**Protocolul SET şi sisteme electronice de plăţi**

**Comert electronic** inseamna, in acceptiune "traditionla", utilizarea in retele cu valoare adaugata a unor aplicatii de tipul transferului electronic de documente (EDI), a comunicatilor fax, codurilor de bare, transferului de fisiere si a postei electronice. Extraordinara dezvoltare a interconectivitatii calculatoarelor in Internet, in toate segmentele societatii, a condus la o tendinta tot mai evidenta a companiilor de a folosi aceste retele in aria unui nou tip de comert, comertul electronic in Internet, care sa apeleze - pe langa vechile servicii amintite - si altele noi. Este vorba, de exemplu, de posibilitatea de a se efectua cumparaturi prin retea, consultand cataloage electronice "on" pe Web sau cataloage "off" pe CD-ROM si platind prin intermediul cartilor de credit sau a unor portmonee electronice. Pentru altii, comertul Internet reprezinta relatiile de afaceri care se deruleaza prin retea intre furnizori si clienti, ca o alternativa la variantele de comunicatii "traditionale" prin fax, linii de comunicatii dedicate sau EDI pe retele cu valoare adaugata. In fine, o alta forma a comertului Internet implica transferul de documente - de la contracte sau comenzi pro forma, pana la imagini sau inregistrari vocale.

Acest nou tip de comert a stimulat insa cererea pentru noi metode adecvate de plata. In cadrul noului concept de "sat global" (global village), dezvoltarea unor activitati comerciale intre participanti situati la mari distante geografice unii de altii nu poate fi conceputa fara folosirea unor sisteme electronice de plati. Aceste noi mijloace de plata permit transferarea comoda, sigura si foarte rapida a banilor intre partenerii de afaceri. De asemenea, inlocuirea monedelor si bancnotelor (actualele forme traditionale de numerar) prin ceea ce denumim bani electronici conduce, pe langa reducerea costurilor de emitere si mentinere in circulatie a numerarului, si la o sporire a flexibilitatii si securitatii sistemelor de plati.

In domeniul mijloacelor electronice de plata, cercetarile sun in plina desfasurare. Exisa numeroase sisteme in curs de experimentare, altele abia au fost cercetate si supuse analizei. Este normal ca prudenta si securitatea sa fie cuvintele cheie ale acestor demersuri. Vom prezenta in continuare cateva sisteme de plati electronice mai cunoscute, grupate in patru categorii:

* sisteme cu carduri bancare
* sisteme on-line
* microplati
* cecuri electronice

**Protocolul SET (Secure Electronic Transaction)**

Multe cumparari de bunuri si servicii prin Internet se fac platindu-se cu carduri bancare obisnuite (Visa, MasterCard etc.). Insa tranzactiile cu carduri contin informatii confidentiale privind cardul si informatiile personale ale clientilor, informatii ce pot fi interceptate in timpul transmisiei prin Internet. Fara un soft special, orice persoana care monitorizeaza traficul pe retea poate citi continutul acestor date confidentiale si le poate folosi ulterior Este necesara elaborarea unor standarde specifice sistemelor de plati, care sa permita coordonarea partilor legitime implicate in transfer si folosirea corecta a metodelor de securitate.

In 1996, MasterCard si Visa au convenit sa consolideze standardele lor de plati electronice intr-unul singur, numit SET (Secure Electronic Transaction). Protocolul SET isi propune sapte obiective de securitate in e-commerce:

1. Sa asigure confidentialitatea instructiunilor de plata si a informatiilor de cerere care sunt transmise odata cu informatiile de plata.
2. Sa garanteze integritatea tuturor datelor transmise.
3. Sa asigure autentificarea cumparatorului precum si faptul ca acesta este utilizatorul legitim al unei marci de card.
4. Sa asigure autentificarea vanzatorului precum si faptul ca acesta accepta tranzactii cu carduri prin relatia sa cu o institutie financiara achizitoare.
5. Sa foloseasca cele mai bune metode de securitate pentru a proteja partile antrenate in comert.
6. Sa fie un protocol care sa nu depinda de mecanismele de securitate ale transportului si care sa nu impiedice folosirea acestora.
7. Sa faciliteze si sa incurajeze interoperabilitatea dintre furnizorii de soft si cei de retea.

Aceste cerinte sunt satisfacute de urmatoarele caracteristici ale acestei specificatii:

**Confidentialitatea informatiei** - Pentru a facilita si incuraja comertul electronic folosind cartile de credit, este necesara asigurarea detinatorilor de cartele ca informatiile de plata sunt in siguranta. De aceea, contul cumparatorului si informatiile de plata trebuie sa fie securizate atunci cand traverseaza reteaua, impiedicand interceptarea numerelor de cont si datele de expirare de catre persoane neautorizate. Criptarea mesajelor SET asigura confidentialitatea informatiei.

**Integritatea datelor** - Aceasta specificatie garanteaza ca nu se altereaza continutul mesajelor in timpul transmisiei acestora prin retea. Informatiile de plata trimise de cumparator la vanzator contin informatii de cerere, date personale si instructiuni de plata. Daca una din aceste informatii este modificata, tranzactia nu se va face corect. Protocolul SET foloseste semnatura digitala pentru integritatea datelor.

**Autentificarea cumparatorului** - Vanzatorul are nevoie de un mijloc de verificare a clientului sau, a faptului ca acesta este utilizatorul legitim al unui numar de cont valid. Un mecanism care face legatura dintre posesorul cartii de credit si un numar de cont specific va reduce incidenta fraudei si, prin urmare, costul total al procesului de plata. SET utilizeaza semnatura digitala si certificatele cumparatorului pentru autentificarea acestuia.

**Autentificarea vanzatorului** - Aceasta specificatie furnizeaza un mijloc de asigurare a clientului ca furnizorul are o relatie cu o institutie financiara, permitandu-i acestuia sa accepte cartile de credit. SET utilizeaza semnatura digitala si certificatele vanzatorului pentru autentificarea acestuia.

**Interoperabilitate** - Protocolul SET trebuie sa fie aplicabil pe o varietate de platforme hardware si soft. Orice cumparator trebuie sa poata sa comunice, cu softul sau, cu orice vanzator. Pentru interoperabilitate, SET foloseste formate de mesaje si protocoale specifice.

**Cumpararea electronica** - Intr-un scenariu tipic de e-commerce, etapele procesului de cumparare sunt urmatoarele:

1. Cumparatorul poate cauta bunuri si servicii avand mai multe posibilitati:

* Foloseste un browser pentru a consulta cataloage online din pagina de Web a vanzatorului;
* Consulta un catalog suplimentar aflat pe un CDROM;
* Consulta un catalog pe hartie.

2. Cumparatorul alege bunurile pe care doreste sa le cumpere.

3. Cumparatorului ii este prezentata o lista a bunurilor, incluzand pretul acestora si pretul total, cu tot cu taxe. Aceasta lista trebuie furnizata electronic de serverul vanzatorului sau de softul de cumparare electronica din calculatorul clientului. Uneori se accepta negocierea pretului.

4. Cumparatorul alege mijloacele de plata. Sa consideram ca este ales ca mijloc de plata cartela de credit (cardul).

5. Cumparatorul trimite vanzatorului o cerere impreuna cu instructiunile de plata. In aceasta specificatie, cererea si instructiunile de plata sunt semnate digital de catre cumparatorii care poseda certificate.

6. Vanzatorul solicita autorizatia de plata a clientului sau de la institutia financiara a acestuia.

7. Vanzatorul trimite confirmarea cererii.

8. Vanzatorul trimite bunurile sau indeplineste serviciile solicitate in cerere.

9. Vanzatorul solicita plata bunurilor si serviciilor de la institutia financiara a cumparatorului.

**Criptografia in SET** - Pentru a asigura securitatea platilor, SET foloseste perechi de chei RSA pentru a crea semnaturi digitale si pentru secretizare. Prin urmare, fiecare participant in procesul de tranzactionare poseda doua perechi de chei asimetrice: o pereche de chei "de schimb" - folosita in criptare si decriptare - si o pereche "de semnatura", pentru crearea si verificarea semnaturii digitale. De mentionat faptul ca rolul cheilor "de semnatura" este inversat in procesul de semnare digitala unde cheia privata este folosita pentru criptare (semnare), iar cea publica este folosita pentru decriptare (verificare a semnaturii).

Autentificarea este intarita de utilizarea certificatelor. Inainte ca un destinatar B sa primeasca un mesaj semnat digital de catre un emitator A, el vrea sa fie sigur ca detine cheia publica a lui A si nu a altuia care s-a recomandat drept A prin retea. O alternativa ar fi ca receptorul B sa primeasca cheia publica direct de la A printr-un canal de comunicatie securizat. De cele mai multe ori, insa, aceasta solutie nu poate fi practicata. Transmisia securizata a cheilor este realizata de un "tert de incredere" numit Autoritate de Certificate (AC), care-l asigura pe B ca A este proprietarul cheii publice pe care o detine. Autoritatea de Certificate furnizeaza certificate care fac legatura dintre un nume de persoana si o cheie publica. Utilizatorul A prezinta AC-ului informatii de identitate. AC-ul creaza un mesaj cu numele lui A si cheia publica a acestuia. Acest mesaj, numit certificat, este semnat digital de catre Autoritatea de Certificate. El contine informatii de identificare a proprietarului, precum si o copie a cheii publice (de schimb sau de semnatura). Participantii SET vor avea, de asemenea, doua certificate pentru cele doua perechi de chei: certificate "de semnatura" si certificate "de schimb". Certificatele sunt create si semnate in acelasi timp de catre AC.

Protocolul SET introduce o noua aplicatie a semnaturilor digitale, si anume conceptul de semnatura duala. Sa consideram urmatorul scenariu: vanzatorul B trimite o oferta cumparatorului A si o autorizatie bancii sale pentru a transfera banii, daca A accepta oferta. Insa B doreste ca banca sa nu vada termenii ofertei, si nici cumparatorul informatiile sale de cont. In plus, B vrea sa faca o legatura dintre oferta si transfer, astfel incat banii vor fi transferati doar daca A accepta oferta sa. El realizeaza toate acestea semnand digital ambele mesaje intr-o singura operatie care creeaza semnatura duala.

O semnatura duala este generata prin calcularea rezumatelor ambelor mesaje si concatenarea celor doua rezumate. Rezultatului obtinut i se calculeaza, la randul sau, un rezumat si, in cele din urma, acest ultim rezumat este cifrat cu cheia privata de semnatura a emitatorului. Trebuie inclus si rezumatul celuilalt mesaj pentru ca oricare din cei doi primitori sa valideze semnatura duala. Un primitor al oricarui mesaj ii poate verifica autenticitatea prin generarea rezumatului acestuia, concatenarea cu rezumatul celuilalt mesaj, si calcularea rezumatului rezultatului concatenarii. Daca noul rezumat se potriveste cu semnatura duala decriptata, primitorul poate fi sigur de autenticitatea mesajului.

Daca A accepta oferta lui B, trimite un mesaj bancii indicand acceptul sau si incluzand rezumatul ofertei. Banca poate verifica autenticitatea autorizatiei de transfer a lui B si se asigura ca acceptul este pentru aceeasi oferta prin utilizarea rezumatului autorizatiei pe care l-a primit de la B si a rezumatului ofertei prezentat de A pentru a valida semnatura duala. Astfel, banca poate controla autenticitatea ofertei, dar nu poate vedea termenii ofertei.

In cadrul protocolului SET, semnatura duala este folosita pentru a face legatura dintre un mesaj de comanda trimis vanzatorului si instructiunile de plata continand informatii de cont trimise achizitorului. Cand vanzatorul trimite o cerere de autorizatie achizitorului, include instructiunile de plata primite de la cumparator si rezumatul informatiilor de comanda. Achizitorul foloseste rezumatul primit de la vanzator si calculeaza rezumatul instructiunilor de plata pentru a verifica semnatura duala.

In prezent, tot mai multe produse de e-commerce implementeaza protocolul SET, ceea ce confera securitate platilor Internet cu card, prin mijloace criptografice.

**Bibliografie**

1. Curs 7
2. <https://www.referatele.com/referate/diverse/online10/Sisteme-electronice-de-plati-referatele-com.php>
3. <https://ro.scribd.com/document/50485339/Sisteme-electronice-de-plati>
4. <https://profs.info.uaic.ro/~mihaela/teach/biz/curs04biz.pdf>