Protocolul 3-D Secure

Prof. Dr. Adrian Atanasiu

Universitatea București

January 2, 2016

Introducere

Protocolul *SET*: foarte sigur dar complex și costisitor în resurse. 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 entități ("*domenii*").

Introducere

Protocolul *SET*: foarte sigur dar complex și costisitor în resurse.
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 entități ("*domenii*").
Scopul lor este acela de a defini clar responsabilitățile părților implicate în tranzacție.
Cele trei domenii (3-D: Three Domanins) sunt:

Introducere

Protocolul *SET*: foarte sigur dar complex și costisitor în resurse.
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 entități ("*domenii*").
Scopul lor este acela de a defini clar responsabilitățile părților implicate în tranzacție.
Cele trei domenii (3-D: Three Domanins) sunt:

1. *Domeniul Emitentului*: cuprinde deținătorii de card și emitenții cardurilor lor;

Introducere

Protocolul *SET*: foarte sigur dar complex și costisitor în resurse.
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 entități ("*domenii*").
Scopul lor este acela de a defini clar responsabilitățile părților implicate în tranzacție.
Cele trei domenii (3-D: Three Domanins) sunt:

1. *Domeniul Emitentului*: cuprinde deținătorii de card și emitenții cardurilor lor;
2. *Domeniul Acceptatorului*: cuprinde comercianții și acceptatorii lor;

Introducere

Protocolul *SET*: foarte sigur dar complex și costisitor în resurse.
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 entități ("*domenii*").
Scopul lor este acela de a defini clar responsabilitățile părților implicate în tranzacție.
Cele trei domenii (3-D: Three Domanins) sunt:

1. *Domeniul Emitentului*: cuprinde deținătorii de card și emitenții cardurilor lor;
2. *Domeniul Acceptatorului*: cuprinde comercianții și acceptatorii lor;
3. *Domeniul de Interoperabilitate*: asigură comunicarea între emitenți, acceptatori și sistemul Visa.

Domeniul emitentului

- Când cumpărătorul inițiază plata, comerciantul va cere 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).
- Deci comerciantul va începe întotdeauna prin a cere emitentului să-i autentifice întâi cardul, apoi deținătorul de card.

Domeniul emitentului

- Când cumpărătorul inițiază plata, comerciantul va cere 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).
- Deci comerciantul va începe întotdeauna prin a cere emitentului să-i autentifice întâi cardul, apoi deținătorul de card.
- Deținătorul de card trebuie să se înregistreze (*enrollment*) în sistem la emitentul său și să-și declare un nume și o parolă prin care emitentul poate să-l autentifice în momentul tranzacției; această autentificare este trimisă comerciantului.

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

- După ce îl autentifică, emitentul va genera un răspuns semnat electronic pe care îl trimite comerciantului pentru a-i confirma autenticitatea deținătorului de card.
  Comerciantul va putea trece acum la faza de autorizare normală a tranzacției.
- Deținătorul de card poate să-și instaleze un portofel electronic (*eWallet*), care va conține informațiile de identitate (nume, adresă, parolă etc) și cele de card (tip card, număr card, dată de expirare) necesare 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* al cardurilor și deținătorilor de card păstrând într-un server de înregistrare (*Enrollment Server*) numerele de card, numele și parola deținătorilor.

- Emitentul dispune de un serviciu de înregistrare în sistemul *3-D Secure* al cardurilor și deținătorilor de card păstrând într-un server de înregistrare (*Enrollment Server*) numerele de card, numele și parola deținătorilor.
- Emitentul mai dispune și de un server de control al accesului (*ACS – Access Control Server*) cu rolul de a primi cererea de autentificare a cumpărătorului venită de la comerciant, de a face autentificarea și de a trimite răspunsul semnat înapoi la comerciant.

Domeniul inter-operabilitate

- În acest domeniu, Visa (sau MasterCard, care a aderat ulterior la sistem) dispune de un Director (*Directory Service*): server central cu acces la Internet 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.

Domeniul inter-operabilitate

- În acest domeniu, Visa (sau MasterCard, care a aderat ulterior la sistem) dispune de un Director (*Directory Service*): server central cu acces la Internet 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 ulterioare)

Domeniul acceptatorului

Aici acceptatorii trebuie să dispună de o poartă de acces (*payment gateway*) la sistemul de plată prin carduri Visa/MasterCard, iar comercianții trebuie să-și instaleze un modul *3-D Secure* cu numele *MPI* (*Merchant Plug-In module*).

Domeniul acceptatorului

Aici acceptatorii trebuie să dispună de o poartă de acces (*payment gateway*) la sistemul de plată prin carduri Visa/MasterCard, iar comercianții trebuie să-și instaleze un modul *3-D Secure* cu numele *MPI* (*Merchant Plug-In module*).

- Acest modul de comerciant *3-D Secure* va genera cereri către emitent de autentificare a cardului și a cumpărătorului, iar după primirea răspunsului va trimite cererea de autorizare a tranzacției către poarta de acces a acceptatorului (prin intermediul modului client de *eComerț*).

Domeniul acceptatorului

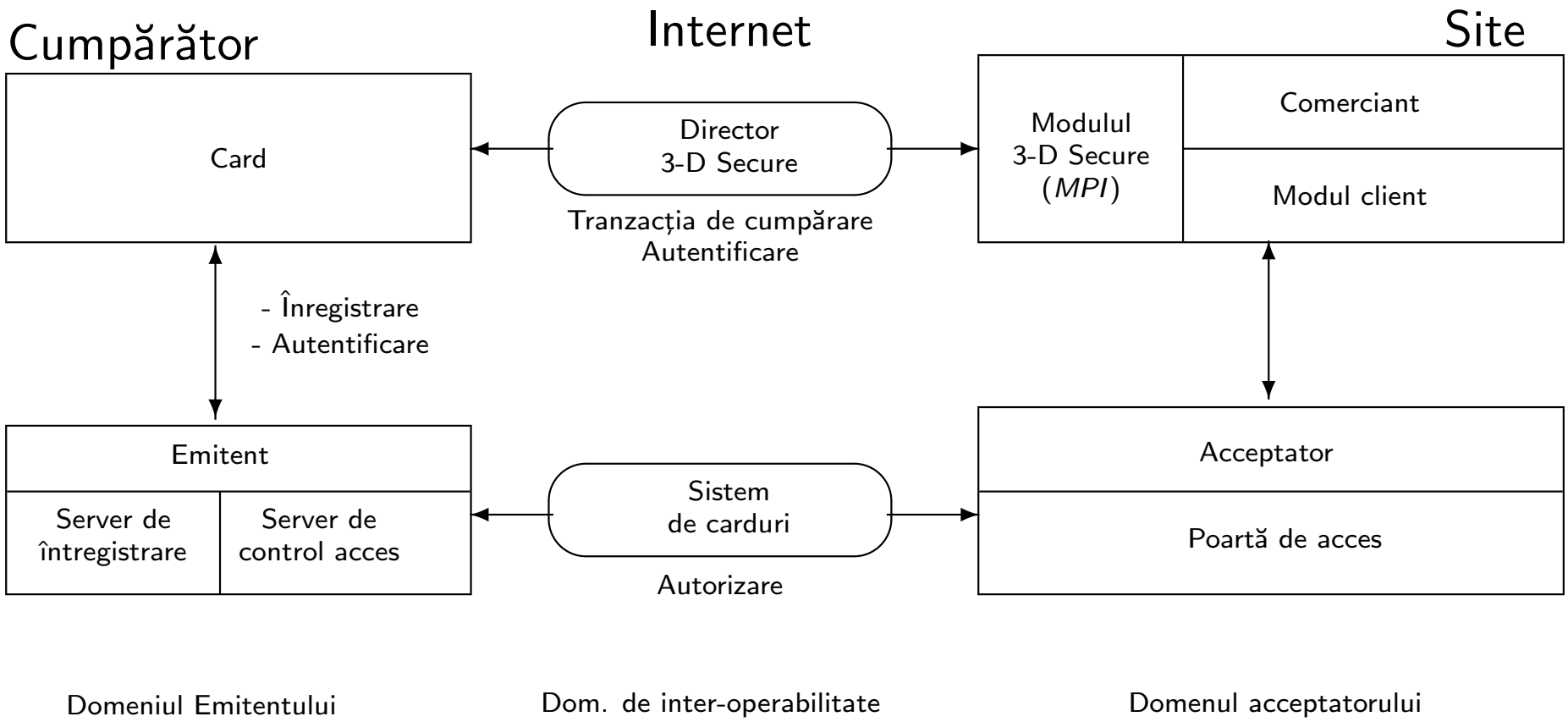
Aici acceptatorii trebuie să dispună de o poartă de acces (*payment gateway*) la sistemul de plată prin carduri Visa/MasterCard, iar comercianții trebuie să-și instaleze un modul *3-D Secure* cu numele *MPI* (*Merchant Plug-In module*).

- Acest modul de comerciant *3-D Secure* va genera cereri către emitent de autentificare a cardului și a cumpărătorului, iar după primirea răspunsului va trimite cererea de autorizare a tranzacției către poarta de acces a acceptatorului (prin intermediul modului client de *eComerț*).
- La rândul lui, acesta 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 printr-o parolă, iar Directorul va face același lucru față de comerciant. Deci, la fiecare tranzacție are loc în paralel și o autentificare a comerciantului.

- În cursul acestei operații modulul *MPI* al comerciantului se va autentifica față de Director printr-un certificat de autenticitate sau printr-o parolă, iar Directorul va face același lucru față de comerciant. Deci, la fiecare tranzacție are loc în paralel și o autentificare a comerciantului.
- După primirea răspunsului de autorizare, modulul comerciantului va trimite clientului 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 clientului și va trece direct la autorizare, sau va respinge tranzacția.

Schema de principiu a domeniilor protocolului *3-D Secure*



- Mesajele privind autentificarea circulă între Domeniile emitentului și acceptatorului, prin intermediul Domeniului de inter-operabilitate.

- Mesajele privind autentificarea circulă între Domeniile emitentului și acceptatorului, prin intermediul Domeniului de inter-operabilitate.
- Mesajele prin care se face autentificarea deținătorului de card circulă între acesta și emitentul său, în cadrul Domeniului emitentului.

- Mesajele privind autentificarea circulă între Domeniile emitentului și acceptatorului, prin intermediul Domeniului de inter-operabilitate.
- 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 schimbate între acceptator și emitent – în vederea realizării autorizării și procesării plății – circulă prin sistemul de carduri (VisaNet, BankNet) în cadrul Domeniului de inter-operabilitate.

- Legăturile prin Internet sunt securizate, efectuate prin protocolul *SSL*, în care fiecare entitate server dispune de un certificat iar mesajele sunt criptate.
  Comerciantul nu are acces la datele cardului de plată (care nu sunt stocate pe site-ul său, și poate vedea numai decizia finală de autentificare dată de emitent.

- Legăturile prin Internet sunt securizate, efectuate prin protocolul *SSL*, în care fiecare entitate server dispune de un certificat iar mesajele sunt criptate.
  Comerciantul nu are acces la datele cardului de plată (care nu sunt stocate pe site-ul său, și poate vedea numai decizia finală de autentificare dată de emitent.
- Protocolul *3-D Secure* verifică autenticitatea cardului și a deținătorului de card.

- Legăturile prin Internet sunt securizate, efectuate prin protocolul *SSL*, în care fiecare entitate server dispune de un certificat iar mesajele sunt criptate.
  Comerciantul nu are acces la datele cardului de plată (care nu sunt stocate pe site-ul său, și poate vedea numai decizia finală de autentificare dată de emitent.
- Protocolul *3-D Secure* verifică autenticitatea cardului și a deținătorului de card.
- Protocolul poate fi folosit în principiu și pe alte canale de plată: telefoane mobile, asistenți digitali personali (PDA) sau televiziunea digitală prin cablu.

SecureCode

Este un grup de trei protocoale de autentificare a deținătorului de card oferite de MasterCard: *SPA/UCAF*, *CAP*, și protocolul *3-D Secure* în versiunea MasterCard.

SecureCode

Este un grup de trei protocoale de autentificare a deținătorului de card oferite de MasterCard: *SPA/UCAF*, *CAP*, și protocolul *3-D Secure* în versiunea MasterCard.

- Protocolul *SPA* (*Secure Payment Application*) folosește mecanismul *UCAF* (*Universal Cardholder Authentification Field*) de transport de date prin rețeaua MasterCard, bazat pe un "caracter de autentificare" (*authentication token*) pentru a autentifica deținătorul de card care a făcut tranzacția.

SecureCode

Este un grup de trei protocoale de autentificare a deținătorului de card oferite de MasterCard: *SPA/UCAF*, *CAP*, și protocolul *3-D Secure* în versiunea MasterCard.

- Protocolul *SPA* (*Secure Payment Application*) folosește mecanismul *UCAF* (*Universal Cardholder Authentification Field*) de transport de date prin rețeaua MasterCard, bazat pe un "caracter de autentificare" (*authentication token*) pentru a autentifica deținătorul de card care a făcut tranzacția.
- Protocolul *CAP* (*Chip Card Authentication Program*): variantă a *SPA* pentru plata cu smartcarduri. Presupune de regulă cuplarea la calculator a unui cititor de astfel de carduri.

SecureCode

Este un grup de trei protocoale de autentificare a deținătorului de card oferite de MasterCard: *SPA/UCAF*, *CAP*, și protocolul *3-D Secure* în versiunea MasterCard.

- Protocolul *SPA* (*Secure Payment Application*) folosește mecanismul *UCAF* (*Universal Cardholder Authentification Field*) de transport de date prin rețeaua MasterCard, bazat pe un "caracter de autentificare" (*authentication token*) pentru a autentifica deținătorul de card care a făcut tranzacția.
- Protocolul *CAP* (*Chip Card Authentication Program*): variantă a *SPA* pentru plata cu smartcarduri. Presupune de regulă cuplarea la calculator a unui cititor de astfel de carduri.
- MasterCard adoptă în 2002 protocolul *3-D Secure* într-o variantă proprie, folosit tot sub denumirea *SecureCode*.

Protocolul *SPA/UCAF*

- Protocolul cere participarea directă a emitentului – care autentifică cumpărătorul – și a comerciantului, care dispune de un modul client de *e-commerce* specific *SPA*.

Protocolul *SPA/UCAF*

- Protocolul cere participarea directă a emitentului – care autentifică cumpărătorul – și a comerciantului, care dispune de un modul client de *e-commerce* specific *SPA*.
- El 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 (“*SPA applet*”) are atât funcția de *ePortofel* (deține datele de identificare și de card de plată), cât și aceea de a interacționa cu comerciantul și cu emitentul cardului.

Protocolul *SPA/UCAF*

- Protocolul cere participarea directă a emitentului – care autentifică cumpărătorul – și a comerciantului, care dispune de un modul client de *e-commerce* specific *SPA*.
- El 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 (“*SPA applet*”) are atât funcția de *ePortofel* (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 pe calculatorul lor personal.

Autentificare

- În momentul înregistrării cumpărătorul își va defini o parolă (sau un *PIN*), după care va fi autentificat ulterior.

Autentificare

- În momentul înregistrării cumpărătorul își va defini o parolă (sau un *PIN*), după care va fi autentificat ulterior.
- Când începe tranzacția, *ePortofelul* se activează și 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.

Autentificare

- În momentul înregistrării cumpărătorul își va defini o parolă (sau un *PIN*), după care va fi autentificat ulterior.
- Când începe tranzacția, *ePortofelul* se activează și 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 verifică datele introduse cu cele păstrate la momentul înregistrării în sistem și va genera un mesaj cu un "caracter de autentificare" pe care îl trimite *ePortofelului*. Acest caracter de autentificare poartă numele de *AAV* (*Accountholder Authentication Value*) și arată – în esență – dacă parola introdusă este corectă; caz în care deținătorul de card este declarat autentic.

Autentificare

- Comercianții au un modul-client de *eComerț* specific protocolului, furnizat de acceptatorul participant la sistem.

  Acesta interacționează cu cumpătorii și cu *ePortofelele* lor, precum și cu poarta de acces a acceptatorului.

Autentificare

- Comercianții au un modul-client de *eComerț* specific protocolului, furnizat de acceptatorul participant la sistem.

  Acesta interacționează cu cumpătorii și cu *ePortofelele* lor, precum și cu poarta de acces a acceptatorului.
- Când clientul declanșează tranzacția de cumpărare, comerciantul va adauga la datele tranzacției și caracterul de autentificare.

  Pachetul astfel format este trimis spre acceptator.

Autentificare

- Comercianții au un modul-client de *eComerț* specific protocolului, furnizat de acceptatorul participant la sistem.

  Acesta interacționează cu cumpătorii și cu *ePortofelele* lor, precum și cu poarta de acces a acceptatorului.
- Când clientul declanșează tranzacția de cumpărare, comerciantul va adauga la datele tranzacției și caracterul de autentificare.

  Pachetul astfel format este trimis spre acceptator.
- Acesta trimite mai departe către emitent cererea de autorizare a tranzacției și semnul de autentificare.

Autentificare

- Comercianții au un modul-client de *eComerț* specific protocolului, furnizat de acceptatorul participant la sistem.

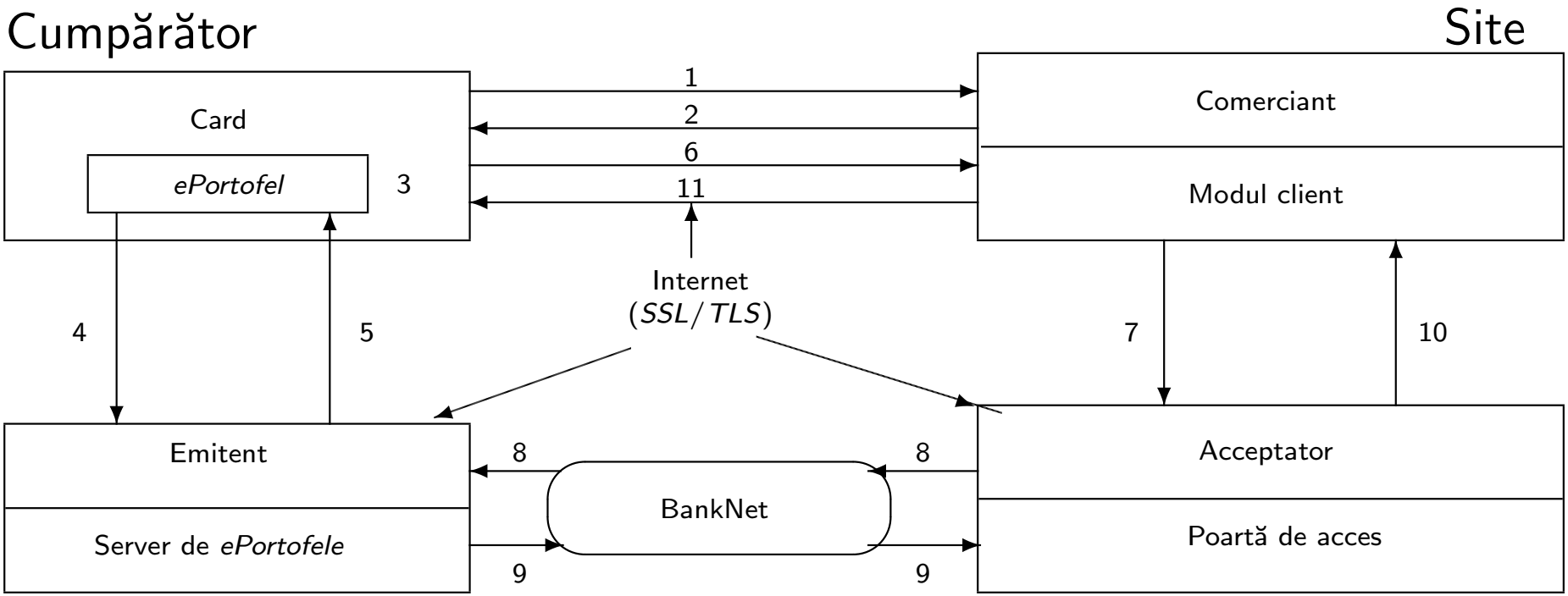
  Acesta interacționează cu cumpătorii și cu *ePortofelele* lor, precum și cu poarta de acces a acceptatorului.
- Când clientul declanșează tranzacția de cumpărare, comerciantul va adauga la datele tranzacției și caracterul de autentificare.

  Pachetul astfel format este trimis spre acceptator.
- Acesta trimite mai departe către emitent cererea de autorizare a tranzacției și semnul de autentificare.
- Emitentul compară semnul de autentificare primit cu cel generat la autentificarea cumpărătorului.

  Dacă ele coincid, trece la procedura de autorizare, încheiată cu un mesaj de răspuns trimis acceptatorului.

Mod de funcționare

O tranzacție de *e-commmerce* realizată cu protocolul *SPA/UCAF*:



Sistem de carduri
Master Card

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.
5. Emitentul autentifică cumpărătorul și generează caracterul de autentificare *AAV* pe care îl trimite (ca pe un certificat de autenticitate) *ePortofelului*.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.
5. Emitentul autentifică cumpărătorul și generează caracterul de autentificare *AAV* pe care îl trimite (ca pe un certificat de autenticitate) *ePortofelului*.
6. *ePortofelul* va transmite acest caracter către comerciant și va completa automat toate datele din formularul de comandă al comerciantului.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.
5. Emitentul autentifică cumpărătorul și generează caracterul de autentificare *AAV* pe care îl trimite (ca pe un certificat de autenticitate) *ePortofelului*.
6. *ePortofelul* va transmite acest caracter către comerciant și va completa automat toate datele din formularul de comandă al comerciantului.
7. Comerciantul trimite către acceptator o cerere de autorizare a tranzacției, împreună cu caracterul de autentificare.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.
5. Emitentul autentifică cumpărătorul și generează caracterul de autentificare *AAV* pe care îl trimite (ca pe un certificat de autenticitate) *ePortofelului*.
6. *ePortofelul* va transmite acest caracter către comerciant și va completa automat toate datele din formularul de comandă al comerciantului.
7. Comerciantul trimite către acceptator o cerere de autorizare a tranzacției, împreună cu caracterul de autentificare.
8. Acesta va expedia cererea către emitent folosind rețeaua BankNet a MasterCard, în vederea autorizării.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.
5. Emitentul autentifică cumpărătorul și generează caracterul de autentificare *AAV* pe care îl trimite (ca pe un certificat de autenticitate) *ePortofelului*.
6. *ePortofelul* va transmite acest caracter către comerciant și va completa automat toate datele din formularul de comandă al comerciantului.
7. Comerciantul trimite către acceptator o cerere de autorizare a tranzacției, împreună cu caracterul de autentificare.
8. Acesta va expedia cererea către emitent folosind rețeaua BankNet a MasterCard, în vederea autorizării.
9. Emitentul compară caracterul de autentificare primit acum cu cel generat de el la pasul 5.
   Dacă acestea coincid, va executa procedura de autorizare și va expedia răspunsul de autorizare către acceptator.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.
5. Emitentul autentifică cumpărătorul și generează caracterul de autentificare *AAV* pe care îl trimite (ca pe un certificat de autenticitate) *ePortofelului*.
6. *ePortofelul* va transmite acest caracter către comerciant și va completa automat toate datele din formularul de comandă al comerciantului.
7. Comerciantul trimite către acceptator o cerere de autorizare a tranzacției, împreună cu caracterul de autentificare.
8. Acesta va expedia cererea către emitent folosind rețeaua BankNet a MasterCard, în vederea autorizării.
9. Emitentul compară caracterul de autentificare primit acum cu cel generat de el la pasul 5.
   Dacă acestea coincid, va executa procedura de autorizare și va expedia răspunsul de autorizare către acceptator.
10. Răspunsul este trimis mai departe la comerciant.

Detalii tranzacție

1. *ePortofelul* cumpărătorului detectează un site de comerciant membru al sistemului,
2. Citește de pe site-ul acestuia date referitoare la formularul de comandă și identitatea comerciantului.
3. În momentul inițierii cumpărăturii, realizează o procedură de cerere de date de autentificare.
4. În final, *ePortofelul* trimite datele asupra tranzacției și cele de autentificare furnizate de cumpărător, către serverul de *ePortofele* al emitentului.
5. Emitentul autentifică cumpărătorul și generează caracterul de autentificare *AAV* pe care îl trimite (ca pe un certificat de autenticitate) *ePortofelului*.
6. *ePortofelul* va transmite acest caracter către comerciant și va completa automat toate datele din formularul de comandă al comerciantului.
7. Comerciantul trimite către acceptator o cerere de autorizare a tranzacției, împreună cu caracterul de autentificare.
8. Acesta va expedia cererea către emitent folosind rețeaua BankNet a MasterCard, în vederea autorizării.
9. Emitentul compară caracterul de autentificare primit acum cu cel generat de el la pasul 5.
   Dacă acestea coincid, va executa procedura de autorizare și va expedia răspunsul de autorizare către acceptator.
10. Răspunsul este trimis mai departe la comerciant.
11. Comerciantul memorează răspunsul și tranzacția și afișează un raport cu rezultatul tranzacției, care se va păstra și în *ePortofel*.

Asemănări între *3-D Secure* și *SPA/UCAF*

- Ambele protocoale sunt simple și pot fi implementate cu costuri mai mici decât protocolul *SET* (acesta însă oferă o securitate mai bună).

Asemănări între *3-D Secure* și *SPA/UCAF*

- Ambele protocoale sunt simple și pot fi implementate cu costuri mai mici decât protocolul *SET* (acesta însă oferă o securitate mai bună).
- Ambele protocoale fac autentificarea cumpărătorului deținător de card, verificată de emitentul cardului.
  Emitenții sunt liberi să-și aleagă și alte metode de autentificare deoarece ei generează decizia finală prin care cumpărătorul este declarat autentic și deținător legal al cardului.

Asemănări între *3-D Secure* și *SPA/UCAF*

- Ambele protocoale sunt simple și pot fi implementate cu costuri mai mici decât protocolul *SET* (acesta însă oferă o securitate mai bună).
- Ambele protocoale fac autentificarea cumpărătorului deținător de card, verificată de emitentul cardului.
  Emitenții sunt liberi să-și aleagă și alte metode de autentificare deoarece ei generează decizia finală prin care cumpărătorul este declarat autentic și deținător legal al cardului.
- În ambele protocoale emitenții trebuie să dispună de programe 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 specific protocolului.

Deosebiri între *3-D Secure* și *SPA/UCAF*

- La *3-D Secure*, cumpărătorul nu trebuie să facă nici o modificare în calculatorul său, pe când la *SPA/UCAF* acesta trebuie să ceară de la emitent un program (*ePortofel* sau "*SPA applet*") pe care trebuie să și-l instaleze.

Deosebiri între *3-D Secure* și *SPA/UCAF*

- La *3-D Secure*, cumpărătorul nu trebuie să facă nici o modificare în calculatorul său, pe când la *SPA/UCAF* acesta trebuie să ceară de la emitent un program (*ePortofel* sau "*SPA applet*") pe care trebuie să și-l instaleze.
- Protocolul *SPA/UCAF* este mai simplu și mai rapid decât *3-D Secure* (acesta din urmă necesită o autentificare în mai mulți pași și sunt schimbate mai multe mesaje prin Internet).

Deosebiri între *3-D Secure* și *SPA/UCAF*

- La *3-D Secure*, cumpărătorul nu trebuie să facă nici o modificare în calculatorul său, pe când la *SPA/UCAF* acesta trebuie să ceară de la emitent un program (*ePortofel* sau "*SPA applet*") pe care trebuie să și-l instaleze.
- Protocolul *SPA/UCAF* este mai simplu și mai rapid decât *3-D Secure* (acesta din urmă necesită o autentificare în mai mulți pași și sunt schimbate mai multe mesaje prin Internet).
- În *3-D Secure* autentificarea se face la fiecare tranzacție, în vreme ce la *SPA/UCAF* autentificarea se obține o singură dată la începutul unei sesiuni de cumpărături, iar rezultatul este păstrat în *ePortofel*; aceasta permite efectuarea unei serii întregi de cumpărături de pe mai multe site-uri de comercianți folosind o singură autentificare.

Deosebiri între *3-D Secure* și *SPA/UCAF*

- În *3-D Secure* comerciantul se autentifică explicit față de Directorul sistemului, în vreme ce la *SPA/UCAF* comerciantul se autentifică implicit (prin modulul client specific recunoscut de *ePortofel*).

Deosebiri între *3-D Secure* și *SPA/UCAF*

- În *3-D Secure* comerciantul se autentifică explicit față de Directorul sistemului, în vreme ce la *SPA/UCAF* comerciantul se autentifică implicit (prin modulul client specific recunoscut de *ePortofel*).
- Sistemul *3-D Secure* este un sistem centralizat (toate cererile de autentificare ale comercianților trec printr-un Director central) în vreme ce sistemul *SPA/UCAF* este descentralizat (o autentificare implică doar comunicarea între cumpărător și emitentul său, lipsind conceptul de Director).

Deosebiri între *3-D Secure* și *SPA/UCAF*

- În *3-D Secure* comerciantul se autentifică explicit față de Directorul sistemului, în vreme ce la *SPA/UCAF* comerciantul se autentifică implicit (prin modulul client specific recunoscut de *ePortofel*).
- Sistemul *3-D Secure* este un sistem centralizat (toate cererile de autentificare ale comercianților trec printr-un Director central) în vreme ce sistemul *SPA/UCAF* este descentralizat (o autentificare implică doar comunicarea între cumpărător și emitentul său, lipsind conceptul de Director).
- În sistemul *SPA/UCAF* "verdictul de autenticitate" este atașat explicit fiecărei tranzacții și este păstrat împreună cu ea, ceea ce rezolvă probleme de non-repudiere; la *3-D Secure* acest lucru nu se întâmplă.

Inițializarea

1. Deținătorul de card – care dorește să facă tranzacții de comerț electronic folosind protocolul *3-D Secure* – se adresează emitentului său.

Inițializarea

1. Deținătorul de card – care dorește să facă tranzacții de comerț electronic folosind protocolul *3-D Secure* – se adresează emitentului său.
2. Emitentul stabilește datele de autentificare (de exemplu numele înscris pe card și o parolă).
   Emitentul ar putea cere deținătorului de card să-și cumpere un certificat de autenticitate sau să folosească un smartcard (de exemplu Visa VSDC) prin intermediul unui cititor de smartcarduri cuplat la calculatorul său.

Inițializarea

1. Deținătorul de card – care dorește să facă tranzacții de comerț electronic folosind protocolul *3-D Secure* – se adresează emitentului său.
2. Emitentul stabilește datele de autentificare (de exemplu numele înscris pe card și o parolă).
   Emitentul ar putea cere deținătorului de card să-și cumpere un certificat de autenticitate sau să folosească un smartcard (de exemplu Visa VSDC) prin intermediul unui cititor de smartcarduri cuplat la calculatorul său.
3. Emitentul – după verificarea datelor deținătorului – va înscrie numărul de card în Directorul sistemului *3-D Secure*.

Inițializarea

1. Deținătorul de card – care dorește să facă tranzacții de comerț electronic folosind protocolul *3-D Secure* – se adresează emitentului său.
2. Emitentul stabilește datele de autentificare (de exemplu numele înscris pe card și o parolă).
   Emitentul ar putea cere deținătorului de card să-și cumpere un certificat de autenticitate sau să folosească un smartcard (de exemplu Visa VSDC) prin intermediul unui cititor de smartcarduri cuplat la calculatorul său.
3. Emitentul – după verificarea datelor deținătorului – va înscrie numărul de card în Directorul sistemului *3-D Secure*.

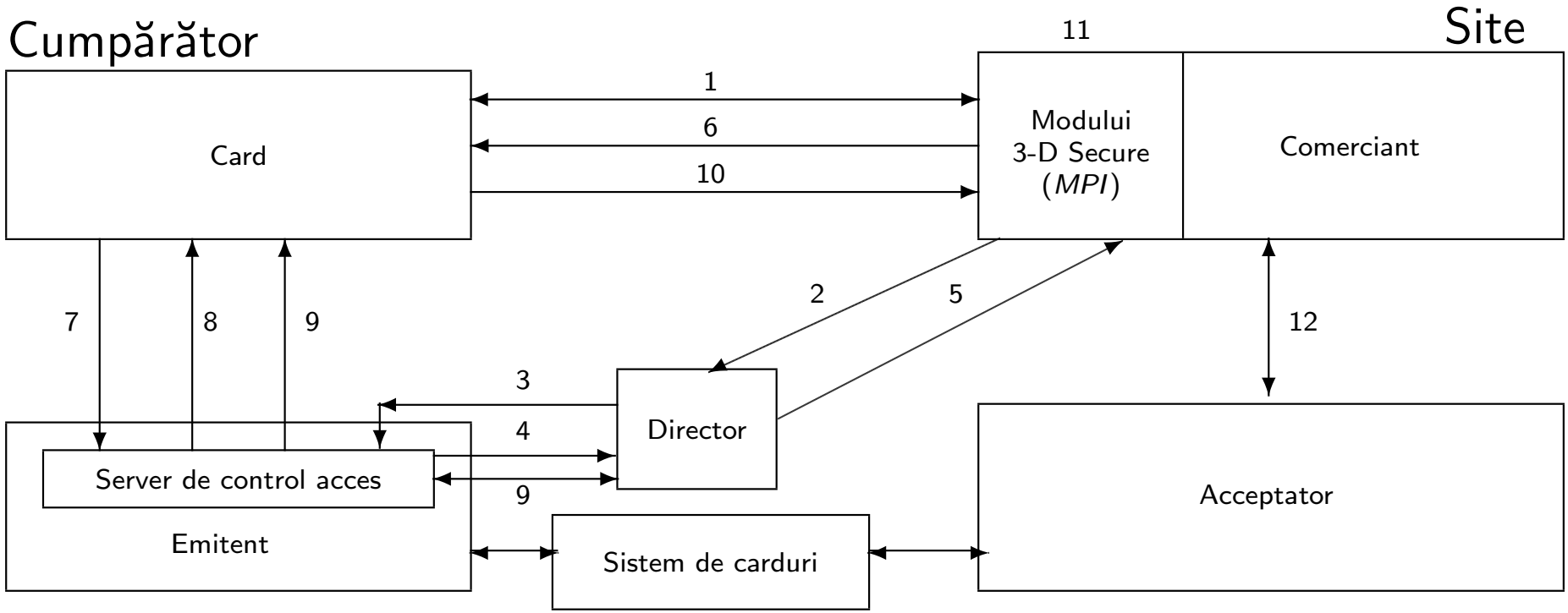
Din acest moment deținătorul de card și cardul său sunt verificați și înregistrați (*enrolled*) în sistemul *3-D Secure*.

- Tranzacția este inițiată de un card prin intermediul unui calculator personal (smartphone, tabletă) cuplat la Internet care dispune de un browser Internet Explorer sau Netscape.
- Legăturile prin Internet folosesc protocoale *SSL* sau *TLS* care asigură confidențialitatea transmisiunii, integritatea mesajelor și autentificarea serverului.

- Tranzacția este inițiată de un card prin intermediul unui calculator personal (smartphone, tabletă) cuplat la Internet care dispune de un browser Internet Explorer sau Netscape.
- Legăturile prin Internet folosesc protocoale *SSL* sau *TLS* care asigură confidențialitatea transmisiunii, integritatea mesajelor și autentificarea serverului.
- După ce clientul – după ce a ajuns pe site-ul comerciantului, a ales produsele și le-a pus în coșul de cumpărături – apasă pe butonul care declanșează cumpărarea, iar mesajele circulă între părțile implicate după figura:

Structura unei tranzacții cu *3-D Secure*

Schema este comună pentru Visa și MasterCard.



1. Datele privind tranzacția de plată sunt în posesia comerciantului, care le înregistrează (dar nu le poate accesa).

1. Datele privind tranzacția de plată sunt în posesia comerciantului, care le înregistrează (dar nu le poate accesa).
2. Modulul de comerciant *3-D Secure*, *MPI* (*Merchant Plug-In*), din site-ul comerciantului stabilește o legătură *SSL/TLS* cu Directorul sistemului și îi trimite numărul de card în vederea declanșării autentificării cardului și a deținătorului de card. Modulul *MPI* se autentifică față de Director.

1. Datele privind tranzacția de plată sunt în posesia comerciantului, care le înregistrează (dar nu le poate accesa).
2. Modulul de comerciant *3-D Secure*, *MPI* (*Merchant Plug-In*), din site-ul comerciantului stabilește o legătură *SSL/TLS* cu Directorul sistemului și îi trimite numărul de card în vederea declanșării autentificării cardului și a deținătorului de card. Modulul *MPI* se autentifică față de Director.
3. Directorul va cerceta dacă numărul de card implicat în plată este înregistrat și identifică 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 trimite un mesaj către modulul *MPI* al comerciantului, iar acesta va sări peste autentificare și va trece la autorizarea tranzacției (pasul 5), realizând o tranzacție de *e-commerce* fără autentificarea deținătorului de card.

4 Serverul de control acces al emitentului verifică dacă numărul de card este generat de emitent și dacă există metodă de autentificare pentru el, după care trimite răspunsul la Director.

4 Serverul de control acces al emitentului verifică dacă numărul de card este generat de emitent și dacă există metodă de autentificare pentru el, după care trimite răspunsul la Director.

5 Directorul trimite răspunsul către modulul *MPI* de comerciant. Dacă modulul constată că metoda de autentificare nu este disponibilă pentru acel număr de card, trece la autorizarea tranzacției, sărind din nou peste autentificare.

4 Serverul de control acces al emitentului verifică dacă numărul de card este generat de emitent și dacă există metodă de autentificare pentru el, după care trimite răspunsul la Director.

5 Directorul trimite răspunsul către modulul *MPI* de comerciant. Dacă modulul constată că metoda de autentificare nu este disponibilă pentru acel număr de card, trece la autorizarea tranzacției, sărind din nou peste autentificare.

6 Dacă autentificarea se face, modulul *MPI* expediează o cerere de autentificare a deținătorului de card către serverul de control acces *ACS* al emitentului cardului.

4. Serverul de control acces al emitentului verifică dacă numărul de card este generat de emitent și dacă există metodă de autentificare pentru el, după care trimite răspunsul la Director.
5. Directorul trimite răspunsul către modulul *MPI* de comerciant. Dacă modulul constată că metoda de autentificare nu este disponibilă pentru acel număr de card, trece la autorizarea tranzacției, sărind din nou peste autentificare.
6. Dacă autentificarea se face, modulul *MPI* expediează o cerere de autentificare a deținătorului de card către serverul de control acces *ACS* al emitentului cardului.
7. Serverul *ACS* recepționează cererea de autentificare și începe procedura de autentificare.

8 *ACS* cere deținătorului de card numele și parola (eventual și alte date de autentificare).
În final *ACS* generează un mesaj de răspuns de autentificare, pe care îl semnează.

8 *ACS* cere deținătorului de card numele și parola (eventual și alte date de autentificare).
În final *ACS* generează un mesaj de răspuns de autentificare, pe care îl semnează.

9 Trimite acest mesaj deținătorului de card, care îl va direcționa către modulul *MPI* al comerciantului.
Datele de autentificare sunt trimise și către Directorul sistemului pentru a fi păstrate în arhiva sa de autentificări.

8 *ACS* cere deținătorului de card numele și parola (eventual și alte date de autentificare).
În final *ACS* generează un mesaj de răspuns de autentificare, pe care îl semnează.

9 Trimite acest mesaj deținătorului de card, care îl va direcționa către modulul *MPI* al comerciantului.
Datele de autentificare sunt trimise și către Directorul sistemului pentru a fi păstrate în arhiva sa de autentificări.

10 Modulul *MPI* din site-ul comerciantului recepționează mesajul de răspuns la cererea de autentificare.

8 *ACS* cere deținătorului de card numele și parola (eventual și alte date de autentificare).
În final *ACS* generează un mesaj de răspuns de autentificare, pe care îl semnează.

9 Trimite acest mesaj deținătorului de card, care îl va direcționa către modulul *MPI* al comerciantului.
Datele de autentificare sunt trimise și către Directorul sistemului pentru a fi păstrate în arhiva sa de autentificări.

10 Modulul *MPI* din site-ul comerciantului recepționează mesajul de răspuns la cererea de autentificare.

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

12 Dacă autentificarea deținătorului de card a fost pozitivă, modulul *MPI* trece controlul către etapa de autorizare a tranzacției, în care se generează o cerere obișnuită de autorizare care se trimite (legătură *SSL*/*TLS*) porții de acces a acceptatorului.

12 Dacă autentificarea deținătorului de card a fost pozitivă, modulul *MPI* trece controlul către etapa de autorizare a tranzacției, în care se generează o cerere obișnuită de autorizare care se trimite (legătură *SSL/TLS*) porții de acces a acceptatorului.

Acceptatorul obține în final un răspuns de autorizare de la emitentul cardului, pe care îl trimite modulului client de *e-commerce* din site-ul comerciantului.
Acesta afișează – prin navigatorul calculatorului clientului – o pagină cu raportul privind desfășurarea tranzacției (raport echivalent unei chitanțe).

Mulțumesc pentru atenție !