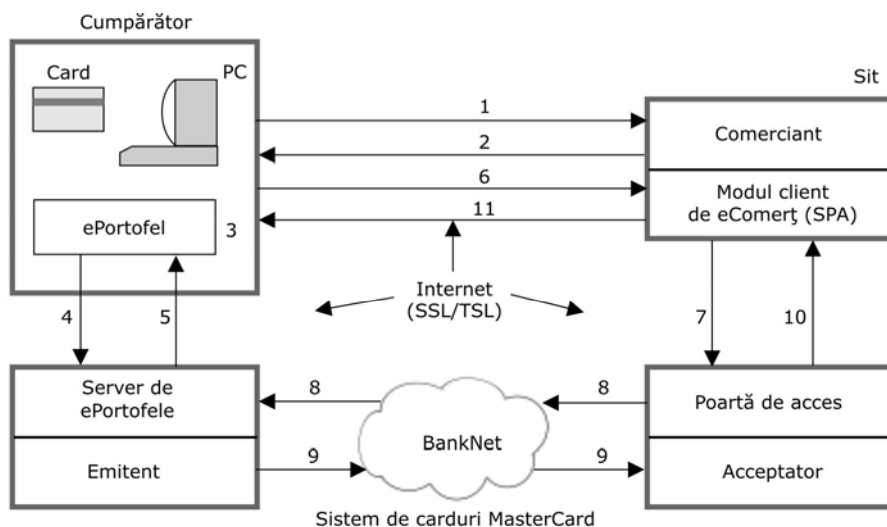


Figura 6-5. Schema de principiu a unei tranzacții MasterCard SecureCode, cu protocolul SPA/UCAF

În figura 6.5 se prezintă simplificat modul de desfășurare a unei tranzacții de eComerț realizate prin tehnologia MasterCard SecureCode, cu protocolul SPA/UCAF. Tranzacția se desfășoară, în mare, în felul următor.

ePortofelul cumpărătorului detectează automat (pas 1) un sit de comerciant membru al sistemului, citește date (pas 2) referitoare la formularul de comandă și identitatea comerciantului de pe situl acestuia, și în momentul inițierii cumpărării, realizează o procedură de cerere de date de autentificare (pas 3) de la cumpărător, după care trimite (pas 4) datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de ePortofele al emitentului. Emitentul autentifică cumpărătorul și generează (pas 5) semnul de autentificare (valoarea AAV) pe care îl trimite (ca pe un certificat de autenticitate) ePortofelului. ePortofelul va transmite acest semn către comerciant și va completa automat toate datele din formularul de comandă al comerciantului (pas 6). Comerciantul va trimite (pas 7) o cerere de autorizare a tranzacției, împreună cu semnul de autentificare (memorat în mesajele ce conțin câmpul UCAF, ale sistemului), către acceptator, care o va expedia (pas 8) mai departe prin rețeaua BankNet a MasterCard către emitent, pe calea de autorizare. Emitentul va compara semnul de autentificare primit acum cu cel generat în pasul 5 și dacă acestea coincid va executa procedura de autorizare și va expedia (pas 9) răspunsul de autorizare către acceptator, de unde va ajunge (pas 10) la comerciant. Comerciantul va memora răspunsul și tranzacția, și va afișa (pas 11) prin navigatorul cumpărătorului, un raport cu rezultatul tranzacției, care se va memora și în ePortofel.

**d) O scurtă comparație a protocoalelor 3-D Secure și SPA/UCAF**

Ambele protocoale sunt mai simple și mai ieftin de implementat decât protocolul SET, însă acesta din urmă asigură maxima securitate. Ambele protocoale fac autentificarea cumpărătorului deținător de card de regulă prin parolă (singurul secret ce dovedește autenticitatea), care e verificată de emitentul cardului, dar emitenții sunt liberi să-și aleagă și alte metode de autentificare întrucât ei generează decizia finală prin care cumpărătorul este declarat autentic și legal deținător al cardului. În ambele protocoale emitenții trebuie să dispună de programe specializate specifice protocolului (server de acces și eventual, de înregistrare, la 3-D Secure, și server de ePortofele la SPA/UCAF), iar comercianții trebuie să-și instaleze un modul client de asemeni specific protocolului. Ambele protocoale asigură un eComert global, internațional, prin faptul că se bazează pe sistemele de carduri Visa și MasterCard care realizează plăți transfrontaliere.

Protocolul SPA/UCAF este mai simplu și mai rapid decât 3-D Secure, pentru că în acesta din urmă autentificarea se desfășoară în mai mulți pași și sunt schimbate mai multe mesaje, toate prin Internet. Deasemeni în 3-D Secure autentificarea se face la fiecare tranzacție, în vreme ce la SPA/UCAF autentificarea se obține o singură dată într-o sesiune de cumpărături, la începutul ei, iar rezultatul este păstrat în ePortofel ceea ce permite efectuarea unei serii întregi de cumpărături la mai multe situri de comercianți, fără ca autentificarea să se mai facă pentru fiecare tranzacție.

În 3-D Secure comerciantul se autentifică explicit față de Directorul sistemului în vreme ce la SPA/UCAF comerciantul se autentifică implicit, doar prin faptul că are un modul client specific care e recunoscut de ePortofel.

Sistemul 3-D Secure este un sistem centralizat, în care toate cererile de autentificare ale tuturor comercianților trec printr-un Director central, aflat în legătură cu toți emitenții și toți acceptatorii participanți la sistem, în vreme ce sistemul SPA/UCAF este descentralizat, iar o autentificare implică numai comunicarea directă între cumpărător și emitentul său, neexistând conceptul de Director.

În sistemul SPA/UCAF "verdictul de autenticitate", păstrat în semnul de autentificare (authentication token), este atașat explicit fiecărei tranzacții, călătorește cu aceasta și e păstrat împreună cu ea, ceea ce reprezintă un lucru util în rezolvarea eventualelor dispute, în vreme ce în 3-D Secure acest lucru nu se întâmplă.

Deosebirea esențială între cele două protocoale constă în faptul că, în cazul lui 3-D Secure, cumpărătorul nu trebuie să facă nici o modificare în calculatorul său

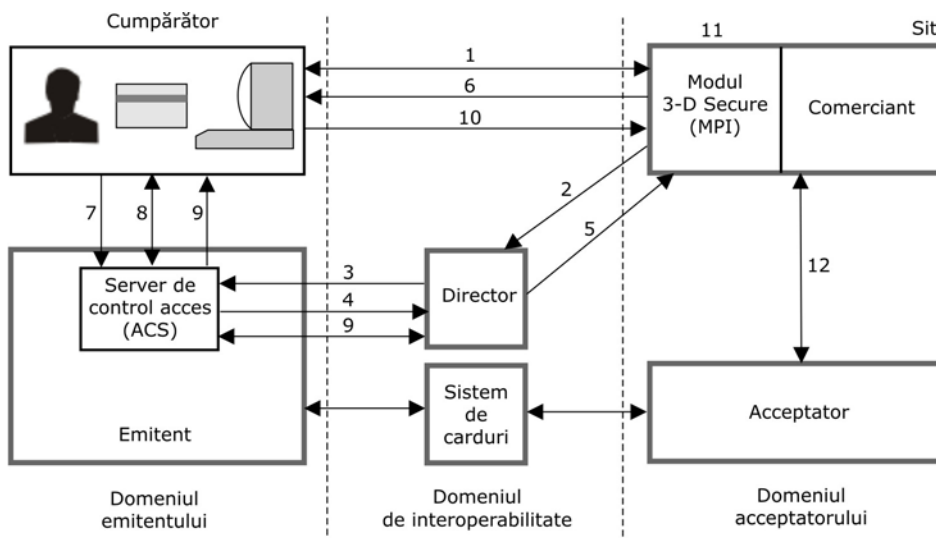


personal, în vreme ce în cazul lui SPA/UCAF acesta trebuie să ceară de la emitentul lui un program (ePortofel sau "SPA applet") pe care trebuie să și-l instaleze singur.

Concluzia finală până în acest moment este aceea că avantajul oferit de 3-D Secure prin faptul că deținătorul de card nu trebuie să aducă nici o modificare în calculatorul său personal, depășește dezavantajele pe care le poate avea față de SPA/UCAF, iar acest lucru îl face să tindă să devină un standard de facto al autentificării în eComerțul prin Internet. Faptul că MasterCard a adoptat 3-D Secure și-l prezintă sub marca proprie este o dovadă în acest sens.

## **6.6. Anatomia unei tranzacții de eComerț care folosește protocolul 3-D Secure**

Pe baza figurii 6.4 care descrie domeniile protocolului 3-D Secure, în figura 6.6 se prezintă anatomia unei tranzacții de eComerț care folosește acest protocol. Schema din figura 6.6 este aceeași și pentru Visa și pentru MasterCard, Directorul din sistem, și sistemul de carduri, putând aparține lui Visa sau lui MasterCard (și altor sisteme ce aderă la acest protocol, cum e cazul sistemului de carduri JCB). În prezent există în paralel un Director Visa și un Director MasterCard.



**Figura 6-6. Anatomia unei tranzacții de eComerț în care se folosește protocolul 3-D Secure**

Tranzacția din figura 6.6 este inițiată de un card prin intermediul unui calculator personal cuplat la Internet care dispune de un navigator major (Internet Explorer sau Netscape). Legăturile prin Internet folosesc protocoale SSL sau TLS și sunt legături sigure, adică confidențialitatea transmisiunii, integritatea mesajelor și autentificarea serverului sunt toate asigurate. Comerciantul se poate autentifica față de Director printr-un certificat, sau printr-un identificator de comerciant (merchant ID) și o parolă (password) ce i-au fost alocate de acceptator, după ce a fost verificat și acceptat de acesta prin contractul de comerciant pe Internet, iar acceptatorul i-a instalat pe sit un modul de comerciant 3-D Secure (MPI), alături de (sau integrat cu) modulul client de eComerț.

Deținătorul de card care dorește să facă tranzacții sigure de eComerț folosind protocolul 3-D Secure, se adresează în acest scop emitentului său. Emitentul, care alege metoda de autentificare pe care o va aplica la momentul tranzacției deținătorului de card, stabilește împreună cu acesta datele de autentificare, de exemplu numele înscris pe card și o parolă. Emitentul ar fi putut cere deținătorului de card să-și cumpere un certificat de autenticitate și să-l instaleze în calculator, sau să folosească un card inteligent (de exemplu Visa VSDC) prin intermediul unui cititor de carduri inteligente cuplat la calculatorul său personal. Apoi emitentul, după verificarea datelor deținătorului, va înscrie numărul de card în Directorul sistemului 3-D Secure indicând și identitatea sa de emitent și adresa de Internet (URL) a serverului său de control de acces, ACS. Din acest moment deținătorul de card și cardul său sunt verificați și înregistrați (enrolled) în sistemul 3-D Secure. În descrierea care urmează vom presupune că deținătorul de card înregistrat se autentifică față de emitent prin nume și parolă.

Din clipa în care cumpărătorul, după ce a ajuns pe situl comerciantului, a ales produsele și le-a pus în coșul de cumpărături, apasă pe butonul care declanșează cumpărarea, mesajele circulă între părțile implicate după cum urmează:

*Pas 1.* Datele privind tranzacția de plată (de identitate deținător, și de card, suma, etc) sunt în posesia comerciantului, care le înregistrează (dar nu le poate accesa).

*Pas 2.* Modulul de comerciant 3-D Secure, MPI (Merchant Plug-In), din situl comerciantului stabilește o legătură SSL/TLS cu Directorul sistemului și îi trimite acestuia numărul de card (PAN-ul) în vederea declanșării autentificării cardului și a deținătorului de card. Modulul MPI se va autentifica față de Director.

*Pas 3.* Directorul va cerceta în evidența proprie dacă numărul de card implicat în plată este înregistrat, și dacă este, determină emitentul și adresa de Internet (URL) a serverului de control de acces (ACS) al emitentului. Dacă cardul deținătorului nu este

Înregistrat în sistemul 3-D Secure, Directorul va trimite un mesaj corespunzător către modulul MPI al comerciantului, iar acesta va sări peste autentificare și va trece la autorizarea tranzacției (pasul 5), realizând o tranzacție de eComerț fără autentificarea deținătorului de card. Dacă cardul este înregistrat, Directorul va verifica cu serverul de control acces al emitentului dacă există o metodă de autentificare pentru card.

*Pas 4.* Serverul de control acces al emitentului verifică dacă numărul de card este într-adevăr cel generat de emitent și dacă există metodă de autentificare pentru acel număr de card, după care trimite răspunsul înapoi la Director.

*Pas 5.* Directorul trimite mai departe răspunsul primit către modulul de comerciant, MPI. Dacă modulul constată din răspuns că metoda de autentificare nu este disponibilă pentru acel număr de card (din variate motive), va trece imediat la autorizarea tranzacției, sărind din nou peste autentificare.

*Pas 6.* Dacă autentificarea se face, modulul MPI va expedia acum o cerere de autentificare a deținătorului de card către serverul de control acces ACS al emitentului cardului. Aceasta se face pasând adresa de Internet a serverului ACS către navigatorul din calculatorul deținătorului de card și redirecționându-l (legătură SSL/TLS) către serverul ACS al emitentului.

*Pas 7.* Serverul ACS recepționează cererea de autentificare și începe procedura de autentificare.

*Pas 8.* Serverul ACS începe un dialog cu deținătorul de card (prin afișarea unui formular marcat ca aparținând emitentului) prin care îi cere acestuia numele și parola. După autentificare serverul ACS va forma un mesaj de răspuns de autentificare, pe care îl semnează cu semnătura sa electronică pentru a garanta integritatea și autenticitatea mesajului.

*Pas 9.* Serverul ACS va trimite acest mesaj către navigatorul calculatorului deținătorului de card pe care îl va direcționa înapoi către modulul MPI al comerciantului. În același timp va trimite datele de autentificare și către Directorul sistemului pentru a fi păstrate în arhiva de autentificări a acestuia. Această arhivă a Directorului este disponibilă (accesul se face după o autentificare) emitenților și acceptatorilor în cazul în care între aceștia se declanșează o dispută privind vreo iregularitate în desfășurarea tranzacției.

*Pas 10.* Modulul MPI din situl comerciantului recepționează mesajul de răspuns la cererea de autentificare.

*Pas 11.* Modulul MPI validează semnătura electronică a serverului ACS al emitentului și verifică integritatea mesajului.

*Pas 12.* Dacă autentificarea deținătorului de card a fost pozitivă, modulul MPI va trece controlul către etapa de autorizare a tranzacției, în care se generează o cerere obișnuită de autorizare care se trimite (legătura SSL/TLS) porții de acces a acceptatorului. Acceptatorul va obține prin sistemul de carduri un răspuns de autorizare de la emitentul cardului, pe care îl va trimite apoi modulului client de eComerț din situl comerciantului, iar acesta la rândul său va afișa, prin navigatorul calculatorului cumpărătorului, o pagină cu raportul privind desfășurarea tranzacției, acest raport fiind echivalent unei chitanțe.

## **6.7. Exemple de comerț electronic actual. Piețe electronice, licitații, furnizori de servicii de plăți pe Internet**

Cele prezentate în subcapitolele anterioare reprezintă modele descriptive și explicative a căror menire este de a permite înțelegerea mecanismelor principale prin care se efectuează comerțul electronic. Sistemele reale existente se bazează pe aceste modele dar diferă mai întotdeauna de ele prin modalitatea de implementare, prin gama de servicii oferite sau prin alte caracteristici tehnice particulare. În cele ce urmează vom face scurte prezentări ale unor sisteme existente, mai cunoscute, incluzând comerțul electronic între consumatori și companii (B2C), între companii (B2B), cel domestic și cel global (internațional sau transfrontalier), piețe electronice cu, și fără, licitații, și companiile care sunt furnizori de servicii de plată pe Internet (PSP, Payment Service Provider, sau IPP, Internet Payment Provider). Exemplele alese au și rolul de a întregi și îmbogăți imaginea asupra comerțului electronic așa cum a fost ea formată numai din prezentarea principiilor și mecanismelor generale.

### **6.7.1. Comerțul electronic între consumatori și companii, sau comerțul electronic cu amănuntul (B2C)**

Acesta este eComerțul care implică numărul cel mai mare de participanți chiar dacă volumul valoric al acestui comerț este nesemnificativ în comparație cu volumul valoric al eComerțului ce are loc între companii (B2B). Totuși, în 2003 în SUA, volumul eComerțului cu amănuntul a atins cifra de peste 75 miliarde de dolari, cu

tendințe de creștere (dar reprezintă numai circa 1% din volumul întregului comerț cu amănuntul).

Includem în aceste cifre și vânzarea pe Internet a serviciilor agențiilor de voiaj (travel agents), agențiilor de rezervări bilete, a produselor pentru adulți, jocuri de noroc, etc. Aceste vânzări prin Internet par a fi foarte concentrate – în ianuarie 2004 peste jumătate din toți utilizatorii americani de Internet (adică peste 83 de milioane) au vizitat cel puțin o dată siteurile eBay sau Amazon (1).

Siturile de comerț sunt foarte variate – de la comercianți ce vând un singur produs sau serviciu, până la siteuri prin care comerciantul prezintă mii de produse (cum ar fi compania engleză de componente electronice Maplin Electronics – [www.maplin.co.uk](http://www.maplin.co.uk) - care oferă peste 12.000 produse distincte).

### **a) Amazon**

Compania americană Amazon ([www.amazon.com](http://www.amazon.com)), cu sediul în Seattle, este cel mai mare comerciant cu amănuntul de pe Internet. În perioada Crăciunului 2003 prin toate siteurile sale aflate în mai multe țări, a primit peste 2 milioane de comenzi într-o singură zi. Începând ca un vânzător de cărți, compania s-a extins mult ajungând în prezent să vândă produse variate (electronice, calculatoare, muzică, software, DVD-uri, etc) și în același timp să ofere spre vânzare prin siteurile sale și produsele altor mari companii cu care a semnat înțelegeri în acest sens, fiind o adevărată piață electronică. De asemenea orice persoană poate vinde produse prin Amazon: își prezintă produsul (cu preț), Amazon pune produsul în vânzare și anunță persoana prin email când produsul a fost vândut, persoana livrează produsul cumpărătorului, Amazon îi expediază banii la o bancă indicată. Siteul prezintă în detaliu această metodologie.

Compania este, în esență, un mare intermediar între cumpărători și producători, întrucât nu deține stocuri de produse, nu este o bancă și nu livrează produse la domiciliu, ci are aranjamente contractuale cu toți participanții la actul de comerț care realizează aceste funcții. Amazon are însă un foarte bine dezvoltat catalog de produse, adică o sofisticată (și interactivă) metodologie de prezentare a produselor și a caracteristicilor acestora, și un bine pus la punct sistem de plată.

Metodele de plată sunt variate – prin carduri (Visa, MasterCard, AMEX, JCB, Dinners Club, Discover), cecuri electronice, ordine de plată electronice (money order, purchase order) și, pentru companii în mod special, prin cont de credit Amazon pe care se emit ordine de cumpărare electronice. Amazon este desigur un comerciant al

unei bănci acceptatoare care e membră a tuturor sistemelor de carduri menționate, și care acceptă și celelalte forme de plată electronică. Prin legături cu astfel de acceptatori aflați în mai multe țări, compania are prezență internațională.

Livrarea produselor cumpărate se face printr-un mijloc care poate fi ales de cumpărător, iar traseul pe care îl urmează produsul către adresa de livrare specificată în ordinul de cumpărare poate fi urmărit prin Internet pe situl companiei de transport alese – UPS, DHL, FedEx, Eagle, Airborne Express și altele.

### **b) *InterActivCorp, IAC – agent de călătorii pe Internet***

Compania americană IAC este cel mai mare agent de servicii de călătorie, este proprietara companiilor Expedia.com (www.expedia.com) și Hotels.com (www.hotels.com) și a vândut pe Internet rezervări de călătorie (transport, hotel, etc) în valoare de peste 10 miliarde de dolari în 2003. În același an peste 35 de milioane de americani i-au folosit serviciile.

Produsul principal vândut este "pachetul de călătorie" (travel package) care cuprinde variate combinații de călătorii – zboruri, hoteluri, închirieri mașini, tururi de vizitare, bilete de spectacole, etc., acestea putând fi personalizate după dorința cumpărătorului.

Plata se face prin toate cardurile majore – Visa, MasterCard, AMEX, Dinners Club, Discover.

Alți mari furnizori de servicii de călătorie prin Internet sunt Travelocity și Orbitz din SUA, Ebookers și Opodo din Anglia, sau pentru rezervări hotel Hilton, Marriott și Hyatt din SUA, Accor Hotels din Franța și Le Meridien din Anglia.

### **c) *Google, Yahoo!, MSN și AOL***

Aceste companii nu sunt numai celebre motoare de căutare pe Internet ci și participanți direcți la eComerț (a se vedea de exemplu situl Microsoft MSN, www.msn.com, care este și un portal-piață electronică de eComerț).

Serviciile lor de căutare sunt folosite din ce în ce mai mult pentru a descoperi și cumpăra produse pe Internet. Se oferă și serviciul de a compara prețurile afișate de mai mulți vânzători pentru un același produs (a se vedea serviciul Froogle oferit de Google, fie prin buton, fie direct la adresa <http://froogle.google.com>).

### **6.7.2. Piețe electronice, licitații electronice**

Piețele electronice sunt portaluri, adică situri de mari dimensiuni, care oferă servicii complexe asemănătoare unor piețe reale – prezentarea produselor mai multor vânzători, posibilitatea de a organiza licitații pentru cumpărarea unui produs, mijloace variate de plată și de livrare. Piața electronică este esențialmente un comerciant al unei bănci acceptatoare care acceptă plăți prin cardurile majore sau prin alte mijloace de plată electronică.

Piețele electronice permit ambele tipuri de eComerț – cu amănuntul (B2C), sau între companii (B2B) și pot fi publice, universale, accesibile oricărui cumpărător și vânzător, sau specializate (și oarecum închise, existând numai pentru cei din domeniu) cum e cazul între grupuri de companii aflate într-o relație de achiziție-furnizare (supply chain, lanțul de aprovizionare) pe tipuri de produse, și bazate pe sisteme și proceduri specializate, cu rețele proprii de telecomunicații sau sisteme proprii (bazate pe software specific) de eComerț.

#### ***a) Piețe electronice specializate pentru comerțul electronic între companii (B2B)***

Un astfel de mare sistem specializat de eComerț între companii este, de exemplu, Chem Connect ([www.chemconnect.com](http://www.chemconnect.com)) pentru produse chimice, plastic și combustibili. Lozinca companiei este "conectăm cumpărători și vânzători din întreaga lume". Această piață cuprinde peste 9000 de companii membre din peste 150 de țări, iar vânzările totale din 2002 au atins cifra de afaceri de 9 miliarde de dolari. Compania se declară cea mai mare piață electronică globală de eComerț între companii și oferă și serviciul de licitație prin Internet. Compania dispune de un Centru de telecomunicații propriu (Central Connectivity Hub) prin intermediul căruia toți membrii se pot lega între ei, și pot schimba orice fel de informații – de piață, de licitație, de plată și livrare, etc.

În eComerțul între companii plata efectivă se poate face și prin mijloacele tradiționale, ne-electronice. În acest caz numai prima parte a actului de comerț se desfășoară prin Internet, în piața electronică – prezentarea produselor, licitația, stabilirea condițiilor de plată, asigurare și livrare, etc.

Există de asemenea companii care oferă soluții și aplicații speciale (software) prin care se pot implementa piețe electronice de specialitate (vânzare, cumpărare, licitație, plată, livrare, etc) per domenii – de exemplu Forest Industry Network

(www.forestindustry.com) pentru companiile din domeniul industriei forestiere, sau Farms Technology, LLC (www.farmstech.com) pentru domeniul agricol (ambele din SUA) (14).

### ***b) Piețe electronice deschise pentru comerțul electronic între companii (B2B)***

Crearea unei piețe electronice universale, deschise, nespecializate pe un domeniu sau altul, este o problemă mai dificilă. Trei sisteme sunt deja cunoscute în această privință – sistemul WWRE, sistemul Bolero și sistemul Tradecard. Toate urmăresc să asigure toate facilitățile necesare desfășurării unui comerț pe Internet între companii, indiferent de țara de origine a companiei și de natura produselor vândute sau cumpărate.

Sistemul WWRE (Worldwide Retail Exchange, www.wwre.com) este dedicat comerțului cu amănuntul între companii. Sistemul are în prezent 64 de companii membre (între care Tesco, JCPenney, GlaxoSmithKline, Marks&Spencer) din toată lumea și peste 100.000 de furnizori. Companiile membre își pot prezenta cataloagele de produse și pot licita și negocia între ele prin intermediul platformei Exchange bazate pe software-ul "B2B Commerce Platform" al companiei Ariba și "Trade Matrix" al companiei i2.

Sistemul Bolero creat de compania americană Bolero Internațional Ltd. (www.bolero.net), în parteneriat cu celebra cooperativă bancară SWIFT (Society for Worldwide Interbank Financial Telecommunications), crează o comunitate de participanți internațională care pot schimba între ei, prin protocoale sigure, toate informațiile necesare actului de comerț.

Sistemul Tradecard creat de compania americană TradeCard Inc. din New York (www.tradecard.com) oferă, în esență, același lucru ca sistemul descris anterior, și asigură atât plăți domestice cât și transfrontaliere (14).

### ***c) Piețe electronice publice, deschise. Licitații***

Aceste piețe sunt deschise oricărui vânzător sau cumpărător, persoană fizică (consumator) sau companie, și oricărui produs sau serviciu, de la cărți vechi și muzică până la avioane cu reacție. Există multe astfel de piețe ca de exemplu eBay, Amazon, MSN, Barclaycard sau Yahoo!. Vom face o scurtă prezentare a celei mai cunoscute, eBay.



**eBay** (www.ebay.com) este cea mai mare și cea mai cunoscută piață electronică din lume. În primul trimestru din 2004 prin eBay s-au vândut produse și servicii în valoare de 8 miliarde de dolari. Veniturile nete așteptate ale companiei eBay pe 2004 sunt de circa 3 miliarde de dolari, profitul net pe 2003 fiind de 442 milioane de dolari. Comunitatea eBay are peste 100 de milioane de membri înregistrați în întreaga lume. Oricine dorește să participe, ca vânzător sau cumpărător, trebuie să se înregistreze ca membru. În fiecare zi se prezintă spre vânzare milioane de articole. Compania are situri locale (sub diverse nume) în 28 țări, în fiecare țară fiind adaptată la specificul țării respective - în Franța se vinde îndeosebi vin, iar în Coreea de Sud îndeosebi brânză, pe lângă desigur orice alt produs. Situl EachNet din China, aparținând eBay, are circa 2,4 milioane de membri. Compania oferă comercianților și serviciul de găzduire de magazine virtuale proprii, având în prezent peste 150.000 de astfel de magazine, care vând orice (1).

Cumpărătorii pot cumpăra produse sau servicii la prețuri variabile, prin licitație, sau la prețuri fixe, în funcție de oferta vânzătorului. Plata se poate face în felul în care convin cele două părți sau prin Internet prin faimosul serviciu al companiei, PayPal, care aparține lui eBay din 2002. PayPal cere numai adresă de email și un cont de membru deschis la PayPal (care nu este o bancă) și asigură plăți între oricare doi astfel de membri. Această facilitate este extrem de atractivă pentru companiile vânzătoare care nu mai trebuie să-și deschidă un cont de comerciant pe Internet la o bancă acceptatoare, ci pot avea contul propriu la orice bancă doresc.

O licitație între un cumpărător și un vânzător are loc, în esență, în felul următor.

*Cumpărare.* Cumpărătorul introduce suma maximă pe care e dispus s-o dea pentru produsul sau serviciul dorit, această sumă rămânând secretă față de alți cumpărători participanți la licitație. eBay urmărește toate ofertele și o reține pe cea mai mare existentă la sfârșitul perioadei de licitație (de regulă 7 zile). Câștigătorul licitației intră în contact direct cu vânzătorul, cumpărătorul plătește și vânzătorul expediază produsul. Plata se poate face prin card dacă se folosește serviciul PayPal.

*Vânzare.* Produsul oferit este descris, inclusiv prin fotografii, iar vânzătorul indică un preț de pornire și durata licitației. Cumpărătorii care licitează pot vedea în orice moment care este oferta maximă curentă; dar numai vânzătorul poate vedea toate ofertele. Oricare cumpărător poate să-și crească oferta pe durata licitației întrucât poate vedea în permanență care este prețul cel mai mare oferit curent.

Atât licitatorii cât și vânzătorii își pot verifica reciproc reputația pentru a stabili încrederea de care e nevoie pentru asigurarea vânzării. Un vânzător poate refuza o

oferă dacă nu are încredere în licitantul care a făcut-o. eBay poate cere celor care se înregistrează să-și dea o adresă de email prin care li pot cere informații suplimentare.

### **6.7.3. Furnizorii de servicii de plată prin Internet**

Piețele electronice și siturile simple de comerciant își afișează mijloacele proprii prin care se poate face plata. Cel mai frecvent mijloc electronic de plată este cardul, urmat de cecul electronic și ordinele de plată de diverse forme. Plata se poate face însă și printr-o companie specializată care oferă servicii de plată (IPP, Internet Payment Provider, sau PSP, Payment Service Provider).

Vom face o scurtă prezentare a celor mai cunoscute servicii de plată prin Internet - PayPal, Yahoo!PayDirect, VeriSign și Bibit (15).

#### **a) PayPal**

Compania americană PayPal, cu sediul în California, este cel mai mare furnizor de servicii de plată prin Internet, având peste 45 de milioane de membri cu cont PayPal, aflați în 45 de țări și efectuând transferuri anuale de peste 17 miliarde de dolari. Serviciul de plată PayPal admite plăți și prin telefonie mobilă cu protocolul WAP. Compania a fost cumpărată în 2002 de eBay pentru a-i servi drept metodă principală de plată între cumpărători și vânzători. Obiectivul declarat al companiei este de a deveni un standard de facto global pentru plățile prin Internet, iar compania intenționează să se extindă cu situri locale în țările importante din Europa și Asia.

În esență, PayPal permite oricărui cumpărător sau companie, care dispune de o adresă de email, să trimită și să primească bani în timp real. Pentru aceasta, fiecare doritor se înregistrează ca membru, și i se alocă un cont de membru PayPal la o bancă a companiei. Banca companiei este un acceptator în toate sistemele mari de plată prin carduri, cecuri electronice, etc. Acest cont servește ca intermediar între contul unui expeditor și contul unui receptor, conturi care pot fi deschise la orice bancă. PayPal nu este o bancă ci doar un intermediar care transmite bani între conturi aflate în diferite bănci din lume prin intermediul unui cont propriu de tranzit. Serviciul este deosebit de util micilor comercianți și persoanelor fizice, care pot primi, sau cere, plăți pentru produsele vândute prin Internet fără a mai fi nevoie să-și

deschidă un cont de comerciant pe Internet la o bancă acceptatoare care să facă parte din unul, sau mai multe, sisteme de plăți prin carduri, cecuri electronice, etc.

Transferul de bani între entități care sunt cumpărători sau vânzători, persoane fizice sau companii, se poate face ca urmare a unui act de comerț, sau ca un simplu transfer de fonduri între două conturi. Serviciul este folosit pentru transferul de fonduri în toate combinațiile - între persoane (P2P), între companii (B2B), între persoane și companii (B2C) și chiar pentru plata taxelor în SUA (P2G).

Transferul poate fi inițiat fie de expeditor printr-o operație de Trimitere de bani (Send money), fie de receptor printr-o operație de Cerere de bani (Request money) echivalentă cu trimiterea unei facturi care trebuie onorată. Receptorii plătesc un comision de 0,3 USD plus 2,2%...2,9% din suma primită, în funcție de țară. Se mai adaugă 2,5% dacă are loc o conversie de valută. Pentru a încuraja microplățile, de exemplu pentru cumpărarea (download) de muzică digitală, PayPal a introdus tarife foarte mici pentru astfel de cumpărături imediate.

Trimiterea de bani către un receptor se desfășoară în felul următor. De la calculatorul expeditorului cuplat la [www.paypal.com](http://www.paypal.com) se introduce într-un formular adresa de email a receptorului și suma de expediat, specificându-se dacă plata se face dintr-un cont de card sau un cont bancar. După plată, receptorul va primi imediat un mesaj de email prin care este anunțat că a primit banii. Acest mesaj conține o legătură (link) la PayPal unde receptorul își poate vedea contul de membru cu suma tocmai intrată. Receptorul poate cere apoi transferul sumei din contul său de membru PayPal către contul său deschis la banca proprie, operație care este efectuată de PayPal prin transfer electronic interbancar sau prin eliberarea unui cec.

PayPal va obține mai întâi banii din contul de card al celui care trimite, și abia apoi îi va depune în contul de membru PayPal al receptorului. Pentru aceasta PayPal va executa o tranzacție de tip POS cu datele de card și va obține de la emitent autorizarea și apoi transferul de fonduri în propria bancă PayPal.

Un avantaj important al acestei metode de plată este faptul că receptorul, dacă este un comerciant pe Internet, nu vede detaliile cardului de plată al cumpărătorului, ceea ce micșorează serios temerile uzuale ale deținătorilor de carduri.

Cererea de bani de la un membru se desfășoară similar - se furnizează în formularul de plată afișat adresa de email a plătitorului și suma de bani cerută (echivalent cu trimiterea unei note de plată). Plătitorul va primi un mesaj de informare și instrucțiuni asupra modului de plată.

### **b) Yahoo!PayDirect**

Serviciul de plăți PayDirect al companiei Yahoo este similar lui PayPal și servește în special microplăților (1 cent...10 dolari) între persoane (P2P). Membrii cu adresă de email și domiciliul în SUA se înregistrează, primesc un cont de membru PayDirect și un portofel electronic (Yahoo!Wallet) în care sunt păstrate informațiile de plată - datele de card, adresa de facturare și de livrare. Portofelul electronic va fi folosit pentru completarea automată a formularului de plată afișat. Contul de membru PayDirect se alimentează și se debitează prin transfer bancar inițiat de membru prin operații speciale efectuate de PayDirect (Add Money și Withdraw Money).

Contul de membru e apoi folosit pentru a expedia sau cere bani (operațiile Send Money și Request Money) către, sau de la, orice alt membru din SUA. În cazul unei cereri de bani pentru un produs sau serviciu vândut, PayDirect va genera o factură electronică pe care o va trimite plătitorului.

Ca o măsură de securitate PayDirect va verifica adresa declarată de membru prin trimiterea unei scrisori prin poștă de la care așteaptă un răspuns. În același scop PayDirect va face și două mici depuneri (sub 1 dolar) în contul membrului deschis la banca proprie și când va primi confirmarea depozitelor va ști că acel cont declarat de membru există (confirmarea e dată de membru prin mesaj email). Conturile de membru PayDirect sunt păstrate la banca internațională HSBC, cu care Yahoo are un parteneriat.

### **c) VeriSign**

Compania americană VeriSign, Inc., cu sediul în California, este o companie binecunoscută pe Internet mai ales prin faptul că este o Autoritate de Certificare care eliberează certificate de autenticitate pentru serverele care stabilesc legături de telecomunicații prin protocolul SSL/TLS, și în special pentru serverele care găzduiesc situri de comercianți. Acest lucru oferă cumpărătorilor garanția că serverul pe care se află situl comerciantului este într-adevăr cine apare că este, iar comercianții găzduiți au fost verificați de compania care deține serverul și sunt și ei cine par a fi.

VeriSign este un mare furnizor de servicii de plată pentru siturile de comercianți, asigurând procesarea a peste 30% din toate tranzacțiile de eComert din America de Nord.

În esență VeriSign (Centrul de Operații, dotat cu servere sigure) este un procesator independent de plăți prin carduri, cecuri electronice și transferuri bancare ACH (Automated Clearing House), care se interpune în poziția de poartă de plăți (payment gateway) între siturile de comercianți și procesatorii mari de tranzacții cu carduri din SUA care procesează pentru aproape toate băncile americane acceptatoare. Astfel de mari procesatori independenți sunt de exemplu First Data, Paymentech, Nova și TeleCheck (după principiul ilustrat în figura 6.2, VeriSign fiind amplasat între norul Internet și procesatori). VeriSign este conectat la acești procesatori prin linii private sigure.

Serviciul de plată reprezentativ care este oferit comercianților este Payflow Pro. Comercianții care cumpără acest serviciu (prețul este de 250 dolari pentru instalare plus un comision lunar de 60 de dolari; se adaugă costuri pentru servicii suplimentare) își instalează o aplicație (modul XML) client, de circa 400 kbytes, care va primi informațiile de plată furnizate de cumpărător în formularul afișat și le va trimite la VeriSign. Centrul VeriSign va trimite cererea de autorizare (pentru plata prin card și cec electronic) către procesatorul ce lucrează pentru acceptatorul comerciantului, și va înapoia răspunsul de autorizare primit către clientul din situl de comerciant. Serviciul poate asigura și prelucrarea tranzacțiilor care autentifică cumpărătorul prin sistemele Verified by Visa (3-D Secure) și SecureCode.

O variantă mai simplă a tehnologiei de plată Payflow este serviciul Payflow Link prin care comerciantul adaugă în situl său doar o legătură (link) HTML la VeriSign, care îi va furniza formularul de plată la fiecare tranzacție și va prelua apoi prelucrarea tranzacției introduse.

VeriSign oferă și un serviciu de monitorizare a fraudei (fraud screening) care se face în timp real prin "filtrarea" ordinelor de plată ale cumpărătorului după astfel de criterii ca - valoare mare, număr mare de articole cumpărate într-o singură tranzacție, țara de origine a cumpărătorului, și altele (în total 19 criterii). Se calculează un scor total final pe toate riscurile, iar comerciantul poate refuza (prin setarea unui parametru în modulul client) ordinul de cumpărare, chiar dacă tranzacția a fost autorizată de emitent.

Serviciile de plăți ale lui VeriSign sunt atrăgătoare în special pentru noii comercianți pe Internet, cărora le oferă facilități și consultanță în toate etapele

constituirii unei întreprinderi de comerț pe Internet - sugerează furnizori siguri de servicii de Internet (ISP) care găzduiesc situri de comerț, procesatori sau bănci acceptatoare care admit conturi de comerciant, serviciile de plată Payflow, evaluarea în timp real a riscului unei tranzacții, centre de asistență permanentă, etc.

#### **d) Bibit**

Compania europeană Bibit Global Payment Services, cu sediul în Olanda și filiale în alte țări europene, este un furnizor de servicii de plată (PSP, Payment Service Provider) orientat în mod special pe plățile transfrontaliere (eComerț internațional) care se remarcă prin bogăția extraordinară a metodelor de plată - peste 70 de metode, purtând specificul multor țări.

Scopul lui Bibit este de a da posibilitatea unui cumpărător dintr-o țară să plătească produsele unui comerciant pe Internet din altă țară, folosind metodele de plată care sunt obișnuite în țara cumpărătorului. Printre multele metode de plată, atât în timp real cât și tradiționale, se află transferuri bancare electronice, debit direct, carduri (incluzând portomenul electronic), plăți prin telefonul mobil și plăți între persoane (prin PayPal de exemplu, care e una din metodele de plată).

Bibit oferă clienților săi, comercianții pe Internet, un serviciu complet, prin externalizare - noii comercianți pot semna cu Bibit un contract de comerciant pe Internet (banca acceptatoare este a lui Bibit), iar compania le oferă serviciile complete de eComerț prin centrul său de procesare, și aplicațiile Java instalate în situl comerciantului. Compania este conectată direct cu un mare număr de bănci din toată lumea și poate asigura autorizarea unei tranzacții în câteva secunde.

O tranzacție tipică de cumpărare pe un sit de comerciant Bibit se desfășoară în felul următor: cumpărătorul umple căruciorul de cumpărături cu produsele dorite și dă ordinul de cumpărare; comerciantul (aplicația client din sit) afișează o listă de metode de plată specifică țării cumpărătorului, din care cumpărătorul face o alegere; apar o serie de formulare specifice metodei de plată alese, iar cumpărătorul le completează și acceptă plata (dialogul se poartă în una din 6 limbi de circulație internațională, aleasă de cumpărător); tranzacția e trimisă la centrul Bibit care va obține autorizarea de la instituția financiară implicată după care anunță automat cumpărătorul și comerciantul; dacă tranzacția nu a fost acceptată, cumpărătorului i se oferă alegerea unei alte metode de plată.

Bibit oferă un sistem de plăți complex și foarte puternic. Printre marii clienți ai companiei se numără companiile Dell, NEC, Expedia și Yahoo.

## **6.8. Comerțul electronic în România**

Comerțul electronic în România s-a dezvoltat rapid în ultimii ani și apare în prezent sub trei forme principale: a) comercianți cu cataloage de produse pe Internet și plata la livrare; b) comercianții care acceptă plata prin carduri în timp real prin protocolul 3-D Secure, și c) situri de licitație electronică destinate achizițiilor administrației publice.

Un caz aparte de comerț electronic îl reprezintă tranzacționarea pe Internet a acțiunilor societăților de la Bursa de Valori București prin intermediul Societăților de Servicii de Investiții Financiare, SSIF (16).

Recent compania românească GeCAD ePayment International SRL, membră a Grupului GeCAD, în înțelegere cu Banca Țiriac, a anunțat că oferă comercianților servicii complete care dau acestora posibilitatea comodă de a-și deschide magazine virtuale și de a accepta plata în timp real prin carduri Visa și MasterCard în sistemul 3-D Secure, sau prin transfer și ramburs ([www.epayment.ro](http://www.epayment.ro)).

### ***a) Comercianții cu cataloage de produse pe Internet și plata la livrare***

Aceasta este prima formă de comerț electronic prin Internet apărută în România. Există în prezent un număr relativ mare de astfel de comercianți (17).

Comercianții prezintă pe sit un catalog de produse, cu descrieri și preț, iar cumpărătorul poate folosi un cărucior de cumpărături, după care lansează ordinul de cumpărare. Livrarea se face la domiciliu sau produsele pot fi ridicate de la sediul comerciantului. Unele situri fac doar prezentare de produse fără posibilitatea de a da comandă.

Plata se face la livrarea produselor prin numerar la sediul comerciantului sau al cumpărătorului, prin cec, transfer bancar, mandat poștal, în rate, și chiar prin card, în momentul livrării, printr-un POS mobil.

### ***b) Comercianți pe Internet cu plata prin card***

Începând cu anul 2004 trei mari bănci acceptatoare și emitente (BCR, Raiffeisen Bank, Banca Tîriac) și o bancă emitentă (AlphaBank) oferă comerț electronic prin Internet cu plata în timp real prin carduri Visa și MasterCard, folosind protocolul 3-D Secure sub siglele Verified by Visa și Secure Code, respectiv. Procesarea acestor tranzacții este asigurată de Romcard care este procesatorul celor trei mari bănci și care oferă acest serviciu, în principiu, și altor bănci. Certificarea Romcard de către Visa și MasterCard în calitate de procesator 3-D Secure este o premieră europeană, realizată prin proiecte pilot de cele două mari sisteme de carduri, întrucât până în prezent procesarea 3-D Secure era realizată de fiecare bancă în parte. Se poate spune că, datorită Romcard, România dispune în prezent de eComerț modern, cu un grad de siguranță mult sporit. Vom reveni în capitolul 12.2 asupra acestei probleme.

Comercianții români care doresc să folosească sistemul vor încheia contracte de comerciant pe Internet cu una din cele trei bănci acceptatoare, iar cumpărătorii care doresc să folosească carduri Visa sau MasterCard emise în România de cele patru bănci menționate pentru a face cumpărături în toată lumea prin acest sistem se vor adresa acestor bănci pentru înregistrarea în sistem (18).

### ***c) Achiziții electronice prin licitație în administrația publică***

În cadrul Sistemului Electronic Național, SEN, promovat de Ministerul Comunicațiilor și Tehnologiei Informației sunt dezvoltate o serie de servicii electronice de mare interes pentru cetățeni și pentru administrația publică din România. Un astfel de serviciu este Sistemul Electronic de Achiziții Publice (19).

Acest sistem permite cumpărătorilor, numiți autorități contractante (unități ale administrației publice) să organizeze licitații pe produse pentru achiziția la cel mai bun preț de la vânzătorii numiți ofertanți. Metodologia este asemănătoare, în principiu, celei descrise în capitolul precedent pentru sistemul eBay și este descrisă pe situl guvernamental [www.e-licitatie.ro](http://www.e-licitatie.ro).

Licitația electronică publică este organizată pe două categorii de produse - produse standardizate și produse complexe.

## **Note și bibliografie**



1. The Economist, May 15-21, 2004, A perfect market, A survey of e-commerce, pag.9, pag. 1-16.
2. Electronic Commerce and Development Report 2001, UNCTAD, United Nations, UNCTAD/SDTE/ECB/1, [www.unctad.org/ecommerce](http://www.unctad.org/ecommerce). A se vedea și versiunea raportului din 2003 (UNCTAD/SDTE/ECB/2003/1).
3. Ministerul Comunicațiilor și Tehnologiei Informațiilor, Statistici, [www.mcti.ro](http://www.mcti.ro).
4. MasterCard e-B2B Solutions, The Choice Strategy for Seizing a \$30 Trillion Opportunity, [www.mastercardbusiness.com](http://www.mastercardbusiness.com).
5. BCR – [www.bcr.ro](http://www.bcr.ro), Banc Post – [www.bancpost.ro](http://www.bancpost.ro). A se vedea și revista eFinance, Carduri virtuale pentru o lume virtuală, Nr.39, noiembrie 2003.
6. Sistemele mari de plăți prin carduri au fost realizate inițial pe baza modelului de plată cu un card cu bandă magnetică. Dezvoltările ulterioare constând în plățile cu carduri cu cip și plățile cu card din eComerț sau mComerț, au constat, esențialmente, în "reducerea" noilor tipuri de tranzacții la modelul tranzacției generate de un card cu bandă magnetică pentru a putea fi procesate de sistemele existente, cu extensiile necesare. Astfel o tranzacție cu un card cu cip, sau de comerț electronic sau mobil, conține toate datele unei tranzacții cu bandă magnetică la care se adaugă, sau din care lipsesc, câteva date suplimentare și specifice.
7. VeriSign Inc., [www.verisign.com/products/](http://www.verisign.com/products/), What Every Merchant Should Know About Internet Fraud, 2003.
8. Electronification of Payments in Europe, European Central Bank (ECB), Monthly Bulletin, May 2003.
9. Implementing Electronic Card Payment Systems, Cristian Radu, Artech House, Computer Security Series, 2003, [www.artechhouse.com](http://www.artechhouse.com).
10. The SSL 3.0 Protocol, Freier A. Karlton P., Kocher P., Internet-Draft, Nov. 1996. The TLS Protocol - Version 1.0, Dierks T., Allen C., Internet-Draft, Nov. 1997
11. Set Secure Electronic Transactions, LLC, sau SET Co, oferă documentația completă a standardului (The SET Standard Book 1,2,3), [www.setco.org](http://www.setco.org)
12. Visa 3-D Secure System Overview, [http://international.visa.com/fb/paytech/secure/pdfs/3DS\\_70015\\_01\\_System\\_Overview\\_external\\_v1.0.2\\_May\\_2003.pdf](http://international.visa.com/fb/paytech/secure/pdfs/3DS_70015_01_System_Overview_external_v1.0.2_May_2003.pdf).
13. MasterCard Secure Code este descris în mai multe locuri: [www.mastercardmerchant.com/securecode/getstarted.html](http://www.mastercardmerchant.com/securecode/getstarted.html); [www.mastercardintl.com/docs/ecaf\\_sell\\_sheet\\_final.pdf](http://www.mastercardintl.com/docs/ecaf_sell_sheet_final.pdf); [www.mastercardintl.com/docs/secure\\_code\\_user\\_brochure.pdf](http://www.mastercardintl.com/docs/secure_code_user_brochure.pdf);

[www.mastercardintl.com/docs/secure\\_merchant\\_brochure.pdf](http://www.mastercardintl.com/docs/secure_merchant_brochure.pdf);

[www.mastercardintl.com/docs/final\\_ucaf\\_smart\\_card\\_trifold.pdf](http://www.mastercardintl.com/docs/final_ucaf_smart_card_trifold.pdf).

14. Informațiile asupra acestor sisteme sunt generale. Sistemele fiind mai speciale, informațiile complete sunt accesibile numai membrilor.

15. [www.paypal.com](http://www.paypal.com), [www.paydirect.com](http://www.paydirect.com), [www.verisign.com](http://www.verisign.com), [www.bibit.com](http://www.bibit.com).

16. SSIF care oferă această facilitate sunt Vanguard, [www.vanguard.ro](http://www.vanguard.ro), Prime Tranzaction, [www.primet.ro](http://www.primet.ro), Estinvest, [www.estinvest.ro](http://www.estinvest.ro), și Romintrade, [www.onlinebroker.ro](http://www.onlinebroker.ro).

17. Câteva exemple alese la întâmplare: [www.magazinultau.ro](http://www.magazinultau.ro); [www.comenzi.ro](http://www.comenzi.ro); [www.unireashop.ro](http://www.unireashop.ro); [www.flanco.ro](http://www.flanco.ro); [www.dol.ro](http://www.dol.ro); [www.flamingo.ro](http://www.flamingo.ro) (ultimile două sunt situri 3-D Secure).

18. [www.no-cash.ro](http://www.no-cash.ro), 2004 - *Interviul lunii ianuarie* cu Marin Mitroi, director Romcard și "Soluții de plată on-line pentru magazine virtuale", Conferință asupra comerțului electronic în România, 26.02.2004, Hotel Athenee Palace, eveniment No-Cash. Metodologia de folosire a sistemului de către comercianți și cumpărători este descrisă de exemplu pe situl BCR, [www.bcr.ro](http://www.bcr.ro), secțiunea e-comm.

19. MCTI – [www.mcti.ro](http://www.mcti.ro), [www.e-guvernare.ro](http://www.e-guvernare.ro), [www.e-licitatie.ro](http://www.e-licitatie.ro).