Sisteme electronice de plati

Sisteme electronice de plati

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 si,
- cecuri electronice. 18832ubn68flx7e

Sisteme de plati in Internet bazate pe carduri bancare
SET

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:

Sa asigure confidentialitatea instructiunilor de plata si a informatiilor de cerere care sunt transmise odata cu informatiile de plata.
Sa garanteze integritatea tuturor datelor transmise.
Sa asigure autentificarea cumparatorului precum si faptul ca acesta este utilizatorul legitim al unei marci de card.
Sa asigure autentificarea vanzatorului precum si faptul ca acesta accepta tranzactii cu carduri prin relatia sa cu o institutie financiara achizitoare.
Sa foloseasca cele mai bune metode de securitate pentru a proteja partile antrenate in comert.
Sa fie un protocol care sa nu depinda de mecanismele de securitate ale transportului si care sa nu impiedice folosirea acestora.
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. bl832u8168fllx

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.

CyberCash

Fondata in august 1994, firma CyberCash Inc. din SUA propune in aprilie 1995 un mecanism sigur de tranzactii de plata cu carduri, bazat pe un server propriu si oferind servicii client pentru vanzatori. Folosirea serverului CyberCash asigura posibilitatea de trasare si control imediat al tranzactiilor. Pe de alta parte, trecerea prin server face sistemul mai lent si dependent de timpii de raspuns ai acestuia. Aceste lucruri fac CyberCash mai putin confortabil si mai costisitor, in special pentru tranzactiile de plata cu sume mici. Insa cifrarea cu chei publice asigura un nivel inalt de securitate.

CyberCash implementeaza un sistem care realizeaza protectia cardurilor de credit folosite in Internet. Compania - care furnizeaza soft atat pentru vanzatori, cat si pentru cumparatori - opereaza un gateway intre Internet si retelele de autorizare ale principalelor firme ofertante de carduri (Figura "Plati electronice folosind CyberCash"). Cumparatorul incepe prin a descarca softul specific de portofel, cel care accepta criptarea si prelucrarea tranzactiilor. La fel ca un portofel fizic care poate contine mai multe carduri bancare diferite, portofelul soft al cumparatorului poate fi folosit de catre client pentru a inregistra mai multe carduri, cu care va face ulterior platile. Un soft similar furnizeaza servicii la vanzator.

Mesajele sunt cripate folosind un algoritm simetric (DES) cu cheie de 56 de biti generata aleator, anvelopata si ea in mesaj prin criptare cu cheia publica a receptorului. Sistemul de criptare cu chei publice folosit este RSA, cu o lungime de 1.024 biti. Cheia publica CyberCash este memorata in softul de portofel si in cel al vanzatorului. Atunci cand va inregistra in softul portofel cardurile cu care va face platile, cumparatorul isi va genera si propria pereche cheie publica - cheie privata. Apoi cheia sa publica va fi transmisa la CyberCash, care o va inregistra intr-o baza de date. Desi toti participantii in sistem (cumparatori, vanzatori si CyberCash) au propriile lor perechi de chei publice si private, numai CyberCash stie cheile publice ale tuturor. Ca urmare, compania poate schimba informatii in mod sigur cu orice cumparator sau vanzator, dar acestia comunica in clar unii cu altii. Revine ca sarcina lui CyberCash sa autentifice toate semnaturile, cu cheile publice pe care le detine in mod sigur.

Atunci cand se face o cumparatura, produsul dorit este selectat printr-un browser Web. Serverul vanzatorului trimite portofelului cumparatorului un mesaj cerere de plata in clar, semnat criptografic, cerere care descrie cumpararea si tipurile de carduri care sunt acceptate

pentru plata. Softul portofel afiseaza o fereastra care permite cumparatorului sa aprobe achizitia si suma si sa selecteze cardul cu care se va face plata.

Se trimite inapoi vanzatorul un mesaj de plata ce include o descriere a tranzactiei criptata si semnata digital de cumparator, precum si numarul cardului folosit. Vanzatorul trimite mai departe mesajul de plata la gateway-ul CyberCash, impreuna cu propria sa descriere a tranzactiei, criptata si semnata digital. CyberCash decripteaza si compara cele doua mesaje si verifica cele doua semnaturi. Daca lucrurile sunt OK, el autorizeaza cererea vanzatorului trimitand un mesaj specific la softul acestuia. Apoi softul vanzatorului confirma plata portofelului cumparatorului ("Raspuns la plata" in figura "Plati electronice folosind CyberCash").

CyberCash opereaza propriul sau gateway ca un agent al bancii vanzatorului. De aceea, el trebuie sa fie de incredere pentru a decripta mesajele si a le transfera pe retelele de autorizare conventionale ale bancilor.

Intrucat informatiile sunt criptate cu cheia publica a lui CyberCash, cunoscuta de softul ce opereaza sistemul, vanzatorul nu poate vedea care este numarul cardului folosit de cumparator, eliminandu-se riscul refolosirii acestui card la alte cumparaturi neautorizate.

Recent, firma CyberCash a extins sistemul initial de plata bazat pe transmisia sigura a cardurilor cu alte facilitati pentru plati cu bani electronici: Secure Cash/Check si Secure Check, precum si CyberCoin, folosit pentru valori mici. De asemenea, in stransa legatura cu CyberCash, la Universitatea California de Sud au fost dezvoltate alte doua sisteme asemanatoare: NetCash, pentru plati cu sume mici, bazate pe bani electronici si NetCheque, un sistem bazat pe cecuri electronice.

Sistem on-line de plata cu moneda electronica
ECash

ECash reprezinta un exemplu de sistem electronic de plati, care foloseste posta electronica sau Web-ul pentru implementarea unui concept de portofel virtual. A fost dezvoltat de catre firma DigiCash Co. din Olanda, firma fondata de catre celebrul cercetator al sistemelor criptografice, David Chaum. Prima demonstratie a sistemului a fost facuta in 1994 la prima Conferinta WWW, printr-o legatura Web intre Geneva si Amsterdam. Ulterior a fost implementata de banci din SUA (Mark Twain Bank of Missouri), Finlanda si din alte tari. Este prima solutie totalmente soft pentru platile electronice.

ECash reprezinta un sistem de plati complet anonim, ce foloseste conturi numerice in banci si tehnica semnaturilor oarbe. Tranzactiile se desfasoara intre cumparator si vanzator, care trebuie sa aiba conturi la aceeasi banca. Cumparatorii trebuie sa instiinteze banca cu privire la faptul ca doresc sa transfere bani din conturile lor obisnuite in asa numitul cont eCash Mint. In orice moment, cumparatorul poate interactiona de la distanta, prin calculatorul sau, cu contul Mint si, folosind un client soft, poate retrage de aici fonduri pe discul calculatorului sau. Formatul acestor fonduri este electronic - suite de 0 si 1 protejate criptografic. Ca urmare, discul cumparatorului devine un veritabil "portofel electronic".

Apoi, se pot executa plati intre persoane individuale sau catre firme, prin intermediul acestor eCash.

Principiul functionarii lui ECash - ECash are un caracter privat: desi banca tine o evidenta a fiecarei retrageri eCash si a fiecarui depozit Mint, este imposibil ca banca sa stabileasca utilizarea ulterioara a lui eCash. Aceasta proprietate se datoreaza folosirii unor criptosisteme cu chei publice RSA, cu o lungime a cheii de 768 biti. Pe langa anonimitatea platilor, eCash asigura si ne-repudierea, adica acea proprietate care permite rezolvarea oricaror dispute intre cumparator si vanzator privind recunoasterea platilor. De asemenea, prin verificare in baza de date a bancii, este impiedicata orice dubla cheltuire a lui eCash.

La fel ca si banii reali (bancnote, monede), banii electronici eCash pot fi retrasi din conturi sau depozitati, pentru a fi tranzactionati. De asemenea, la fel ca in cazul banilor fizici, o persoana poate transfera posesia unui cont eCash unei alte persoane. Insa, spre deosebire de banii conventionali, atunci cand un client plateste unui alt client, banca electronica joaca un rol aparent modest, dar esential.

ECash reprezinta o solutie de plati soft on-line, care consta in interactiunile dintre 3 entitati:

- banca, care emite monede, valideaza monedele existente si schimba monede reale pentru eCash;

- cumparatorii, care au cont in banca, din care pot incarca monede eCash sau in care pot depune monede eCash;

- vanzatorii, care accepta monede ECash in schimbul unor bunuri sau servicii.

ECash este implementat folosind criptografia cu chei publice RSA. Fiecare utilizator are propria-i pereche de chei (publica - E si privata - D). Este nevoie de un soft special pentru gestiunea eCash:

- pentru client un program numit portofel electronic (cyberwallet);

- pentru vanzator un program special eCash.

Retragerea de monede eCash de la banca - Software-ul cyberwallet al clientului calculeaza cate monede digitale si de ce valori sunt necesare pentru a satisface cererea de plata. Apoi, programul genereaza in mod aleator numere de serie pentru aceste monede. Aceste numere sunt suficient de mari (100 de cifre zecimale) pentru ca sa fie foarte mica probabilitatea ca altcineva sa genereze aceleasi valori. Aceste numere de serie sunt apoi facute "anonime", cu ajutorul tehnicii semnaturilor oarbe. Acest lucru se realizeaza prin multiplicarea lor cu factor aleator. Acesti bani "anonimi" sunt apoi impachetati intr-un mesaj, semnati digital cu cheia privata a clientului, cifrati cu cheia publica a bancii si apoi trimisi electronic la banca.

Cand banca receptioneaza mesajul, ea verifica semnatura. Apoi suma retrasa poate fi debitata din contul clientului care a semnat cererea. Banca semneaza monedele electronice cu cheia sa privata si le returneaza la client, criptate cu cheia publica a acestuia.

Prin folosirea semnaturii oarbe, se previne ca banca sa poata recunoaste monedele ca venind dintr-un anumit cont. Ideea este aratata in figura "Retragerea de monede Ecash". In loc ca banca sa creeze monezi electronice "albe", calculatorul unui utilizator (in exemplul nostru Dan) este cel care creeaza in mod aleator monezile. Apoi ascunde aceste monezi, fiecare intr-o anvelopa digitala speciala, si le trimite pe rand catre banca. Banca retrage la fiecare receptie dolari din contul lui Dan si construieste validarea digitala a monedei, ca o "stampila" pe plicul pe care Dan tocmai l-a trimis. Plicul astfel "stampilat" este returnat catre Dan. Atunci cand calculatorul lui Dan va inlatura plicul, va obtine o moneda digitala dupa cum si-a dorit, insa validata de stampila bancii. Dar pentru ca banca nu a vazut moneda ascunsa in plic, aceasta nu va putea spune, atunci cand va receptiona o plata, din partea cui provine aceasta - adica cui apartin acei bani.

Dupa ce clientul primeste banii anonimi semnati de banca, decripteaza mesajul si anuleaza anonimitatea banilor prin impartire la factorul aleator. Figura 3 arata cei doi participanti in tranzactia de retragere: banca si clientul. Moneda digitala, care urmeaza sa fie retrasa dinn contul lui Dan din banca, va fi depozitata pe discul PC-ului sau.

Cheltuirea monedelor eCash - Atunci cand Dan are eCash pe discul sau, poate cumpara ceva de la magazinul lui Vlad (figura "Cheltuirea monedelor eCash"). Primind o cerere de plata de la Vlad, Dan o aproba prin apasarea butonului "Yes" din fereastra. Programul sau eCash va alege din portofelul lui (pe disc) monedele electronice potrivite pentru a forma totalul de plata. Dupa aceasta, va sterge aceste monede si le va trimite prin retea catre magazinul lui Vlad. Atunci cand programul lui Vlad a receptionat monedele, le va trimite automat catre banca. Apoi va astepta pana cand acestea sunt acceptate sau respinse, inainte de a trimite bunurile cumparate catre Dan.

Clientul lanseaza in executie softul cyberwallet si clientul Web. Cu acesta din urma navigheaza pana gaseste un magazin virtual pe retea. Softul client eCash lucreaza impreuna cu serverul si clientul Web. Un magazin virtual nu este altceva decat un document HTML, cu URL-uri reprezentand articolul cu produsele de vanzare. Pentru a cumpara un produs, clientul selecteaza un URL care reprezinta articolul. Cumpararea se face in urmatorii pasi (vezi fig.5):

1. Utilizatorul clientului Web trimite un mesaj HTTP de cerere a URL-ului catre serverul Web al vanzatorului. URL-ul va apela un program CGI (Common Gateway Interface).

2. Programul CGI apelat este softul eCash al vanzatorului. Lui i se vor transmite detalii ale articolului selectat in URL. Localizarea calculatorului cumparatorului va fi transmisa printr-o variabila de la server la softul eCash al vanzatorului.

3. Softul vanzatorului va contacta programul portofel al cumparatorului printr-o legatura TCP/IP, cerandu-i plata.

4. Cand portofelul de la client primeste cererea, el va intreba cumparatorul daca accepta plata. In caz afirmativ, va trimite catre vanzator exact monedele electronice necesare. Acestea vor fi criptate cu cheia publica a vanzatorului:

EVÂNZATOR (Monede)

In cazul in care nu se dispune de monedele care sa satisfaca exact cererea de plata, se trimite un refuz vanzatorului.

5. Cand vanzatorul primeste monedele, le decripteaza cu cheia sa privata; apoi trebuie sa verifice validitatea lor si eventuala dubla cheltuire. Pentru aceasta, se contacteaza banca si i se trimite un mesaj format din monedele, semnate cu cheia a vanzatorului si apoi criptate cu cheia publica a bancii:

EBANCA (DVÂNZATOR (Monede)

6. Banca decripteaza mesajul cu cheia sa privata si apoi valideaza banii, verificand numerele de serie cu cele inscrise in baza sa de date ca fiind deja cheltuite. Daca seriile trimise de vanzator sunt gasite in baza de date, inseamna ca banii sunt invalidati, ei fiind deja cheltuiti. Daca insa ei nu sunt in baza de date si sunt semnati corect de banca cu cheia sa privata, banii sun validati. Valoarea lor crediteaza contul vanzatorului, banii sunt distrusi iar seriile le sunt memorate in baza de date. Softul bancii notifica vanzatorului incheierea cu succes a depunerii.

7. Se returneaza un mesaj-chitanta semnat electronic catre softul portofel al cumparatorului.

8. Un mesaj de confirmare se trimite apoi de la portofel catre serverul Web.

9. Serverul Web inainteaza informatia catre clientul Web al cumparatorului.

Acest scenariu va putea fi urmarit in exemplul real ce va fi prezentat in caseta "Exemple de utilizare eCash".

NetCash

NetCash reprezinta un alt exemplu de sistem electronic de plati de tip on-line. A fost elabortat la Information Science Institute de la University of Southern California. Cu toate ca sistemul nu asigura anonimitatea totala a platilor ca eCash (banii pot fi identificati), NetCash ofera alte mijloace prin care sa se asigure platilor un anumit grad de anonimiatate. Sistemul se bazeaza pe mai multe servere de monede distribuite, la care se poate face schimbul unor cecuri electronice (inclusiv NetCheque) in moneda electronica.

Sistemul NetCash consta dinn urmatoarele entitati:

- cumparatori,

- vanzatori,

- servere de moneda (SM).

O organizatie care doreste sa administreze un server de moneda va trebui sa obtina o aprobare de la o autoritate centrala de certificare. Serverul de moneda va genera o pereche de chei RSA, publica si privata. Cheia publica este apoi certificata prin semnatura autoritatii centrale de certificare. Acest certificat contine un identificator (ID), numele serverului de moneda, cheia publica a serverului de moneda, datele de eliberare si expirare, toate semnate de autoritatea centrala:

Dautoritatea-centrala (ID, Nume-SM, ESM , Data-eliberarii, Data-expirarii)

Monedele electronice eliberate de serverul SM constau in urmatoarele:

- Nume-SM;

- Adresa retea a SM;

- Data-expirarii;

- Numarul de serie;

- Valoarea.

Banii sunt apoi semnati cu cheia privata a serverului SM:

DSM (Nume-SM, Adresa-retea-SM , Data-expirarii, Numarul-serie, Valoarea)

SM tine evidenta tuturor seriilor de bani emisi de el. In acest caz, validitatea si dubla cheltuire pot fi verificate de fiecare data cand se face o cumparare sau un schimb de cec. Atunci cand se face verificarea unor bani ce se cheltuiesc, seriile lor sunt sterse din baza de date a SM iar banii sunt inlocuiti cu alte serii. Un cec electronic poate fi schimbat la un SM cu bani electronici.

Pentru asigurarea anonimitatii platilor, SM nu este autorizat sa memoreze persoanele si adresele lor retea carora le emite bani electronici. Detinatorul unor astfel de monede poate merge apoi la orice alt SM pentru a le schimba, cu altele monede emise de acel SM.

Figura "Pasii procesului de cumparare cu NetCash" arata modul in care un cumparator foloseste NetCash pentru a achizitiona un articol de la un vanzator. In aceasta tranzactie cumparatorul ramane anonim, intrucat vanzatorul vrea sa stie doar adresa de retea de unde actioneaza cumparatorul. NetCash face presupunerea ca orice cumparator poate obtine cheia publica a vanzatorului, iar acesta din urma are cheia publica a SM.

Tranzactia de cumparare folosind NetCash se face in 4 pasi:

1. Cumparatorul trimite monedele electronice in cadrul mesajului de plata, identificatorul serviciului de cumparare (S-Id), o cheie secreta generata doar pentru acea tranzactie (KCUMPARATOR) si o cheie publica de sesiune (ECUMPARATOR), toate criptate cu cheia publica a vanzatorului. Cheia secreta K va fi folosita de vanzator pentru stabili un canal criptat cu cumparatorul. Cheia publica E este folosita ulterior pentru verificarea cererilor de plata venite de la acel cumparator.

EVÂNZATOR (Monede, KCUMPARATOR, ECUMPARATOR , S-Id)

2. Vanzatorul trebuie sa verifice validitate monedelor electronice primite. Pentru aceasta, le va trimite SM pentru a le schimba cu alte monede electronice sau cu un cec. Vanzatorul genereaza o noua cheie secreta simetrica de sesiune KVÂNZATOR pe care o va trimite impreuna cu banii la SM. Intreg mesajul este criptat cu cheia publica a serverului:

ESM (Monede, KVÂNZATOR, Tip-tranzactie)

3. Serverul SM verifica faptul ca banii sunt valizi, consultand baza sa de date. Un ban este valid daca numarul sau serial apare in baza de date. SM va returna vanzatorului noi monede electronice sau un cec, criptate cu cheia secreta de sesiune a vanzatorului:

KVÂNZATOR (Noi-monede).

4. Primind noii bani (sau cecul), vanzatorul se convinge ca a fost corect platit de cumparator. Acum el va returna acestuia o confirmare, semnata cu cheia sa privata si cifrata cu cheia secreta de sesiune a cumparatorului:

KCUMPARATOR (DVÂNZATOR (Suma, Id-tranzactie, data)).

Avantajele folosirii NetCash sunt scalabilitatea sistemului si securitatea. El este scalabil, intrucat se pot instala SM multiple. Securitatea este asigurata de protocoalele sale criptografice. Insa spre deosebire de eCash, sistemul NetCash nu este complet anonim. Este dificil - dar nu imposibil - pentru un SM sa pastreze inregistrari despre persoanele carora li se emite monede si de la care se primesc acesti bani inapoi. Abilitatea cu care se folosesc mai multe servere SM creste gradul de anonimitate al platilor.

Sisteme de micro-plati
Exista deja, asa cum s-a vazut pana acum, un numar de protocoale de plata in comertul electronic destinate unor tranzactii "mari", de 5 USD, 10 USD si mai mult. Costul per tranzactie este, de obicei, de cativa centi plus un procent din suma vehiculata. Atunci cand aceste costuri sunt aplicate la tranzactii cu valori mici (50 de centi sau mai putin), costul devine semnificativ in pretul total al tranzactiei. Ca urmare, pentru a obtine efectiv un pret minim pentru anumite bunuri si servicii "ieftine" ce urmeaza a fi cumparate, vor trebui utilizate noi protocoale.

Exista o serie de servicii on-line, care promoveaza ziare, magazine, referinte de munca si altele, toate avand articole individuale care sunt ieftine daca sunt vandute separat.

Avantajul de a cumpara articole individuale ieftine poate face aceste servicii mai atractive utilizatorilor ocazionali ai Internet-ului. Un utilizator care nu agreeaza ideea de a deschide un cont de zece dolari cu un editor de publicatii necunoscut, poate fi dispus sa cheltuiasca cativa centi pentru a cumpara un articol interesant la prima vedere. O aplicatie "ieftina" frecventa o reprezinta plata vizitarii siturilor in Internet.

Sub forma de concept si proiecte experimentale, micro-platile se adreseaza nevoii existentei unei scheme simple, ieftine, care sa poata suporta economic plati foarte mici, cativa dolari, centi si chiar fractiuni de centi. Vom analiza cateva propuneri din aceasta categorie de sisteme electronice de plati.

MilliCent

MilliCent este un protocol simplu si sigur pentru comertul electronic in Internet. A fost creat pentru a accepta tranzactii comerciale in care sunt implicate costuri mai mici de un cent. Este un protocol bazat pe o validare descentralizata a banilor electronici pe serverele vanzatorilor, fara comunicatii aditionale, criptari scumpe sau procesari separate.

Cheia inovatiei MilliCent este aceea de a introduce utilizarea broker-ilor si a scrip-urilor. Broker-ii (cei care vand scrip-uri) au ca sarcina managementul conturilor, facturari, mentinerea functionalitatii conexiunilor si stabilirea de conturi cu vanzatorii. Scrip-ul este moneda digitala, specifica fiecarui vanzator in parte. Vanzatorii au sarcina de a valida local scip-ul pentru a preveni furtul, cum ar fi de exemplu dubla cheltuire din partea clientilor.

O piesa de scrip reprezinta un cont al clientului, care a fost stabilit cu vanzatorul. In orice moment, vanzatorul are de rezolvat scrip-urile (conturile deschise) cu clientii cei mai recenti. Balanta contului este actualizata dupa valoarea scrip-ului. Atunci cand clientul face o cumparatura cu scrip, costul cumparaturii este dedus din scrip-ul total, iar valoarea care ramane formeaza noul scrip (cu o noua valoare/balanta cont), care este returnat ca rest. Atunci cand clientul a terminat mai multe tranzactii, el poate "incasa" valoarea ramasa a scrip-ului (inchide contul).

Broker-ii servesc drept conturi intermediare intre clienti si vanzatori. Clientii intra intr-o relatie de lunga durata cu broker-ii, in mare cam in acelasi mod cum s-ar face o intelegere cu o banca, o companie de carduri de credit sau un ISP (furnizor de servicii Internet). Broker-ii cumpara si vand scrip-uri apartinand vanzatorilor, ca un serviciu catre clienti si vanzatori. Serverele de scrip ale broker-ilor au o moneda comuna pentru clienti (folosita pentru cumpararea scrip-ului vanzatorilor) si pentru vanzatori (pentru a returna banii pe scrip-ul nefolosit).

MilliCent reduce costurile pe mai multe cai:

- Costul comunicatiei este redus prin verificarea locala a scrip-ului, pe situl vanzatorului; se elimina astfel costurile comunicatiilor (care sunt absente), costurile pentru aparatura informatica ce ar da o puterea de calcul suficienta pentru o derulare normala a unui numar

mare de tranzactii; de asemenea, nu este nevoie de servere centralizatoare, de protocoale scumpe etc.

- Costurile criptografice sunt reduse deoarece nu este necesara o schema criptografica puternica si scumpa la valorile foarte mici care sunt tranzactionate. Este nevoie de un cost care sa nu depaseasca valoarea scrip-ului insusi.

- Costurile conturilor sunt reduse prin utilizarea broker-ilor care manuiesc conturile si facturile. Clientii stabilesc conturi cu un broker; broker-ul stabileste propriul sau cont cu vanzatorul. Aceasta separare reduce numarul total de conturi prin eliminarea tuturor combinatiilor client-vanzator.

Modelul de securitate si incredere - Modelul de securitate pentru MilliCent este bazat pe presupunerea ca moneda "scrip" este folosita pentru plati mici. Oamenii obisnuiti si cei de afaceri trateaza monedele diferit, in functie de valoarea lor; la fel se intampla si in cazul facturilor, cand facturile mici sunt tratate diferit de facturile mari. Ca si atunci cand un om cumpara o bomboana de la un automat si nu are nevoie de o chitanta, el nu are nevoie de chitanta nici atunci cand cumpara un articol utilizand scrip-ul . Daca o persoana nu doreste sa plateasca pentru ceva, renunta si va primi inapoi suma implicata. Daca aceasta suma (moneda) se va pierde, persoana respectiva nu va fi foarte suparata. Se presupune ca un utilizator va avea, la un moment dat, doar cativa dolari sub forma de scrip. Rezulta ca nu este rentabil sa se fure un scrip.

Modelul de incredere MilliCent se bazeaza pe o relatie asimetrica de incredere compusa din trei entitati - clientul, broker-ul si vanzatorul. Broker-ii sunt presupusi ca fiind mult mai de incredere decat vanzatorii, si in final, clientii. Se tinde ca broker-ii sa fie institutii financiare redutabile, mari si bine cunoscute, (cum ar fi Visa, MasterCard, sau bancile) sau un mare furnizor de servicii Internet sau servicii on-line (cum ar fi CompuServe, NETCOM, sau AOL). Se asteapta sa fie multi vanzatori, acoperind un spectru larg de activitati si, de asemenea, un numar mare de clienti, iar relatiile de incredere sa fie la fel ca si in lumea reala.

Trei factori fac frauda broker-ilor in micro-plati sa fie nerentabila:

- programele client si vanzator pot sa analizeze in mod independent scrip-ul si sa mentina balanta contului, deci orice frauda a broker-ului poate fi detectata;

- clientii nu detin, la un moment de timp, multe scripuri - deci broker-ul va trebui sa comita mai multe tranzactii frauduloase pentru a obtine vreun castig, iar acest lucru il face mai usor de depistat;

- reputatia broker-ilor este importanta pentru atragerea clientilor, iar un broker poate sa piarda rapid aceasta reputatie daca exista probleme in tranzactiile clientilor sai. Faptul de a avea multi clienti activi este mult mai valoros pentru un broker decat furtul de scrip din conturi.

Frauda vanzatorului consta in nelivrarea bunului sau serviciului pentru un scrip valid. Daca acest lucru se intampla, clientul se va plange la broker-ul sau, iar broker-ul va renunta la un vanzator care a cauzat mai multe plangeri. Acest act inseamna un mecanism coercitiv, deoarece vanzatorii au nevoie de broker-i pentru a li se facilita desfasurarea afacerilor cu MilliCent.

Ca urmare, protocolul MilliCent este intarit pentru a preveni frauda clientilor (falsificarea si dubla cheltuire) si promoveaza detectia indirecta a fraudelor broker-ilor si vanzatorilor.

Securitatea tranzactiilor MilliCent cuprinde urmatoarele aspecte:

- Toate tranzactiile sunt protejate: fiecare tranzactie cere ca clientul sa stie parola asociata scrip-ului. Protocolul nu va trimite niciodata o parola in clar, deci este eliminat riscul ca cineva, tragand cu "urechea", sa asculte ceva util. Nici o unitate de scrip nu poate fi reutilizata. Fiecare cerere este semnata cu o parola, deci nu exista nici o cale pentru a intercepta si a reutiliza un scrip.

- Tranzactiile cu valoare mica limiteaza valoarea fraudelor: tranzactiile mici cer o securitate ieftina; nu este rentabila folosirea unor resurse computationale scumpe pentru a fura scrip-uri ieftine. In plus, folosirea ilegala a scrip-ului in mai multe actiuni ilegale, pentru a strange mai multi bani, face mult mai probabila depistarea hotului.

Frauda este detectabila si eventual localizabila: detectarea se face atunci cand clientul nu obtine bunul dorit sau atunci cand balanta returnata catre client nu este corecta. Daca un client triseaza, atunci vanzatorul pierde doar costul scrip-ul fals detectabil. Daca vanzatorul triseaza, clientul va raporta problema broker-ului. Atunci cand broker-ul primeste plangeri de la mai multi clienti impotriva unui vanzator, poate localiza cine provoaca frauda si va anula toate intelegerile cu respectivul vanzator. Daca broker-ul triseaza, vanzatorul va primi scrip fals de la mai multi clienti, toti avand legatura cu un singur broker.

Interactiunea dintre Client, Broker si Vanzator - Se prezinta in continuare pasii pentru o sesiune completa MilliCent, incluzand cumpararea de catre broker a scrip-ului vanzatorului.

- Pasul initial se petrece doar o sigura data pe sesiune. Clientul face o conexiune sigura cu broker-ul pentru a obtine un scrip de la broker. Clientul cere un scrip de la broker, de exemplu la inceputul zilei. Broker-ul returneaza scrip-ul broker initial si secretul asociat.

- Al doilea pas se petrece de fiecare data cand clientul nu mai are scrip pentru un vanzator. El contacteaza broker-ul, folosind scrip-ul broker-ului pe care il detine din pasul 1, cerand sa cumpere un scrip vanzator.

- Al treilea pas apare doar daca broker-ul trebuie sa contacteze vanzatorul pentru a cumpara scrip. Daca broker-ul nu are deja scrip de la vanzator, il cumpara. Va cere un scrip de la vanzator iar acesta i-l va returna impreuna cu secretul asociat.

- In al patrulea pas broker-ul furnizeaza scrip-ul vanzatorului catre client. Broker-ul returneaza la client scrip-ul vanzatorului si restul (in scrip broker).

- In al cincilea pas clientul, utilizand scrip-ul, face o cumparatura de la vanzator. Acesta returneaza restul (in scrip-ul vanzatorului) la client.

Intr-o tranzactie tipica MilliCent, atunci cand clientul are deja scrip-ul vanzatorului, il utilizeaza direct pentru a face o cumparatura. Aici nu mai exista vreun mesaj suplimentar sau interactiune cu broker-ul.

CyberCoin

Sistemul de micro-plati CyberCoin poate realiza in Internet plati de la sume mici de cativa centi, pana la 10 $, acoperind astfel o zona in care sistemul ce utilizeaza cartile de credit nu este economic. Vanzatorii de pe Web ce vand servicii si produse la preturi foarte mici si doresc sa livreze imediat respectiva marfa, au nevoie de o metoda de plata diferita de cartelele cu microprocesor, dar asemanatore cu plata cash ce se efectueaza si in magazine. Serviciul CyberCoin de la CyberCash a fost lansat in septembrie 1996, ca un prim sistem de micro-plati in Internet. Consumatorii pot folosi conturile existente deja in banci pentru a transfera valori in softul portofel electronic propriu. Alta posibilitate este de a incarca fonduri direct de pe o carte de credit, printr-o tranzactie obisnuita cu astfel de mijloace. In ambele cazuri, banii reali raman in custodia bancilor.

Odata portofelul "umplut "cu fonduri, consumatorul poate incepe sa efectueze micro-plati pe situri Web ce sunt inregistrate de CyberCash si detin un program numit CashRegister. Acest soft suporta, de asemenea, si plati cu carti de credit (VISA, MasterCard, American Express si Discover) si cecuri electronice PayNow.

Din perspectiva utilizatorului, protocolul CyberCoin lucreaza asemanator cu un browser de Internet; trebuie aleasa o adresa URL - comanda HTML get. Comerciantul prezinta in pagina sa HTML o adresa de plata (payment URL), impreuna cu pretul afisat. Utilizatorului nu-i ramane decat sa selecteze adresa URL respectiva pentru a achizitiona bunul sau serviciul ales.

Serviciul CyberCoin este implementat utilizand un concept cunoscut sub numele de sesiune CyberCoin. O sesiune indeplineste o singura functie primara: initierea unui sub-cont tranzitoriu, sub contul portofelului, pentru fiecare suma care este cheltuita sau colectata. O sesiune poate semana cu un carnet de cecuri ce contine n cecuri. Fiecare "cec" poate fi utilizat doar o singura data. Sesiunea se termina atunci cand s-au consumat toate cecurile sau acestea au expirat. Un cec poate fi folosit doar pentru o singura plata sau depozitare.

Pe timpul rularii unei sesiuni, protocolul CyberCoin realizeaza o viteza de procesare optima si un cost redus, prin criptarea mesajelor cu cifrul DES. Initierea se face printr-un schimb al unei chei generate aleator si transportate (anvelopate) intr-un mesaj criptat cu RSA, pe 768 de biti. Fiecare "cec" de plata utilizeaza o cheie de tranzactie DES unica. Deci prin

spargerea cheii dupa sesiune nu se poate obtine nici un profit, deoarece aceasta nu mai este folosita la criptarea altor mesaje.

Plati prin cecuri electronice
Cecurile electronice au fost dezvoltate printr-un proiect al lui FSTC -Financial Services Technology Consortium. FSTC cuprinde aproape 100 de membri, incluzand majoritatea marilor banci, furnizorii tehnologiei pentru industria financiara, universitati si laboratoare de cercetare. Partea tehnica a realizarii proiectului cecului electronic a fost realizata intr-un numar de faze: generarea conceptelor originale, realizarea cercetarilor preliminare, construirea si demonstrarea unui prototip, formularea specificatiilor pentru un sistem pilot si implementarea acestui sistem. In prezent, cecurile electronice incep sa fie utilizate intr-un program pilot cu Departamentul Trezoreriei Statelor Unite care plateste furnizorii Departamentului de Aparare.

Cecurile electronice sunt create pentru a realiza plati si alte functii financiare ale cecurilor pe hartie, prin utilizarea semnaturilor digitale si a mesajelor criptate, pe suportul retelei Internet. Sistemul cecurilor electronice este proiectat pentru a asigura integritatea mesajelor, autenticitatea si nerepudierea proprietatii, toate conditii suficiente pentru a preveni frauda din partea bancilor sau a clientilor lor.

Un cec este un document pe hartie, semnat, care autorizeaza banca sa plateasca o suma de bani din contul celui ce a semnat cecul, dupa o data specificata. Cecurile pe hartie sunt cele mai utilizate instrumente de plata (dupa folosirea banilor cash) in majoritatea statelor occidentale. Acestea au avantajul ca platitorul si cel care incaseaza suma pot fi persoane individuale, mici afaceristi, banci, corporatii, guverne sau orice alt tip de organizatii. Aceste cecuri pot fi transmise direct de la platitor la incasator.

Cecurile electronice (e-cecurile) sunt bazate pe ideea ca documentele electronice pot substitui hartia, iar semnaturile digitale cu chei publice pot substitui semnaturile olografe. Prin urmare, e-cecurile pot inlocui cecurile pe hartie, fara a fi nevoie sa se creeze un nou instrument, inlaturandu-se astfel problemele de legalitate, reglementare si practica comerciala ce pot fi provocate de schimbarea si impunerea unui instrument de plata nou. Figura 9 arata fluxul normal al tranzactiilor cu e-cecuri.

Pentru ca un e-cec trebuie sa contina imputernicirea specifica, informatiile optionale si semnatura digitala (criptografica), acesta este scris in limbajul FSML (Financial Services Markup Language), un limbaj specific, care utilizeaza standardul SGML (Standard Generalized Markup Language). Structura documentului si datele care compun un e-cec sunt delimitate de tag-ur", similar cu cele folosite in HTML (HyperText Markup Language), un alt limbaj definit utilizand SGML.

FSML este creat pentru a accepta structura de date si semnaturile criptografice de care este nevoie pentru cecurile electronice, dar nu poate fi generalizat si extins pentru alte documente de servicii financiare. Cecurile electronice scrise in FSML vor contine toate informatiile care se gasesc in mod normal in cecurile clasice, incluzand pe cele scrise de mana, pre-tiparite si cele cu banda magnetica. Structura FSML si mecanismul de semnare

ofera posibilitatea de a incapsula si cripta alte documente atasate, cum ar fi avize de plata, facturi, sau informatii de remitere.

Pentru promovarea verificarilor semnaturilor cu cheia publica a e-cecurilor, este utilizat protocolul pentru certificate X.509. Banca emite un certificat atunci cand un client isi deschide un cont pentru cecuri electronice si va innoi acest certificat inainte ca el sa expire, realizand cu aceasta o protectie a contului si a expunerii semnaturii cu cheie privata a semnatarului. Certificatul X.509 doar informeaza verificatorul semnaturii despre faptul ca respectiva cheie publica a fost legitimata in asociere cu un semnatar si un cont de banca, la data la care certificatul a fost emis. Un certificat X.509 nu implica faptul ca e-cecul este garantat in ambele sensuri. Alte verificari asupra semnaturii cecului electronic pot oferi incredere ca cecul a fost semnat cu o cheie privata ce apartine unui detinator legitim de cont pentru cecuri electronice si e-cecul nu a fost alterat.

Pentru protejarea impotriva furtului si folosirii abuzive a cecului electronic, este utilizat un smart-card. Utilizarea hardului criptografic al cardului ofera semnaturii mai multa confidentialitate. Astfel, cheia privata pentru semnarea cecurilor nu este niciodata transferata catre computerul semnatarului, deci nu este niciodata expusa furtului din respectivul computer conectat in retea. Procesorul smart-cardului numeroteaza automat fiecare cec electronic, atunci cand il semneaza, in ordine, pentru a se asigura unicitatea e-cecurilor si pastreaza o istorie a cecurilor pentru a fi consultata in cazul unei dispute. Smart-cardul este protejat prin introducerea unui cod PIN, cunoscut numai de posesorul cardului.

Semnarea criptografica este suficienta in sistemul cu cecuri electronice ca masura de securitate impotriva fraudelor prin falsificari de mesaje. In afara de acestea, sistemul cu cecuri electronice si nivelul aplicatie criptografica pot fi exportate si utilizate international. Atunci cand este nevoie de confidentialitate intre oricare doua parti, criptarea poate fi folosita la nivelul legatura de date.

Standardele actuale pentru cecuri electronice intre banci sunt ANSI X9.46 si X9.37. Electronic Check Clearing House Organization (ECCHO) a adoptat o serie de reguli pentru clearingul inter-bancar cu cecuri electronice, care sunt considerate a avea statutul de "instrumente negociabile".

Caracteristici ale prelucrarii cecurilor electronice - In exemplul din figura 10, tranzactia de afaceri incepe cu trimiterea de catre incasator a unei facturi catre platitor. Atunci cand soseste momentul pentru plata unei facturi, informatiile referitoare la aceasta factura sunt trimise de la sistemul incasatorului, iar aceste date sunt utilizate pentru a crea un cec. Acest cec electronic va include informatii din cecurile obisnuite (cum ar fi numele incasatorului, suma si data). Pentru a semna e-cecul, platitorul introduce codul PIN pentru a debloca smart-cardul ce detine "carnetul de cecuri". Formatul facturii nu este fix, putand fi flexibil, cu conditia de a respecta lungimea, forma si datele ce trebuie continute.

Cecul electronic semnat si factura sunt transmise catre incasator (platit) prin e-mail sau printr-o tranzactie Web. Incasatorul verifica semnatura platitorului din e-cec si factura,

separa informatiile facturii si pune suma platita in contul de primire. Incasatorul introduce codul sau PIN pentru deblocarea smart-cardului sau, utilizeaza acest "carnet electronic de cecuri" pentru a aproba e-cecul si semneaza un depozit electronic pentru a incasa suma din e-cec. Cecul aprobat (semnat de incasator) este dat mai departe bancii incasatorului pentru depozitare. Ambele banci, cea a platitorului si cea a incasatorului, intre care se realizeaza de fapt tranzactia reala a sumelor, verifica toate semnaturile si aprobarile din e-cec, utilizand doua nivele de certificate. Banca platitorului verifica daca cecul electronic transmis nu este duplicat, daca certificatul incasatorului si contul sunt in prezent valide, dupa care depoziteaza e-cecul in contul de stocare a cererilor platitorului. In final, platitorul primeste un articol care descrie intreaga tranzactie.

Semnaturi digitale pe cecuri electronice - Atunci cand este creat un cec electronic, in el este scris un set minim de informatii si cecul este semnat. Odata cu vehicularea e-cecului, alte informatii si alte semnaturi sunt adaugate atunci cand acesta este transmis intre parti. De exemplu, e-cecul trebuie sa fie:

- creat de platitor,

- co-semnat de co-platitor,

- certificat de banca,

- aprobat de incasator (platit),

- co-aprobat de co-incasator,

- depozitat si

- platit.

Unele din informatiile aditionale, cum ar fi certificatele si aprobarile, sunt parti permanente ale e-cecului si raman intacte pana in momentul returnarii la platitor. Alte informatii, cum ar fi timpul de intarziere, pot fi asociate e-cecului pentru o perioada a existentei sale si vor fi inlaturate si procesate separat. Acestea cer o structura flexibila a documentului si mecanismelor de semnare. Principalele caracteristici ale mecanismului FSML de semnare sunt:

- Documentul consta dintr-o secventa de blocuri, iar blocurile trebuie sa fie delimitate.

- Semnatura implementeaza algoritmi criptografici si/sau functii hash, si exista blocuri speciale ce se refera la acestea;

- Blocurile semnatura referite prin blocurile nume sau numar serial, refera blocul certificat ce face corespondenta cu cheia publica.

Semnatarul e-cecului poate opta pentru a include alte date personale, cum ar fi nume, adresa, numar de telefon, adresa e-mail etc. Aceste date sunt inregistrate in carnetul de cecuri electronice, la initializare, de catre banca si pot fi schimbate doar dupa ce carnetul respectiv a fost de-protejat, utilizand codul de administrare PIN al bancii. Aceasta metoda de promovare a informatiilor personale nu este la fel de sigura ca atunci cand aceste informatii sunt incluse in certificatul X.509 sau in blocul cont.

Carnetul de cecuri electronice - O semnatura olografa este influentata de miscarea muschilor mainii si de particularitatile biometrice ale semnatarului. Acestea fac foarte dificil pentru un falsificator sa realizeze o semnatura falsa perfecta, chiar daca falsificatorul dispune de un exemplu al semnaturii. In opozitie, o falsificare perfecta a semnaturii criptografice poate fi facuta de catre orice persoana care detine cheia privata a semnatarului de drept. Este foarte greu sa stabilesti, dispunand de o cheie publica, daca un e-cec este autentic sau falsificat. Smart-cardurile ce contin carnete de cecuri electronice sau alte dispozitive hard criptografice sunt utilizate tocmai pentru a ajuta la asigurarea ca o cheie privata este protejata cat mai bine si, in consecinta, semnaturile se realizeaza doar de catre semnatarii legitimi. Aceste dispozitive hard standardizeaza si simplifica generarea cheilor, distributia si utilizarea lor, deci se poate stabili un inalt nivel de incredere.

Distributia carnetelor de cecuri electronice poate diferi considerabil de la o banca la alta; raman insa cerintele de baza care includ:

- Certificatele X.509 semnate de banci si conturile sa corespunda specificatiilor FSML.

- Partea hard si soft a cecurilor electronice sa corespunda cerintelor si specificatiilor API referitoare la carnetele de cecuri electronice.

- Politicile de autoritati de certificare ale bancilor sa corespunda cerintelor si reglementarilor legale.

Unele dintre operatii, cum ar fi initializarea cardului si autoritatea de certificare a bancii, pot fi indeplinite de alte firme, ce actioneaza ca agenti ai bancii.

Serverele bancilor - Serverele de cecuri electronice din banci sunt utilizate pentru receptionarea e-cecurilor de la clienti prin e-mail, procesarea e-cecurilor primite si realizarea unei interfete cu sistemul de mentinere a inregistrarilor despre conturile cec - DDA. Functiile executate in mod tipic de un server de cecuri electronice dintr-o banca, sunt urmatoarele. Acest server primeste de la incasatori e-mail-uri care contin e-cecuri aprobate si depozite. E-cecurile sunt procesate si retinute in baza de date, pana cand sunt platite cu bani cash (clearingul). E-cecurile raman pe server si depozitele sunt trimise la sistemul DDA pentru procesare. E-cecurile problematice sunt returnate catre o statie speciala, pentru o analiza manuala si interventii.

Concluzii
Viteza cu care evolueaza tehnologia Internet-ului este impresionanta. Daca acum se apreciaza ca exista cateva milioane de oameni care folosesc serviciile Internet in fiecare

moment, numarul lor va creste exponential in anii urmatori. Dintr-un recent sondaj a reiesit ca, daca cu un an in urma 70% din utilizatorii Internet-ului apreciau e-mail-ul ca principal beneficiu si doar 30% Web-ul, astazi 50% din persoane considera pe primul loc e-mail-ul, 40% Web-ul si, deja 10%, comertul si platile electronice. In acest domeniu revolutia abia a inceput: sa observam ca platile electronice reprezinta un fel de e-mail in raport cu banii reali, asa cum posta electronica reprezenta, acum cativa ani, o adevarata revolutie in comunicatiile dintre persoane. Departe de a fi rezolvate problemele de securitate si acceptabilitate necesare, sistemele electronice de plata, puternic cercetate si experimentate azi, vor progresa rapid, devenind o realitate a Cyberspace-ului anilor viitori.