UNIVERSITATEA TITU MAIORESCU

FACULTATEA: INFORMATICĂ
DEPARTAMENT: INFORMATICĂ
Programa de studii: INFORMATICĂ
DISCIPLINA: INTELIGENȚĂ ARTIFICIALĂ

IA – *Testul de evaluare nr.* 18

Standarde Smart Card

Grupa	Numele și prenumele	Semnătură student	Notă evaluare

Data: ____/____/_____

CS-I dr.ing.

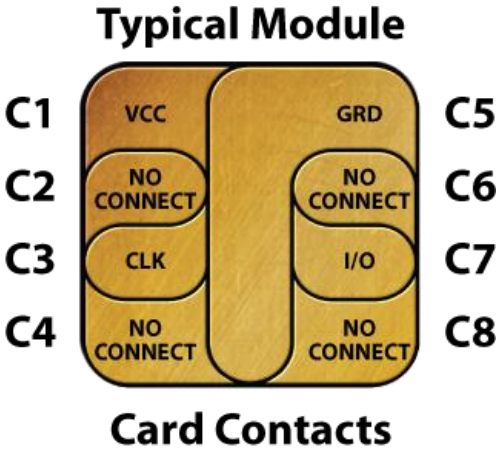
Lucian Ștefăniță GRIGORE

Conf.dr.ing.

Iustin PRIESCU

Ș.L.dr.ing.

Dan-Laurențiu GRECU



Cuprins

1. NOȚIUNI INTRODUCTIVE

Un card inteligent este un card de plastic, care în mod curent conține un cip, în care este încorporată o memorie, pe post de calculator[1] sau de microprocesor[2], al cărui rol este de a stoca și tranzacționate date. Aceste date sunt, de obicei, asociat cu o valoare, informații, fără valoare, sau toate și sunt stocate și procesate de către cipul cardului.

Datele de pe card se tranzacționează prin intermediul unui cititor, care este parte a unui sistem de calcul.

Sistemele care utilizează carduri inteligente sunt utilizate în prezent în mai multe domenii cheie: asistența medicală, sistmul bancar, divertisment, transport etc. Toate aplicațiile sunt particularizate atât ca și caracteristici dar și ca elemente de securitate suplimentare.

Potrivit Eurosmart[3], transporturile la nivel mondial care utilizează smartcard-uri au atins în 2010 10% din piață, respectiv până la 5.455 miliarde de carduri.

Piețele care au fost în mod tradițional deservit de mașini care puteau fi citit tehnologiile vechi de carduri, cum ar fi coduri de bare și bandă magnetică, sunt de convertite azi în sistemele care utilizează carduri inteligente, procedeul fiind reiterat an de an, la fiecare revizie a sistemului precedent de către emitentul de carduri.

1.1 Aplicații

Introdus pentru prima dată în Europa[4] cu aproape trei decenii în urmă, cardurile inteligente au debutat ca un instrument de stocare a numerelor de telefon pentru telefoanele mobile, de asemenea și pentru a putea preveni furtul, prin blocarea sim-ului de către operatorul de telefonie. Utilizatorii de carduri inteligente și alte carduri avansate prin implementarea de cip-uri mai performante, au considerat că pot fi utilizate și pentru alte aplicații: carduri de credit și pentru achizițiile obișnuite, concomitent cu eliminarea sistemului de evidență bazat pe suport hârtie.

În SUA[5], consumatorii de servicii de orice natură au încuraja dezvoltarea și utilizarea smartcard-urilor cu cip pentru: acces la biblioteci, cumpărarea alimentelor, achiziția biletelor de cinema cât și a popcorn suc etc. în cadrul biletului, astfel încât smartcard-urile au devenit ceva obișnuit, cotidian. Mai multe state din SUA au în curs de desfășurare pentru aplicații guvernamentale programe de implementare a smartcard-urilor cu cip. Cel mai avansat departament de stat din acest punct de vedere este Departamentul de Transporturi care utilizează sistemul Electronic Benefit Transfers[6] (EBTs). La nivel industrial pentru produse de larg consum au implementat sistemele de smartcard-uri, cum ar fi: telefoane digitale celulare GSM[7], precum și decodoare[8] TV pentru transmisiunea prin satelit.

1.2 De ce smartcard?

Tehnologia smartcard-urilor au condus la îmbunătățirea confortului și a securității oricărei tranzacții. Acestea oferă posibilitatea unei stocări de date protejate la furtul de identitate sau de falsificare a identității utilizatorului și în sistemul bancar a contului. Sisteme de smartcard-uri s-au dovedit a fi mai fiabile decât alte sisteme de carduri care pot fi citite de cititoare de card-uri, cum ar fi banda magnetică și codul de bare. Multe studii demonstrează că utilizarea de smartcard-uri este net

[1] http://www.smartcardbasics.com/smart-card-types.html#memory-cards
[2] http://www.smartcardbasics.com/smart-card-types.html#microprocessor-cards
[3] http://www.eurosmart.com/
[4] https://en.wikipedia.org/wiki/Smart_card
[5] http://web.mit.edu/ecom/Spring1997/gr12/0intro.htm
[6] https://www.ebt.acs-inc.com/
[7] http://www.gsm.org/
[8] https://en.wikipedia.org/wiki/Television_encryption

superioară oricăror alte sisteme și poate un alt aspect la fel de important îl constituie costul redus al mentenanței.

Cartele inteligente, sunt de asemenea, componente vitale ale securității sistemului de schimb de date de-a lungul aproape a oricărui tip de rețea. Ele protejează împotriva a o gamă completă de amenințări de securitate, de la depozitarea neglijentă a parolelor de utilizator la sistemul sofisticat de decriptare a datelor de către hack-eri. Costurile de gestionare privind resetarea parolei pentru o organizație sau întreprindere sunt foarte mari, astfel, smartcard-urile reprezintă o soluție eficientă în acest context. Cardurile multifuncționale (*Multifuction cards*[9]) pot fi, de asemenea, folosite pentru a administra accesul în sistemul de rețea și de a stoca valori și alte date. La nivel mondial, oamenii folosesc deja smartcard-uri pentru o mare varietate de sarcini de zi cu zi, care includ:

1.2.1 Carduri SIM și telecomunicații

Aplicația cea mai importantă a tehnologiei smartcard este în Subscriber Identity Modules (SIM[10]), necesare pentru toate sistemele de telefonie din cadrul sistemul global de comunicații mobile (GSM) standardizate. Fiecare telefon utilizează codul unic de identificare, stocat în cartela SIM, pentru a gestiona drepturile și privilegiile fiecărui abonat pe diverse rețele. Acest caz de utilizare reprezintă peste jumătate din toate carduri inteligente consumate în fiecare an. Sistemul universal Subscriber Identification Modules (USIM[11]), este de asemenea utilizat pentru a reduce decalajul de identitate a telefoanelor de tranziție între operatorii de rețele GSM, UMTS[12], și 3G[13].

1.2.2 Loialitate și valoare stocată

O altă utilizare a smartcard-urilor inteligente este de a stoca valori, în special programe de loialitate, care pista și să ofere stimulente pentru a atrage clienți. Valoarea stocată este mai convenabilă și mai sigură decât în numerar. Pentru emitenții, float[14] se realizează pe conturi și reziduurile necheltuite privind soldurile care nu sunt utilizate.

Pentru lanțurile de comercianții cu amănuntul care administrează programe de loialitate din multe companii diferite și sisteme POS, smartcardurile pot localiza central și urmări toate datele. Aplicațiile sunt numeroase, cum ar fi transportul, parcare, spălătorie, jocuri de noroc, vânzare cu amănuntul și divertisment.

1.2.3 Asigurarea datelor stocate și a activelor fizice

În plus față de securitatea informațiilor, cardurile inteligente pot asigura o mai mare securitate de servicii și echipamente de restricționare a accesului autorizat doar la utilizator(i).

Informațiile inclusiv cele de divertisment sunt livrate la domiciliu prin intermediul sateliților (în mod direct cu o antenă parabolică), prin cablu (cablu coaxial, fibră optică) la player-ul DVR sau la PC prin cablu UTP sau fibră optică. Livrarea la domiciliu a serviciilor amintite se realizează sub formă criptată/decriptată[15] accesul abonaților fiind efectuat prin intermediul smart cardurilor. Sistemele de difuzare video digitale au adoptat deja pentru cheile de protecție carduri inteligente.

Cardurile inteligente, de asemenea, pot fi utilizate ca și chei de setări ale echipamentelor de laborator sensibile, a dozatoarele pentru medicamente, instrumentelor, cardurilor de bibliotecă, echipamentelor pentru clubul de sănătate etc. În unele medii, smartcardurile pentru SD și micro SD[16] au rolul de a proteja conținutul digital așa cum este livrat pentru telefoanele mobile care deservesc sistemul de telefonie mobilă.

[9] http://www.smartcardbasics.com/smart-card-types.html
[10] http://www.cardlogix.com/products/cards/smart/scfamilies/delos.asp
[11] https://en.wikipedia.org/wiki/Subscriber_identity_module
[12] https://en.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System
[13] https://en.wikipedia.org/wiki/3G
[14] http://www.euromoney.com/Article/1015476/Hutchison-Whampoa-Mixed-signals-from-3G-float.html
[15] http://www.smartcardbasics.com/smart-card-security_2.html#cryptography
[16] https://en.wikipedia.org/wiki/Secure_Digital

1.2.4 Comerțul electronic (e-commerce)

Cardurile inteligente facilitează consumatorilor stocarea în siguranță a informațiilor și a finanțelor necesare pentru cumpărături. Avantajele pe care le oferă consumatorilor sunt:

- cardul poate conține contul personal, de credit și de cumpărare și permite accesarea de preferință a informațiilor stocate cu un click de mouse în loc de a completa formulare;
- cardurile pot gestiona și controla a cheltuielile, în mod automat și cu raportare;
- programele de loialitate de pe Internet pot fi implementate la mai mulți furnizori cu sisteme POS disparate, cartela acționând ca un depozitar central pentru puncte sau recompense;
- Micro Plăți - plata costurilor nominale fără comisioane de tranzacție asociate cu cardurile de credit, sau pentru tranzacții prea mici, cum ar fi taxele de imprimare la bancomat spre exemplu.

1.3 Emiterea de smartcarduri de către bănci

La nivel mondial, banca controlează inclusiv acțiunile[17] în societățile cooperative[18] (Visa[19], MasterCard[20], Discover[21] și American Express[22]) și au lansat milioane de carduri inteligente sub standardul EMV[23] (Europay[24], MasterCard, VISA).

Adesea se fac referiri la cardurile cu cip și PIN[25]; acestea sunt tipurile de facto de carduri pentru eliberarea de valori bancare în majoritatea țărilor, cu excepția SUA. Canada tocmai a început recent trecerea de reglementare a carduri EMV, SUA va fi singura țară din America de Nord, care nu a făcut încă adoptarea, deoarece conform datelor din SUA, fraudele bancare sau înmulțit atât în arealul cardurilor de debit dar și de credit. Cu toate acestea, cardurile inteligente s-au dovedit cele mai sigure în privința tranzacțiilor regulate, astfel încât norma EMV a devenit un standard.

Deoarece băncile sunt concurente pe piețele nou deschise, cum ar fi în domeniul brokerajului și a investițiilor, ele trebuie să realizeze o protecție crescută privind asigurarea tranzacțiilor prin carduri inteligente la un nivel crescută. Acest lucru înseamnă:

- încrederea în utilizarea cardurilor inteligente crește prin îmbunătățirea securității. Doi factori de autentificare asigură protecția datelor, precum și valoarea atunci când folosesc ca suport de trafic de date Internetul. Amenințările, cum ar fi „*Man in the Middle*[26]” și „*Trojan Horses*[27]”, sunt eliminate în momentul introducerii unui nume de utilizator și a unei parole;
- acest lucru conduce la îmbunătățirea serviciilor pentru clienți. Clienții pot folosi carduri inteligente securizate pentru tranzacții rapide, cu transfer de fonduri electronice pe internet în maxim 24 de ore;
- costurile sunt reduse: tranzacțiile care în mod normal ar necesita timp pentru un angajat al băncii și redactarea/completarea de documente pot fi gestionate electronic de către client prin intermediul smart card-ului.

[17] https://en.wikipedia.org/wiki/The_Co-operative_Bank
[18] https://www.us.hsbc.com/1/PA_1_083Q9FJ08A002FBP5S00000000/content/usshared/Personal%20Services/Home%20Loans/Mortgage/FYI/Shared/Coop%20Guide.pdf
[19] https://en.wikipedia.org/wiki/Visa_Inc.
[20] https://en.wikipedia.org/wiki/MasterCard
[21] https://www.discover.com/
[22] https://www.americanexpress.com/
[23] http://www.emvco.com/
[24] https://en.wikipedia.org/wiki/Europay_International
[25] https://en.wikipedia.org/wiki/EMV
[26] https://en.wikipedia.org/wiki/Man-in-the-middle_attack
[27] https://en.wikipedia.org/wiki/Trojan_horse_(computing)

1.3.1 Healthcare Informatics[28]

Explozia de date privind starea/îngrijirea sănătății introduce noi provocări în menținerea unei eficiențe din punct de vedere al asistenței de sănătate concomitent cu garanția de securitate a datelor aferente istoricului medical al unui pacient. Cardurile inteligente pot aborda simultan ambele provocări în siguranță, respectiv stocarea și distribuirea de informații despre un pacient, de la datele de urgență până la statutul de asigurat (beneficii ale sistemului de asigurare asumat). Multe țări au adoptat deja pentru sistemul de asigurări sociale de sănătate tehnologia cardurilor inteligente cât și pentru citirea acreditărilor pentru rețelele de sănătate și ca un mijloc care permite realizarea imediată a unei consultații și de raportare imediată „*Electronic Health Record - EHR*[29]". Printre beneficiile utilizării Beneficii smart cardurilor în cadrul asistenței medicale se numără:

- identificarea rapidă și exactă a pacienților; posibilitatea îmbunătățirii tratamentului;
- reducerea fraudelor prin identificarea furnizorului/vizitelor la pacient și a eligibilității asigurării de sănătate;
- capacitatea de a transfera date între sistemele medicale sau cu site-urile medicale;
- reducerea costurilor și a timpului pentru mentenanță.

1.3.2 Dispozitiv de control medical încorporat

De ani de zile, au fost încorporate mai multe sisteme de control pe mai multe tipuri de mașini, care să reglementează calitatea și precizia funcției lor. În sistemul de sănătate, introducerea cardurilor inteligente asigură cea mai bună și cea mai sigură metodă de livrare a informațiilor medicale privind tratamentul pentru care sunt utilizate echipamente și tehnologii, cum ar fi aparatele de dializă, analizoare de sânge și echipamente chirurgie cu laser la ochi.

1.3.3 Companiile care se ocupă de securitatea rețelelor

Microsoft Windows, Sun Microsystems (o filială a Oracle Corporation) și toate versiunile noi de Linux au construit un software pentru a implementa cardurile inteligente ca un înlocuitor pentru nume de utilizator și parolă. Microsoft a construit o platformă completă în jurul Furnizorului[30] Scard DLL[31] și Crypto Service Provider[32] (CSP). Instituțiile medicale și de profil software și-au dat seama că Public Key Infrastructure[33] (PKI) reprezintă o securitate sporită și de asemenea s-a concluzionat că angajații din sistemul medical trebuie să poarte o insignă tip card inteligent conform noului standard din domeniul sănătății. Business-to-business Intranet și rețelele virtuale private (VPN[34]) sunt îmbunătățite prin utilizarea de carduri inteligente. Utilizatorii pot fi autentificați și autorizați să aibă acces la informații specifice în funcție de privilegiile prestabilite. Aplicațiile suplimentare variază în funcție de un e-mail securizat specific comerțului electronic.

1.3.4 Accesul fizic

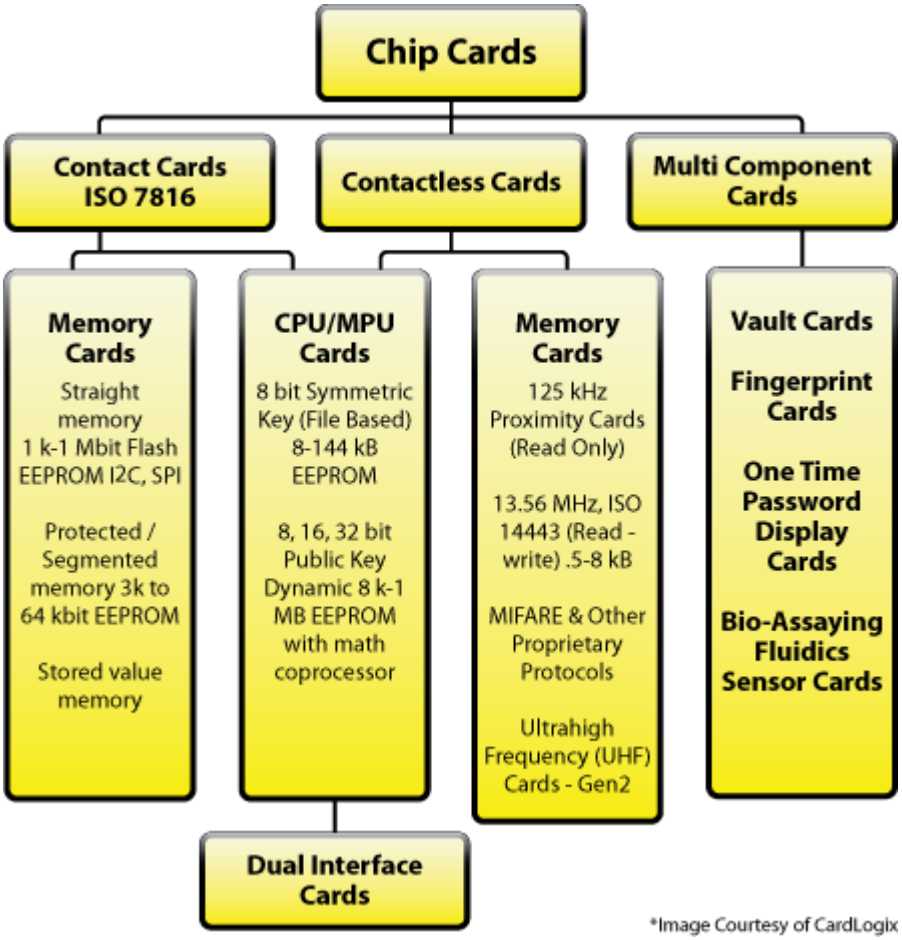
Întreprinderile și universitățile de toate tipurile au nevoie de cărți de identitate simple pentru toți angajații și studenții. Cele mai multe dintre aceste persoane sunt arondate, de asemenea, acces la: anumite date, echipamente, și departamente în funcție de statutul lor. Multifuncțional, carduri inteligente bazate pe microprocesoare[35] care includ date privind identitatea concomitent cu privilegiile de acces și poate stoca, de asemenea, o valoare pentru a fi utilizată în diverse locații, cum ar fi cafenele și magazine. Multe hoteluri au adoptat standardul ISO 7816[36] care securizează accesul personalului hotelier în camere și la facilitățile funcționale.

---

[28] http://www.cardlogix.com/products/cards/smart/scfamilies/healthcare.asp
[29] https://en.wikipedia.org/wiki/Electronic_health_record
[30] http://www.cardlogix.com/docs/whitepapers/CardLogix_WP_IssuesInSmartCardDevelopment.pdf
[31] http://www.smartcardbasics.com/
[32] https://en.wikipedia.org/wiki/Cryptographic_Service_Provider
[33] https://en.wikipedia.org/wiki/Public_key_infrastructure
[34] https://en.wikipedia.org/wiki/Virtual_private_network
[35] http://www.smartcardbasics.com/smart-card-types.html
[36] https://en.wikipedia.org/wiki/ISO/IEC_7816

Toate agențiile guvernamentale ale SUA și multe companii au încorporat cititoare contactless[37] acum un ca punct de acces la instalațiile lor. Unele companii au implementate componente biometrice pentru acces. Altele au sisteme de detectare a unui om de tip proximitate bazate pe un gatekeeper[38]. Întrucât cerințele de securitate au devenit mai mari și costul standardelor au devenit mai mici, s-a adoptat sistemul ISO 14443[39] destul de rapid. Această schimbare de piață este parțial determinată de adoptarea de către guvernul SUA a standardului Personal Identity Verification[40] (PIV). Există un ecosistem bogat de furnizori și integratori de acest standard. Există un ecosistem bogat de furnizori și integratori ai acestui standard.

Cartelele inteligente sunt definite în conformitate cu (*Contact Cards*[41]). Cum datele cardului sunt și scrise conform (*Memory Cards*[42]). În figura următoare este prezentat tipul de cip implantat în card și a capacitățile sale. Există o gamă largă de opțiuni pentru a-l alege încă din momentul proiectării sistemului respectiv[43]. Cardurile inteligente pot adăuga confort și siguranță pentru orice tranzacție de valori și de date; dar alegerile cu care se confruntă managerii de astăzi poate fi descurajatoare din punct de vedere al evaluărilor de performanță, cost și securitate, care va produce un sistem smart card care se potrivește nevoilor de astăzi și celor de mâine.



[37] https://en.wikipedia.org/wiki/Contactless_smart_card
[38] http://smartcardamerica.com/
[39] https://en.wikipedia.org/wiki/ISO/IEC_14443
[40] http://csrc.nist.gov/groups/SNS/piv/
[41] http://www.smartcardbasics.com/smart-card-types.html#contact-cards
[42] http://www.smartcardbasics.com/smart-card-types.html#memory-cards
[43] http://www.cardlogix.com/products/cards/smart/memory.asp

1.4 Construcția Cardurilor

Cea mai mare parte ta chip cardurilor sunt construite din straturi de materiale diferite, sau substraturi, ca, atunci când s-au reunit în mod corespunzător cardul prinde viață și o funcționalitate specifică. Astăzi cardurile sunt realizate în special din următoarele materiale: PVC[44], Poliester[45] sau Policarbonat[46].

Straturile cardurilor sunt tipărite și apoi laminate la rece/cald (în funcție de tehnologi) și în final sunt presate, într-o presă[47] de 300 t/forță. Următorul pas îl reprezintă decuparea capacelor albe și apoi introducerea într-o matriță pentru determinarea conturului dorit. În continuare se introduce cip-ul și se înregistrează datele pe acesta. În general există aproximativ 30 de etape pentru realizarea unui samrt card. Deși în realitate este confecționat din 12 straturi, el este livrat ca un produs compact (vezi fig. următoare).

[44] https://en.wikipedia.org/wiki/Polyvinyl_chloride
[45] https://en.wikipedia.org/wiki/Polyester
[46] https://en.wikipedia.org/wiki/Polycarbonate
[47] http://frenchoil.com/blog/lamination-press/hydraulic-vacuum-lamination-press/

1.5 Contacele smart cardului (Contact cards)

În figura următoare este prezentat cel mai uzual tip de smart card, respectiv cipul cu care vin echipate. Contactele electrice sunt amplasate pe partea exterioară a cardului pentru a se putea conecta la un cititor de card, atunci când se introduce cardul. Acest conector este legat la cipul încapsulat în card.

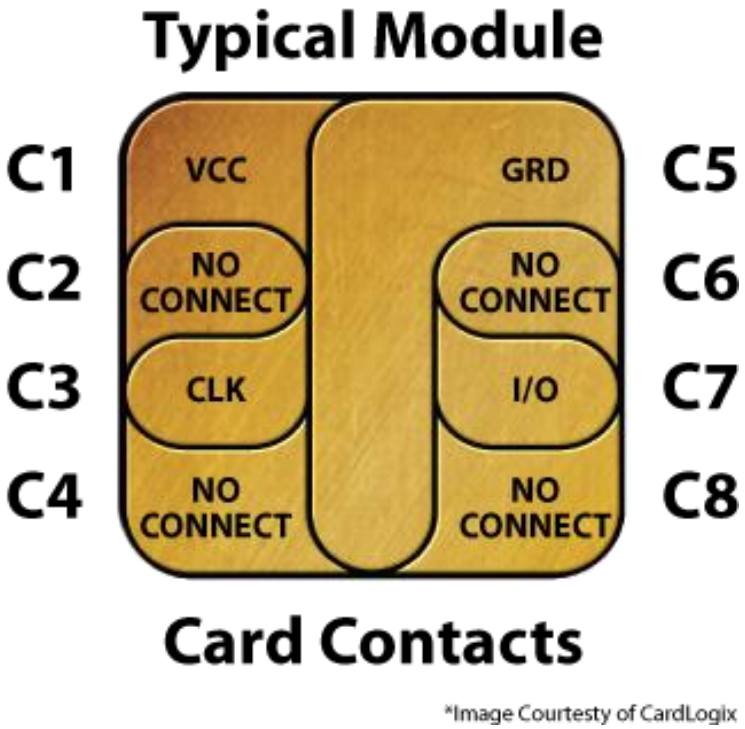


*Image Courtesty of CardLogix

Multiplicarea niveluri de putere de procesare, creșterea flexibilității și a capacității memoriei vor conduce la creșterea costurilor. În schimb cele mai rentabile smart carduri sunt cele cu o singură funcție. Alegerea tipului potrivit de smart card pentru aplicația unui utilizator presupune deținerea de informații privind nivelul necesar de securitate și evaluarea costurilor versus funcționalitate în raport cu costul de alte elemente hardware regăsite în fluxul de producție. Toate aceste variabile ar trebui să fie la sfârșitul ciclului de viață greutate împotriva preconizată a cardului. În medie, cardurile reprezintă 10÷15% din costul total cu infrastructura, emiterea, software-ul, cititorii, formarea și publicitatea care alcătuiesc 85%.

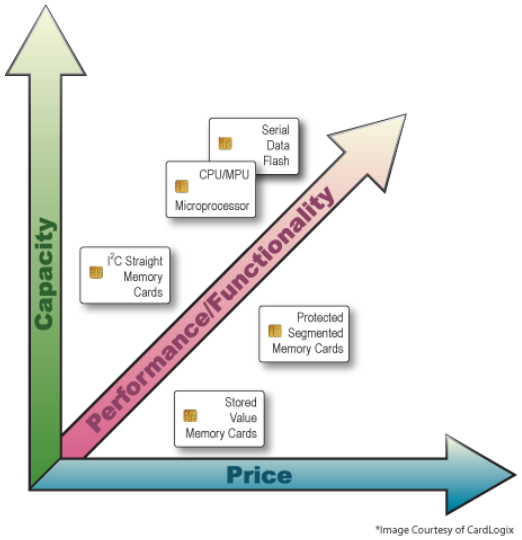


*Image Courtesy of CardLogix

2. FUNCȚIILE SMARTCARD-ului

2.1 Carduri de memorie

Cardurile de memorie nu pot gestiona fișiere și nu au nici o putere de procesare pentru gestionarea datelor. Toate cardurile de memorie comunică cititorilor prin intermediul unor protocoale sincron. Toate cardurile de memorie se pot citi și inscripționa la o adresă fixă pe card.

Există trei tipuri principale de carduri de memorie: directe (*Straight*[48]), protejate (*Protected*[49]), și cu stocare de valori (*Stored Value*[50]).

Înainte de proiectarea acestor carduri într-un sistem propus, emitentul ar trebui să verifice dacă cititorii și/sau terminalele pot susține protocoalele de comunicare ale chip-ului.

Cele mai multe carduri contactless sunt variante ale memoriilor protejate / segmente de memorie idiom card de memorie.

2.2 Carduri de memorie directe (Straight Memory Cards)

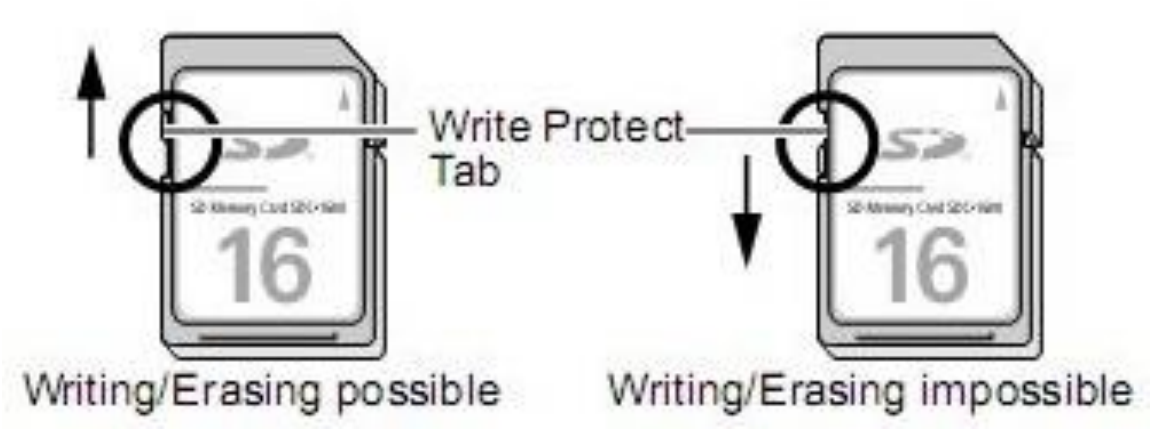
Aceste carduri sunt construite doar pentru a stoca date și nu au capacități de prelucrare a datelor. Adesea cu I2C sau semiconductori Flash serie, aceste carduri au în mod tradițional cel mai mic cost per bit de memorie. Acest lucru a permis realizarea de cantități mai mari de procesoare pentru piața GSM. Acest lucru a condus la reducerea avantajului acestor tipuri de dispozitive. Acestea ar trebui să fie considerate ca dischetele de diferite dimensiuni, fără mecanismul de blocare. Aceste carduri nu se pot identifica de către cititor, astfel încât sistemul gazdă trebuie să știe ce tip de card este introdus într-un cititor. Aceste carduri sunt ușor de reprodus și nu pot fi urmărite de către identificatori on-card.

2.3 Carduri de memorie protejate / segmentate (Protected / Segmented Memory Cards)

Aceste carduri sunt construite pentru a putea controla accesul la memoria cardului. Denumite uneori pe carduri de memorie inteligente (*Intelligent Memory cards*), aceste dispozitive pot fi setate pentru a proteja o parte sau întreaga matrice de memorie la scriere. Unele dintre aceste carduri pot fi configurate pentru a restricționa accesul atât la scris cât și la citit. Acest lucru se poate face de obicei printr-un sistem de chei sau parole. Cardurile de memorie segmentate pot fi împărțite în secțiuni

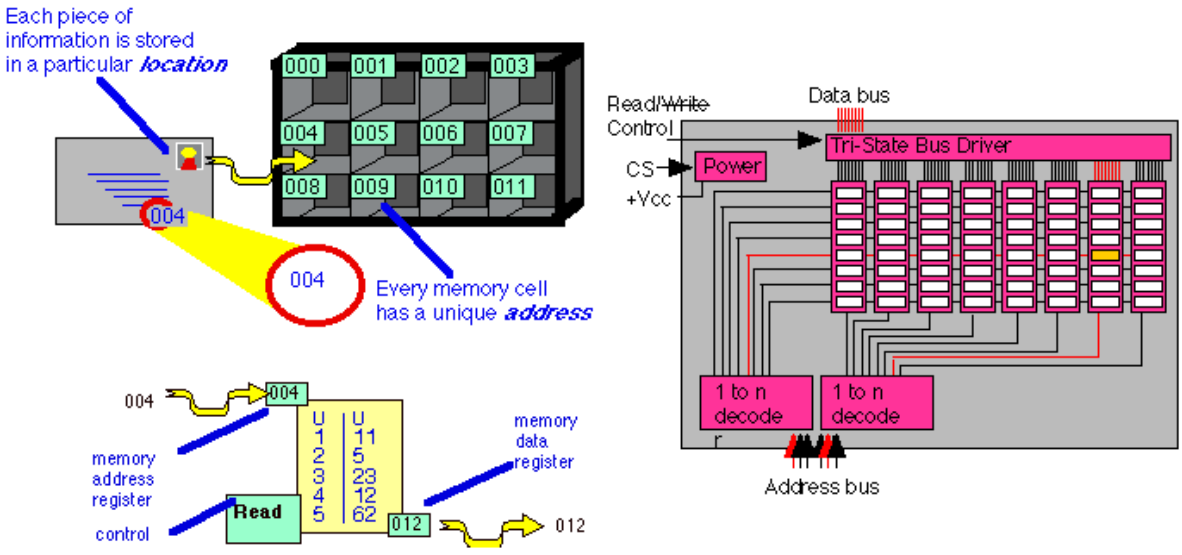
[48] http://www.engadget.com/2011/03/15/lexar-now-shipping-128gb-and-64gb-sdxc-cards-from-the-future-str/
[49] http://www.tomsguide.com/answers/id-2033680/card-write-protect-switch-set-lock-screen-unlock.html
[50] http://www.erg.abdn.ac.uk/users/gorry/eg2069/mem.html

logice multi-funcționalitate pentru planificare. Aceste carduri nu sunt ușor de replicat, dar pot fi, eventual, personificate de către hackeri. Ele de obicei pot fi urmărite de către un identificator on-card.



2.4 Carduri de memorie cu valori stocate (Stored Value Memory Cards)

Aceste carduri sunt proiectate pentru scopul specific de a stoca o valoare sau jetoane. Cardurile sunt fie de unică folosință sau reîncărcabile. Cele mai multe carduri de acest tip încorporează măsuri permanente de securitate la punctul de fabricație.



Aceste măsuri pot include chei de parolă și de logică care sunt hard-coded introduce în chip de către producător.

Matricea de memorie de pe aceste dispozitive sunt setate ca evoluție descrescătoarea sau tip contoare. Acest lucru reprezintă foarte puțin sau deloc despre memoria din stânga, pentru orice funcție. Pentru aplicații simple, cum ar fi un card de telefon, cipul are 60 sau 12 celule de memorie, câte unul pentru fiecare unitate de telefonie. O celulă de memorie este eliminată de fiecare dată când o unitate de telefon este utilizată. Odată ce sunt folosite toate unitățile de memorie, cardul devine inutil și este aruncat. Acest proces poate fi inversat în cazul cardurilor reîncărcabile.

2.5 CPU / MPU Microprocesor pentru carduri multifuncționale

Aceste carduri cu privire la on-card au capacități dinamice de procesare a datelor. Cardurile inteligente multifuncționale alocă memoriei cardului în secțiuni independente sau în fișiere atribuite

o funcție sau o aplicație specifică. În card este un cip microprocesor sau microcontroler care administrează această alocare de memorie și accesul la fișiere.

Acest tip de chip este similar cu cele găsite în interiorul calculatoarelor personale și atunci când sunt implantate într-un smart card au rolul de a administra datele în structuri de fișiere organizate, printr-un sistem de operare pentru carduri (COS[51]). Spre deosebire de alte sisteme de operare, acest software de control are acces la memoria de utilizator de pe card. Această capacitate permite diferite și multiple funcții și / sau diferite aplicații pentru card, care permite întreprinderilor să emită și să mențină o diversitate de "produse" prin intermediul cardului. Un exemplu în acest sens este un card de debit care permite, de asemenea, accesul în incinta unui campus de colegiu. Cardurile multifuncționale de care beneficiază emitenți, le permit acestora să își comercializeze produsele și serviciile lor prin state-of-the-art al tranzacțiilor și a tehnologiei de criptare. Mai exact, tehnologia permite identificarea sigură a utilizatorilor și permite actualizări de informații fără înlocuirea bazei instalate pe carduri, modificarea programelor duce la simplificarea și reducerea costurilor. Pentru utilizatorul de card multifuncțional înseamnă un confort și securitate crescut, și, în final, consolidarea selecția mai multor carduri până la consolidarea structurii dorite vor permite deservirea mai multor scopuri.

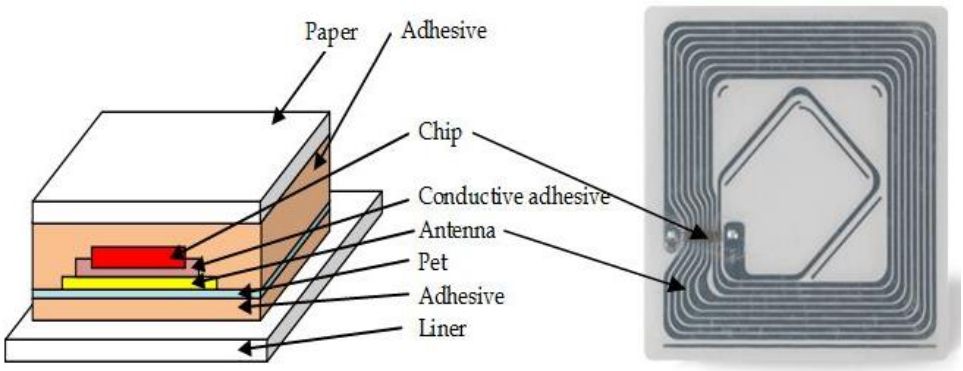
Există mai multe configurații de chips-uri în această categorie, inclusiv chip-uri care suportă sistemul de criptare Public Key Infrastructure (PKI)

Există mai multe configurații de chip-uri în această categorie, inclusiv chip-uri care acceptă cheile criptografice *Public Key Infrastructure* (PKI), care sunt echipate cu funcții matematice incluse în co-procesoare, sau în sistemul JavaCard®[52] cu blocuri hardware ca mașini virtuale. Ca o regulă empirică - mai multe funcții, conduc la o creștere a costurilor.

2.6 Carduri fără contact

Acestea sunt carduri inteligente care folosesc o frecvență radio (RFID[53]) pentru comunicarea între card și cititor fără să fie necesară inserția fizică a cardului în cititor. În schimb, cardul este trecut de-a lungul exteriorului cititorului și citit. Tipurile de carduri includ noțiunea de proximitate, astfel spus este vorba de tehnologie read-only pentru construirea porților de acces. Aceste carduri funcționează cu o memorie foarte limitată și folosesc frecvența de comunicație la 125 MHz. Un alt tip de card este Gen 2 UHF[54] care operează între frecvențele 860 ÷ 960 MHz.

Cardurile fără contact au fost utilizate pentru prima dată în aplicații de transport pentru decrementarea rapidă și reîncărcarea cu valori tarifare diferite și mai ales că securitatea informațiilor nu era o problemă prea mare, datorită valorile asociate destul de mici. Acestea comunică în frecvența de 13.56 MHz și sunt conforme cu standardul ISO 14443.



[51] http://www.cardwerk.com/smartcards/smartcard_operatingsystems.aspx
[52] https://en.wikipedia.org/wiki/Java_Card
[53] https://en.wikipedia.org/wiki/Radio-frequency_identification
[54] http://skyrfid.com/RFID_Gen_2_What_is_it.php

Aceste carduri sunt adesea tipuri de memorie protejate. De asemenea, ele sunt preferate datorită valorii stocate, deoarece pot efectua tranzacții fără scăderea veniturilor de procesare a tranzacțiilor (de exemplu, Visa și MasterCard), spre deosebire de cardurile inteligente tradiționale.

În ISO 14443 sunt specificate 3 tipuri de chip-uri utilizate de către diverșii emitenți:

- A = NXP-(Philips);
- B = Everybody else;
- C = Sony only chips.

Dezavantajele cardurilor fără contact față de carduri cu microprocesor, se datorează limitelor funcțiilor criptografice a capacității memoriei, și a distanței de comunicație necesar pentru funcționare între card și cititor, care este limitată.

2.6.1 Cardurile multi-mod (Multi-mode Communication Cards)

Aceste carduri au mai multe metode de comunicare, descrise în ISO7816, ISO14443 și UHF Gen 2. Cum se poate determina dacă cardul este un hibrid sau un card cu interfață dual. Standardele includ, de asemenea, cardurile care au bandă magnetică și/sau coduri de bare.

2.6.2 Cardurile hibride (Hybrid Cards)

Cardurile hibride au mai multe chip-uri. Acestea sunt de obicei atașate separat fiecărei interfețe, cum ar fi un cip MIFARE și o antenă cu contact 7816[55].

2.6.3 Carduri cu Interfață dublă (Dual Interface Card)

Aceste carduri au un singur cip de control pentru interfețele de comunicare. Cipul poate fi atașat la antena încorporată printr-o conexiune puternică, prin metoda inductivă sau cu ajutorul unui mecanism de denivelare flexibil.

2.6.4 Carduri multi-component (Multi-component Cards)

Aceste tipuri de carduri reprezintă o soluție specifică de piață, respectiv ieftină. De exemplu, există carduri în cazul în care senzorul de amprentare digitală este inclus pe card. Sau o companie a construit o carte care generează o parola one-time și afișează datele pentru a fi utilizate cu o aplicație on-line banking. Cardurile Vault au banda magnetică reinscripționabilă. Fiecare dintre aceste tehnologii sunt specifice unui anumit furnizor și este de obicei patentat.

2.7 Smart Carduri cu factori de formă (Smart Card Form Factors)

Forma de așteptat pentru carduri este adesea menționată în CR80[56]. Cardurile bancare și de identitate sunt reglementate de specificațiile ISO 7810. Dar această formă nu este singurul factor de formă utilizat pentru carduri. În întreaga lume sunt utilizate carduri cu decupaje particularizate cu module și/sau antene. Cele mai frecvente forme sunt SIM. Cardurile SD si microSD pot fi acum

[55] http://www.smartcardalliance.org/smart-cards-faq/
[56] http://www.alphacard.com/standard-blank-pvc-cards-cr80-30mil

implementate pe cipurile de pe smart card. Token-uri USB flash drive sunt de asemenea disponibile folosind aceeași tehnologie cu factori de formă diferiți.

2.7.1 Circuite integrate și sisteme de operare pentru carduri

Cele două tipuri principale de sisteme de operare pentru cardurile inteligente sunt:

1. Structură de fișiere fixe;
2. Sistem de aplicare dinamic.

Ca și în cazul tuturor tipurilor de carduri inteligente, alegerea unui sistem de operare de card depinde de aplicația care este destinată cardului. Cealaltă diferență constă în definirea capacitățile de criptare ale sistemului de operare și cipul. Tipurile de criptare sunt simetrice și asimetrice cheie publică (Public Key).

Selecția cipurilor pentru aceste funcții este vastă și susținută de mulți producători de semiconductori. Diferențele dintre cipurile de pe smart card și cele de pe microcontrolere este dată de calitatea siliciului utilizat. Aparatul în sine este proiectat pentru a stoca în siguranță datele și să reziste la câmpurile electromagnetice și la procesul de hacking. Aceste caracteristici suplimentare de securitate includ o listă lungă de mecanisme, cum ar fi, puncte de test, măști speciale de metal de protecție și machete neregulate ale structurilor porților de siliciu. Lista furnizor de semiconductori din siliciu de calitate de mai jos este valabilă pentru anul 2010:

- Atmel;
- EM Systems;
- Infineon;
- Microchip;
- NXP;
- Renesas Electronics;
- Samsung;
- Sharp;
- Sony;
- ST Microelectronics.

Multe dintre caracteristicile pe care utilizatorii se așteaptă să le vadă la smartcard-uri, sunt algoritmi de criptare specifici, să fie încorporați în hardware și software cât și bibliotecile arhitecturilor de cip. Acest lucru poate conduce de multe ori la faptul că un producător de carduri nu introduce ultimele inovații de designul și de asemenea ca sistemele de operare ale cardurilor să nu poată fi portate decât la un anumit dispozitiv. Instrumentele și middleware care sprijină sistemele de operare de carduri sunt la fel de importante ca și chip-ul în sine.

În continuare se prezintă secțiunea de securitate cu privire la PKI:

- Fixed File Structure Card Operating System

Acest tip tratează cardul ca un dispozitiv securizat de calcul și de stocare. Fișierele și permisiunile sunt setate în prealabil de către emitent. Acești parametri specifici sunt ideal și economici pentru un tip fix de structura și de funcții ale cardurilor care nu se vor schimba în viitorul apropiat. Pe aceste carduri se pot salva valori mari și din domeniul sănătății, aplicațiile memorate fiind sigure. Un exemplu de asemenea cardul de acces al angajaților. Contrar unor articole părtinitoare, aceste carduri pot fi folosite foarte eficient și cu o componentă biometrică stocată și care poate fi citită. La nivel global, aceste tipuri de carduri cu microprocesor sunt cele mai comune.

- Dynamic Application Card Operating System

Acest tip de sistem de operare, care include Java Card® și varietățile de carduri MULTOS, permite dezvoltatorilor să construiască, sisteme de testare, și să implementeze diferite sisteme de siguranță. Deoarece sistemele de operare și aplicațiile de carduri sunt separate, actualizările pot fi făcute independent. Un card de exemplu este un card SIM pentru GSM mobil în cazul în care actualizările și securitatea sunt descărcate pe telefon și modificate în mod dinamic. Acest tip de implementare a cardurilor presupune că aplicațiile din domeniul se vor schimba într-un interval de timp foarte scurt, necesitând astfel nevoia de extindere dinamică a cardului ca o platformă de calcul. Costurile pentru a schimba aplicațiile din domeniu sunt destul de mari, din cauza cerințelor de securitate Eco sistemice

pentru schimbul de chei odată cu fiecare acreditare. Aceasta este o variabilă care ar trebui să fie examinată cu atenție în faza de proiectare a sistemului de operare al cardului. Standardele pentru cardurile inteligente guvernează proprietățile fizice, caracteristicile de comunicare, și identificatorii de aplicație ai cipurilor și a datelor încorporate. Aproape toate standardele se referă la ISO 7816-1, 2 și 3 ca o referință de bază.

3. ORGANIZAȚIA INTERNAȚIONALĂ de STANDARDIZARE - ISO (International Organization for Standardization)

ISO facilitează crearea de standarde voluntare printr-un proces care este deschis tuturor părților. ISO 7816 este standardul internațional pentru carduri cu circuit integrat (de obicei cunoscut sub numele de carduri inteligente) care utilizează contactele electrice de pe card, precum și carduri care comunică cu cititorii și terminale fără contact, și cu frecvență radio (RF / Contactless) tehnologie.

Oricine este interesat în obținerea unei înțelegere tehnice despre cardurile inteligente trebuie să se familiarizeze cu ceea ce ISO 7816 și 14443 nu acoperă, precum și ceea ce nu face. Copii ale acestor standarde pot fi achiziționate prin intermediul American National Standards Institute (ANSI[57]).

Copii ale standardelor ISO[58] sunt de vânzare pe ISO website.

Proprietățile specifice aplicației sunt în curs de dezbatere cu multe organizații mari și grupurile care propun standardele lor. Interoperabilitate este un sistem deschis care ar trebui să se aplice la mai multe niveluri, pentru:

a) cardul în sine;
b) terminalele de acces a cardului (cititori);
c) rețele;
d) sistemele proprii de emitenți de carduri.

Interoperabilitate ca sistem deschis se poate atinge doar prin conformitatea cu standardele internaționale.

Sponsorii acestui site sau angajat să respecte standardele de securitate și ISO ITSEC, precum și inițiativele industriei, cum ar fi EMV, MULTOS, Platforma Global, Open Card Framework și specificațiile PC / SC.

Aceste organizații sunt active în procesul de standardizare al smartcardurilor. Următoarele standarde și organizații care sunt cele mai implicate în industria smart card:

- ISO / IEC este unul dintre organismele de standardizare la nivel mondial pentru tehnologi, inclusiv carduri de plastic;
- standardele primare pentru carduri inteligente sunt: ISO / IEC 7816, ISO / IEC 14443, ISO / IEC 15693 și ISO / IEC 7501.

3.1 ISO/IEC 7816

ISO / IEC 7816 este un standard internațional multi-part rupt în paisprezece părți.

ISO / IEC 7816 părțile 1, 2 și 3 se referă numai la cardurile de contact inteligente și definesc diferitele aspecte ale cardului și interfețele sale, inclusiv dimensiunile fizice ale cardului, interfața electrică și protocoalele de comunicare.

ISO / IEC 7816 Piese 4, 5, 6, 8, 9, 11, 13 și 15 sunt relevante pentru toate tipurile de carduri inteligente (de contact, precum și fără contact). Ele definesc structura logică de card (fișiere și elemente de date), diverse comenzi utilizate de interfața de programare a aplicațiilor pentru utilizarea de bază, managementul de aplicare, verificarea biometrică, servicii criptografice și aplicații numerice.

ISO / IEC 7816 Partea 10 este folosit de carduri de memorie pentru aplicații cum ar fi cartele telefonice pre-plătite sau distribuitoare automate.

ISO / IEC 7816 Partea 7 definește o abordare sigură bază de date relațională pentru carduri inteligente bazate pe interfețele SQL (SCQL).

[57] http://www.ansi.org/
[58] http://www.iso.org/iso/home.html

3.2 ISO/IEC 14443

ISO / IEC 14443 este un standard internațional care definește interfețele și protocoalele pentru un card inteligent fără contact "de aproape", inclusiv interfața de frecvență radio (RF), interfața electrică, precum și de comunicarea și anti-coliziune.

ISO / IEC 14443 Carduri conforme operează la 13,56 MHz și au o gamă operațională de până la 10 cm (3,94 inchi). ISO / IEC 14443 este un standard primar smart card fără contact utilizat pentru cererile de tranzit, și de control al accesului financiar. Acesta este, de asemenea, utilizat în pașapoartele electronice și în cartea de PIV FIPS 201.

3.3 ISO/IEC 15693[59]

ISO / IEC 15693 descrie standardele pentru carduri de "vecinătate". Mai exact, se stabilesc standardele pentru caracteristicile fizice, de puterea pentru radio frecvență și de interfață cu semnale, și protocoale de anti-coliziune și de transmisie pentru cardurile din vecinătate care operează la un maxim de 1 metru (aproximativ 3,3 feet).

3.4 ISO/IEC 7501[60]

ISO / IEC 7501 descrie standardele pentru documentele de călătorie care pot fi citite de mașini și au o imagine clară asupra topologiei smart cardului.

3.4.1 International Civil Aviation Organization (ICAO)[61]

ICAO emite orientări privind standardizarea și specificațiile pentru citit automat documentele de călătorie (Machine Readable Travel Documents - MRTD[62]), cum ar fi pașapoarte, vize, și documente de călătorie. ICOA a publicat caietul de sarcini pentru pașapoartelor electronice, folosind un cip inteligent fără contact pentru a stoca în siguranță datele de călătorie.

3.4.2 Federal Information Processing Standards (FIPS)[63]

Standardele FIPS, au fost elaborate de către Computer Security Division în cadrul National Institute of Standards and Technology (NIST[64]). Standardele FIPS sunt concepute pentru a proteja activele federale, inclusiv sistemele de telecomunicații. Următoarele standarde FIPS aplicate cardurilor inteligente se referă la standardele pentru semnătură digitală, standarde de criptare avansate, precum și cerințele de securitate pentru modulele criptografice.

3.4.3 FIPS 140 (1-3)[65]

Cerințele de securitate prevăzute în FIPS 140 (1-3) se referă la domenii legate de proiectarea sigură și punerea în aplicare a unui modul criptografic, și conține: caietul de sarcini pentru modulul criptografic; modulele criptografice aferente porturilor și interfețelor; roluri, servicii și autentificare; modelul pentru aplicații guvernamentale; securitatea fizică; mediu operațional; gestionarea cheilor de criptografie; interferențe electromagnetice / compatibilitate electromagnetică (EMI / EMC); auto-teste; asigurare a calității proiectului; și de atenuare a altor atacuri.

3.4.4 FIPS 201[66]

Această specificație se referă la toate aspectele legate de cardurile multifuncționale utilizate în sistemele de management al identității de către guvernul SUA.

---

[59] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39694
[60] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45562
[61] http://www.icao.int/Pages/default.aspx
[62] http://www.icao.int/security/mrtd/Pages/default.aspx
[63] http://www.nist.gov/itl/fips.cfm
[64] http://www.nist.gov/
[65] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm
[66] https://en.wikipedia.org/wiki/FIPS_201

3.5 Europay, MasterCard, and Visa (EMV)[67]

Europay, MasterCard, și Visa formatate de EMV Company, și LLC au creat "Caietul de sarcini pentru Cardurile cu Circuit integrat pentru sistemele de plată". Aceste specificații se referă la ISO 7816 și are rolul de a crea o bază tehnică comună pentru punerea în aplicare a cardurilor și a sistemelor pentru stocarea de valori. Cardurile cu Circuit integrat pentru sistemele de plată pot fi obținute de la un membru bancar: Visa, MasterCard sau Europay.

3.5.1 PC/SC[68]

A fost implementat la nivel global un standard pentru carduri și cititoare de carduri, în baza caietului de sarcini PC / SC. Acest standard se aplică numai cardurilor cu contact CPU. Cardurile folosesc versiunea 2.0 pentru PIN pad[69] communication. Toate aplicațiile de la Apple, Oracle-Sun, Linux și Microsoft folosesc acest standard.

Serviciile/aplicațiile dezvoltate de Microsoft pentru PC / SC necesare cardurilor inteligente suportă mai multe tipuri de mecanisme de securitate pentru carduri si sisteme. PC / SC este acum o interfață middleware destul de comună pentru aplicații PC logon. Standardul este un set extrem de abstract de componente middleware care permit cele mai comune interacțiuni pentru card reader.

3.5.2 Comité Européen de Normalisation (CEN)[70] and European Telecommunications Standards Institute (ETSI)[71] – (Comitetul European de Reglementare (CEN) și Institutul European de Standarde în Telecomunicații - ETSI)

CEN și ETSI se concentrează asupra telecomunicațiilor, care utilizează SIM-uri GSM pentru telefoanele celulare. GSM 11.11 și ETSI300045.

3.5.3 The Health Insurance Portability and Accountability Act (HIPAA)[72]

HIPAA adoptă standardele naționale de punere în aplicare a unui sistem electronic securizat de tranzacție pentru sănătate în operațiunile SUA. Exemplu tranzacțiile includ creanțele, înscrierea, eligibilitatea, plata și coordonarea prestațiilor. Cardurile inteligente sunt reglementate de cerințele de HIPAA referitoare la securitatea datelor și intimitatea pacientului.

3.5.4 IC Communications Standards[73]

Standardele de Comunicații IC care utilizau memorii non-volatile au adoptat utilizarea de chip-uri pentru smart card. Acest lucru este valabil în special pentru interfețele EEPROM I2C și SPI.

3.5.5 Global System for Mobile Communication (GSM)[74]

Standardul GSM deține poziția dominantă în industria de telefonie mobilă și folosește carduri inteligente, abonatul apelat fiind identificat prin intermediul *Subscriber Identification Modules* (SIM-uri), care sunt configurate cu informații esențiale pentru autentificarea unui telefon compatibil cu mobil-GSM, permițând astfel unui telefon să utilizeze serviciile ori de câte ori telefonul este în aria de acoperire a unei rețele adecvată. Acest standard este gestionat de Institutul European pentru Standarde de Telecomunicații[75] (*European Telecommunication Standards Institute*). Cele două standarde mai frecvente pentru carduri sunt 11.11 și 11.14.

---

[67] http://www.smartcardalliance.org/publications-emv-faq/
[68] http://www.pcscworkgroup.com/
[69] https://en.wikipedia.org/wiki/PIN_pad
[70] https://www.cen.eu/Pages/default.aspx
[71] http://www.etsi.org/
[72] http://www.hhs.gov/ocr/privacy/hipaa/administrative/statute/hipaastatutepdf.pdf
[73] http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf06129.html
[74] http://searchmobilecomputing.techtarget.com/definition/GSM
[75] http://www.etsi.org/standards

3.5.6 OpenCardT Framework[76],[77]

Cadrul OpenCardT este un standard învechit. Următoarele date sunt doar scop informativ.

Cadrul OpenCard a constat dintr-un set de ghiduri implementate de IBM, Netscape, NCI, și Sun Microsystems pentru integrarea cardurilor inteligente în rețelele de calculatoare. Liniile directoare au fost bazate pe standarde deschise și au oferit o arhitectură și un set de interfețe de programe de aplicare (API) care permit dezvoltatorilor de aplicații și furnizorilor de servicii să poată construi și implementa soluții smart card pe orice computer din rețeaua compatibilă OpenCard. Prin utilizarea unui card inteligent, un sistem de operare (conform) OpenCard ar fi permis accesul la date și servicii personalizate de la orice computer din rețea și descărca dinamic de pe Internet toate driverele de dispozitiv care sunt necesare pentru a comunica cu cardul inteligent. Prin furnizarea de o interfață de nivel înalt, care poate suporta mai multe tipuri de carduri inteligente, Cadrul OpenCard a fost destinat să permită interoperabilitatea cardurilor pentru furnizorii independenți. Sistemul încorporat Public Key Cryptography Standard (PKCS) - 11 a trebuit să fie extins pentru a include și alte mecanisme de chei publice.

3.5.7 GlobalPlatform (GP)[78]

GlobalPlatform este o asociație internațională, non-profit. Misiunea sa este de a stabili, menține și coordona adoptarea standardelor pentru a permite o infrastructură deschisă și interoperabilă pentru cardurile inteligente, dispozitive și sisteme care simplifică și accelerează dezvoltarea, implementarea și gestionarea aplicațiilor din industrii. Standardul GP a fost adoptat de aproape toate băncile din întreaga lume pentru a încărca JavaCard® ca baza de date criptografică. Standardul stabilește mecanisme și politici care să permită comunicații sigure cu un canal acreditat.

3.5.8 Common Criteria (CC)[79]

Common Criteria este un cadru de evaluare de securitate aprobat la nivel internațional care oferă o evaluare clară și fiabilă a capacităților de securitate ale produselor IT, inclusiv circuite integrate, sisteme de operare smart card, și software de aplicație. CC oferă o evaluare independentă a capacității unui produs de a îndeplini standardele de securitate. Clienții cum ar fi guvernele naționale, sunt conștienți de necesitatea securității certificării CC, în luarea deciziilor de cumpărare. Având în vedere că cerințele de certificare sunt clar stabilite, vânzătorii pot viza nevoile de securitate specifice oferind în același timp ofertele de produse.

3.6 Biometric Standards[80]

Multe noi implementări de sisteme cu ID securizat, utilizează atât elementele biometrice integrate cât și cardurile inteligente pentru a îmbunătăți securitatea și confidențialitatea unui sistem de identitate.

3.6.1 ANSI-INCITS 358-2002[81]

Specificațiile pentru ANSI-INCITS 358-2002, BioAPI se regăsesc în - (ISO/IEC 19784-1). BioAPI este destinat să furnizeze un nivel ridicat (un model) de autentificare biometrică generică potrivită pentru orice formă de tehnologie biometrică. Acesta acoperă funcțiile de bază privind înscrierea, verificarea, identificarea, și include o interfață de baze de date pentru a permite unui furnizor de servicii biometric (BSP) să gestioneze dispozitivul tehnologic astfel încât identificarea populației să se încadreze în limitele unei performanțe optime. Acesta prevede, de asemenea primitive care permit aplicarea de a gestiona separat captarea probelor pe o stație de lucru, înregistrarea, verificarea, și identificarea funcțiilor de pe un server. Cadrul BioAPI a fost adaptat pentru Win32,

[76] http://www.openscdp.org/ocf/
[77] http://www.gemalto.com/techno/opencard
[78] https://www.globalplatform.org/
[79] http://www.commoncriteriaportal.org/
[80] http://www.biometrics.gov/standards/
[81] https://standards.incits.org/apps/group_public/download.php/24527/National_Standards_Published_as_of_09_08_2010.pdf

Linux, UNIX, și WinCE. De reținut că nu există un BioAPI optim pentru un microcontroler, mai ales când aceste este inclus într-o unitate de cititor de control al accesului pe ușă, el fiin încorporat într-un procesor de smart card. BioAPI este mai potrivit atunci când există un calculator de uz general disponibil.

3.6.2 ANSI-INCITS 398[82]

Formatul cadru pentru date biometrice ANSI-INCITS 398, este comun cu (CBEFF) - (ISO / IEC 19785-1). The Common Biometric Exchange Formats Framework (CBEFF) descrie un set de elemente necesare pentru a sprijini tehnologiile biometrice și schimbul de date într-un mod comun de date. Aceste date pot fi plasate într-un singur fișier folosit pentru schimbul de informații biometrice între componentele diferite ale sistemului sau între sisteme diferite. Rezultatul promovează interoperabilitatea programelor și sistemelor dezvoltate de diferiti furnizori de aplicații biometrice permițând schimbul de date biometrice. Această specificație este o versiune revizuită (și augmentată) a originalului CBEFF, Common Biometric Exchange File Format, au fost inițial publicate ca NISTIR 6529.

3.6.3 ANSI-INCITS

Normele de schimb de date în format biometric sunt reglementate de către ANSI-INCITS. ANSI-INCITS a creat o serie de standarde care specifică formatul de schimb de date pentru datele biometrice. Aceste standarde specifică un format de înregistrare a datelor pentru stocarea, înregistrarea, și transmiterea informațiilor dintr-un eșantion biometric într-o structură de date CBEFF. ANSI-INCITS a publicat standardele de schimb de date. Există echivalente ISO pentru fiecare standard indicat în continuare:

- **ANSI-INCITS 377-2004**[83]**:** Finger Pattern Based Interchange Format;
- **ANSI-INCITS 378-2004**[84]**:** Finger Minutae Format for Data Interchange;
- **ANSI-INCITS 379-2004**[85]**:** Iris Interchange Format;
- **ANSI-INCITS 381-2004:** Finger Image Based Interchange Format;
- **ANSI-INCITS 385-2004:** Face Recognition Format for Data Interchange;
- **ANSI-INCITS 395-2005:** Signature/Sign Image Based Interchange Format;
- **ANSI-INCITS 396-2004:** Hand Geometry Interchange Format.

3.7 ISO/IEC 19794

Seria de standarde ISO / IEC 19794 reglementează formatul de schimburi de date biometrice:

- Partea 1 este cadrul;
- Partea 2 definește datele caracteristice a punctelor privind amprenta digitală;
- Partea 3 definește datele privind modelul spectral legat de amprentarea digitală;
- Partea 4 definește datele pentru imaginea amprentării digitale;
- Partea 5 definește datele pentru imagine amprentării faciale;
- Partea 6 definește datele de imagine pentru iris, și încă în dezvoltare;
- Partea 7 va defini semnătura datelor ca serii de timp;
- Partea 8 va defini datele scheletice pentru deget;
- Partea 9 va defini datele de imagine vasculară.

[82] http://www.fema.gov/media-library-data/20130726-1828-25045-8545/nims_guide_0004_2008.pdf

[83] https://www.google.ro/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB8QFjAAahUKEwiv0eW2sMvHAhUFyRQKHXcpAUE&url=https%3A%2F%2Fwww.hsdl.org%2F%3Fview%26did%3D464494&ei=VR7gVe_SE4WSU_fShIgE&usg=AFQjCNEzrKpr9gLDqZIdQU6GssdPqTV17g&sig2=ZDcwtzP4K1kyGCI9dqNxHQ

[84] http://www.nist.gov/itl/iad/ig/incits_data.cfm

[85] http://www.incits.org/news-events/press-releases/incits-announces-the-approval-of-five-biometric-data-interchange-format-standards