6 PLĂȚI CU CARTELE CU BANDĂ MAGNETICĂ

6.1 Tranzacții POS

6.2 Standarde de comunicare pentru tranzacții cu cartele

6.3 Securitatea tranzacțiilor POS

6.4 Sistemul 3-D Secure

6.5 Migrarea spre EMV

6.6 Sumar

6 PLĂȚI CU CARTELE CU BANDĂ MAGNETICĂ

O serie de standarde internaționale de standardizare, ISO/IEC 7810, ISO/IEC 7811, ISO/IEC 7812, ISO 8583 și ISO/IEC 4909, definesc proprietățile fizice ale cartelelor, flexibilitatea, localizarea benzii magnetice, caracteristicile magnetice și formatele de date. Ele oferă, de asemenea, standardele pentru cartelele financiare, inclusiv alocarea diapazoanelor de numere de cartele diferitelor instituții emitente de cartele.

Cartelele cu bandă magnetică sunt încă folosite în numeroase aplicații - retragerea de numerar, plata anticipată a creditului/debitului, depozitarea valutei sau jetoanelor, controlul accesului și așa mai departe - în special în Statele Unite.

6.1 Tranzacții POS

Cartelele cu bandă magnetică constau din suport din plastic dreptunghiular, cu elemente pentru identificarea și autentificarea emitentului pe ambele părți. Unele dintre semnele distinctive de pe fața sunt următoarele:

- logosul emitentului cartelei, al instituției financiare și al operatorului schemei bancare;
- numărul de cont principal al cartelei (PAN) reliefat, numele titularului cartelei și data de expirare reliefată;
- marcaje ultraviolete care strălucesc la o iluminare specială;
- o hologramă pentru a crește securitatea și a face mai dificilă contrafacerea.

Măsurile de securitate nu au împiedicat falsificarea cartelelor. În 2012, a fost lansat un sit Web denumit "fakeplastic.net" pentru vânzarea cartelelor de credit și de debit contrafăcute, precum și a unor holografii utilizate pentru a elibera licențe de conducător auto fals în Statele Unite.

PAN este format din 10-19 cifre împărțite în grupuri a câte patru. Prima cifră a primului grup identifică rețeaua schemei cartelei bancare (4 pentru Visa, 5 pentru MasterCard, etc.). Următoarele sunt codurile privind: țara, reprezentantul schemei cartelei bancare din țara respectivă și banca emitentă a cartelei. Ultima cifră formează un cod de verificare numit "cheia lui Luhn" și este selectat pentru a îndeplini următoarea condiție:

$$\sum_{i\ even} n_i + \sum_{i\ odd} (2n_i) mod 9 = 0 \bmod 10.$$

.

6.1 Tranzacții POS

Pe cealaltă parte, este loc pentru semnătura deținătorului cartelei ș.a.

Aceasta are o bandă magnetică cu trei căi de înregistrare, fiecare la 0,28 cm lățime și separate de o mică distanță.

Datele de personalizare sunt înregistrate pe primele două căi. Calea 1, utilizată în industria aeriană și, opțional, în majoritatea aplicațiilor de plată, constă din 79 octeți (79 caractere ASCII) într-un câmp separat pentru a descrie numărul contului, data expirării, numele complet al titularului cartelei, unele date de serviciu ce specifică cum terminalul ar trebui să citească cartela și suma de control pentru verificarea integrității datelor de cititorul de cartele.

Calea 2 conține o versiune mai scurtă a datelor de pe Calea 1; are o lungime de 40 octeți și include PAN, data de expirare, un cod de serviciu și suma de control. Utilizarea unei versiuni trunchiate a datelor este o moștenire din zilele terminalelor de plată rapidă prin apel telefonic și a fost utilizată pentru a accelera comunicarea cu centrele de autorizare.

Calea 3 este una de citire/scriere și este, uneori, folosită pentru permisele de conducere și alte informații. Pe unele cartele Calea 3 lipsește.

Terminalele POS citesc una din primele două căi, iar în caz că o cale este defectă, datele se citesc de pe cealaltă cale.

.

6.1 Tranzacții POS

O tranzacție de vânzare-cumpărare prin POS sau ATM (puncte de vânzare) folosind o cartelă bancară include etapele :

1. Dispozitivul POS citește datele înregistrate în căile magnetice ale cartelei.

2. Pentru verificarea identității, deținătorul cartelei poate fi rugat să introducă un număr de identificare personal (PIN).

3. Terminalul compară PIN-ul introdus cu cel recuperat din banda magnetică a cartelei.

4. Dacă PIN-ul este valabil, se pregătește o cerere de autorizare cu toate datele de pe cartelă, precum și suma tranzacției. Cererea este trimisă dobânditorului care, ulterior, o transmite emitentului.

5. Emitentul ia o decizie de autorizare pe baza datelor din cererea de autorizare. Răspunsul este trimis către cumpărător care îl transmite terminalului.

6.1 Tranzacții POS

Aprobarea în timp real a plăților reprezintă o moștenire a disponibilității largi a serviciilor de telefonie.

Atunci când serverul de autentificare nu este disponibil, emitenții de cartele limitează valoarea unei tranzacții fără autorizație la așa-numita "limită de sus".

Limitele cheltuielilor zilnice sau retragerilor de numerar pot fi codate în banda magnetică. Alte limite se referă la valoarea maximă permisă pentru o singură tranzacție sau tranzacții internaționale.

Principalele vulnerabilități ale tranzacțiilor la terminale POS cu cartele cu bandă magnetică sunt:

1. Informațiile deținătorului cartelei nu sunt cifrate. În consecință, orice cititor de cartele magnetice poate prelua datele de personalizare stocate pe banda magnetică.

2. Cartela nu poate procesa date, fiind astfel un participant pasiv la tranzacție. Acest lucru este diferit de cartelele de circuite integrate care pot efectua calcule cifrografice pentru confidențialitate, integritate și autentificare.

3. Schimburile între cartelă și cititorul de cartele sunt necifrate.

4. După citirea datelor de pe cartelă, nu există interacțiuni suplimentare între POS sau ATM și cartelă.

6.1 Tranzacții POS

În consecință, este ușor de citit datele de pe bandă magnetică și de a clona cartela cu un codificator de bandă magnetică conectat la un calculator.

De asemenea, atunci când comerciantul nu are acces la cartela fizică sau nu poate autentifica titularul cartelei în persoană (cartela nu este prezentă), cum ar fi tranzacțiile prin Internet, prin comandă prin poștă și prin comenzi telefonice (IMOTO), verificarea autenticității și integrității tranzacțiilor cu cartele cu bandă magnetică nu sunt întotdeauna posibile.

Este necesar un cod PIN pentru retragerile de numerar de la ghișeele automate. Plățile cu cartele de debit pot necesita fie o semnătură, fie un cod PIN, în timp ce tranzacțiile cu cartele de credit necesită de obicei o semnătură.

Tranzacțiile de debit cu semnătură, cum ar fi tranzacțiile cu cartele de credit, sunt direcționate către rețeaua de procesare financiară, în mod tipic rețelele Visa sau MasterCard. Tranzacțiile de debit cu specificarea PIN necesită cifrarea codului PIN în solicitarea de autorizare. Operațiunile de debitare a PIN-urilor pot fi direcționate fie în rețelele Visa sau MasterCard, fie în rețelele de debit cash/PIN, cum ar fi Interlink, STAR, Maestro sau New York Exchange (NYCE).

6.1 Tranzacții POS

Există mai multe moduri de a introduce datele deținătorului cartelei la un terminal de vânzare:

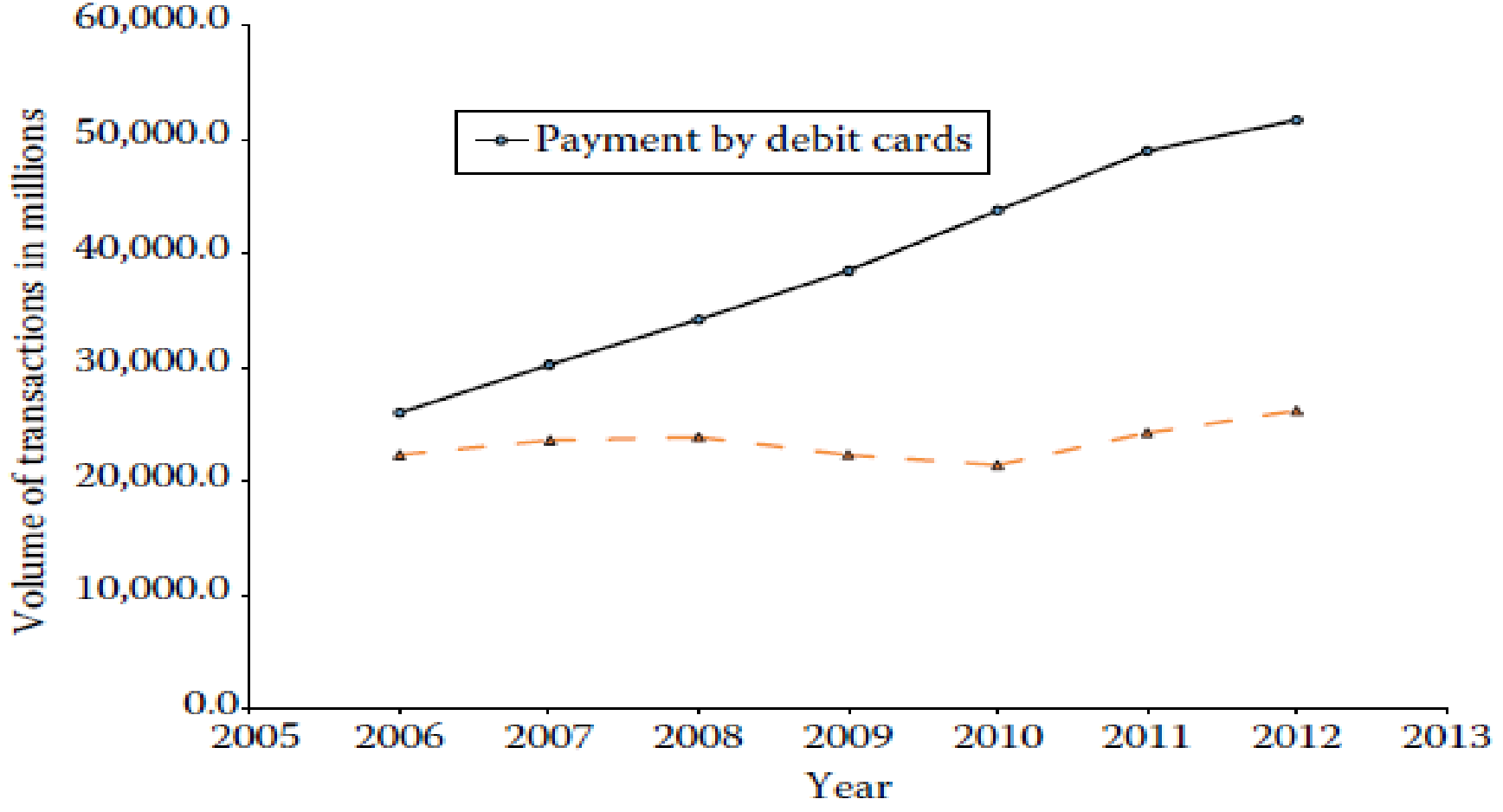
1. *Introducere manuală*. La această metodă, casierul introduce pe o tastatură numărul contului și data expirării gravate pe partea frontală a cartelei. Această metodă este adesea folosită dacă banda magnetică este deteriorată și nu poate fi citită. Autentificarea deținătorului cartelei se bazează pe o comparație a semnăturii clientului cu semnătura pe spatele cartelei, precum și pe orice identificare oficială.

2. *Cititor de benzi magnetice*. Cititorul de benzi magnetice scanează banda magnetică pentru a extrage datele de personalizare. Unele cititoare au capacități de cifrare care sunt utilizate pentru cifrarea punct-la-punct.

3. *Suport de PIN* (*PIN pad*). Un suport de PIN este un dispozitiv cu informații pentru identificarea deținătorului printr-un PIN. Echipamentul există fie independent, fie integrat în registre de numerar. Multe dispozitive suport de PIN au un modul de securitate rezistent la acțiuni neautorizate, care efectuează calcule cifrografice. Utilizarea unui suport de PIN crește nivelul de securitate, deoarece clonarea semnăturilor scrise de mână este mai ușoară decât furtul unui asemenea suport.

6.1 Tranzacții POS

Evoluția volumului tranzacțiilor folosind cartele de debit și de credit în SUA:



♦

6.2 Standarde de comunicare pentru tranzacții cu cartele

ISO 8583 este standardul pe care organizațiile financiare îl folosesc pentru a comunica și a încheia tranzacții cu cartele, fie de la un bancomat (ATM), de la un terminal POS, prin Internet sau printr-o rețea mobilă. Prima sa versiune datează din 1987, cu revizuiri succesive în 1993, 1998 și 2003; majoritatea implementărilor, cu toate acestea, sunt conforme cu specificațiile din 1987.

Standardul definește mesajele sistem-sistem pentru schimburile de chei securizate, reconcilierea totalurilor și alte scopuri administrative.

Un mesaj constă din trei componente: un identificator de tip de mesaj, un bitmap de lungime variabilă și până la 192 de elemente de date. Primii 2 octeți ai mesajului indică lungimea totală a mesajului.

Câmpul de identificare a tipului mesajului constă din 4 octeți:

1. Primul octet reprezintă versiunea standardului.

2. Cel de-al doilea octet reprezintă tipul tranzacției. Tipurile de tranzacții includ: achiziții, retrageri, depozite, rambursări, inversări, anchete privind soldul, plăți și transferuri între conturi.

3. Cel de-al treilea octet indică funcția mesajului.

4. Ultimul octet reprezintă originea mesajului.

6.2 Standarde de comunicare pentru tranzacții cu cartele

Elementele de date reprezintă specificul real al tranzacției, fiecare rezervat pentru o anumită informație.

De exemplu, un element de date poate indica numărul contului principal, suma tranzacției, datele și ora transmiterii, moneda, rata de conversie a monedei, identitatea comerciantului, tipul afacerii, metoda de captare, tipul tranzacției, etc. Dacă este necesar un element particular, modelul de biți corespunzător trebuie să fie inclus în bitmap.

Specificația inițială din 1987 a inclus 128 de elemente de date, iar numărul lor a fost mărit la 192 în revizuirile ulterioare.

Lungimea elementelor de date poate fi fixă sau variabilă. Un indicator de lungime precede unui câmp de lungime variabilă.

Unul sau mai multe scheme bitmap indică elementele de date prezente. Prezența a până la 64 de elemente de date este indicată într-o hartă de biți primară. Un bitmap secundar este necesar pentru până la 128 de elemente de date. În cele din urmă, este nevoie de un bitmap terțiar pentru până la 192 de elemente de date.

6.2 Standarde de comunicare pentru tranzacții cu cartele

ISO 8583 permite diverse concretizări de implementare, ceea ce ridică probleme de interoperabilitate:

- **ISO 8583 definește formatul mesajului și fluxul de comunicare, dar nu specifică schema de codificare care poate fi ASCII, hexazecimală, etc.;**
- **unii furnizori adaugă informații de proprietate în câmpul lungimii mesajului;**
- **plasările câmpurilor, cum ar fi elementul valutar, pot varia în funcție de versiunile utilizate;**
- **rețelele cartelelor financiare (de ex., Visa, MasterCard) au adaptat standardul adăugând câmpuri personalizate proprietare.**

Pentru interoperabilitatea a două implementări diferite ale ISO 8582, trebuie adăugată o anumită funcție de interconectare. Aceasta nu este o opțiune scalabilă, deoarece procesul trebuie repetat pentru fiecare implementare separată. ISO 20022 este o posibilă abordare deoarece oferă o platformă comună bazată pe limbajul unificat de modelare (UML). ISO 20022 folosește o anvelopă XML a mesajelor, care extinde cerințele privind lățimea de bandă, mai ales atunci când numărul tranzacțiilor în timp real este mare. De asemenea, nici o rețea majoră de plăți cu cartele nu acceptă în prezent tranzacții conforme cu ISO 20022. Astfel, adoptarea globală a standardului ISO 20022 pentru plățile cu cartele este puțin probabil să aibă loc în viitorul apropiat. ♦

6.3 Securitatea tranzacțiilor POS

Cartelele de plată au fost aplicate mai întâi pentru comerțul direct. Emitenții s-au bazat pe comercianți pentru a efectua autentificarea titularului cartelei, utilizând o cartelă de identitate oficială sau un permis de conducere.

De asemenea, comercianții ar fi trebuit să compare semnătura pe chitanță cu semnătura titularului pe spatele cartelei. Semnătura de mână a fost utilizată ca o altă măsură de autentificare, precum și un instrument de nerepudiere.

Cu toate acestea, chitanțele aruncate au permis fraudulosilor să reutilizeze informațiile inscripționate la imprimarea cartelelor contrafăcute și să efectueze tranzacții false, în special de la terminale nesupravegheate, cum ar fi distribuitoarele de numerar.

O măsură evidentă a fost ca amprenta să reproducă doar ultimele patru numere ale PAN. O alta a fost de a adăuga un cod pentru controlul fraudelor, de obicei, dar nu neapărat, înregistrat în Calea 2. Codul, denumit valoare de verificare a cartelei (CVV) sau cod de verificare a cartelei (CVC), constă dintr-o cifrogramă generată de un algoritm cifrografic utilizând o cheie sub controlul emitentului de la PAN, data expirării și alte elemente de identificare.

Deoarece codul a fost disponibil doar pe calea magnetică și nu a fost gravat, imprimantele de primire nu puteau fi folosite pentru a extrage toate informațiile care urmează să fie codate în cartele contrafăcute. Trebuie remarcat faptul că acest lucru este diferit de noua cifrogramă adăugată mai târziu pentru a asigura tranzacțiile online.

6.3 Securitatea tranzacțiilor POS

Au fost introduse, de asemenea, măsuri de securitate opționale pentru a descuraja frauda prin inspecția vizuală, cum ar fi includerea imaginii titularului cartelei, a graficii complexe și a hologramelor. Datorită costurilor lor, aceste măsuri nu sunt respectate în mod uniform; în plus, acestea nu sunt eficiente în cazul terminalelor nesupravegheate sau al tranzacțiilor IMOTO. În cele din urmă, în medii cu cifra mare de afaceri, măsurile de securitate sunt relaxate pentru a îmbunătăți fluxul.

În cazul în care codul PIN asociat cartelei legitime este compromis, se pot efectua tranzacții de debitare frauduloase, inclusiv retragerea de numerar de la automatele de distribuire a numerarului.

6.3.1 Standardele PCI

În 2006, mai multe mărci (brand-uri) de plată globală - American Express, Discover, Japan Credit Bureau (JCB), MasterCard și Visa - au stabilit Consiliul Standardelor de Securitate a Industriei Cartelelor de Plăți (Payment Card Industry Security Standards Council) pentru a dezvolta standarde de securitate pentru industria de plăți. Industria cartelelor de plată (PCI) cuprinde organizații care stochează, procesează și transmit datele deținătorilor cartelelor.

6.3.1 Standardele PCI

Unul dintre rezultatele Consiliului PCI este PCI Data Security Standard (PCI DSS). PCI DSS se concentrează asupra mediului de procesare a tranzacțiilor în magazinele de comerț cu amănuntul și centrele de procesare a plăților, care au fost istoric locul de încălcări privind datele.

Un număr mare de reguli și recomandări se referă la "date în repaus", adică datele sensibile stocate în sistemele comerciale, terminalele virtuale și porțile de plată după ce o tranzacție a fost autorizată. Directivele sale vizează asigurarea procesării plăților prin cartele, protejarea datelor deținătorilor de cartele, prevenirea utilizării neautorizate a informațiilor personale și reacția la incidentele de securitate.

În particular, următoarele elemente de date nu pot fi stocate chiar și într-o formă cifrată: datele complete de pe benzile magnetice, CVV și codul PIN. Alte elemente de date păstrate pe bază de necesități includ doar numele deținătorului cartelei, adresa PAN, data de expirare și codul de serviciu. Pentru trasabilitate și responsabilitate, fiecare persoană care accesează o aplicație sau un server care procesează sau stochează informații privind cartelele de plată trebuie să aibă un cod de acces unic și o parolă.

6.3.1 Standardele PCI

Toate părțile și entitățile (de exemplu, terțe părți sau contractori) implicate în procesarea cartelelor de plată trebuie să fie certificate, să respecte cerințele PCI DSS și să își reînnoiască certificarea anual. Comercianții se încadrează în patru categorii de conformitate PCI, în funcție de numărul de tranzacții pe care le procesează în fiecare an și dacă aceste tranzacții sunt efectuate dintr-o locație corporativă sau prin Internet. Fiecare marcă de cartele de plată (Visa, MasterCard, etc.) are propriile cerințe și definiții ale nivelurilor de conformitate PCI. Concepțiile privind nivelul de conformitate PCI ale VISA sunt prezentate în tabel:

PCI Compliance	Number of Visa Transactions Processed Annually
Level 1	6 million (all channels)
Level 2	1–6 million (all channels)
Level 3	20,000–1 million (e-commerce transactions)
Level 4	Up to 20,000 e-commerce transactions or up to 1 million transactions on all channels

6.3.1 Standardele PCI

Unele dintre dispozițiile privind securitatea pentru "datele în tranzit" sunt următoarele:

- **PAN trebuie să fie cifrat în timpul transmisiei și stocării utilizând orice metodă standard de cifrare aprobată de Institutul Național de Standarde și Tehnologie (NIST);**
- **CVC/CVV trebuie să fie dezactivat în timpul intrării într-o aplicație și să nu fie stocat după primirea autorizației.**

Un alt standard PCI este Standardul de securitate a datelor pentru aplicații de plată (*Payment Application Data Security Standard* – PA-DSS), denumit anterior "Best Practices Application Application" (PABP).

Acesta ghidează dezvoltarea aplicațiilor de plată pentru a îndeplini cerințele PCI DSS, inclusiv procedurile de testare și documentația utilizatorului.

Semnarea codului și a fișierelor de configurare și de date protejează integritatea tuturor aspectelor i-aplicațiilor.

Semnarea certificatelor de o autoritate publică de certificare va evita necesitatea instalării certificatelor de bază pentru fiecare sistem țintă. ♦

6.3.2 Cifrarea punct-la-punct

Standardul PCI de cifrare punct-la-punct (P2PE) oferă cerințe detaliate privind testarea securității și proceduri de testare pentru furnizorii de aplicații și furnizorii de soluții pentru a verifica dacă produsele lor protejează datele de plată. Standardul acoperă toate aspectele capăt-la-capăt, adică de la dispozitivul de introducere a datelor până la centrul de date al porții de plată sau procesorul de plată, via terminalul POS, inclusiv mediul de vânzare cu amănuntul și rețeaua de transfer date.

La capătul de cifrare, modulul respectiv al dispozitivului este desemnat ca modul de securitate împotriva defecțiunilor (*Tamper-Resistant Security Module* – TRSM), deoarece este proiectat să detecteze intruziunile fizice și, în acest caz, să distrugă cheile. Descifrarea este efectuată la centrul de date într-un modul de securitate hardware (HSM), care este un aparat sau o extensie instalată în procesorul de plăți dedicat calculelor cifrografice de mare viteză.

În soluțiile hibride, echipamentul efectuează anumite funcții, în timp ce altele sunt realizate în i-programe. De exemplu, gestionarea cheilor este în echipament, în timp ce cifrarea sau descifrarea sau ambele sunt realizate în i-programe. Sistemele sunt descrise ca parte de cifrare/descifrare.

6.3.3 Fraude POS

Există mai multe modalități de a fura datele înregistrate pe căile magnetice pe cartelele de plată, unele mai sofisticate decât altele. Cartelele cadou preplătite cu bandă magnetică sunt anonime, astfel încât clonarea lor nu prezintă dificultăți semnificative, deoarece identitatea titularului nu este disponibilă.

Metodele de recoltare a PIN-urilor includ:

- "navigarea pe umeri" la terminalele casieriei sau la terminalele ATM pentru a observa ce combinație a introdus un proprietar de cartelă;
- plăcuțele PIN compromise;
- camerele de luat vederi clandestine ș.a.

Fraudatorii au plasat, de asemenea, dispozitive POS false pentru a captura toate datele necesare. Multe dispozitive au fost atașate la ATM-uri pentru a fura datele cartelei și codul PIN asociat. De ex., mașinile false pot fi stivuite direct pe mașinile legitime de distribuire a banilor. Aceste mașini ar avea camere de tip "pinhole" pentru a înregistra proprietarii de cartele care nu știu să-și distrugă codul PIN, în timp ce cititoarele false ar accesa datele înregistrate pe banda magnetică. În unele cazuri, dispozitive speciale ar prinde chiar cartela reală și nu îl vor returna utilizatorului după efectuarea tranzacției. Datele furate vor fi transmise imediat prin mesaje text pentru a crea mii de cartele false. Desigur, tranzacțiile ar trebui să fie făcute înainte ca cartela să fie raportată ca pierdută.

6.3.3 Fraude POS

Un alt mecanism de fraudă este de a intercepta cartelele nou emise furate pe traseu către deținătorul legitim al cartelei. Pentru a combate această fraudă, emitenții de cartele au instituit proceduri de activare a cartelelor. La primirea cartelelor, deținătorii de cartele trebuie să sune și să se autentifice pentru a-și activa noua cartelă. Agentul centrului de apel solicită de obicei răspunsuri la un set de întrebări pentru a verifica dacă acesta este în mâinile destinatarului legitim. Mulți emitenți folosesc sisteme automate de activare care recunosc numărul de telefon al apelului și pun la dispoziția telefonului informații de bază care trebuie validate. De asemenea, codul PIN și cartela sunt trimise separat pentru a reduce riscul de interceptare.

Frauda de aplicație apare atunci când infractorii creează identități fictive utilizând informațiile personale disponibile în înregistrările publice. Atacurile asupra bazelor de date centralizate, cum ar fi cele întreținute de marile lanțuri de magazine sau de solicitanții de birouri de credit, contribuie la fenomenul furtului de identitate. Informațiile furate sunt vândute pentru a face cereri frauduloase în numele altei persoane fără permisiunea lor, ceea ce este mult mai dificil de detectat. În mod tipic, emitenții de cartele se bazează pe un număr de baze de date partajate pentru a examina solicitanții și pentru a semnala observații care ar putea fi suspecte.

6.3.3 Fraude POS

Pe parcursul perioadei 2006-2010, falsificarea cartelelor a devenit cea mai importantă sursă de fraudă cu debit de semnături în Statele Unite (41% față de 25% pentru cartele pierdute sau furate și 22% pentru IMOTO).

Pentru tranzacțiile cu PIN (retragere numerar și debit), acesta se află pe locul al doilea (44%) în spatele cartelelor pierdute sau furate (49%).

Consecințele fraudei variază în funcție de tipul cartelei. Deoarece clonarea semnăturilor este mai ușoară decât furtul PIN-urilor, pierderea per dolar pentru plata autorizată prin semnătură este semnificativ mai mare decât pierderile pentru plățile autorizate prin PIN.

Rețelele de plată cu debit PIN necesită cifrarea PIN-ului și, prin urmare, frauda în cazul achizițiilor personale cu debite prin PIN (adică tranzacții cu cartela prezentă) nu este mare, decât dacă datele cartelei și PIN-ul au fost compromise.

6.3.3 Fraude POS

Pierderile cauzate de tranzactiile cu cartele false în SUA în 2009 [3]:

Payment Card	Loss per US$	Value of Transaction in Millions of US$	Value of Losses in Millions of US$
PIN debit card	0.0319	563,100	179.6
Signature debit card	0.1271	857,500	1089.9
General-purpose credit card[a]	0.1271	1,714,000	2178.5
Prepaid cards	0.0401	140	0.6
Total		13,134,740	3448.1

Migrarea la autentificarea cip-și-PIN cu EMV impune modificări la terminalele POS, precum și la sistemele back-office care procesează tranzacțiile.

Industria comerțului cu amănuntul și industria bancară nu au putut să convină asupra modului de împărțire a costului tranziției către sistemele compatibile cu EMV. Există chiar dezacorduri cu privire la costul acestei migrații, variind de la $8 mlrd până la aproximativ $26-230 mlrd, în plus față de aproximativ $2 mlrd pentru înlocuirea cartelelor.

6.3.3 Fraude POS

Migrarea la așa-numita autentificare cip-și-PIN cu EMV impune modificări la terminalele POS, precum și la sistemele back-office care procesează tranzacțiile. Cu toate acestea, industria comerțului cu amănuntul extrem de fragmentată și industria bancară nu au putut să convină asupra modului de împărțire a costului tranziției către sistemele compatibile cu EMV. Există chiar dezacorduri cu privire la costul acestei migrații, variind de la 8 miliarde dolari până la aproximativ 26-230 miliarde de dolari, în plus față de aproximativ 2 miliarde de dolari pentru înlocuirea cartelelor. ♦

6.4 Tranzacțiile prin Internet

Procedura de bază pentru tranzacțiile prin Internet este ca titularul cartelei să introducă datele de autentificare, inclusiv numărul cartelei, adresa, numele deținătorului cartelei și cifrograma de securitate a cartelei de pe spatele cartelei.

Verificarea tranzacțiilor exploatează diferite baze de date pentru a evalua factorii de risc înainte de a începe tranzacția.

Codurile de securitate online și parolele unice sunt folosite pentru a spori robustețea securității.

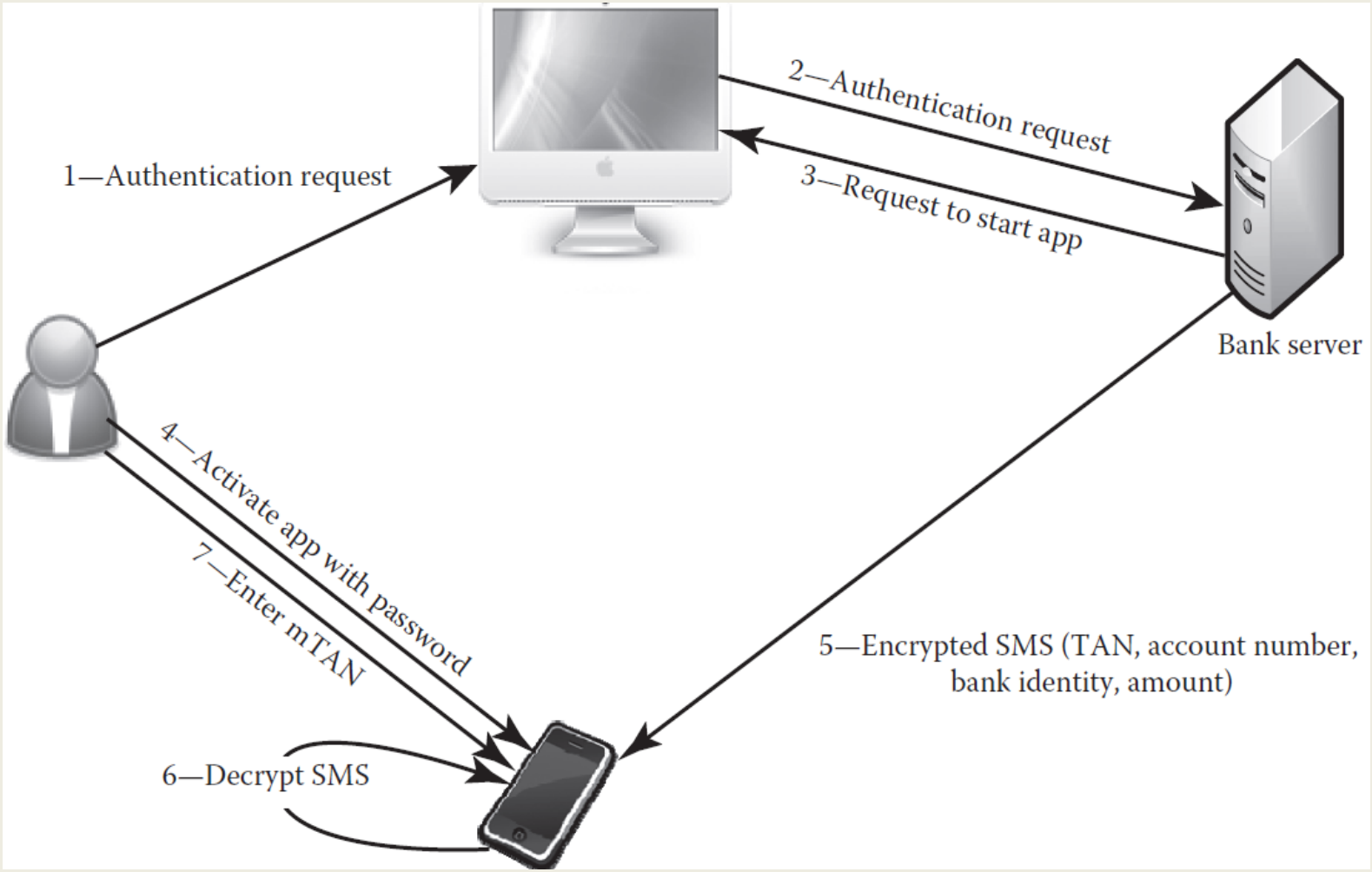
Unele atacuri de tip "omul-în-mijloc" constau în interceptarea mesajelor dintre cartelă și terminalul bancar, prin mascarea lor ca terminal de cartelă, în ceea ce privește utilizatorul, și ca utilizator în ceea ce privește terminalul.

Pentru a autentifica deținătorul cartelei în tranzacțiile bancare online cu cartele cu bandă magnetică se aplică diverse măsuri.

Una din acestea este Parola de unică folosință (OTP).

6.4 Tranzacțiile prin Internet

Schema de autentificare a deținătorul cartelei în tranzacțiile bancare online cu Parolă de unică folosință [3]:



6.4 Tranzacțiile prin Internet

Pierderile cauzate de fraude cu cartele în SUA în perioada 2001-2009 [3]:

Year	Revenue Lost (in Billions of US $)	Percentage of Revenue Lost
2001	1.70	3.20
2002	2.10	2.90
2003	1.90	1.70
2004	2.60	1.80
2005	2.80	1.60
2006	3.10	1.40
2007	3.70	1.40
2008	4.00	1.40
2009	3.30	1.20
2010	2.70	0.90
2011	3.40	1.00
2012	3.50	0.90

♦

6.5 Sistemul 3-D Secure

6.5.1 Aspecte generale

3-D Secure este introdus de Visa în 2001 pentru a preveni trei surse principale de fraudă: utilizarea cartelelor neautentificate, furtul numerelor cartelelor de credit și afirmațiile frauduloase ale comercianților neetici.

Scopul este de a facilita plățile de la distanță, indiferent de canalul de acces: Internet, televiziunea digitală în bandă largă, mesaje text prin intermediul Serviciului de mesaje scurte (SMS), WAP și așa mai departe.

Soluția solicită utilizatorilor să înregistreze și să stabilească un PIN cu emitentul cartelei pentru autentificare în timpul unei tranzacții online.

Codul PIN este solicitat la verificare la comercianții cu amănuntul online participanți. În acest fel, 3-D Secure permite comercianților să verifice de la distanță dacă o anumită cartelă este sub controlul unui anumit utilizator.

3-D Secure a devenit operațional în 2003 sub marca Verified by Visa. MasterCard a stabilit un serviciu echivalent numit SecureCode.

6.5 Sistemul 3-D Secure

Arhitectura are în vedere trei domenii: domeniul emitentului, domeniul achizitorului și domeniul de interoperabilitate prin intermediul rețelei de plăți Visa, unde intermediarul Visa pentru 3-D Secure verifică părțile.

În cadrul domeniului emitentului, fiecare emitent al cartelei este obligat să mențină un server special cunoscut ca Server de control al accesului (ACS) pentru a sprijini autentificarea cartelei.

Directoriul Visa se află în domeniul interoperabilității și mediază comunicarea dintre comerciant și emitent.

3-D Secure utilizează patru conexiuni SSL/TLS punct-la-punct pentru a conecta cumpărătorul, comerciantul și poarta de plată.

Legăturile sunt următoarele:

- **Titularul cartelei ↔ Comerciant;**
- **Comerciant ↔ Directoriul Visa;**
- **Titularul cartelei ↔ Serverul de control al accesului;**
- **Directoriul Visa ↔ Serverul de control al accesului.**

Acesta este motivul pentru care soluția a fost denumită inițial 3-D SSL (3-Domain SSL).

6.5 Sistemul 3-D Secure

Utilizarea SSL/TLS oferă servicii de confidențialitate, integritate și autentificare la nivelul Transport. Acest model de operare păstrează canalele bancare existente, iar circuitele de verificare și de decontare financiară continuă să treacă prin rețelele de cartele.

Soluția evită instalarea oricăror i-programe suplimentare pe terminalele utilizatorului, în timp ce comercianții trebuie doar să adauge un plug-in pe serverul de plăți.

Visa/MasterCard preia rolurile porții de plată și ale autorității de certificare și oferă următoarele servicii suplimentare:

- un serviciu de directoare care determină dacă există un șir de numere de cartele care include numărul principal de cont (PAN) verificat;
- o funcție de certificare pentru generarea certificatelor X.509 necesare;
- un depozit pentru istoricul autentificării care înregistrează fiecare încercare de autentificare a plății, indiferent dacă a avut succes.

Comerciantul are acces la toate informațiile despre contul titularului cartelei.

Nonrepudierea la nivelul Aplicație se realizează prin utilizarea semnăturilor, în special deoarece titularul cartelei introduce o parolă sau un cod PIN.

6.5.2 Înrolarea

Pentru a participa la programul 3-D Secure, băncile emitente și dobânditoare furnizează numerele lor de identificare bancară (BIN) și adresele URL ale serverelor respective.

Clientul se înregistrează prin orice canal selectat de banca emitentului. În mod similar, mecanismul de autentificare a titularului cartelei este lăsat de emitent. Acesta poate fi un cod PIN, o cartelă inteligentă, un certificat de identitate sau o măsură biometrică. Implicit este o parolă pe care utilizatorul o alege la înscriere. Dacă este necesar, banca emitentă va furniza tot ceea ce este necesar (echipament sau programe) pentru autentificare. Visa/MasterCard va păstra toate datele referitoare la această cartelă (identitatea titularului, coordonatele băncii, versiunea, etc.) în directorul său securizat.

Comerciantul subscrie serviciului prin intermediul băncii achizitoare, care furnizează și activează modulul plug-in pentru serverul de comerciant (*merchant server plug-in* – MPI). Emitentul își asumă riscul de tranzacții frauduloase și nu sunt permise compensații. Aceasta înseamnă că deținătorul cartelei este în cele din urmă responsabil pentru plăți.

În cele din urmă, exploratorul clientului trebuie să accepte JavaScript pentru a oferi un canal de comunicare între comerciant și banca emitentului fără intervenția cumpărătorului.♦

6.5.3 Protocolul de procurări și plăți

Negocierea dintre cumpărător și comerciant este în afara domeniului de aplicare 3-D Secure. Dacă 3-D Secure a fost activat pentru cartelă, situl comerciantului direcționează cumpărătorul către un sit Web unde are loc autentificarea cartelei. Mesajele sunt codificate în XML.

Autorizația de plată continuă după cum urmează (pentru exemplul Visa):

1. 3-D Secure este pornit atunci când cumpărătorul indică intenția de a cumpăra făcând clic pe butonul „Buy" corespunzător.

2. După primirea comenzii de achiziție cu instrucțiunile de plată, plug-in-ul comerciantului (MPI) solicită lista cu diapazoane de cartele participante din directorul 3-D Secure al Visa cu mesajul CRED (Card Range Request). Aceasta este pentru a verifica dacă numărul principal de cont (PAN) se încadrează în intervalul de cartele participante.

3. Răspunsul directoarelor se găsește în mesajul Response Range Card (CRRes). În funcție de parametrii solicitării inițiale, CRR-urile pot conține fie întreaga listă a gamei de cartele participante, fie modificările de la ultima schimbare. Informațiile returnate pot fi utilizate pentru a actualiza memoria cache internă a MPI. Acest schimb poate fi ignorat dacă MPI are capacitatea de a stoca conținutul directorului Visa, cu condiția ca cache-ul local să fie actualizat, cel puțin la fiecare 24 de ore.

6.5.3 Protocolul de procurări și plăți

4. Apoi, MPI trimite mesajul Verify Enrollment Request (VEReq) în directorul Visa pentru a determina dacă autentificarea Secure 3-D este disponibilă pentru un anumit PAN. Directorul verifică dacă comerciantul, cumpărătorul și titularul cartelei PAN pot fi autentificați utilizând 3-D Secure. Dacă răspunsul indicat în mesajul Verify Response Enrollment (VERes) este negativ, tranzacția poate continua în mod tradițional. În caz contrar, directorul va interoga ACS al băncii emitente pentru autorizarea sa.

5. Mesajul VERes de la serverul de control al accesului al băncii emitente indică dacă titularul este înregistrat în programul 3-D Secure. Într-un astfel de caz, acesta conține adresa URL la care exploratorul deținătorului de cartelă va posta datele furnizate de modulul plug-in pentru comerciant. Dacă titularul cartelei nu este participant la programul 3-D Secure, tranzacția poate continua de-a lungul liniilor tipice.

6. La primirea răspunsului din director, MPI trimite o solicitare de autentificare a plătitorului (PAReq) la serverul de control al accesului emitent (ACS) utilizând adresa URL obținută la etapa anterioară. PAReq conține detalii despre achiziția care trebuie aprobată. Acesta este prezentat într-unul din următoarele moduri:

a) informațiile pot apărea cumpărătorului într-o fereastră pop-up secundară;

b) comerciantul poate apărea utilizând o tehnică HTML denumită *frame inline* sau iframe. Comerciantul definește cadrul pentru pagina de autentificare a achiziției și primește URL-ul pentru a încorpora iframe-ul.

6.5.3 Protocolul de procurări și plăți

7. Transferul controlului la ACS trece prin exploratorul utilizatorului folosind un JavaScript care se află pe pagina de autentificare. În mod alternativ, o modalitate mai sigură ar fi să cereți intervenția explicită a utilizatorilor pentru a continua tranzacția 3-D Secure. Pentru a proteja datele de la modificarea neintenționată de către explorator, ele sunt codificate cu codare Base64. Deoarece în această codificare, fiecare 3 octeți de date sunt extinși în 4, datele sunt comprimate înainte de codificare. Mai mult, pentru dispozitivele de pe Internet mobil, Solicitarea de autentificare a plătitorilor de tip Condensed Payer (*Condensed Payer Authentication Request* – CPRQ) este utilizată pentru a reduce utilizarea lățimii de bandă.

8. Emitentul ACS stabilește o sesiune SSL/TLS cu terminalul deținătorului cartelei și afișează detaliile tranzacției, obținute de MPI, și îi solicită titularului un identificator (un PIN, prin mijloace biometrice, prin introducerea unei cartele într-un cititor de cartele, etc.) și pentru aprobarea achiziției. Titularul cartelei vede o fereastră care conține detaliile achiziției pentru a introduce parola Verified by Visa. ACS leagă PAReq cu mesajele VERes.

6.5.3 Protocolul de procurări și plăți

9. După autentificarea titularului, ACS construiește o valoare de verificare a autentificării deținătorului cartelei (CAVV) de 20 de octeți. CAVV conține o cifrogramă de 2 octeți calculată ca semnătura pentru a valida integritatea sa. CAVV este trimis către MPI în mesajul Response Authentication Payer (PARES), mesaj, semnat cu cheia de semnătură a emitentului. ACS utilizează CAVV pentru a garanta comerciantului că a autentificat deținătorul cartelei. Mesajul folosește codarea Base64, cu datele comprimate înainte de codificare. Pentru dispozitivele mobile, se utilizează răspunsul solicitării de autentificare a plătitorului cu compensare (CPRS).

10. Răspunsul este trimis la serverul de istoric de autentificare pentru arhivare în cadrul mesajului Solicitare tranzacție de autentificare a plătitorului (PATransReq). Confirmarea arhivării este în mesajul de răspuns la tranzacția de autentificare a plătitorului (Payer Authentication Transaction Response – PATransRes).

11. Serverul comerciantului verifică semnătura (CAVV) înainte de a depune o cerere de decontare către banca achizitoare.

Pentru a rezuma, schimburile menționate mai sus cuprind patru faze:

1. Actualizarea cache-ului comerciantului cu intervalele de conturi valabile.

2. Verificarea faptului că un număr de cartelă dat este înregistrat în secțiunea 3-D Secure și, în acest caz, autentificarea deținătorului cartelei pentru a autoriza o anumită tranzacție.

3. Verificarea integrității informațiilor de plată cu semnătura emitentului.

4. Arhivarea încercării de autentificare.

6.5.4 Aprobarea și decontarea

După primirea răspunsului la autentificare, serverul comerciantului extrage informațiile necesare pentru a face o solicitare de captare.

Acesta trimite această solicitare băncii sale cu o indicație că tranzacția este asigurată în conformitate cu 3-D Secure.

Banca achizitor solicită aprobarea de către Visa Directory Server (sau a echivalentului MasterCard).

Serverul compară datele primite de la banca emitent și banca dobânditoare înainte de aprobarea sa.

Odată ce aprobarea a fost acordată, decontarea se efectuează în conformitate cu procedurile obișnuite. ♦

6.5.5 Securitatea

3-D Secure este o încercare de a consolida plățile la distanță prin intermediul cartelelor bancare, bazându-se pe o infrastructură aflată sub controlul Visa/MasterCard și a băncilor asociate.

Diferite entități primesc certificate X.509 Vers. 3 după cum urmează:

1. Directorul Visa/MasterCard are un certificat de server în ceea ce privește comerciantul și un certificat client în ceea ce privește emitentul.

2. MPI are un certificat de server în ceea ce privește titularul cartelei și un certificat client în ceea ce privește directorul Visa și emitentul.

3. ACS are un certificat de server și un certificat de semnătură pentru a semna mesajul PARes; ACS inițiază două sesiuni utilizând certificatele de server: unul la deținătorul cartelei și celălalt la comerciant.

Autoritatea de certificare poate fi Visa/MasterCard sau una dintre autoritățile de certificare recunoscute.

6.5.5 Securitatea

Suita de cifruri obligatorie este (TLS_RSA_WITH_3DES_EDE_CBC_SHA): SHA-1 pentru hash, Triple DES pentru cifrare simetrică și RSA pentru semnătura statică. În mod obișnuit, cheia simetrică utilizată pentru cifrarea traficului care implică suportul de cartelă este de 40 de biți pentru DES (securitate pe 80 de biți pentru Triple DES), datorită proliferării exploratoarelor exportabile din SUA.

Dimensiunea minimă a cheii RSA pentru semnare este de 768 de biți, iar valoarea recomandată este de 1024 biți. O suită de cifruri opțională este (TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA), unde algoritmul Diffie-Hellman (DH) este utilizat pentru a schimba cheile și RSA pentru a semna mesajele din schimbul de chei pentru a-și asigura integritatea. Se preferă seturile de cifruri SSL/TLS de 128 biți ori de câte ori este posibil. În special, conexiunile dintre MPI, terminalul deținător de cartelă și emitentul ACS utilizează HTTPS. Fiecare tranzacție solicită cel puțin cinci legături punct-la-punct securizate cu SSL/TLS.

iFrame-urile sau ferestrele pop-up nu au bară de adrese, astfel încât nu există o cale ușoară de a verifica cine solicită parola.

Emitentul are toate detaliile tranzacției, inclusiv descrierea bunurilor sau serviciilor achiziționate. ♦

6.5.6 Evaluarea

Autentificarea titularului cartelei este mai puternică în cazul tranzacțiilor 3-D Secure, deoarece utilizatorii introduc o parolă suplimentară care trebuie verificată de emitentul cartelei în timpul fazei de autorizare. Clientul 3-D Secure este ușor de instalat și de utilizat. Complexitatea procedurii de securitate este mutată de la utilizator și comercianți la intermediarul de plăți.

3-D Secure are mai multe limitări. Parola este statică, astfel încât securitatea este vulnerabilă dacă parola este compromisă. Nu toate exploratoarele, în special pe dispozitivele mobile, suportă JavaScript; această capacitate este dezactivată de obicei în rețelele corporative din motive de securitate. Exploratorul trebuie să fie configurat să suporte iframe și pop-up-uri. iFrame-urile sau ferestrele pop-up nu au bară de adrese, astfel că nu există o modalitate ușoară de a verifica cine solicită parola. Nu există nici o protecție împotriva siturilor de pihishing care vizează produsul 3-D Secure prin afișarea ferestrei inline "Verified by Visa" sau "MasterCard SecureCode". O resetare a parolei utilizează de obicei o metodă numită Activare în timpul cumpărăturilor (ADS). În această metodă, se solicită o formă slabă de autentificare (cum ar fi data nașterii), care poate fi disponibilă din registrele publice. Emitentul are toate detaliile tranzacției, inclusiv cele achiziționate. Deci, beneficiile pe care le primesc deținătorii de cartele nu sunt proporționale cu creșterea lor în răspunderea pentru fraudă și pierderea vieții private. Acest lucru a limitat utilizarea tehnologiei 3-D Secure. ♦

6.6 Migrarea spre EMV

Sofisticarea crescândă a atacurilor asupra sistemelor de procesare a cartelelor, a sistemelor de plăți comerciale sau a sistemelor pentru intermediari, cum ar fi procesatorii de plăți, a creat probleme pentru industria de plăți cu cartele. În cele din urmă, au apărut noi posibilități de fraudă în legătură cu cartelele, în paralel cu creșterea utilizării Internetului și a telefoniei mobile.

Pentru a face față sofisticării în creștere a atacurilor asupra sistemelor de tranzacții electronice, industriile cartelelor de plată au impus migrarea de la benzi magnetice la cartelele cu microcipuri care rulează protocolul EMV.

În scopul motivării băncilor și comercianților de a-și îmbunătăți echipamentul pentru a se conforma EMV, mărcile cartelelor de plată au schimbat răspunderea cartelei care nu prezintă fraudă părții care nu respectă EMV.

De exemplu, un comerciant echipat pentru EMV poate accepta plăți cu o cartelă cu bandă magnetică, dar banca deținătorului cartelei va fi responsabilă în cazurile contestate. În schimb, dacă cumpărătorul are o cartelă cu cip, dar comerciantul nu are mijloacele să îl accepte, banca comerciantului va fi responsabilă de orice tranzacție repudiată.

Băncile europene au trecut la tehnologia EMV în ianuarie 2005. În Statele Unite însă, migrația s-a confruntat cu o rezistență semnificativă, în special din industria comerțului cu amănuntul.

6.6 Migrarea spre EMV

Introducerea cartelelor EMV a redus falsificarea cartelelor. Frauda globală a crescut brusc în primul an de la introducerea EMV, după care a scăzut continuu.

Numărul de cartele pierdute sau furate crește cu tranzacțiile IMOTO, ceea ce conduce la convingerea că scopul principal al furtului este obținerea codului PIN din banda magnetică.

EMV oferă un mod de rezervă de operare cu bandă magnetică pentru a găzdui terminalele moștenite, precum și cartelele aflate în circulație. Concentrându-se pe aceste terminale, infractorii au reușit să forțeze cartelele cu circuite integrate pentru a folosi datele de pe banda lor magnetică.

Spike-ul fraudei după introducerea cartelelor cu cip poate fi explicat prin încercările de a exploata pe deplin această fereastră de vulnerabilitate cât mai mult posibil, înainte ca emitenții să blocheze cartelele și băncile să-și actualizeze terminalele.

Frauda totală a scăzut pentru câțiva ani, deoarece toate aceste vulnerabilități au fost fixate până când s-au descoperit noi căi, care reflectă creșterea ratei de fraudă.

6.6 Migrarea spre EMV

EMV a fost conceput pentru tranzacții față-în-față și nu pentru tranzacții online. Prin urmare, reducerea fraudei în tranzacțiile IMOTO nu a fost la fel de dramatică ca și pentru alte tipuri de tranzacții și este atribuită altor factori, cum ar fi generalizarea sistemului 3-D Secure. Aceeași observație a fost făcută și în Franța, unde rata de fraudă în tranzacțiile IMOTO a crescut la 61% din volumul total al tuturor plăților cu cartele franceze în 2011, în timp ce tranzacțiile IMOTO contribuie numai la 8,4% din valoarea totală a tuturor plăților cu cartele. Pentru a contracara această amenințare, autoritățile franceze au recomandat adoptarea programului 3-D Secure.

În majoritatea țărilor, a fost nevoie de 7-10 ani pentru a lansa infrastructura EMV. În scopul sprijinirii tranziției la EMV, MasterCard și Visa au inițiat crearea unui grup trans-industrial pentru a ajuta băncile, comercianții cu amănuntul, producătorii de dispozitive POS și alții. ♦

6.7 Sumar

Doar o mică parte din tranzacțiile cu cartele de plată sunt potențial frauduloase, însă consecințele unei astfel de fraude asupra actorilor industriali sunt semnificative în ceea ce privește pierderile monetare, relațiile publice și inconvenientele pentru clienți.

Principalele surse de fraudă cu cartele de plată sunt cartelele pierdute sau furate, contrafacerea cartelelor și/sau achizițiile online. Cartelele de plată cu bandă magnetică sunt deosebit de vulnerabile la falsificare. Au fost încercate mai multe abordări de protejare a tranzacțiilor cu cartele cu bandă magnetică, dar nici una dintre ele nu a fost pe deplin satisfăcătoare. Cartelele cu circuite integrate îmbunătățesc protecția împotriva contrafacerii. Totuși, atâta timp cât banda magnetică este menținută, fie într-o cartelă tradițională, fie într-una cu circuite integrate, acestea vor continua să deschidă zone vulnerabile pentru a fi exploatate pentru fraudă.

Pe măsură ce abilitatea de a contraface cartelele se reduce, se așteaptă ca infractorii să exploreze vulnerabilități, cum ar fi implementarea incorectă a EMV sau controlul scăzut al afacerilor.■