Securitatea sistemelor de Comerţ electronic

Comerţul electronic poate fi definit ca un demers de cumpărare sau vânzare prin intermediul transmiterii de date la distanţă.

Acest demers este specific politicii expansive a marketingului companiilor comerciale.

Prin intermediul Internetului se dezvoltă o relaţie de servicii şi schimb de mărfuri între ofertant şi viitorul cumpărător.

Categorii generale de comerţ electronic:

- **business-to-consumer** - companiile vând produse şi servicii consumatorilor individuali;
- **business-to-business** - companiile vând produse şi servicii altor companii;
- **consumer-to-consumer** - participanţii de pe o piaţă online pot să îşi vândă/cumpere reciproc bunuri;
- **business-to-government** - companiile pot vinde bunuri şi servicii agenţiilor guvernamentale.

- **procese de business** - companiile menţin şi folosesc informaţii pentru a identifica şi evalua clienţii, furnizorii şi angajaţii; în acelaşi timp, partajează aceste informaţii, în mod atent controlat, cu clienţii, furnizorii, angajaţii şi partenerii de afaceri;

Caracteristici plata electronica

- Valoarea platii trebuie sa depaseasca costul tranzactiei.
- Se pot face plati foarte mici (micro-payments) pentru mediile in care este necesar acest lucru
- Anonimitatea cumparatorului, detaliile de plata este posibil sa nu fie legate de cumparator fara detalii externe
- Asigura trasabilitate pentru urmarirea cumparaturilor suspecte (alcool, medicamente, etc)
- Durata ciclului masurat de la initierea platii pana in momentul transferului bancar.
- Instrument: credit card / debit card / Internet money

Forme si sisteme de plata electronice

Forme de plata electronice:

- Prepaid: contul platitorului (payer) este debitat înainte de folosirea serviciului
- Pay-now: contul este debitat la livrarea serviciului.
- Pay later (postpaid): contul platitorului este debitat dupa livrarea serviciului

Sisteme de plata: SET (Secure Electronic Transfer)

- Online cu digital cash
- Micropayments
- Card cu valoare stocata (smartcard)
- Cecuri electronice

Sisteme de plata: SET (Secure Electronic Transfer)

Multe companii financiare elaborează un şir de aplicaţii personale pentru efectuarea comerţului electronic şi în rezultat mai apare o problemă, compatibilitatea acestor aplicaţii, adică asemenea aplicaţii trebuie să aibă toţi participanţii la tranzacţie.

Pentru înlăturarea acestor probleme companiile VISA şi MasterCard împreună cu alte companii inclusiv şi IBM, au determinat specificul şi lista protocoalelor standartului SET.

Această specificare deschisă a devenit standartul comerţului electronic. Semnătura digitală şi certificatele digitale asigură identificarea şi autentificarea participanţilor la tranzacţia electronică.

Semnătura digitală de asemenea se foloseşte pentru asigurarea integrităţii datelor.

Sisteme de plata: SET (Secure Electronic Transfer)

SET asigură următoarele cerinţe speciale a securităţii operaţiunilor comerţului electronic:

- confidenţialitatea rechizitelor de plată şi confidenţialitatea informaţiei despre comandă, transmisă împreună cu datele de plată;
- păstrarea integrităţii datelor despre plăţi; integritatea este asigurată cu ajutorul semnăturii digitale;
- utilizează un sistem criptografic special cu chee deschisă pentru efecturea autentificării;
- autentificarea posesorului după card, care se asigură cu aplicarea semnăturii digitale şi certificatelor posesorului de carduri;
- autentificarea vînzătorului şi a posibilităţilor de a primi plăţile pe carduri cu utilizarea semnăturii digitale şi certificatelor vînzătorului;
- confirmarea situaţiei, că banca vînzătorului este o organizaţie reală, ce activează şi poate primi şi efectua plăţi cu carduri prin reţeua cu sistem de procesare; această confirmare este asigurată prin semnătura digitală şi certificatelor băncii vînzătorului;

Sisteme de plata: SET (Secure Electronic Transfer)

- efectuarea plăţilor în rezultatul autentificării certificatului cu cheea deschisă pentru toate părţile participante la tranzacţie;
- pretecţia transmiterii datelor în majoritatea cazurilor cu ajutorul algoritmilor criptografici.
- Prioritatea de bază a standartului SET faţă de celelalte sisteme existente de asigurare a securităţii informaţionale constă în utilizarea certificatelor digitale (standartul X509, versiunea 3), care asociază deţinătorul cardului şi banca vînzătorului cu un şir de instituţii bancare ce utilizează sistemele de plată VISA şi MasterCard. Set permite păstrarea relaţiilor existente dintre bancă, deţinătorul de card şi vînzători, şi se integrează cu sistemele existente, bazînduse pe următoarele calităţi:
- standart complet documentat pentru industria financiară;
- bazat pe standartele internaţionale a sistemelor de plăţi;
- bazat pe tehnologiile şi mecanizmele legislative ale industriei financiare existente

Sisteme de plata: SET (Secure Electronic Transfer)

- CyberCash (credit card);
- CyberCoin (monede electronice); sub 10 dolari, se cumpara monede digitale pastrate la CyberCash;
- Smartcard cu valoare stocata:
  - Mondex: nu utilizeaza banca drept intermediar;
  - First Virtual: fara criptare, dar schimba mereu numarul cardului; verificat prin e-mail.
  - CyberCash Check (cecuri electronice):
  - NetCheck: platitorul are carnet de cecuri de tip smartcard cu PIN. Semnatura electronica. Cecul cu semnatura electronica, împreuna cu factura, este transmis încasatorului, care-l încaseaza de la banca.
- Payline / SG2: cardul trece printr-un gestionar securizat, nu trece pe la comerciant.

Protocol SET

Scop

Stabilirea de tranzactii financiare care:

- Asigura confidentialitatea informatiilor;
- Asigura integritatea instructiunilor de plata pentru bunurile si serviciile comandate;
- Autentifica detinatorul de card si comerciantul

Entitati

- Detinator de card (Cardholder)
- Comerciant (Merchant - web server)
- Banca Comerciant (payment gateway, acquirer)
- Banca detinator card

Mod lucru SET

Conditie: Comerciantul si cumparatorul sunt inregistrati la o CA

Pasi:

1. Clientul decide ce cumpara
2. Clientul trimite comanda si informatiile de plata (mesaj cu 2 parti)
   - Comanda – pentru comerciant
   - Informatii despre card – pentru banca comerciantului
3. Comerciantul trimite informatia despre card la banca sa
4. Banca comerciantului verifica cu cea a cumparatorului autorizarea de plata
5. Banca cumparatorului trimite autorizarea la cea a comerciantului
6. Banca comerciantului trimite autorizarea la comerciant
7. Comerciantul completeaza comanda si trimite confirmare clientului
8. Comerciantul captureaza tranzactia de la banca sa
9. Cumparatorul tipareste chitanta pentru client

Securitatea cardurilor de credit

- Cartile de credit (cardurile bancare) sunt cele mai utilizate mijloace de plată.

- Securitatea tranzactiilor s-a imbunatatit, insa nu semnificativ

- Bancile si furnizorii sistemelor de plata dezvolta noi metode de securizare pentru a preintampina fraudele. Mai raspandite: **codurile CVC / CVV** (cod format din 3-4 cifre, situat pe verso-ul cardului) sau **protocolul 3D Secure**, ambele sunt utilizate la tranzactiile pe Internet.

Roluri 3D Secure

Issuer (Emitent)

- Gestioneaza serviciul de inregistrare a detinatorului de card (inclusiv verificarea identitatii fiecarui detinator la inregistrare) si autentifica detinatorul de card la plata on-line

Acquirer (Achizitor)

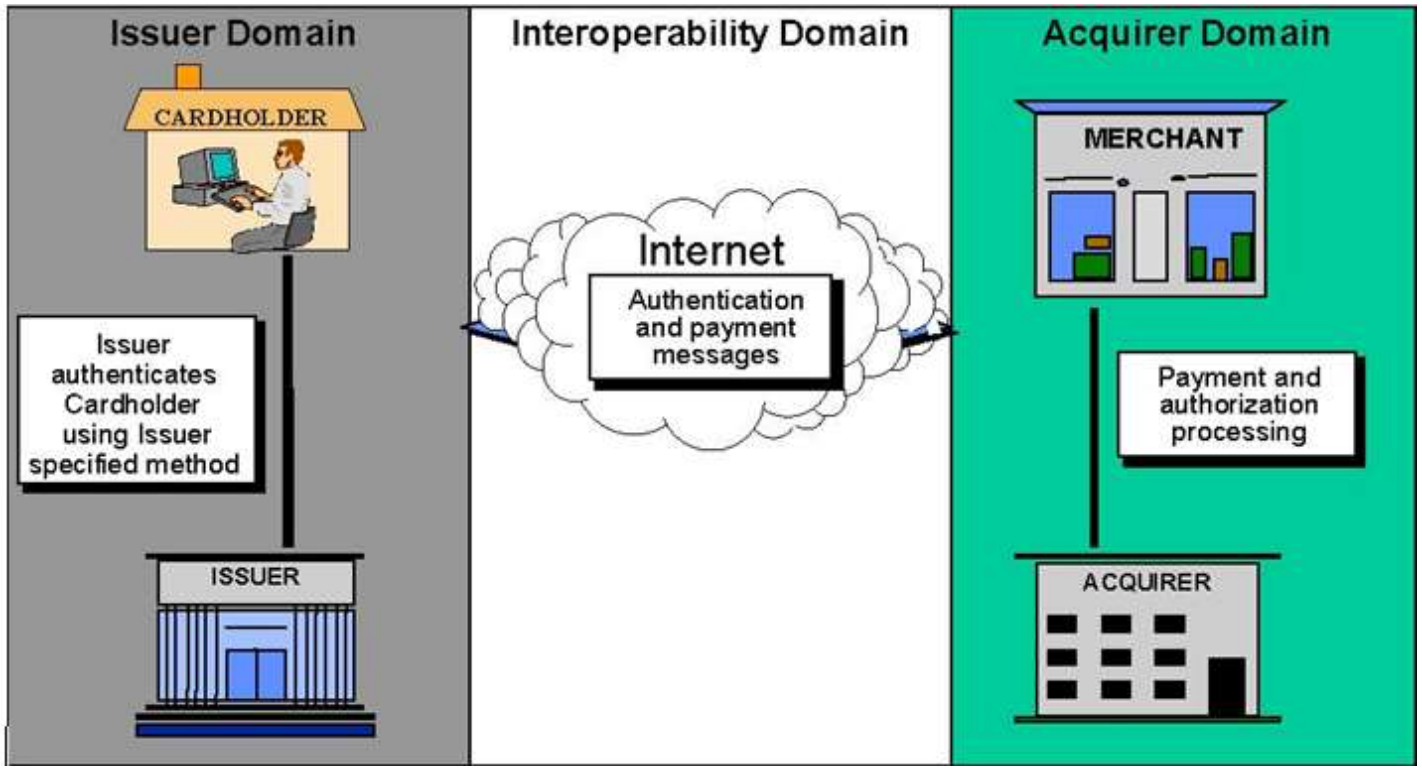
- Asigura ca vanzatorul participant la tranzactia Internet opereaza sub o intelegere cu Acquirer si furnizeaza procesarea tranzactiei pentru autentificare

Interoperability (Interoperabilitatea)

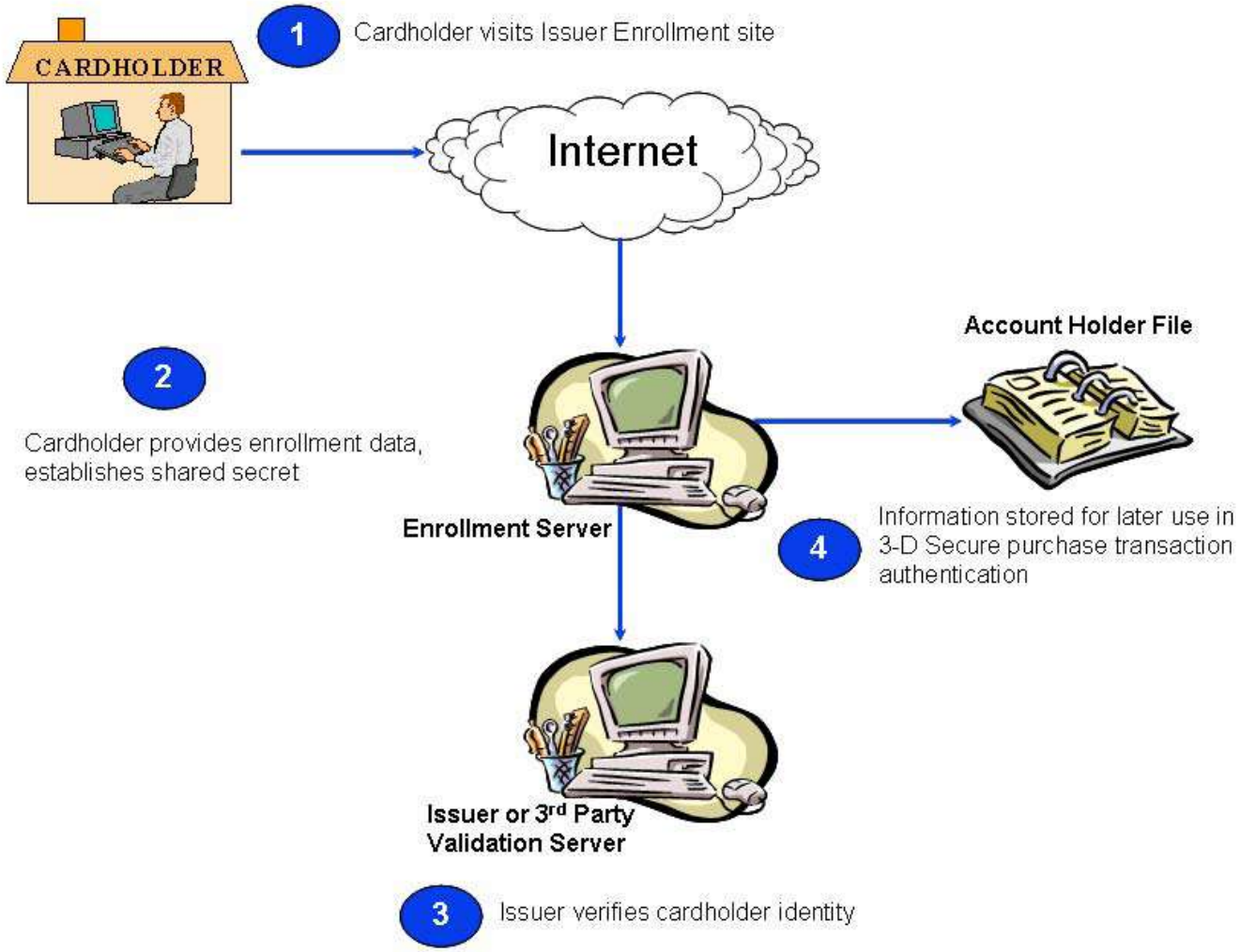
- Faciliteaza schimbul de informatii intre cele doua domenii pe baza unui protocol uzual si partajaza serviciile

Oferit de VISA şi MasterCard sub numele “Verified by VISA”, respectiv “MasterCard SecureCode”

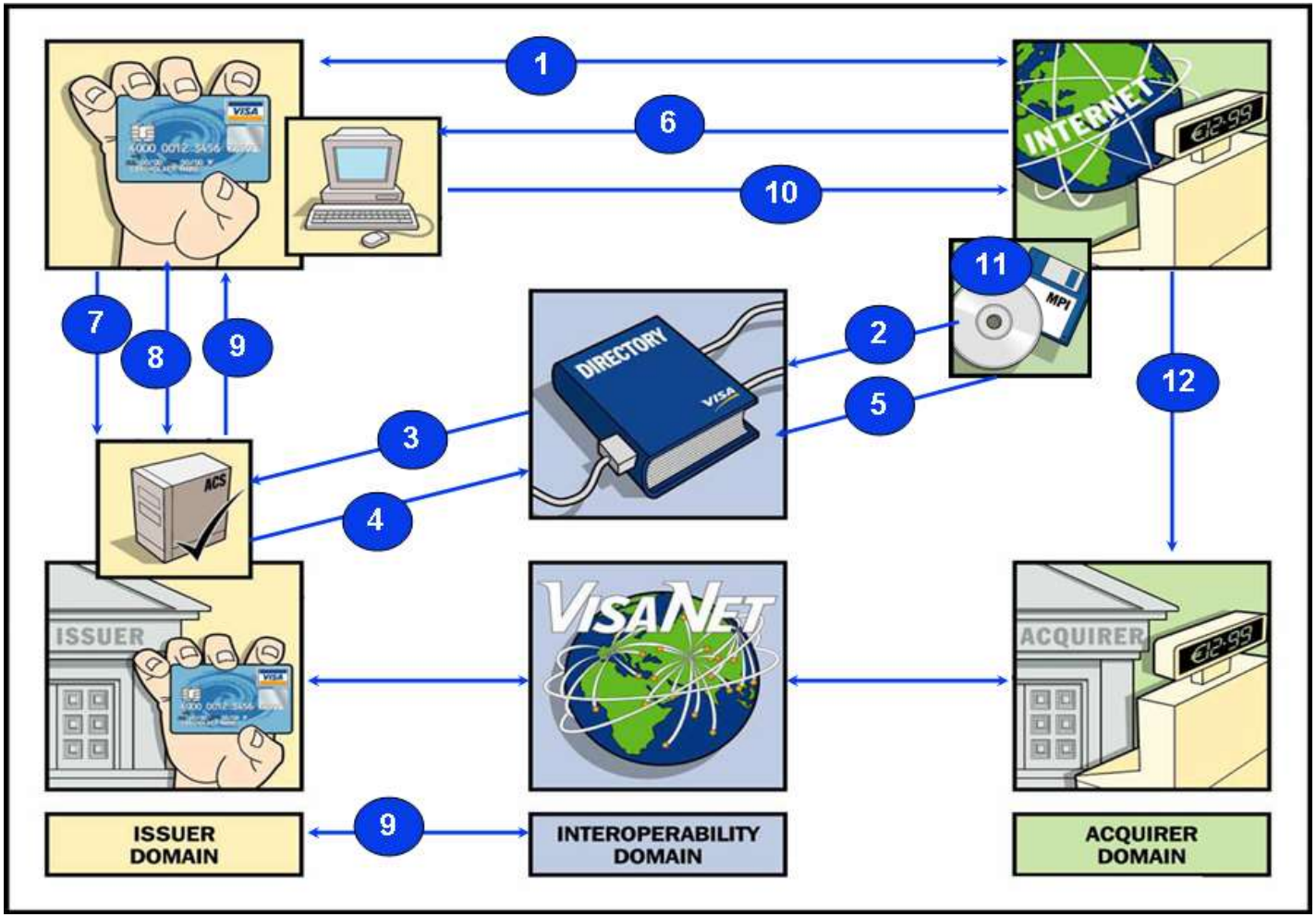
Arhitectura 3D Secure



Procesul de inregistrare (enrollment)



Exemplu tranzactie



Pasi (1)

- Pas 1 – cumparatorul creaza cosul de cumparaturi si declanseaza procesul de plata;
- Pas 2 – Merchant Server Plug-in (MPI) trimite (Primary Account Number) PAN si informatii despre device utilizator la Directory Server (DS).
- Pas 3 - DS interogheaza Access Control Server (ACS). Pentru autentificarea este disponibil PAN si tipul de device. Daca ACS nu este disponibil DS trimite mesaj la MPI si sare la pas 5.
- Pas 4 - ACS raspunde catre DS
- Pas 5 - DS inainteaza raspunsul de la ACS sau cel propriu la MPI. Daca nu s-a autentificat procesarea tranzactiei se incheie.
- Pas 6 - MPI trimite Payer Authentication Request la ACS prin echipamentul cumparatorului (PC, device mobil..).
- Pas 7 - ACS receptioneaza Payer Authentication Request

Pasi (2)

- Pas 8 - ACS autentifica cumparatorul utilizand procesele aplicabile la PAN (password, chip, PIN, etc.) si formeaza Payer Authentication Response message cu valorile corespunzatoere si il semneaza.
- Pas 9 - ACS returneaza Payer Authentication Response la MPI prin device cumparator si trimite datele selectate la Authentication History Server (AHS).
- Pas 10 – MPI receptioneaza Payer Authentication Response.
- Pas 11 - MPI valideaza semnatura Payer Authentication Response (fie singur, fie prin pasarea mesajului la un server de validare)
- Pas 12 – Comerciantul incepe autorizarea cu propriul achizitor.

Dupa acest pas achizitorul face autorizarea cu un sistem (ex VisaNet) si returneaza rezultatul comerciantului

Sfaturi utile

- Evitarea operatiunilor online banking si logarea la diferite conturi de pe alte calculatoare decat cele personale;
- Nu se introduc date personale pe site-uri ce nu accepta legaturi securizate;
- Atentie la phishing;
- La tranzactiile online acceptati daca se cere codul CVV, dar refuzati tranzactia daca se cere codul PIN;

Baza legislativă

- Legea Republicii Moldova privind comerţul electronic, nr.284-XV din 22.07.2004:

  - creează cadrul juridic pentru efectuarea comerţului electronic;

  - stabilirea principiilor de reglementare şi susţinere de către stat a activităţii în domeniul comerţului electronic;

  - stabilirea regimului juridic al contractelor şi comunicărilor electronice privind vînzarea bunurilor, executarea lucrărilor sau prestarea serviciilor.