7 PLĂȚI CU CARTELE CU CIRCUITE INTEGRATE

7.1 Descrierea cartelelor cu circuite integrate

7.2 Integrarea cartelelor inteligente cu sistemele de calcul

7.3 Standarde pentru cartelele cu circuite integrate

7.4 Securitatea cartelelor cu circuite integrate

7.5 Cartele EMV

7.6 Atacuri asupra cartelelor inteligente

7.7 Sumar

7 PLĂȚILE CU CARTELE CU CIRCUITE INTEGRATE

Utilizarea cartelelor cu circuite integrate (cartele inteligente) în aplicațiile de plată a început în Franța pentru cartele telefonice și cartele de retragere de la ATM.

O extindere majoră a utilizării acestora a urmat succesului companiei Groupe Spécial Mobile (GSM-Global System for Mobile Communication) – Specificațiile europene pentru rețelele celulare digitale.

Au urmat alte aplicații de plată în sistemele de tranzit public și elaborarea specificațiilor EuroPay, MasterCard și Visa (EMV) pentru tranzacțiile financiare.

7.1 Descrierea cartelelor cu circuite integrate

7.1.1 Tipuri de memorie

O cartelă inteligentă tipică utilizează un procesor pe 8 biți, o memorie ROM de 16 Ko, memorie cu acces aleator (RAM) de 256, 512 sau 1024 octeți și memorie PROM de la 3 până la 32 Ko. Există și cartele inteligente cu resurse mai perforante.

ROM-ul conține sistemul de operare al cartelei și o mască configurată în funcție de aplicație, cum ar fi telefonia sau banca. ROM-ul are două forme principale: memorie numai pentru citire programabilă electric (EPROM) și memorie programabilă (EEPROM) ce poate fi ștearsă electric. Conținutul EPROM este șters numai după expunerea la radiații ultraviolete. Acest tip de memorie se găsește adesea pe cartele de unică folosință. Cartelele programabile sau securizate utilizează memorii EEPROM pentru a stoca chei de cifrare, actualizări sau corecții de erori. Această categorie de memorii necesită două cicluri de ceas pentru a scrie un octet de date, primul care șterge datele existente, iar cel de-al doilea pentru a înregistra noul octet. Noile tehnologii de memorie, cum ar fi flash sau RAM pe ferita (FeRAM), pot reduce timpul de scriere și consumul de energie.

RAM-ul este programabil și poate conține rezultate intermediare. Conținutul RAM static (SRAM) rămâne stabil, în timp ce conținutul RAM dinamic (DRAM) trebuie actualizat periodic pentru a preveni pierderile.

7.1.1 Tipuri de memorie

Funcțional, memoria unei cartele cu circuit integrat securizat este organizată sub forma unei ierarhii de zone:

- **zona de fabricație - partea de memorie înregistrată înainte de personalizare. Aceasta include numărul de lot al plachetei, numele fabricantului și numărul lui de serie, numărul de serie al cartelei și identitatea furnizorului de cartele;**
- **zona secretă blochează informațiile confidențiale ale titularului cartelei, cum ar fi codul PIN sau cheile cifrografice secrete și fișierele cu date personale;**
- **tranzacțiile sau zona de lucru stochează informațiile confidențiale temporare referitoare la tranzacțiile individuale, cum ar fi suma, soldul valorii stocate și detaliile legate de vânzător. Această parte este împărțită între diferitele aplicații din cartelele multiplicație;**
- **zona de control al accesului înregistrează, sub controlul microprocesorului, toate încercările de acces sau de acces cu succes la zona secretă sau la zona de tranzacții (dacă această zonă este protejată). Astfel, este posibil de blocat accesul la cartelă după trei încercări nereușite;**
- **zona liberă de citire sau zona cu acces deschis, unde sunt stocate informații neconfidențiale, cum ar fi numele deținătorului și emitentului și data de expirare. Această zonă este accesibilă pentru diferitele aplicații ale cartelelor multiaplicație.**

Accesul la memorie este controlat de o logică de securitate care depinde de puterea de procesare disponibilă pe cip. ♦

7.1.2 Capabilități de procesare

În funcție de capacitatea lor de calcul, cartelele cu circuite integrate pot fi împărțite în mai multe categorii:

- **cartele de memorie. Aceste cartele includ un microprocesor cu capacitate redusă care poate stoca date și oferă chiar și o protecție minimă a datelor; puterea de procesare este adaptată la plățile anticipate, cum ar fi pentru cartelele telefonice;**
- **cartele logice prin cablu. Aceste cartele sunt utilizate pentru a oferi controlul accesului la canalele de televiziune cifrate;**
- **cartele inteligente adecvate sau cartelele cu circuite integrate. Acestea sunt mașini programabile care sunt capabile de calcule complexe. Cartelele microprocesor sunt flexibile și utilizate în principal în aplicații sensibile la securitate, cum ar fi identificarea abonaților în telefonia celulară sau în i-plăți.**

7.1.2 Capabilități de procesare

Cartelele telefonice preplatite tradiționale sunt cartele de contact, monoaplicație și de unică folosință. Valoarea totală a unităților telefonice corespunde unui număr egal de celule de memorie. Celulele sunt șterse progresiv, deoarece cartela este utilizată până când toate unitățile au fost epuizate. Capacitatea lor de stocare este de ordinul a 8-256 Kbiți, dar poate ajunge la sute de Mbiți.

Avantajul cartelelor de memorie este că datele stocate pot fi protejate împotriva accesului neautorizat. Accesul este supravegheat de sistemul de operare în conformitate cu o anumită logică de securitate.

Microprocesoarele oferă protecție suplimentară prin implementarea algoritmilor cifrografici.

În mod tipic, se adaugă un coprocesor pentru a se ocupa de calculele cifrografice și pentru a stoca datele securizate.

În cartelele cu aplicație multiplă, securitatea necesită accesul compartimentat la resursele de calcul, astfel încât mai multe aplicații să coexiste fiecare cu propriile acreditări personalizate. ♦

7.1.3 Sisteme de operare

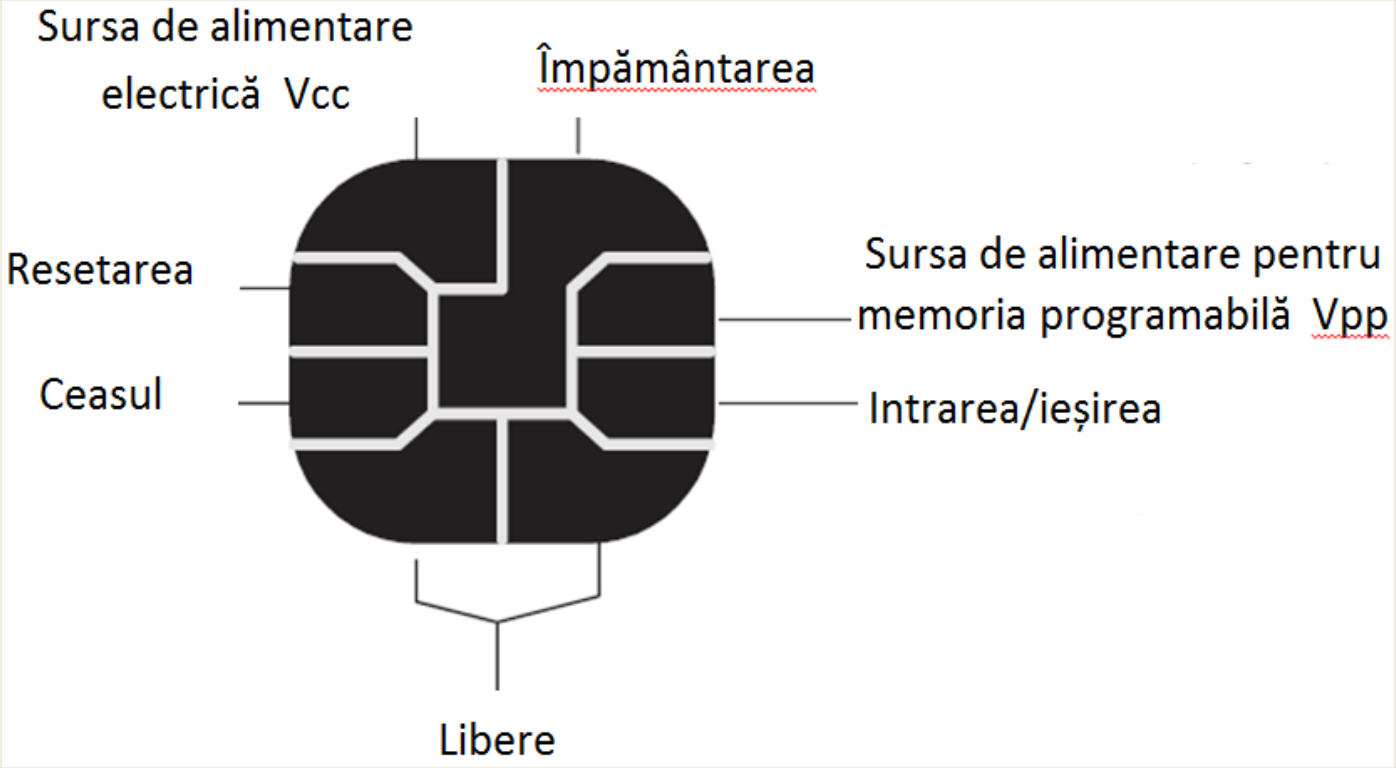
În trecut, sistemul de operare (se află în ROM) a fost specific unui anumit producător, cum ar fi cel M4. Pentru cartelele cu mai multe aplicații, există acum câteva opțiuni standard:

- **Sistemul multifuncțional de operare (MULTOS) a fost dezvoltat de Consorțiul MULTOS, care include producători de cipuri, scheme de cartele de plată, în special MasterCard, furnizori de sisteme de gestionare și personalizare a cartelelor și furnizori de soluții de cartele inteligente (MasterCard, Mondex, EuroPay, Siemens, etc.). Specificațiile tehnice MULTOS acoperă sistemul de operare, limbajul de asamblare al limbajului executabil MULTOS (MEL), API-ul și interfețele de cip. Este proiectat special pentru aplicații de plată sigure;**
- **Java Card a fost dezvoltat de Visa International și aliații săi pentru cartele inteligente bazate pe mașina virtuală Java definită de Forumul Java Card;**
- **Windows for Smart Card de la Microsoft, care are o bibliotecă de comenzi cifrografice și Windows.Devices.Smart Cards API pentru a lucra cu cartele inteligente fizice și virtuale și cititoare de cartele inteligente.**

Există, de asemenea, mai multe sisteme de operare proprietare. De exemplu, cartela Advantis utilizează sistemul de operare TIBC 3.0 (*Tarjeta inteligente y cajas de bancos*), dezvoltat de Visa Spain, pentru aplicarea unui portofel electronic. Compania germană ZeitControl furnizează BasicCard cu un sistem propriu sigur și funcții cifrografice, cum ar fi cifrarea RSA pe 4096 de biți și cifrografia curbelor eliptice pe 512 biți. ♦

7.1.4 Cartele cu circuite integrate cu contacte

O cartelă cu circuite integrate cu contacte are opt puncte de contact specificate în standardul ISO/IEC 7816. Standardul definește locurile contactelor dintre cartelă și cititoarele de cartelă pentru a asigura compatibilitatea acestora. Contactele trebuie să reziste la uzura datorată utilizării și coroziunii cauzate de diverși factori (abraziune, poluare, substanțe chimice,.etc.).



7.1.4 Cartele cu circuite integrate cu contacte

În cartelele cu contacte, rata de ceas variază între 3,5 și 5 MHz. Sursa de alimentare este între 3 sau 5 V. Evoluțiile microelectronicii au eliminat necesitatea unei surse suplimentare de alimentare pentru alimentarea memoriei programabile cu 5-15 V sau chiar 21 V. Aceasta reduce șansele de atacuri externe prin fluctuații de tensiune, contactul a fost folosit pentru transmisia duplex, dublând astfel ratele de date.

Cititoarele de cartele cu contacte sunt, în general, echipate cu un mecanism pentru a prinde cartela automat îndată ce aceasta este introdusă în slot-ul cititorului de cartele. Această configurație îmbunătățește fiabilitatea lecturii și consolidează rezistența cititorului de cartele la abuzul utilizatorilor și la vandalism, deși cu prețul unei complexități sporite și a costurilor operaționale și de întreținere.

Dacă circuitul integrat este programabil, se poate utiliza cifrografia pentru a asigura schimbul de date. În mod tipic, se adaugă un coprocesor pentru a gestiona calculele cifrografice și pentru a stoca datele securizate.

7.1.5 Cartele cu circuite integrate fără contacte

Cartele cu circuite integrate fără contacte (cartele RFID) transmit date pe distanțe scurte folosind frecvențe radio. Cartela este alcătuită dintr-un circuit integrat (transponder de etichetă în cazul RFID), o antenă și circuitele electronice asociate pentru transmisia și prelucrarea datelor, de obicei încorporate într-o carcasă din plastic. Acestea sunt disponibile într-o varietate de forme, cum ar fi: cartelele de plastic, *bobs*, documente și dispozitive mobile.

Operarea fără contacte permite evitarea uzurii sistemelor mecanice, reducând astfel costurile de întreținere. Acestea pot oferi servicii persoanelor care se deplasează la viteze mici, apropiate punctelor de vânzare, automatelor de vânzare, locurilor de parcare, etc., ceea ce duce la accelerarea fluxului. MasterCard Worldwide a constatat că plățile fără contacte reduc durata tranzacției cu mai mult de 50% de la 26,7 la 12,5 sec.

Cartelele active fără contacte au propria lor sursă de energie - baterie. Bateriile sunt, totuși, costisitoare, uzabile și greu de eliminat. Dispozitivele pasive sunt alimentate prin cuplaj inductiv de la cititor.

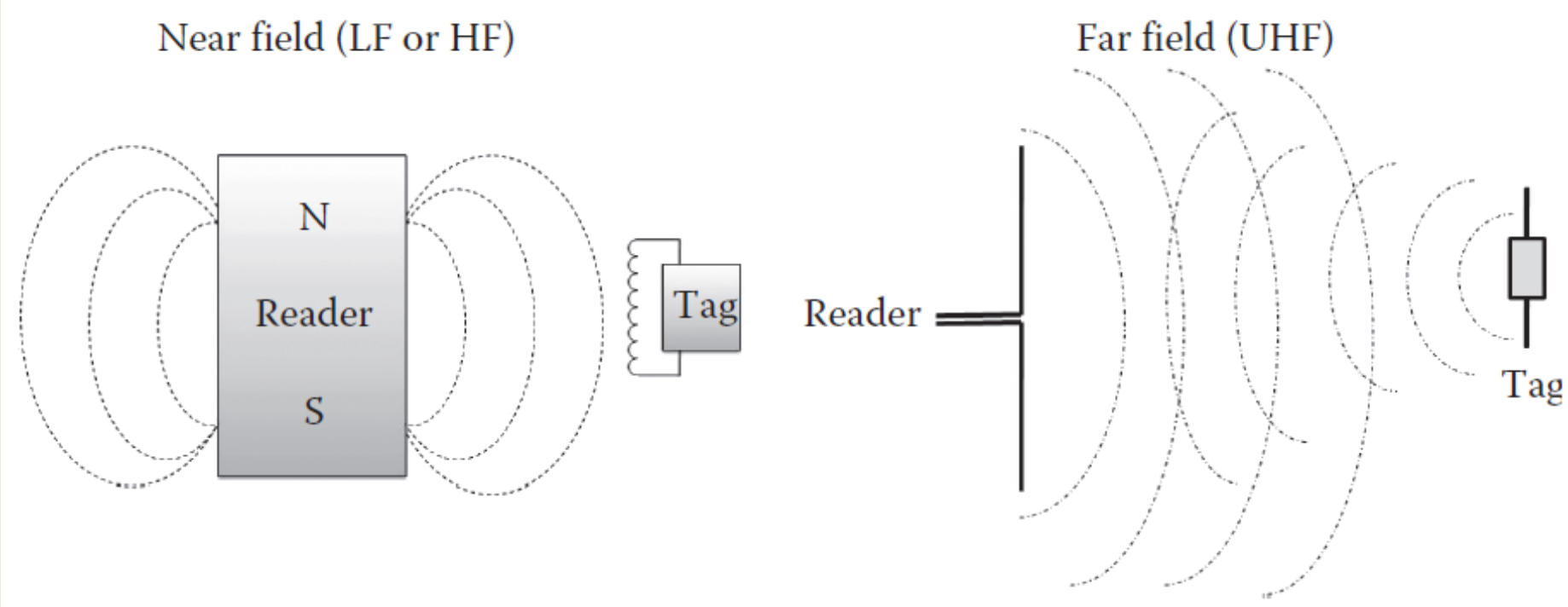
7.1.5 Cartele cu circuite integrate fără contacte

Cartelele de proximitate sunt folosite pentru distanțe sub 40 cm, în timp ce cartelele de vecinătate sunt utilizate pentru distanțe de până la 1-1,5 m. Rata de biți este de obicei mai mare pentru cartelele de proximitate decât pentru cele de vecinătate (106, 212 și 424 Kbps față de până la 26 Kbps), în timp ce consumul de energie al cartelelor de vecinătate este mai mic. Cartelele de proximitate sunt utilizate în aplicațiile de plată, cum ar fi biletele automate în sistemele de transport și terminalele POS.

Pentru distanțe mai mari, comunicarea de la transponder înapoi la cititor utilizează reflexiile antenei circuitului integrat (*backscatter*). Un rezistor de sarcină este conectat în paralel cu antena dispozitivului fără contact și această sarcină este pornită și oprită în funcție de datele care trebuie transmise. Astfel, intensitatea semnalului reflectat de transponder poate fi modulată înapoi. Distanțele implicate sunt de ordinul a 10 m, ceea ce face sistemul potrivit pentru aplicații cum ar fi sistemul de colectare a taxelor pe autostrăzi. Figura 9.2 ilustrează diferența dintre metodele de comunicare „îndeaproape” și „la distanță” între un cititor și etichetă.

7.1.5 Cartele cu circuite integrate fără contacte

Diferența dintre metodele de comunicare „îndeaproape” și „la distanță” între un cititor și etichetă [3].



♦

7.2 Integrarea cartelelor inteligente cu sistemele de calcul

Există mulți actori independenți în arhitectura sistemelor de plăți deschise: producători de cartele, bănci, dezvoltatori de aplicații și furnizori de terminale. De aceea sunt necesare anumite specificații pentru a interconecta diferitele componente și pentru a menține securitatea globală a sistemului de plăți, precum și a componentelor individuale.

Două soluții principale au fost dezvoltate pentru a asigura o interfață securizată unică pentru a accesa cartelele cu circuite integrate cu sistemul de operare Windows, independent de perifericele de acces sau de aplicațiile care se găsesc pe cartelă. Acestea sunt OpenCard Framework (OCF) orientat Java și caseta de instrumente PC/SC pentru Windows.

Pentru a furniza o interfață standard în Linux, a fost elaborată utilita MUSCLE (*Movement for the Use of Smart Cards in a Linux Environment*).

7.2 Integrarea cartelelor inteligente cu sistemele de calcul

7.2.1 Produsul OpenCard Framework

OpenCard Framework (OCF) este produsul consorțiului OpenCard (IBM, Sun Microsystems și Gemplus). Obiectivul a fost de a crea o interfață PC pentru cartele inteligente, independentă de sistemul de operare. Lucrarea s-a încheiat cu OCF versiunea 1.2 și o implementare de referință de către IBM.

OCF este un middleware implementat în Java cu o interfață de programare comună pentru toate aplicațiile Web. Ea permite oricărei aplicații de cartelă inteligentă să acceseze atât cartelele cu contacte, cât și cele fără contacte, care utilizează în comenzile lor APDU (*Application Protocol Data Units*) definite de ISO/IEC 7816. Serviciile OCF protejează aplicațiile Java de specificul fiecărei cartele inteligente sau terminal de acces (terminal ATM, calculator, cititor de cartele, etc.) prin intermediul serviciilor abstracte: CardService pentru cartele și CardTerminal pentru periferice. Acest lucru permite ca grupuri de secvențe complexe de comenzi să fie executate cu un set mai simplu de instrucțiuni, cum ar fi manipularea mai multor solicitări simultane de autentificare, întâlnite în aplicațiile financiare sau din medicină.

7.2.2 Specificația PC/SC

Specificația de interoperabilitate pentru cartelele cu circuite integrate și sistemele de calculatoare personale este o abreviere pentru (Interoperability Specification for Integrated Circuit Cards and Personal Computer Systems - PC/SC) a fost prima propunere de a conveni asupra specificațiilor pentru conectarea cartelelor inteligente la PC-uri.

Aceasta a fost elaborată de producători de cartele cu circuite integrate și furnizori de PC-uri: Gemplus, Hewlett-Packard, IBM, Sun Microsystems și Microsoft.

Ea se bazează pe sistemul de operare Windows și acceptă mai multe limbaje.

Microsoft a publicat propria bibliotecă cifrografică, CryptoAPI, care poate fi utilizată în mediul Windows pentru a accesa funcțiile cifrografice și certificatele stocate pe o cartelă inteligentă. CryptoAPI oferă, de asemenea, servicii de mesagerie securizată și de gestionare a certificatelor. Figura prezintă arhitectura PC/SC.

7.2.3 Activități pentru utilizarea cartelelor inteligente în Linux

MUSCLE a publicat prima versiune a unei interfețe de programare a aplicațiilor Linux pe cartele inteligente în anul 2000.

MUSCLE se bazează pe PC/SC, dar codul sursă este disponibil sub licența GPL, definită de Free Software Foundation.

Astfel, acesta poate fi modificat și extins de alte părți. ♦

7.3 Standarde pentru cartelele cu circuite integrate

Standardele pentru cartelele inteligente sunt necesare pentru creșterea factorului de scalare, care reduce costurile de producție ale unității, și facilitarea creării de rețele la nivel mondial prin interfețe armonizate.

Standardizarea a avansat pe aspectele fizice ale cartelelor; cu toate acestea, lipsa de standardizare la nivel logic împiedică aplicațiile financiare la scară largă.

7.3.1 Standardele ISO pentru cartele cu circuite integrate

ISO/IEC 7816 este un standard internațional multipartit care definește diferite aspecte ale ambelor tipuri de cartele cu circuite integrate: cu contacte și fără contacte. Standardul cuprinde 14 părți. Părțile 1, 2 și 3 tratează interfața fizică dintre plăcile cu circuite integrate și contactele cititoarelor de cartele pentru a asigura compatibilitatea acestora. Părțile 4, 5, 6, 8, 9, 11, 13 și 15 sunt relevante pentru cartelele cu contacte și cartelele fără contacte. Partea 7 definește o bază de date relațională securizată, în timp ce partea 10 se referă la cartele de memorie preplătite. Partea 14 nu există.

ISO/IEC 7816 este baza pentru toate cartelele inteligente. ♦

7.3.2 Standardele ISO pentru cartele fără contacte

Descrierea și funcționarea cartelelor fără contacte sunt acoperite de un set de standarde ISO/IEC (14443, 15693, 18000-3 și 18092). Ele definesc aspectele fizice, mecanice și electrice ale cartelelor fără contacte, precum și protocoalele de comunicare.

Multe aplicații pentru cartelele fără contacte funcționează în banda de frecvență înaltă (HF) la 13,56 MHz, cu o rată de transfer de 106 Kbps.

În alte aplicații RFID, frecvențele utilizate sunt:

- **banda cu frecvență redusă LF (mai joasă de 135 kHz);**
- **banda industrială, științifică și medicală ISM (13,56 MHz și 2,4 GHz);**
- **banda de frecvență superioară SHF (5,8 GHz).**

În funcție de gama de operațiuni, cartelele fără contacte pot fi împărțite în:

- **cartele de proximitate (de obicei, până la 40 cm);**
- **cartele de vecinătate (de obicei, până la 1 m).**

7.3.2 Standardele ISO pentru cartele fără contacte

ISO/IEC 14443 este un standard internațional în patru părți care definește caracteristicile cartelelor de proximitate utilizate pentru identificare și protocoalele de transmisie.

Caracteristicile fizice și funcționarea cartelelor de vecinătate sunt definite în standardul ISO/IEC 15693 din trei părți. Cartelele de vecinătate nu sunt utilizate în aplicațiile de i-comerț; ele sunt folosite pentru a controla accesul în zonele securizate și ca ecusoane de identificare purtate într-o manieră vizibilă.

Cartelele fără contacte pot fi active și pasive. Cartelele pasive sunt inactive până când primesc un semnal de la un cititor; odată ce sunt alimentate, încep să transmită. Un cititor la un moment dat poate energiza o cartelă pasivă; dacă mai multe cititoare încearcă să activeze o cartelă pasivă, apare o condiție cunoscută sub numele de "coliziunea cititoarelor". De asemenea, în sistemele pasive cititorul poate comunica cu mai multe cartele, deci trebuie să le atribuie un ordin de transmisie astfel încât să nu interfereze una cu cealaltă.

Cartelele active fără contacte au o baterie mică, care le permite să înceapă comunicarea și să transmită semnalele care pot fi recepționate la distanțe mai mari decât cartelele pasive. ♦

7.3.3 Standarde RFID

Tehnologia RFID utilizează aceleași principii fizice ca și cartelele cu circuite integrate fără contacte pentru a urmări obiectele. Un sistem fără contacte RFID constă dintr-un transponder sau o etichetă, o antenă, un cititor/înregistrator și un calculator gazdă. Transponderul/eticheta este un pachet compact al unui microcip conectat la antenă, care este fie atașată la un obiect, fie integrată în dispozitiv. Cea mai simplă etichetă este o cartelă de memorie care stochează datele unui produs.

Când eticheta se apropie de cititorul RFID, în antenă este indus un curent electric, alimentând circuitul cipului pentru a efectua anumite calcule înainte de a transmite un răspuns. Deoarece etichetele RFID sunt pasive, prețul lor poate fi atractiv pentru aplicațiile în masă.

Comunicarea pasivă între cititor și transponder este stabilită în unul din două moduri: primul vorbește cititorul (ITF) sau eticheta vorbește numai după ascultare (TOTAL). În sistemele ITF, eticheta modulează coeficientul său de reflexie a antenei cu un semnal de informare numai după ce cititorul îi permite să facă acest lucru. Sistemul este notat ca TOTAL dacă eticheta ascultă mai întâi modulul cititorului și determină ce sistem este, iar, dacă este ITF, transmite informațiile fără a aștepta permisiunea.

7.3.3 Standarde RFID

Sistemele RFID au crescut independent de multe sectoare industriale și au fost optimizate pentru un anumit domeniu de aplicare.

În consecință, terminologiile, precum și standardele aferente nu sunt complet armonizate.

În special, absorbția rapidă a RFID în lanțul de distribuție cu amănuntul conduce în prezent la standardizare, chiar dacă cartelele fără contacte au fost utilizate pentru prima dată în aplicații de control al accesului și de plată.

De exemplu, transponderele RFID sunt denumite în mod obișnuit etichete (*tags*), deoarece acestea sunt aplicate produselor înainte de expediere pentru urmărire și inventar în locul codurilor cu bare.

În aplicațiile de colectare a taxelor, transponderele sunt numite unități de bord.

Cititoarele sunt uneori numite interogatoare.

Acestea pot fi numite validatoare în sistemele de transport public urban și în unitățile rutiere în sisteme inteligente de transport.

7.3.3 Standarde RFID

Unele caracteristici ale dispozitivelor (tags) RFID [3]:

Frequency Band	Frequency Range	Read Range	Cost	Applications	Standards
Low frequency (LF)	125–135 kHz	10 cm (passive) to 1 m (active)	Low	Access control inventory control, timing for sporting events	ISO 11784/11785 ISO/IEC 18000-2
High frequency (HF)	13.553–13.567 (13.56)[a] MHz	3 cm to 1 m	Medium	Contactless cards, near-field communication, passive transponders/tags	ISO/IEC 15963,14443A, 14443B, 18000-3, 18092 EPC Class 0/1
Ultra high frequency (UHF)	433 MHz	15–100 m		Transponders in containers	ISO/IEC 18000-7
	850–950 MHz	60 cm to 3 m (passive) >10 m (active)	High	Transponders in pallets	EPC Class 0/1 EPC UHF Gen 2 ISO/IEC 18000-6
	2.45[a] GHz	1–6 m (passive)		Container/toll collection	ISO/IEC 18000-4
Super high frequency (SHF)	5.8[a] GHz	15–100 m (active)		Toll collection	None

7.3.4 Standarde de comunicare în apropiere

Comunicarea în apropiere (*near-field communication* – NFC) este un subset al tehnologiei RFID, unde eticheta (*tag*) include o bobină mică pentru extragerea energiei de la un curent electric indus de cititor. Tehnologia este cu identificarea fără contacte în conformitate cu ISO/IEC 14443 și cu comunicațiile fără fir la 13,56 MHz. În consecință, există o suprapunere între utilizarea cartelelor de proximitate și a dispozitivelor NFC în aplicațiile de plată. Dispozitivele NFC pot citi cartele de proximitate, iar terminalele fără contacte pot comunica cu etichetele NFC. Astfel, dispozitivele NFC pot înlocui cartelele fără contacte.

Începând cu anul 2014, soluțiile NFC sunt mai populare în Asia și Europa decât în America de Nord. Se estimează că în Europa în 2014 existau cca.100 mln de cartele fără contacte, adică 1/5 din toate cartelele de plată. Visa Europe a început lansarea de terminale comerciale NFC în 2007, iar numărul acestora a ajuns la 1,5 mln în 2014.

NFC a fost coinventat de NXP Semiconductors (fostul Philips Semiconductors) și Sony. Tehnologia este destinată comunicațiilor fără contacte de scurtă distanță (3-10 cm) și este utilizată de sistemele din benzile LF sau HF. Cititoarele NFC fac parte din terminalele POS, porțile de transport public, echipamentele industriale, etc. Spre deosebire de NFC, comunicarea la distanță (*far-field*) este utilizată în benzi UFH și microunde.

7.3.4 Standarde de comunicare în apropiere

Standardizarea tehnologiei NFC a început în Asociația Europeană a Producătorilor de Calculatoare (ECMA) cu ECMA-340 și ECMA-352, care au fost ulterior adoptate ca ISO/IEC 18092 și ISO/IEC 21481.

ISO/IEC 18092/ECMA-340 și ISO/IEC 24181/ECMA-342 definesc interfețele NFC și protocoalele NFCIP-1 și respectiv NFCIP-2.

NFCIP-1 este un superset al ISO/IEC 14443 și FeliCa (JIS X 6319-4). Funcționează la 106, 212 sau 424 Kbps, cu o schemă de modulare și codare pentru fiecare rată de biți. Protocolul NFC este similar cu protocolul pentru cartele de proximitate: comunicare semiduplex, evitarea coliziunilor, etc. O diferență este că ambele părți NFC își pot asuma rolul de master, în timp ce pentru cartelele fără contacte terminalul este întotdeauna masterul. Altă deosebire este că protocolul NFC definește două moduri de comunicare: activ și pasiv. În modul de comunicare activ, fiecare dispozitiv generează propriul câmp de frecvență înaltă la frecvența purtătoare pentru a transmite date. În modul pasiv, numai inițiatorul generează un câmp de frecvență înaltă la frecvența purtătoare, în timp ce țintă utilizează modulația de încărcare pentru transferul de date, adică prin variația sarcinii pe bobină proporțional cu semnalul de transmis.♦

7.4 Securitatea cartelelor cu circuite integrate

Securitatea cartelelor cu circuite integrate acoperă atât datele secrete stocate pe cartelă, cât și drepturile de acces la serviciu. Obiectivele procesului de securitate sunt:

- **prevenirea falsurilor la toate etapele de fabricare;**
- **prevenirea furtului firmware-ului pentru aplicații și securitate;**
- **protejarea informațiilor stocate;**
- **detectarea și prevenirea oricărei utilizări ilegale sau abuzive.**
- **Protecția trebuie acordată atât în timpul fabricației, cât și în timpul utilizării.**

7.4.1 Securitatea în timpul fabricației

În 2015 serviciile de informații americane și britanice au reușit să pătrundă în rețeaua de calculatoare internă a Gemalto, cel mai mare producător de cartele SIM din lume, să planteze programe rău intenționate pe mai multe calculatoare care le-au permis să preia cheile de cifrare ale cartelelor. ♦

7.4.2 Securitatea fizică a cartelelor în timpul folosirii

Fizic, elementele de suport din plastic de formă dreptunghiulară sunt similare cu cartelele cu bandă magnetică, cu excepția contactelor pentru microprocesor de pe fața cartelei. O hologramă este, de asemenea, disponibilă pentru a spori securitatea și a face mai dificilă contrafacerea. Locația acestei holograme este aceeași în toate țările.

Cartelele inteligente au o bandă magnetică pe partea inversă pentru interoperabilitate cu cititoarele vechi. În ceea ce privește cartelele cu bandă magnetică, elementele de identificare și verificare a codului PIN, data de expirare, precum și codurile care descriu privilegiile utilizatorului sunt înregistrate pe căile magnetice pe partea din spate.

Cartelele inteligente includ circuite rezistente la înșelăciuni (*tamper*) care inhibă operațiile de ieșire atunci când se detectează un atac fizic. Un strat dielectric oferă protecție pasivă (circuitelor integrate) de impurități, praf și radiații. Când acest strat pasiv este defectat, circuitul integrat poate reacționa la diferențele de lumină, temperatură, tensiune sau frecvență.

Protecția fizică a celulelor de memorie poate fi folosită pentru a preveni o ștergere selectivă sau pentru a distribui stocarea de cuvinte secvențiale în celule de memorie. Există protecție specială pentru a dezactiva circuitele de testare utilizate înainte de distribuirea cartelelor.♦

7.4.3 Securitatea logică a cartelelor în timpul folosirii

Mai multe măsuri asigură securitatea logică a cartelelor în timpul utilizării.

În sectorul bancar cu amănuntul, standardele actuale pentru gestionarea cheilor sunt ISO 11568 (părțile 1, 2 și 4) și ISO 9564 pentru gestionarea PIN-ului.

ISO 9564 și ISO 16609: 2012 specifică utilizarea operațiunilor cifrografice în cadrul tranzacțiilor financiare cu amănuntul pentru autentificarea prin PIN și autentificarea mesajelor.

Standardul ISO 11568 este aplicabil pentru gestionarea cheilor introduse de aceste standarde.

ISO 11568-1: 2005 se aplică cheilor sistemelor cifrografice simetrice și asimetrice utilizate pentru protejarea confidențialității, integrității sau autentificării în serviciile financiare cu amănuntul: terminale POS, automate de distribuire a numerarului, automate de tranzacționare (ATM), etc.

7.4.3 Securitatea logică a cartelelor în timpul folosirii

În comerțul direct, identificarea cartelei se face de către comerciant prin mijloace fizice (buletin de identitate al titularului, semnătură, etc.) sau prin chemarea unui server de autorizare sau prin utilizarea codului PIN al titularului, care este i-semnătura pentru retragerea de numerar sau pentru plăți.

Sistemele de autorizare online se bazează pe proceduri cifrografice pentru a autentifica participanții (titularul cartelei, cartela și terminalul comerciantului). Procesul constă din două etape: autentificarea reciprocă a deținătorului cartelei și a cartelei și autentificarea reciprocă a cartelei și a terminalului de rețea.

În cazul verificării offline, cartela conține creditul acordat titularului cartelei, cifrat cu un algoritm simetric.

7.4.3 Securitatea logică a cartelelor în timpul folosirii

Primul nivel de protecție constă în autentificarea cartelei și a utilizatorului.

În cazul autorizării online, un canal logic securizat este setat între cartela inteligentă și sistemul gazdă prin intermediul cititorului. Înființarea acestui canal necesită autentificarea reciprocă a cartelei și a serverului de autorizare din rețea. Ștampilarea temporală a tranzacțiilor asigură nerepudierea, care necesită un ceas precis cu alimentarea cu energie asigurată în toate condițiile.

O a doua serie de măsuri include înregistrarea detaliilor tranzacției într-un fișier de audit și contorizarea încercărilor nereușite de accesare a cartelei, cu blocaje când numărul depășește un prag prestabilit.

Există și o perioadă de valabilitate a cartelelor care este limitată pentru a reduce posibilitatea de clonare sau atacuri prin reluarea mesajelor vechi.

Procedurile de autentificare cifrografică se bazează pe algoritmi de cifrare simetrică sau asimetrică.

7.4.3 Securitatea logică a cartelelor în timpul folosirii

Autentificarea cu cifrare simetrică

Avantajul acestui mod de autentificare este de a evita necesitatea unui coprocesor cifrografic și, în consecință, de a reduce costul cartelei.

Schimburile de autentificare au loc în modul următor:

1. După introducerea cartelei în slotul cititorului, cititorul de cartele generează un număr aleator și îl trimite pe cartelă.

2. Cartela calculează Codul de autentificare a mesajului (MAC) prin concatenarea unui număr aleator și a numărului de identificare al cartelei (CID). Derivarea CID depinde de specificațiile sistemului și de numărul de serie al cipului, de numărul contului, de codul secret și de data expirării. Cartela trimite MAC și CID către serverul de autentificare.

3. Utilizând CID, serverul derivă cheia de cifrare a cartelei de la cheia master. Acesta efectuează calculele inverse celor ale cartelei și compară rezultatul cu numărul primit.

4. Rezultatul comparării definește succesul sau eșecul autentificării.

7.4.3 Securitatea logică a cartelelor în timpul folosirii

Autentificarea cu cifrarea cu chei publice

Autentificarea cu cifrare asimetrică poate fi statică sau dinamică.

În autentificarea statică, datele schimbate sunt fixate o dată pentru totdeauna în timpul fabricării cartelei.

Schimburile la autentificarea dinamică variază cu fiecare tranzacție ceea ce oprește fraudatorii să redea codurile de verificare anterioare pentru autentificare. Autentificarea dinamică se numește offline deoarece implică terminalul și nu centrul de autorizare.

Autentificarea statică. Semnătura cartelei este calculată cu algoritmul de chei publice RSA și este stocată în cip. Aceasta este folosită pentru a autentifica cartela pentru fiecare plată. Această metodă este vulnerabilă la atacurile de replicare (*replay*), deoarece cifrograma constantă poate fi refolosită pentru a efectua plăți frauduloase. De asemenea, poate fi copiată în cartele false, permițând clonarea.

7.4.3 Securitatea logică a cartelelor în timpul folosirii

Autentificarea cu cifrarea cu chei publice

Metodă de autentificare dinamică descrisă necesită, de obicei, un coprocesor cifrografic pentru a descărca microprocesorul principal și a accelera calculele. Aceasta ar crește costul cartelelor inteligente. Pentru a depăși această constrângere, a fost propusă autentificarea probabilistică folosind tehnici „de cunoaștere zero”. În cadrul acestei scheme, autentificarea este interactivă și constă în trei schimburi: un angajament al pretendentului, o solicitare a verificatorului și un răspuns al verificatorului. Astfel, crește numărul de schimburi (de la 2 la 3) și este prezentă o eroare reziduală. Cu toate acestea, verificatorul poate reduce probabilitatea erorii solicitând iterații suplimentare.

Punctul de plecare este următoarea ecuație:

$$G \times Q^e \equiv 1 \bmod n,$$

unde:

***G* este cheia publică calculată de cartelă folosind CID;**

***Q* este semnătura CID calculată de o autoritate bancară cu algortmul RSA și cheia sa privată;**

(*e*, *n*) constituie cheia publică a verificatorului, iar *Q* este cheia publică corespondentă.

7.4.3 Securitatea logică a cartelelor în timpul folosirii

Autentificarea cu cifrarea cu chei publice

Schimburile au loc după cum urmează:

1. Cartela trimite verificatorului (serverului sau cititorului) valoarea *t*:

$$t = R^e \bmod n$$

unde *R* este un număr aleator între 1 și (*n* - 1).

2. Verificatorul răspunde cu o solicitare aleatoare *V* între 0 și (*e* - 1).

3. Cartela răspunde cu *T* calculat după cum urmează:

$$T = R\,Q^V \bmod n.$$

4. Verificatorul poate verifica acum autenticitatea cartelei prin reconstituirea angajamentului după cum urmează:

$$G^V\,T^e \bmod n = G^V\,R^e\,(Q^V)^e \bmod n = (GQ^e)^V\,R^e \bmod n = R^e \bmod n.$$

Schimburile sunt ilustrate în Figura. Trebuie remarcat faptul că orice pretendent legitim poate termina fiecare iterație cu succes fără a dezvălui codul secret *Q*. Tot ceea ce poate obține verificatorul este că pretendentul are acreditările necesare fără a putea să-și reconstituie valorile lor. Se poate arăta că un impostor are doar o șansă din (*e* - 1) să ghicească răspunsul. În cazul $e = 2^{16} + 1$, există o posibilitate de înșelăciune în 65536 de tentative, ceea ce pare să fie suficient în aplicațiile bancare.

7.5 Cartele EMV

7.5.1 Aspecte generale

Specificațiile EMV au început cu colaborarea EuroPay, MasterCard și Visa. Din 1999, activitatea este supravegheată de EMVCo, o organizație înregistrată în statul New York și care cuprinde șase organizații membre: American Express, Discover, JCB, MasterCard, UnionPay și Visa.

Primele specificații EMV publicate au fost EMV 2.0 (1995). Au urmat: EMV 3.0 (1996), EMV 3.1.1 (1998), EMV 4.0 (2000), EMV 4.3 (2011).

Primele implementări bazate pe EMV au avut loc în 2002.

Respectarea specificațiilor EMV este verificată pentru terminale, programe și cartele. Nivelul 1 testează conformitatea terminalelor cu caracteristicile electromecanice, interfața logică și cerințele protocolului de transmisie. Testele de Nivel 2 se referă la respectarea cerințelor aplicației de debitare/creditare a i-programelor.

Conformitatea cartelei este verificată la nivel mecanic și funcțional, precum și pentru capacitatea de stocare sigură a cipului și securitatea minimă proiectată pentru a rezista atacurilor cunoscute. Procesul definitiv de aprobare se referă la plățile mobile fără contacte și la aplicațiile mobile.

7.5 Cartele EMV

În Europa, MasterCard și Visa au finalizat tranziția de la cartelele cu bandă magnetică la cartelele inteligente EMV în ianuarie 2005. Băncile care au făcut tranziția după această dată, sunt considerate răspunzătoare pentru fraudele înregistrate la plățile efectuate cu cartelele pe care le-au emis. Băncile și-au modernizat bancomatele pentru a accepta cartele cu cip EMV. Această migrație a avut loc mai repede în Anglia decât în Franța.

EMV este un protocol complex cu multe opțiuni și mai multe revizuiri (1996, 2000, 2008, 2011, etc.), documentate mai ales în limbaj natural.

Este disponibil un model formal pentru cartelă și terminal, precum și o implementare a standardului EMV de tip sursă-deschisă a standardului EMV la adresa http://sourceforge.net/projects/openemv.

7.5 Cartele EMV

7.5.2 Cifrografia EMV

EMV utilizează doi algoritmi de cifrare simetrică: Triple DES (TDES) cu MAC standardizat în standardul ISO 16609 și AES cu o lungime a cheii de 128 biți, 192 biți sau 256 biți. Ambele cifruri sunt specificate în ISO/IEC 18033-3. Valorile pentru exponentul cheii publice sunt 3 și (2^{16} + 1), despre care se știe că accelerează cifrarea. Modulele cheilor publice ale autorității de certificare, a emitentului, a cartelei și de cifrare a PIN-ului nu trebuie să depășească 248 octeți. Hashing-ul se face cu algoritmul SHA-1 standardizat în ISO/IEC 10118-3.

Formatul certificatelor pentru chei publice EMV este definit în secțiunile 5 și 6 din Cartea 2 a Specificației EMV. Ele sunt mai compacte decât certificatele X.509 și sunt create folosind algoritmul de i-semnătură ISO/IEC 9796-2.

Securitatea unei tranzacții EMV se bazează pe cipul cartelei. Dacă tranzacția este finalizată online, emitentul autentifică cartela. Dacă este finalizată offline, terminalul autentifică cartela. EMV este utilizat cu interfețe cu contacte și cele fără contacte, însă abordarea de securitate este diferită.

7.5 Cartele EMV

7.5.2 Cifrografia EMV

Pentru compatibilitatea înapoi cu terminalele moștenite care pot citi doar benzi magnetice, specificațiile EMV permit ca autentificarea deținătorului cartelei să fie înlocuită folosind datele de pe banda magnetică sau utilizând semnătura titularului cartelei. Pentru a face acest lucru, este permisă ocolirea intrării PIN la terminal, la discreția comerciantului sau a deținătorului cartelei. Însă aceasta sporește vulnerabilitatea schemei EMV la fraudă.

Autentificarea offline utilizează una din cele trei moduri de autentificare a datelor:

1. Autentificarea datelor statice offline (SDA).

2. Autentificarea dinamică a datelor (DDA). Acesta este modul în care, în 2011, Visa și MasterCard au mandatat toate cartelele EMV de marcă.

3. Autentificarea datelor dinamice combinate (CDA) cu generarea de cifrograme de aplicație. Acest mod a fost adăugat în versiunea 4.0 atât pentru tranzacțiile offline, cât și pentru cele online.

În timpul unei tranzacții date, poate fi folosită doar o metodă de autentificare.

7.5.2 Cifrografia EMV

Autentificarea datelor statice

Terminalul autentifică cartela utilizând o schemă de i-semnătură bazată pe cifrarea cheilor publice pentru a confirma integritatea datelor stocate în timpul personalizării cartelei. Pentru fiecare aplicație, cartela conține semnătura numerică a datelor critice calculate cu cheia privată a emitentului, precum și certificatul emitentului emis de autoritatea de certificare. Terminalul stochează cheia publică a emitentului și autentifică datele statice semnate cu acea cheie publică. Un terminal trebuie să poată recunoaște cheile publice ale celor șase organizații membre EMVCo pe fiecare aplicație înregistrată.

Deoarece cartela nu posedă capacități cifrografice, PIN-ul introdus de utilizator este trimis pe cartelă pentru verificare în mod clar, adică necifrat. Cartela înregistrează succesul sau eșecul și scade numărul contorului de retur PIN și se blochează dacă devine negativ.

SDA permite detectarea alternanțelor neautorizate la datele critice rămase pe cartelă. Principalul avantaj este că cartelele nu trebuie să suporte procesarea cifrografică, adică devin mai puțin costisitoare.

7.5.2 Cifrografia EMV

Autentificarea datelor statice

Există două probleme majore legate de autentificarea datelor statice:

1. Este vulnerabilă la atacurile de replicare (replay) în tranzacțiile offline.

2. Cifrograma lor poate fi copiată pe o cartelă contrafăcută (clonarea cartelei).

Atacul cu cartela clonată funcționează după cum urmează. O cartelă falsă introdusă într-un terminal de vânzare offline va păcăli terminalul pentru a autoriza tranzacția, deoarece datele critice copiate sunt autentice, inclusiv certificarea emitentului de la autoritatea de certificare a mărcii și cheia privată a emitentului. Potrivit EMV, cartela conformă execută PIN-ul pentru tranzacțiile offline, deci poate fi creată o cartelă SDA furată pentru a accepta orice PIN introdus la terminal. Cu alte cuvinte, poate fi creat un "Yescard" compatibil cu specificațiile EMV. Posibile soluții sunt utilizarea autorizației online (probabil printr-o conexiune Wi-Fi a terminalului de la terminalul POS) și/sau comutarea la autentificarea dinamică a datelor. Dacă sumele implicate sunt mici, totuși, ar putea fi mai economice (adică cartele și terminale mai ieftine și conexiuni nu în timp real) pentru a acoperi doar pierderile.

7.5.2 Cifrografia EMV

Autentificarea datelor dinamice (DDA)

Datele dinamice sunt imprevizibile și dependente de tranzacție. O cartelă care acceptă DDA trebuie să aibă propria pereche de chei de semnătură și capacitatea de a genera semnături numerice. O cartelă este personalizată cu certificatul de cheie publică a emitentului, certificatul său de cheie publică și cheia privată. Terminalul (ATM sau POS) utilizează o copie stocată a cheii publice a autorității de certificare a mărcii cartelelor pentru a verifica certificatul cheii emitentului și pentru a verifica certificatul semnat de emitent pentru cheia publică a cartelei. Fiecare terminal trebuie să recunoască cheia publică a șase autorități de certificare pentru fiecare aplicație înregistrată.

Terminalul autentifică cartela introdusă printr-o solicitare și un răspuns bazat pe chei publice și apoi verifică integritatea datelor de pe acea cartelă. Pentru a evita atacurile de replicare, cartela primește de la terminal un număr aleatoriu care va fi concatenat cu datele referitoare la autentificare (ARD) indicate în specificațiile EMV. Apoi, semnează întregul set cu cheia de semnătură privată SK_{ICC}. Această semnătură este trimisă terminalului cu certificatul de la emitent și certificatul emitentului de la autoritatea de certificare.

7.5.2 Cifrografia EMV

Autentificarea datelor dinamice (DDA)

Odată ce terminalul verifică validitatea ambelor certificate și integritatea semnăturii primite, poate confirma autenticitatea cartelei.

Astfel, următorii pași sunt utilizați în autentificarea DDA:

1. Cheia publică a CA este preluată din depozitul terminalului.

2. Cheia publică CA este utilizată pentru a verifica certificatul emitentului, care conține cheia publică a emitentului.

3. Cheia publică a cartelei este extrasă din certificatul său de la emitent.

4. Semnătura este verificată utilizând cheia publică de semnătură a cartelei.

În mod evident, cartela trebuie să poată efectua anumite calcule cifrografice. Prin urmare, este posibil de utilizat cifrarea PIN-ului în timpul verificării PIN-ului. Dacă această opțiune este exercitată, odată ce titularul cartelei introduce codul PIN, terminalul cifrează codul PIN cu cheia publică de cifrare a cartelei și îl trimite pe cartelă. Cartela raportează succesul sau eșecul și scade numărul contorului de retur PIN.

Acest mod de operare permite verificarea faptului că cartela este autentică și că datele pe care le conține nu au fost modificate. Cu toate acestea, autentificarea se face numai între cartelă și terminal deoarece autorizarea emitentului nu a fost asigurată.

7.5.2 Cifrografia EMV

Autentificarea combinată a datelor dinamice (CDA)

Modul CDA a fost introdus cu EMV 4.0 (EMV2000) ca o îmbunătățire a DDA. Cu CDA, cartela semnează numeric datele la punctele cheie de tranzacție cu cheia privată SK_{ICC} pentru ca terminalul să verifice integritatea acestuia. Aceasta închide efectiv una dintre punctele slabe ale DDA și oferă dovezi valide privind tranzacția în cazul unui litigiu. În timpul autorizării online, va fi solicitată și autorizația emitentului.

CDA este asociat cu două cifrograme de autentificare (AC):

- **cifrograma cererii de autorizare (ARQC), care poate fi trimisă și emitentului online pentru a solicita autorizarea tranzacției;**
- **certificatul de tranzacție (TC) la finalizarea tranzacției.**

O a treia cifrogramă, Cifrograma de autentificare a aplicațiilor (AAC), este trimisă atunci când cartela refuză sau anulează tranzacția. Fiecare cifrogramă este alcătuită dintr-un MAC generat pe datele pe care le trimite folosind DES/3DES în modul CBC. Cu CDA, SDAD este o semnătură pe nonce generată de cartelă și alte date conexe autentificate în plus față de nonce terminale generate. ♦

7.5.3 Operarea EMV

O sesiune EMV cuprinde trei etape:

- **autentificarea cartelei de către terminal;**
- **verificarea deținătorului cartelei;**
- **autorizarea tranzacției.**

Autorizarea tranzacției poate fi efectuată la nivel de terminal (autentificare offline) sau la centrul de autorizare al emitentului (autentificare online).

În timpul autentificării cartelei de către terminal, terminalul determină mai întâi dacă cartela are un cip, de obicei prin citirea benzii magnetice. Dacă nu are cip, atunci modul de rezervă este fie de continuat cu o tranzacție cu bandă magnetică, fie de opriți tranzacția.

Cu cartele cu circuite integrate, terminalul solicită o listă a tuturor aplicațiilor acceptate de cartelă. Aplicația indică rețelele pe care cartela le poate utiliza, programele și aplicația pe care o suportă. Dacă există cel puțin o potrivire, sunt evaluate și alte restricții de procesare, de exemplu, incompatibilitățile dintre versiunile de protocol ale cartelei și ale serverului, restricțiile geografice sau limitele impuse emitentului sau achizitorului.

7.5.3 Operarea EMV

În timpul autentificării titularului cartelei, PIN-ul pe care îl introduce titularul cartelei este comparat cu cel memorat pe cartelă.

Metoda de autentificare este definită în metoda de verificare a titularului cartelei (CVM).

CVM enumeră în ordinea prioritară tipurile de metode de verificare a posesorilor de cartelă pe care emitentul cartelei le acceptă.

Metodele tipice de verificare sunt o semnătură scrisă de mână, un cod PIN fără cifrare, un cod cifrat (offline sau online), o combinație de cod PIN și o semnătură sau nicio verificare.

De asemenea, CVM definește răspunsul în cazul în care verificarea deținătorului cartelei nu reușește, cum ar fi încercarea unei metode de prioritate mai scăzută sau tranzacția eșuată. V

erificarea PIN online ar necesita contactarea emitentului, în timp ce verificarea offline este doar la nivelul terminalului.

Din confirmarea EMV 4.0, verificarea PIN offline poate fi efectuată fie cu schimburi de text simplu, fie cu schimburi cifrate.

7.5.3 Operarea EMV

De menționat:

1. Dacă CVM nu face parte din datele semnate, acesta poate fi modificat. Un intrus, care a furat o cartelă, dar nu cunoaște codul PIN, poate face ca terminalul să se întoarcă înapoi în banda magnetică. Cu datele deținătorului cartelei din banda magnetică și după înregistrarea codului PIN, se poate crea o cartelă contrafăcută.

2. Verificarea codului PIN nu este autentificată.

Autorizația de tranzacție se referă la diverse tehnici de gestionare a riscurilor. În funcție de nivelul de risc, anumite tranzacții pot fi autorizate offline, adică prin intermediul terminalului sau online, de către emitentul însuși. Odată ce tranzacția este finalizată, cipul execută comenzi pe care emitentul le-a trimis pentru a-și actualiza datele.

7.5.4 Limitările EMV

EMV este protocolul principal pentru plățile cu cartele inteligente. Specificațiile au fost elaborate pentru POS, unde terminalul EMV este sub controlul comerciantului și, indirect, al cumpărătorului. Tranzacția este față-în-față, iar terminalul și banca comunică printr-un canal securizat. Implicații:

- **deoarece achiziția se face față-în-față și bunurile sunt livrate imediat cumpărătorului, protocolul nu se referă la autentificarea comerciantului;**
- **SDA nu protejează de clonarea cartelei;**
- **în situațiile față-în-față, introducerea fizică a cartelei în terminal poate fi verificată vizual. Astfel, odată ce autentifică cartela, terminalul nu are nevoie să verifice calculele efectuate de cartelă. În consecință, protocolul nu leagă diferite părți ale tranzacției pentru a verifica dacă aceeași cartelă este utilizată în întregime. CDA evită această problemă care poate apărea în special în cazul terminalelor nesupravegheate;**
- **nu există nici o prevedere pentru ca cartela să autentifice terminalul, iar terminalul nu autorizează în mod explicit sau nu semnează nici o parte a tranzacției. CDA evită parțial această problemă;**
- **deoarece terminalul și emitentul au încredere reciprocă, terminalul nu verifică datele pe care le primește de la emitent, iar emitentul are încredere în terminal pentru a transmite mesajele pe cartelă.**

7.5.4 Limitările EMV

Specificațiile EMV nu sunt adecvate atunci când ipotezele menționate anterior nu sunt îndeplinite, de exemplu, ca în cazul tranzacțiilor la distanță pe rețele nesigure, cum ar fi Internetul sau o rețea mobilă. Pentru a rezolva acest decalaj, în 2014 a fost propusă jetonizarea EMV.

7.5.5 Jetonizarea EMV

Jetoanele de plată sunt jetoane specifice stocate pe cartele cu cipuri EMV sau dispozitive NFC pentru a asigura tranzacții EMV prin Internet, pentru plăți mobile și, în general, pentru toate tranzacțiile fără cartelă. Acestea sunt utilizate ca parte a lanțului de plată și, atunci când sunt transmise într-o tranzacție către sistemul de plăți, ar cauza efectuarea unei plăți. Cu toate acestea, jetoanele sunt limitate la domenii specifice, cum ar fi un comerciant specific sau un anumit operator de portofele numerice, adică nu sunt utilizate ca instrumente de plată generale.

Ca atare, se adresează comercianților i-comerțului și operatorilor de portofele numerice.

7.5.5 Jetonizarea EMV

Jetoanele EMV înlocuiesc numerele PAN, adică numerele cartelelor de credit sau de debit, în cadrul întregii procesări a tranzacțiilor de plată relevante.

Acestea pot fi cartografiate cu siguranță înapoi la numărul contului inițial de cartelă doar de către furnizorul de jeton de plată și entități autorizate.

O posibilitate suplimentară este capacitatea de deconectare a jetonului de la numărul inițial al contului de cartelă în cazul în care acesta nu mai este necesar sau dacă un dispozitiv mobil sau o cartelă a fost pierdută sau furată.

Jetonul de plată are aceleași caracteristici ale unei valori PAN valabile, adică este o valoare numerică de la 13 până la 19 cifre care satisface toate regulile de valabilitate și verificările pe care un PAN trebuie să le îndeplinească, inclusiv codul de verificare numit "cheia lui Luhn".

7.5.5 Jetonizarea EMV

Cu toate acestea, unele reguli adiționale se aplică pentru securitate suplimentară:

1. Jetonul de plată trebuie să corespundă unui PAN valabil.

2. Jetonul ar trebui să aibă o dată de expirare.

3. Numărul unui jeton de plată trebuie să fie diferit pentru numărul oricărei valori PAN valabile.

4. Atunci când se solicită un jeton, trebuie efectuate anumite verificări de identificare și validare. Pe baza acestor verificări, se stabilește un nivel de asigurare a jetonului pentru a indica nivelul de încredere că PAN este într-adevăr cel al titularului cartelei.

5. Jetonul de plată poate fi limitat la un anumit canal, de exemplu, numai pentru NFC sau pentru un comerciant dat sau un portofel mobil sau o combinație a oricăror dintre acestea.

6. Atunci când se solicită un jeton, solicitantul trebuie să indice unde va fi stocat spațiul de depozitare.

7. Un set de parametri este stabilit în timpul emiterii jetonului pentru a impune utilizarea corectă a jetonului de plată în tranzacțiile de plată.

7.5.5 Jetonizarea EMV

Se introduc două noi roluri intermediare, solicitantul serviciului jeton și furnizorul de servicii jeton, care afișează fluxul în timpul solicitării și emiterea unui jeton de plată. Cererea poate veni de la un comerciant online, un terminal POS, un portofel numeric dintr-un smartphone. Alți potențiali solicitanți de jetoane includ emitenții de cartele, producătorii de cipuri cartele, porți de plată în numele comercianților, cumpărătorii ș.a. De exemplu, un comerciant online care are date de pe cartela de plată poate încerca să evite responsabilitatea de a proteja datele de pe cartelă înlocuind PAN cu jetoanele de plată. În orice caz, solicitantul jeton va trebui să se înregistreze la un furnizor de servicii jeton. Conform specificațiilor actuale, fiecare furnizor de servicii jeton demonstrează procesele sale de proprietate pentru colectarea acreditărilor de identitate, revizuirea și aprobarea solicitării jetonului de plată. În cazul în care verifică și aprobă solicitarea, furnizorii de servicii cu jeton stochează jetoanele de plată emise și un depozit securizat împreună cu alți parametri relevanți, cum ar fi data de expirare, locația, restricțiile de domeniu, precum și planurile corespunzătoare.

7.5.5 Jetonizarea EMV

În timpul unei tranzacții, furnizorul de servicii jeton joacă rolul emitentului într-o tranzacție EMV de la un terminal bancar, adică aprobă tranzacția în numele emitentului folosind jetonul în loc de PAN. Acesta apoi cartografiază jetonul la PAN și transmite informațiile emitentului pentru a transfera fondurile către cumpărător. În cazul în care furnizorul de servicii jeton nu este emitentul, vizualizarea capăt-la-capăt pe care a obținut-o EMV este pierdută.

Specificația privind jetonizarea plății introduce elemente de date obligatorii și opționale în schimburile de protocol pentru a stabili simbolurile de plată - *Token Request* și *Response to Token Request* - și pentru a actualiza nivelul de asigurare atribuit unui jeton de plată după emitere: *Token Assurance Level Update Request*, și *Response to Token Assurance Level Update Request*. Schimbarea jetonului de plată pentru a obține PAN original și data de expirare a PAN se numește de-jetonizare și poate fi efectuată fără verificare. Cu verificarea, procesul implică verificarea valabilității jetonului de plată și executarea controalelor privind restricțiile de domeniu asociate cu jetonul de plată. De-jetonizarea implică două schimburi suplimentare: *De-tokenization Query Request* și *Response to De-tokenization Query Request*. Cu verificarea, schimburile se numesc *De-tokenization with Verification Request* și Response to De-tokenization Query Request.

7.5.5 Jetonizarea EMV

Cu toate acestea, schimburile nu au fost definite la nivelul necesar pentru a asigura implementări interoperabile, iar limba utilizată în specificație este ambiguă. De exemplu, jetonizarea introduce o altă cifrogramă în plus față de Cryptograma cererii de autorizare (ARQC) care este transmisă de la terminal la emitent într-o tranzacție EMV. Conform specificației, *Token Requester* generează această nouă cifrogramă pentru a valida utilizările autorizate ale jetonului și le inserează în mesajul de tranzacție pe baza tipului tranzacției și a utilizării asociate. Cu toate acestea, localizarea unei astfel de cifrograme nu a fost standardizată. De asemenea, nu au fost definite schimburile de protocol între furnizorul de servicii jeton și emitent.

În sfârșit, o alternativă la jetonizare este pentru emitenții care pot obține același rezultat prin furnizarea unui număr secundar de cont pentru a fi utilizat pentru tranzacțiile online. ♦

7.5.6 Unele atacuri asupra EMV

Atacuri cauzate de compatibilitatea înapoi

Așa cum a fost deja menționat, poziția de rezervă este de a citi datele necesare din banda magnetică sau de a compara semnătura utilizatorului cu semnătura de pe spatele cartelei.

În acest tip de atacuri, cititorul EMV este compromis, pentru a forța cartela să folosească banda magnetică și apoi să capteze în mod fals schimburile între terminale și cartela legitimă în timpul unei tranzacții.

Aceste schimburi sunt apoi analizate pentru a extrage codul PIN și suficiente date pentru a reconstrui o placă cu bandă magnetică care ar putea fi utilizată într-o cartelă falsă.

7.5.6 Atacuri asupra EMV

Atacuri omul-în-mijloc

O variantă a atacului omul-în-mijloc este de a utiliza un circuit electronic programabil pentru a conecta o cartelă legitimă (furată) și o cartelă falsă introdusă în terminalul POS.

Intrusul nu are nevoie să știe codul PIN al cartelei. În timpul verificării PIN, circuitul interceptează comanda VERIFY pentru a păcăli cartela, crezând că terminalul nu acceptă verificarea PIN-ului și că a optat fie pentru verificarea semnăturii, fie pentru verificarea deținătorului cartelei. Orice cod PIN poate fi introdus, dar PIN-ul fals este interceptat înainte de a ajunge la cartelă.

Terminalul primește de la dispozitivul intermediar codul 0X9000 ca o confirmare a faptului că codul PIN a fost verificat corect.

În mod similar, emitentul nu este conștient, deoarece, conform protocolului, terminalul raportează numai încercările eșuate de verificare a PIN-ului în structura de date privind rezultatele verificării terminalelor.

În consecință, prin această contrapondere, orice cod de 4 cifre va face tranzacțiile considerate normale și acceptate de rețeaua bancară.

7.5.6 Atacuri asupra EMV

Atacuri omul-în-mijloc

PIN-ul fals nu ajunge pe cartelă, astfel încât contorul de retur PIN-ului este neschimbat. După cum a fost menționat, TC (și pentru aprobarea online – ARQC) indică dacă verificarea deținătorului cartelei a fost încercată și a eșuat, dar nu și dacă verificarea a reușit sau dacă nu a fost încercată deloc. Astfel, terminalul consideră că verificarea PIN a avut succes, în timp ce cartela presupune că nu a fost încercat. Pentru tranzacțiile offline, emitentul nu va fi contactat decât după încheierea tranzacției.

Pentru a efectua un astfel de atac, de utilizat o cartelă falsă cu fire subțiri încorporate în substratul plastic pentru a contacta punctele de contact ale cartelei cu un cip de interfață pentru schimbarea nivelului de tensiune. Cipul de interfață este conectat la o placă de destinație generală programabilă pentru poarta (FPGA) care interfațează cu un laptop. Laptopul este conectat la un cititor de cartele inteligente în care este introdusă cartela autentică. Laptopul are un script Python care rulează pentru a intercepta comanda VERIFY și a răspunde terminalului cu rezultatul OK.

7.6 Atacuri asupra cartelelor inteligente

7.6.1 Considerații generale privind securitatea cartelelor inteligente

Există patru categorii principale de atacuri:

- **atacuri logice (neinvazive);**
- **atacuri fizice (distructive);**
- **atacuri care exploatează defectele cauzate de implementările necorespunzătoare;**
- **atacuri asupra canalelor dintre cartelă și cititorul de cartele.**

Aceste atacuri pot fi făcute de amatori, experți tehnici și organizații specializate în inginerie inversă.

Cartelele cu circuite integrate oferă o securitate mai înaltă decât cartelele cu bandă magnetică.

Deși atacurile asupra cartelelor inteligente sunt mai dificile, au fost înregistrate și catalogate o serie de atacuri fizice și logice asupra securității cartelelor inteligente.

7.6 Atacuri asupra cartelelor inteligente

7.6.2 Atacuri fizice (distructive)

Tehnicile distructive încep cu extragerea circuitului integrat din suportul din plastic. Mai întâi, se face o tăietură în plasticul din jurul modulului de cip, până când rășina epoxidică devine vizibilă. Această rășină este apoi tratată cu acid azotic fumător și spălată în acetonă până când suprafața siliciului este complet expusă.

Odată ce cipul este descoperit, este posibil să se probeze comportamentul diferitelor componente și să se recupereze cheile cifrografice încorporate în cartelă prin încercare și eroare.

Utilizarea sondelor laser sau a fasciculelor ionice concentrate permite explorarea stărilor microcontrolerului pentru a extrage informațiile necesare.

Cu toate acestea, costul de a efectua acest tip de atac este relativ ridicat, ceea ce pune aceste atacuri în afara domeniului amatorilor sau hackerilor tipici. ♦

7.6.3 Atacuri logice (neinvazive)

Atacurile neinvazive pot fi active sau pasive. Atacurile active modifică condițiile de mediu pentru a perturba funcționarea circuitelor integrate.

Scrierea operațiunilor în memoria EEPROM poate fi afectată prin modificarea temperaturii ambientale, prin supraîncărcarea instantanee a sursei de alimentare sau prin aplicarea unor impulsuri de ceas mai scurte.

Deoarece cheile de cifrare și programele de securitate sunt stocate în această memorie, securitatea este vulnerabilă la acest tip de atac, numit atacuri *glitch* (acțiune defectuoasă pe un interval de timp scurt), deoarece acestea pot împiedica executarea instrucțiunilor de verificare. De ex.:

- **funcționarea generării de numere aleatorii poate fi perturbată pentru a furniza un număr fix dacă tensiunea este suficient de scăzută;**
- **variațiile sursei de alimentare pot dezactiva mecanismul de securitate sau chiar pot șterge conținutul memoriei;**
- **unele procesoare securizate sunt atât de sensibile la modificările din mediul lor, încât declară multe alarme false;**
- **circuitele interne de testare ar putea fi reactivate, ceea ce le oferă potențialilor atacatori accesul la circuitele operaționale ale cartelei de la un număr limitat de puncte de probă, ceea ce reduce considerabil numărul de combinații care trebuie examinate.**

7.6.3 Atacuri logice (neinvazive)

Atacurile pasive se concentrează pe interceptarea și observarea funcționării cartelei pentru a detecta variațiile sursei de curent sau a scurgerilor de radiație.

Fiecare instrucțiune are o semnătura specifică, care permite distincția, de exemplu, a instrucțiunilor de ramificare sau a operațiilor care implică un coprocesor. La operarea fără contacte, preluarea (*avesdropping*) comunicării între cititor și cartela inteligentă sau etichetă poate fi realizată utilizând o antenă cu bucla mare de 1-2 m.

Printre metodele pasive se numără analiza puterii diferențiale (DPA), care se bazează pe principiul „consumul de energie depinde de biții implicați”.

În Internet, au fost inventate noi metode. O fraudă comună constă în producerea numerelor de cartele. Pentru a face acest lucru, este suficient de încercat abonarea la unul dintre serviciile online utilizând un număr dat; în cazul în care abonamentul este acceptat, acest lucru indică faptul că numărul este valabil. Impostorul poate cumpăra acum cu această cartelă, până când deținătorul adevărat al cartelei va descoperi furtul prin revizuirea declarației și a tranzacțiilor.♦

7.6.4 Atacuri asupra Canalului de comunicare a cititorului cipurilor

Accentul se pune pe legătura dintre circuitul integrat și cititor. Un caz special este atacul releu.

Protecția fizică a cititorului este esențială pentru a preveni manipularea sau înlocuirea acestuia cu o unitate dozată.

O altă posibilă sursă de fraudă sunt datele colectate de pe banda magnetică a unei cartele valide printr-un terminal modificat special. Codul PIN corespunzător poate fi furat prin urmărirea utilizatorului în timpul introducerii codului sau cu o cameră ascunsă.

Unele programe periculoase pot fi proiectate pentru a ataca sistemele POS și a colecta datele de pe cartelă stocate în memoria terminalelor POS. Chiar și atunci când sistemele POS nu accesează Internetul, ele sunt conectate la sistemele *back-office* ale comerciantului. Deci, dacă un atacator este capabil să pătrundă în rețeaua corporativă, codul rău intenționat poate viza cititoarele și poate fi proiectat pentru a ocoli programele de detectare a virușilor.♦

7.6.5 Atacuri releu asupra cartelelor fără contacte

Sistemele fără contacte au un domeniu limitat de funcționare (ca distanță). Comunicarea de succes este atunci când cipul se află în apropierea cititorului. Astfel, presupunerea este că dispozitivele se află în imediata vecinătate atunci când stabilesc o comunicare reușită. Cu toate acestea, dacă ele sunt utilizate la distanțe extinse între cele două dispozitive fără ca acestea să cunoască acest lucru, atacatorul poate iniția acțiuni ce pot necesita o distanță mică între transponder și cititor. Cei doi participanți legitimi primesc schimburi valide reciproc și presupun că sunt apropiați.

Atacul exploatează faptul că atunci când o cartelă falsă fără contacte (numită și proxy, fantomă sau clonă) se află în domeniul de comunicare al cititorului, aceasta este alimentată prin inducție de către cititor. La stratul MAC, cititorul nu îl poate distinge de o cartelă adevărată dacă se conformează interfeței radio și efectuează procedurile de modulare și demodulare necesare. În același timp, un înlocuitor al cititorului (numit și *mole*, *leach* sau *skimmer*) comunică prin *stealth* cu cartela utilizatorului ca și cum ar fi cititorul autentic la nivel fizic, iar straturile acțiunilor *mole* și cele ale unui cititor legitim nu pot fi distinse.

7.6.5 Atacuri releu asupra cartelelor fără contacte

Combinația *mole*/*proxy* (*skimmer/clone* sau *leach/fantomă*) apoi poate trimite comenzile cititorului la cipul legitim al utilizatorului și să trimită (*relay*) răspunsurile înapoi.

Astfel, intervalul de transmisie intenționat pentru care sistemul a fost proiectat, de obicei 5-10 cm, este extins efectiv la cel puțin 40-50 cm, dacă nu mai mult.

Mai mult, *mole/skimmer/leach* interfețează cu cartela de tip secret (adică fără cunoștința proprietarului legitim și fără a atinge ținta) ca cititor pentru a accesa toate informațiile pe care un cititor autentic le-ar putea accesa.

Întârzierea introdusă de sistemul spion nu afectează funcționarea atâta timp cât sincronizarea biților este menținută în limitele intervalului de timp de anticoliziuni specificate de ISO/IEC 14443-3.

7.7 Sumar

Comparativ cu cartelele cu coduri cu bare sau cu bandă magnetică, cartelele inteligente au capacități de procesare care le permit să ia decizii complexe privind tranzacțiile de plată sau de control al accesului. Ele pot susține mai multe aplicații în paralel. În cartelele cu aplicații multiple, distribuirea resurselor între aplicații trebuie să fie strict controlată pentru a menține nivelul de securitate în funcție de fiecare aplicație. Aceasta se numește *sandboxing*.

Securitatea cartelelor inteligente acoperă întregul ciclu de viață. Măsurile de protecție acoperă datele înregistrate în cip și schimburile în care participă. Mijloacele cifrografice sunt folosite pentru a autentifica diferitele părți (cipul, cititorul, utilizatorul și centrul de autorizare) înainte ca orice schimb de date să aibă loc. Cifrografia asigură, de asemenea, confidențialitatea și integritatea tranzacției. Atacurile replay pot fi împiedicate prin includerea numerelor aleatoare, ștampilelor de timp, numerelor de secvențe ș.a. Alte măsuri de securitate logică includ canalele de comunicare ce implică cartele inteligente, cititoare de cartele și sisteme gazdă. De asemenea, este esențial de reacționat rapid odată ce se detectează o intruziune, inclusiv abortarea unei tranzacții în curs de desfășurare.

7.7 Sumar

Cartelele fără contacte sunt expuse unui tip de atac suplimentar, atacul releu, care vizează stratul MAC. Protecția împotriva acestor atacuri poate necesita includerea unor tehnici de limitare a distanței în protocoale pentru a se asigura că cartela legitimă și cititorul legitim sunt în imediata apropiere unul de celălalt.

În aplicațiile bancare, majoritatea sistemelor sunt proprietare, dar migrarea către specificațiile EMV schimbă imaginea la nivelul Aplicație.

De asemenea, interfețele radio ale cartelelor fără contactr converg treptat către diferitele standarde ISO.

Totuși, interoperabilitatea completă nu a fost realizată în toate cazurile, cum este cazul i-mijloacelor de colectare a taxelor. ■