5 Protocolul SET

5.1 Protocolul SET – aspecte generale

5.2 Arhitectura SET

5.3 Serviciile de securitate ale SET

5.4 SET versus TLS/SSL

5.5 Sumar SET

5.1 Protocolul SET – aspecte generale

Protocolul Tranzacții electronice sigure (Secure Electronic Transaction - SET), este destinat securizării tranzacțiilor cu cartele bancare inițiate pe rețele deschise.

SET a fost sponsorizat în comun de Visa și MasterCard în colaborare cu IBM, GTE, Microsoft, SAIC (Science Applications International Corporation), Terisa Systems și VeriSign [specificația SET, 1997]. Secure Electronic Transaction LLC (SETCo) a fost responsabilă pentru menținerea specificațiilor, pentru testarea conformității și interoperabilității și pentru emiterea de acorduri de licențiere.

În ciuda acestei impresionante liste de promotori, piața a optat pentru TLS/SSL mai degrabă decât pentru SET. Din punct de vedere tehnic, studiul SET este totuși util, deoarece a introdus multe inovații care ar putea fi reutilizate în viitor.

5.2 Arhitectura SET

SET asigură tranzacții cu cartele bancare prin Internet. El funcționează la nivelul Aplicație cu accent exclusiv pe tranzacțiile de plată. Adică alte schimburi, cum ar fi cele legate de căutarea sau selecția de bunuri, sunt în afara domeniului de aplicare. SET oferă, de asemenea, o interfață sigură pentru infrastructura bancară pentru autorizare și plată la distanță.

Instituțiile emitente, de obicei o bancă afiliată la Visa sau MasterCard, oferă clienților cartele de plată conforme specificațiilor SET. Deținătorii de cartele sunt autentificați prin cifrografia cu chei publice utilizând un certificat de la o autoritate de certificare care este stocat pe discul fix al calculatorului sau pe un mediu de stocare extern.

SET este orientat pe tranzacții care operează într-un mod de solicitare-răspuns; adică mesajele sunt asociate. Structura mesajului urmează DER (Distinctive Coding Rules) din ASN.1 (Abstract Syntax Notation 1) descrisă în ISO/IEC 8824-1 – ISO/IEC 8824-4. Mesajele sunt încapsulate cu MIME conform PKCS #7 (IETF RFC 2315). În special, SET utilizează următ. structuri PKCS #7:

- **SignedData, pentru datele care sunt semnate;**
- **EnvelopedData, pentru date clare care sunt într-un plic numeric;**
- **DigestedData, pentru rezumat;**
- **EncryptedData, pentru datele cifrate.**

5.2 Arhitectura SET

Specificațiile SET acoperă rolurile și responsabilitățile a 6 entități:

1. **Titularul cartelei.**
2. **Serverul comerciantului.**
3. **Poarta (Centrul) de plată.**
4. **Autoritatea de certificare.**
5. **Instituția emitentă a cartelei bancare a deținătorului cartelei.**
6. **Instituția dobânditor, care este banca comerciantului.**

Deținătorul cartelei, comerciantul, autoritatea de certificare și poarta de plată sunt conectate prin Internet. Clientul comunică cu poarta de plată folosind un tunel care trece prin serverul comerciantului. Fiecare participant are un certificat de la o autoritate de certificare SET. Aceste certificate sunt anexate în fiecare dintre mesajele schimbate între deținătorul cartelei, comerciant și poarta de plată.

Instituțiile emitentului și ale achizitorului sunt conectate printr-o rețea bancară închisă securizată. Poarta de plată interconectează rețelele deschise și cele închise, efectuând convertirile necesare de compatibilitate. Dispune de două interfețe, una corespunde specificațiilor SET, pe partea Internet, iar cealaltă este conformă cu protocolul proprietar folosit în cadrul rețelei financiare securizate.

5.2 Arhitectura SET

SET asigură schimburile între client și comerciant și schimburile între comerciant și poarta de plată. Poarta de plată gestionează plățile în numele băncilor, emitent sau cumpărător. În mod evident, poarta trebuie să fie aprobată de către autoritățile bancare, dacă nu este responsabilă de o instituție financiară care să îndeplinească aceste funcții.

Pe partea client, funcțiile SET sunt implementate într-un pachet special desemnat adesea ca portofel SET.

5.3 Serviciile de securitate ale SET

Operațiunile SET oferă următoarele servicii:

- **înregistrarea titularilor de cartele și a comercianților cu autoritatea de certificare;**
- **livrarea certificatelor către deținătorii de cartele și comercianți;**
- **autentificarea, confidențialitatea și integritatea tranzacțiilor de cumpărare;**
- **autorizarea plății;**
- **capturarea plăților pentru inițierea cererii de decontare financiară în numele comerciantului;**

SET utilizează tehnicile de cifrografie cu chei publice pentru a garanta simultan următoarele:

- **confidențialitatea schimburilor;**
- **integritatea datelor schimbate între client, comerciant și banca achizitoare;**
- **identificarea participanților;**
- **autentificarea participanților.**

5.3 Serviciile de securitate ale SET

O condiție necesară, dar nu suficientă, pentru nerepudierea tranzacțiilor este aceea că titularul cartelei este certificat.

Alte condiții sunt un mecanism de încredere în timp și o autoritate de certificare ireproșabilă.

În cele din urmă, deoarece poarta de plată care verifică exactitatea instrucțiunilor de plată și nu comerciantul, poarta va fi chemată să arbitreze litigiile.

Pentru a facilita implementarea protocolului SET, certificarea cumpărătorului este opțională în versiunea 1.0 a specificațiilor.

Confidențialitatea mesajului se realizează prin algoritmi de cifrare simetrici.

Cheia secretă însăși este distribuită cu algoritmi de cifrografie cu chei publice.

De exemplu, atunci când poarta de plată dorește să trimită comerciantului informații confidențiale, aceasta generează o cheie de cifrare simetrică cu care cifrează datele. Aceeași cheie este cifrată cu cheia publică a comerciantului care, fiind singura entitate cu cheia privată corespunzătoare, este singura parte capabilă să extragă cheia simetrică și să descifreze datele.

5.3 Serviciile de securitate ale SET

Pentru a asigura integritatea mesajului, SET utilizează i-semnătura expeditorului, adică rezumatul mesajului cifrat cu cheia privată a expeditorului. Orice entitate care are acces la cheia publică corespondentă este capabilă să verifice integritatea mesajului. Dacă perechea de chei publică/privată este unică și necompromisă, i-semnătura garantează simultan identitatea expeditorului și integritatea datelor.

În SET, certificatul semnat de către autoritatea de certificare face credibilă asocierea unei chei publice cu proprietarul acesteia, asigurând astfel autentificarea. Procedurile de autentificare ale SET se bazează pe versiunea 3 a Recomandării ITU-T X.509.

Fiecare certificat conține identitatea proprietarului său, o cheie publică legată de algoritmul de cifrare a cheilor publice utilizate și semnătura autorității care a emis certificatul. Pentru autentificarea reciprocă, două părți trebuie să meargă înapoi de-a lungul căii de certificare, până când vor întâlni o autoritate comună. ♦

5.4 SET versus TLS/SSL

SET a fost conceput să fie principala metodă de plată cu cartele bancare prin Internet. Dar nu a reușit să obțină o utilizare pe scară largă. Există mai multe explicații posibile pentru acest rezultat:

1. SET a introdus două entități noi: (a) autoritățile de certificare pentru a certifica actorii și (b) poarta de plată în rețeaua de autorizare. Pe când infrastructura pentru certificarea TLS/SSL este mult mai ușor de stabilit.

2. SET necesită autentificarea fiecărui mesaj, ceea ce adaugă întârzieri și calcule adiționale la fiecare tranzacție. În plus, suprasarcina de procesare SET în implementările soft poate crește substațial timpul de răspuns.

3. În timp ce utilizarea intermediarului de plăți reduce cu un ordin sarcina cifrografică pentru client și pentru comerciant, intermediarii de plăți nu au beneficiat de implementarea SET.

4. Secretele de pe partea deținătorului cartelei sunt stocate pe discul fix al unui calculator, ceea ce introduce un alt set de riscuri. În plus, în momentul introducerii SET, utilizarea cartelelor de plată cu circuite integrate a fost în mare parte în afara Statelor Unite, principala piață a plăților prin Internet.

5.4 SET versus TLS/SSL

5. Pentru implementările SET, pe lângă exlorator trebuie să fie instalată și o i-aplicație client specială (i-portofelul). În contrast, i-aplicația client pentru soluțiile TLS/SSL este integrată în toate exploratoarele.

6. Costul de operare al soluțiilor SET a favorizat alternativele TLS/SSL. Aceste costuri includ:

a) costul terminalelor noi cu echipament specializat;

b) certificarea pe partea client;

c) întreținerea și suportul informatic al cumpărătorului și al comerciantului.

7. Soluțiile TLS/SSL au redus riscul tranzacțiilor frauduloase la un nivel care ar putea fi tolerat fără a trece prin complicația implementării SET. În plus, TLS/SSL a oferit o protecție de tip cuvertură (*blanket*) pentru tranzacțiile prin TCP.

8. Niciun segment al populației țintă nu ar putea fi identificat ca utilizator principal care ar încuraja adoptarea SET. Dimpotrivă, informaticienii din afara comunității bancare nu au fost convinși că au fost necesare sau ar putea fi justificate calculele asociate SET.

9. Nu a existat nicio obligație legală de a reduce frauda la nivelurile pe care le-a atins SET.

5.4 SET versus TLS/SSL

Principalele diferențe în caracteristicile TLS/SLL și SET [3]:

TLS/SSL	SET
Simple and easy to use.	Complex and requires a certification infrastructure.
Generalist protocol.	Banking payment protocol.
Distributed with browsers.	A wallet has to be installed on the client side.
Authentication infrastructure is not mandatory.	Infrastructure for authentication is mandatory.
Authentication is at the beginning of the session.	Each exchange is authenticated.
Point-to-Point Protocol.	Several parties participate in a transaction.
The merchant receives all the details of the order and the payment.	With the dual signature, access to information is restricted to those who need it.

♦

5.5 Sumar SET

SET a fost destinat să fie o soluție dedicată i-comerțului ce păstrează interfețele existente cu rețelele bancare.

În consecință, protocolul oferă cumpărătorului posibilitatea de a verifica autenticitatea sitului comerciantului cu ajutorul certificatelor.

În plus, metoda semnării duale în SET leagă comanda de achiziție pe care clientul o trimite comerciantului, inclusiv Instrucțiunile de plată direcționate către banca emitentă prin intermediul porții de plată SET, cu aceeași semnătură.

Astfel, instrucțiunile de plată sunt trimise cifrate comerciantului, care le transmite doar la poarta de plată.

Mai mult decât atât, numai comerciantul poate citi comanda de achiziție, care rămâne opacă porții, și numai poarta de plată este autorizată să extragă numărul cartelei bancare a cumpărătorului pentru a trimite o solicitare de autorizare rețelei bancare.

5.5 Sumar SET

Principalele caracteristici ale SET sunt:

- **comerciantul păstrează informațiile comenzii care sunt semnate cu cheia privată de semnătură a clientului. De asemenea, comerciantul păstrează răspunsul porții (în mesajul AuthRes) semnat cu cheia privată de semnătură a porții. În cazul în care clientul este certificat, comerciantul are o copie a certificatului deținătorului cartelei și a cheii publice pe care o citează. Cu toate acestea, comerciantul nu are detaliile cartelei bancare a clientului;**
- **titularul cartelei primește un răspuns la comanda de achiziție, semnată cu cheia privată de semnătură a comerciantului. Titularul cartelei primește o copie a certificatului de semnătură a comerciantului, dar nu și certificatul de cifrare utilizat pentru decontarea financiară,**
- **poarta de plată cunoaște detaliile financiare ale tranzacției dintre comerciant și deținătorul cartelei, fără a fi conștientă de subiectul tranzacției;**
- **fiecare dintre aceste tranzacții are un număr de tranzacție unic care este cifrat, ceea ce previne atacurile de replicare (replay).**