UNIVERSITATEA TITU MAIORESCU

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

IA – *Testul de evaluare nr.* 13

SmartCard

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. INTRODUCERE

Tendința de calcul în ultimii ani a fost spre mașini mici și de „*prelucrare distribuită*”. Pur și simplu, înseamnă că se urmărește delegarea sarcinilor către mai multe calculatoare mici, mai degrabă decât tot ce s-a făcut către mașini mari centralizate. De-a lungul timpului, cardurile inteligente vor avea o putere de calcul foarte mare și putem aprecia că deja aceste capacități de calcul sunt similare cu cele folosite la primul zbor pe Lună făcut de către un om. Smartcard-ul este o invenție europeană. Cip-ul introdus pe carduri a fost inventat de Helmut Gröttrup și colegul său Jürgen Dethloff în 1968. Brevetul a fost în cele din urmă aprobat în 1982. Prima utilizare în masă a cardurilor de plată a telefoanelor publice franceze, este datată încă din 1983 (Télécarte).

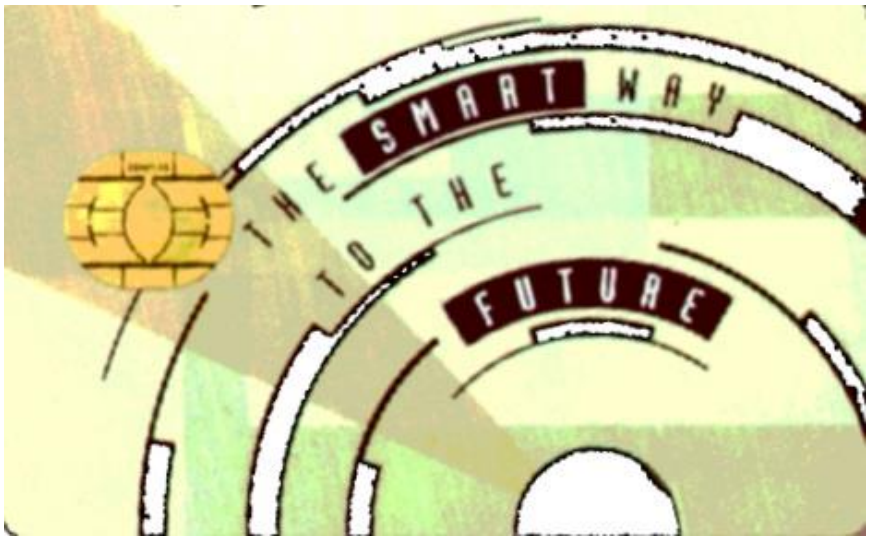
Roland Moreno a patentat de fapt primul său concept de cartelă de memorie în 1974. În 1977, Michel Ugon de la Honeywell Bull a inventat primul microprocesor pentru Smartcard. În 1978, Honeywell Bull a patentat SPOM (Auto programabil One-cip Microcomputer), care definește arhitectura necesară pentru autoprogramarea unui chip. Trei ani mai târziu, Motorola a produs primul „*CP8*” având la bază acest brevet. Honeywell Bull are deja peste 1200 de brevete legate de cardurile inteligente. Abia începând cu anii 1990 Smartcard-urile au înregistrat un boom comercial, odată cu introducerea cartelei SIM. Telefonia mobilă GSM dezvoltată în Europa, a utilizat încă de la început Smartcard-urile.

Pe lângă utilizarea Smartcard-urilor în telefonia mobilă, a început dezvoltarea de sisteme de plată de tipul Master Card, Visa și Europay din anul 1993. Diferențele dintre GSM și Master Card, VISA etc. constau modul în care s-au dezvoltat specificațiile necesare pentru utilizarea Smartcard-urilor. Pentru sistemele de plăți, primele specificații împărțeau aceste instrumente de plăți în cele de debit și cele de credit. Prima versiune a sistemului EMV (Enhanced Motion Vehicle) a fost lansată în 1994.

În 1998 a fost disponibilă o versiune stabilă a specificațiilor EMVco, de către compania responsabilă pentru întreținerea pe termen lung a sistemului, a actualizat caietul de sarcini în anul 2000, cea mai recentă actualizare fiind efectuată în 2004. Scopul EMVco este de a asigura diferitelor instituții financiare și comercianții cu amănuntul specificațiile care păstrează compatibilitatea cu versiunea din 1998. La cardurile inteligente a început să fie utilizată funcția de stocare de date, astfel încât, sunt posibile tranzacțiile monetare accesibile prin intermediul telefoniei mobile, vending retail, transport, tranzacții de vânzare cu amănuntul etc. Soluția inițială de Smartcard a ajuns la un anumit grad de maturizare și nu mai este folosit doar ca sistem de stocare date, el fiind utilizat mai ales pentru prelucrarea informațiilor. Imaginați-vă o societate fără numerar, în cazul în care puteți folosi carduri inteligente pentru a face multe lucruri interesante. Aceasta devine o realitate și cardurile inteligente fac viața oamenilor mult mai ușoară. Cardurile inteligente sunt utilizate pentru sisteme de transport, pentru a stoca informații medicale importante, și chiar pentru a cumpăra articole de mașini. Cardurile inteligente pot fi utilizate și printr-o conectare la Internet. Un cititor de carduri inteligente poate fi conectat la partea din spate a unui calculator personal (PC), astfel încât să se poată achiziționa direct de pe Internet diverse produse, sistemul fiind securizat.

Există carduri inteligente mult mai complicate. Spre exemplu Societatea Americană de Telefonie și Telegraph Company au divizii speciale pentru sistemele Smartcard. În revistele de specialitate de pe Wall Street, sunt descrie multe moduri în care Smartcard-urile au înlocuit mașinile de numerar. Cardul este de așteptat să fie folosit în multe aplicații și mai ales în aplicațiile de securitate legate de personal, cum ar fi controlul accesului, login/logout pentru calculatoare, trimiterea de e-mailuri securizate, trimiterea și regăsirea unor servicii.

Motivul real al creșterii acestor aplicații constă în special în caracteristicile de portabilitate și de securitate ale card-urilor inteligente. În plus, recenta creștere de calculatoare personale - PDA-uri, calculatoare personale sau Pocket PC prezintă o garanție mai bună pentru utilizarea unui Smartcard pentru mai multe aplicații.



Smartcard-ul poate fi semănat cu un Pocket PC, pentru a ne putea da seama de potențialul său. După cum se observă în figura de mai sus nu este mai mare decât cip-ul încorporat în card-urile clasice. Tehnologiile de azi permit realizarea unor dimensiuni foarte mici și o portabilitate crescută, astfel încât se poate aprecia că un Smartcard este un mini PC.

Majoritatea oamenilor transportă portofele pline cu carduri de la bănci, magazine, companii aeriene, companii de asigurări și altele asemenea. În plastic sau pe hârtie, fiecare card identifică emitentul și titularul cardului, dar înregistrarea reală nu este card-ul propriu-zis, ci un fișier găzduit într-un calculator, probabil la sute sau mii de kilometri distanță. Orice tranzacție se efectuează (achiziții, facturi medicale etc.) necesită un calculator central care verifică toate informațiile referitoare la emitent și proprietar și apoi efectuează operațiunile cerute. Prin urmare cardurile fizice reprezintă un suport fizic al unui întreg sistem.

Cardul este creat de un calculator, dar purtat de o persoană, astfel că însăși cardul respectiv reprezintă o înregistrare electronică. Informațiile din microcip pot fi verificate imediat din punct de vedere al identității posesorului de card și a oricăror privilegii cu care cardul este autorizat, pentru acea persoană. Retrageri, vânzări, facturi, toate informațiile pot fi prelucrate electronic la fața locului; mai târziu, dacă este necesar, aceste înregistrări pot fi transmise la un computer central pentru a actualiza fișierele sale.

Ideea din spatele acestor carduri este simplă: se cumpără 10€ valoare de monedă electronică de la o mașină sau un funcționar de vânzări. Acești 10€ sunt stocați pe un card de plastic și se diminuează electronic de fiecare dată când se cumpără ceva. Cu alte cuvinte, cartela are o memorie. La o camera de urgență de la un spital, de exemplu, cardul ar putea identifica pe asiguratul medical și apoi să i se transfere toate informațiile necesare de la microcip la o foaie medicală. Teste, tratamente, facturare cât și prescripțiile ar putea fi prelucrate mai rapid cu ajutorul cardului. Datele clinice majore ar putea fi adăugate la secțiunea de informații medicale în microcip. Cartelele inteligente dețin în mod obișnuit de la 2000 la 8000 bytes electronic de date pe mai multe pagini de informații.

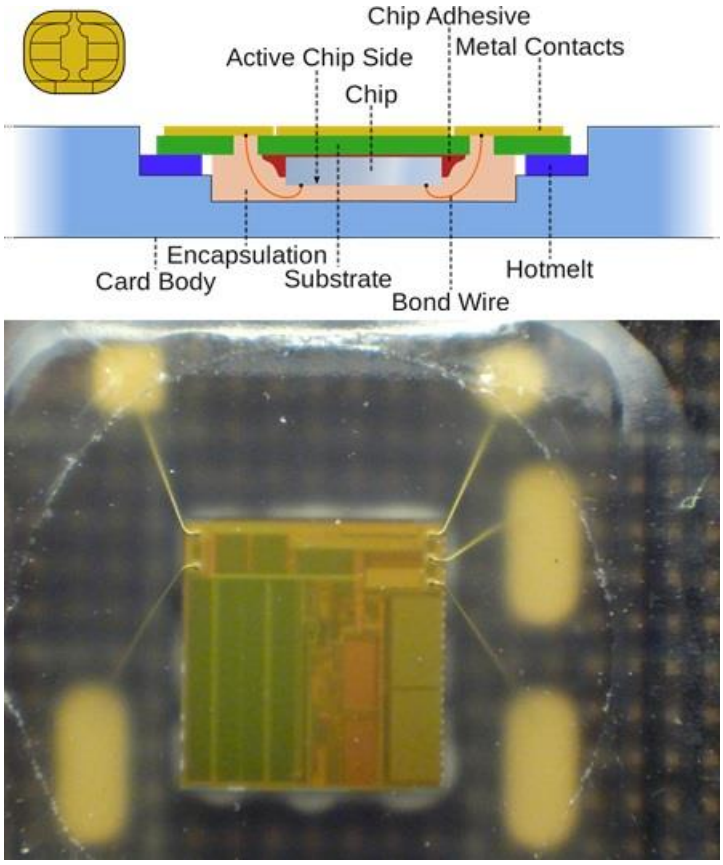
Deoarece acești biți pot fi codificați electronic, capacitatea de stocare efectivă a fiecărui card este semnificativ mai mare decât câteva pagini. Cartelele cu benzi magnetice, cum ar fi cele emise de bănci și companii de carduri de credit, nu sunt protejate precum microcipurile, dar sunt mai ieftine pentru ca ele să poată fi utilizate doar pentru un singur scop. Ca un purtător de mai multe înregistrări pentru scopuri multiple, însă, cardul inteligent este superior.

Datorită nivelului ridicat de securitate al cardurilor inteligente și natura sa off-line, este extrem de dificil pentru „*hackeri*” de a prelua informațiile de pe un card, sau să introducă date neautorizate pe card. Întrucât este greu pentru a obține date fără autorizație, pentru că se potrivește (dimensional) într-un buzunar, se poate spune că Smartcard potrivit pentru stocarea de date securizate și pentru e-commerce. Fără permisiunea deținătorului de card, datele nu pot fi capturate sau modificate. Prin urmare, Smartcard-ul ar putea spori și mai mult confidențialitatea datelor utilizatorului final.

Un Smartcard cu cip, sau cardul cu circuit integrat IC (Integrated Circuit), este definit ca un card de buzunar cu circuite integrate încorporate care pot procesa informații. Acest lucru implică faptul că se pot primi informații procesate - prin intermediul aplicațiilor ICC – și care pot fi livrate ca o ieșire. Există două mari categorii de ICC:

- cardurile de memorie conțin componente de stocare de memorie numai non-volatile, și, probabil, cu sisteme logice de securitate specifice;
- cardurile cu microprocesor conțin memorie și microprocesoare cu componente volatile.

Cardul este realizat din material plastic. Di Giorgio[1] 1997 definește cardul inteligent ca un „*card de credit*”, cu un mic cip de computer încorporat. Din cauza acestui „*cip încorporat*”, Smartcard-ul este, de asemenea, cunoscut sub numele circuit integrat de card ICC (Integrated Circuit Card). Unele Smartcard-uri pot avea un microprocesor încorporat, în timp ce altele pot avea inclus doar o memorie non-volatilă.

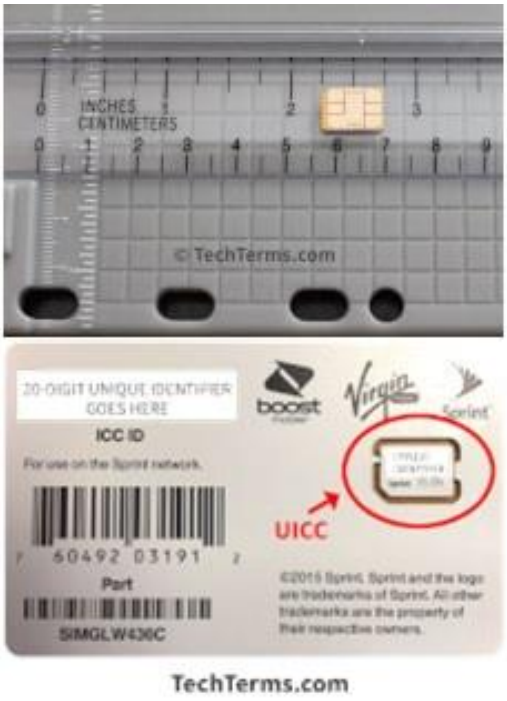


Capacitatea de stocare totală a unui card cu bandă magnetică este de 125 [bytes], în timp ce capacitatea de stocare a unui card clasic variază în plaja 1÷64 [k bytes]. Cu alte cuvinte, conținutul de memorie de pe un card inteligent de mare capacitate poate stoca conținutul de date de pe mai mult de 500 de carduri cu bandă magnetică. Evident, capacitatea de stocare mai mare este unul dintre avantajele în utilizarea de Smartcard-uri, dar caracteristica cea mai importantă a Smartcard-ului constă în faptul că datele stocate pot fi protejate împotriva accesului neautorizat și manipularea

[1] https://www.scribd.com/document/153400989/Smart-Card-Introduction-to-Smart-Card-Technology

frauduloasă. În interiorul unui Smartcard, accesul la conținutul de memorie este controlat de un circuit logic aflat în cip. În timp ce accesul la date poate fi realizat doar printr-o interfață serială supravegheată de sistemul de operare și sistemul logic securizat, datele confidențiale scrise pe card nu pot fi accesate din exterior în mod neautorizat. Aceste date pot fi prelucrate numai de către microprocesorul intern. Prin urmare, Smartcard-ul nu este doar un depozit de date, el poate fi considerat ca fiind un programabil, portabil, cu o memorie pentru stocarea informațiilor cu protecție falsificarea acestora. Microsoft consideră Smartcard-ul ca o extensie a unui computer personal și componenta cheie a infrastructurii publice.

În afară de ICC mai există și Cardul universal cu circuit integrat UICC (Universal Integrated Circuit Card). Un UICC este un Smartcard conceput pentru a funcționa cu tehnologii wireless 3G și 4G, inclusiv tehnologia cunoscută sub denumirea de „*evoluție pe termen lung*” LTE (Long Term Evolution). Acesta poate fi folosit pentru mai multe aplicații, dar este utilizat în mod obișnuit ca o cartelă SIM în telefoanele mobile. UICC-urile au înlocuit cea mai mare parte ICC-urile, care au fost utilizate cu sistemele 2G și 3G.



Un UICC este un card miniatural, care include un circuit integrat. Acest circuit conține un procesor, memorie nevolatilă NVRAM (Non-Volatile Random Access Memory), ROM (Read-Only Memory)și o memorie RAM (Random Access Memory). Fiecare card are un identificator unic care este utilizat pentru a identifica un dispozitiv dintr-o rețea celulară. Cardul poate, de asemenea, să stocheze date, cum ar fi contactele salvate de utilizator. Deși nu există o capacitate de stocare standard pentru UICC, acestea au de obicei cel puțin 256 [k bytes] de spațiu de stocare și pot depăși un gigabyte.

UICC-urile sunt „*universale*”, deoarece un singur card acceptă mai multe aplicații și prin urmare mai multe rețele celulare. Exemplele includ Modul universal de identitate a abonatului USIM (Universal Subscriber Identity Module) pentru rețelele GSM, Modulul de identitate a abonatului CSIM (CDMA Subscriber Identity Module) pentru rețelele CDMA (Code Division Multiple Access) și Modulul de identitate a serviciilor Multimedia ISIM (IP Multimedia Services Identity Module) pentru rețelele UMTS (Universal Mobile Telecommunications System). Caracterul universal al UICC le permite să lucreze cu diverse rețele mobile din întreaga lume.

Pentru a utiliza un UICC, identificatorul unic al cardului (ID-ul ICC) trebuie să fie înregistrat și activat cu un furnizor de servicii de telefonie mobilă. Îndepărtarea cardului de la un smartphone sau de la alt dispozitiv celular va face ca dispozitivul să nu fie recunoscut în rețea. În majoritatea cazurilor, dacă introduceți cardul UICC într-un alt dispozitiv, acesta va fi automat recunoscut și utilizabil în rețea.

2. TIPURI DE SMARTCARD-uri

2.1 Carduri de memorie

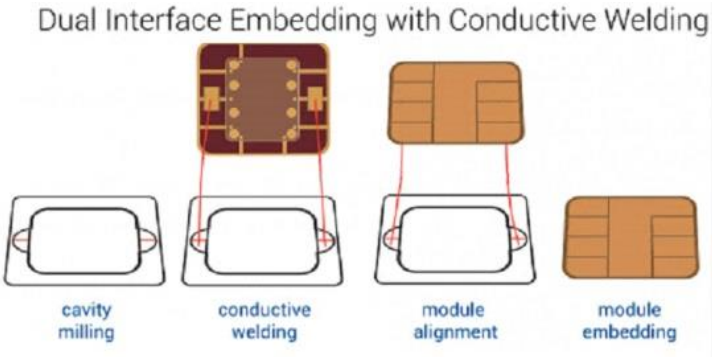
Un card de memorie este un dispozitiv electronic de stocare a datelor și informațiilor în format digital. Acestea sunt utilizate în mod obișnuit în dispozitivele electronice portabile, cum ar fi camerele digitale, telefoanele mobile, laptopurile, tabletele, PDA-urile, playerele portabile, consolele pentru jocuri video, sintetizatoarele, tastatura electronică și pianele digitale

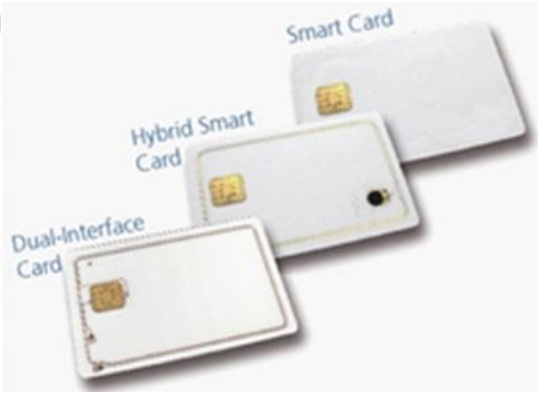
Este similar cu cardul cu bandă magnetică, care nu poate fi utilizat decât pentru stocarea de date. Fără CPU, cardurile de memorie pot fi utilizate doar ca un mecanism de comunicare sincronă între cititor și cardul respectiv, în cazul în care canalul de comunicare este întotdeauna sub controlul direct al cititorului de card. Datele stocate pe card pot fi preluate cu o comandă adecvată de pe card.

În cardurile de memorie tradiționale, nici o logică de control de securitate nu este inclusă. Prin urmare, accesul neautorizat la conținutul de memorie de pe card nu ar putea fi prevenit. În timp ce în cardurile de memorie actuale, cu logica de control de securitate programată pe card, accesul la zona de protecție este limitată doar pentru utilizatori cu un sistem simplu de codificare.

2.2 Smartcard-uri de contact

Smartcardurile de contact au un cip mic de aur de aproximativ 1 [cm^2] pe partea din față. Când este introdus într-un cititor, cipul face contact cu conectorii electrici care pot citi informații de la chip și scrie informații înapoi. Interfața de contact impune ca acest card să fie introdus într-un cititor de card, astfel încât cititorul să poată stabili un contact electric direct cu cipul. Smartcardurile de contact sunt utilizate în general pentru o gamă largă de aplicații, inclusiv tranzacțiile financiare și de control ale accesului logic. Smartcardurile de contact au anumite limitări. Cu timpul, aceste contacte se uzează. Descărcările electrostatice, din cauza unor contacte necorespunzătoare, pot deteriora circuitele. Deținătorii de card scot, uneori, cardurile din cititor înainte ca tranzacția să fie finalizată, ceea ce duce la ruperea cipurilor de aur. Manipularea dură în timpul introducerii cardului conduce la deteriorarea cardului.





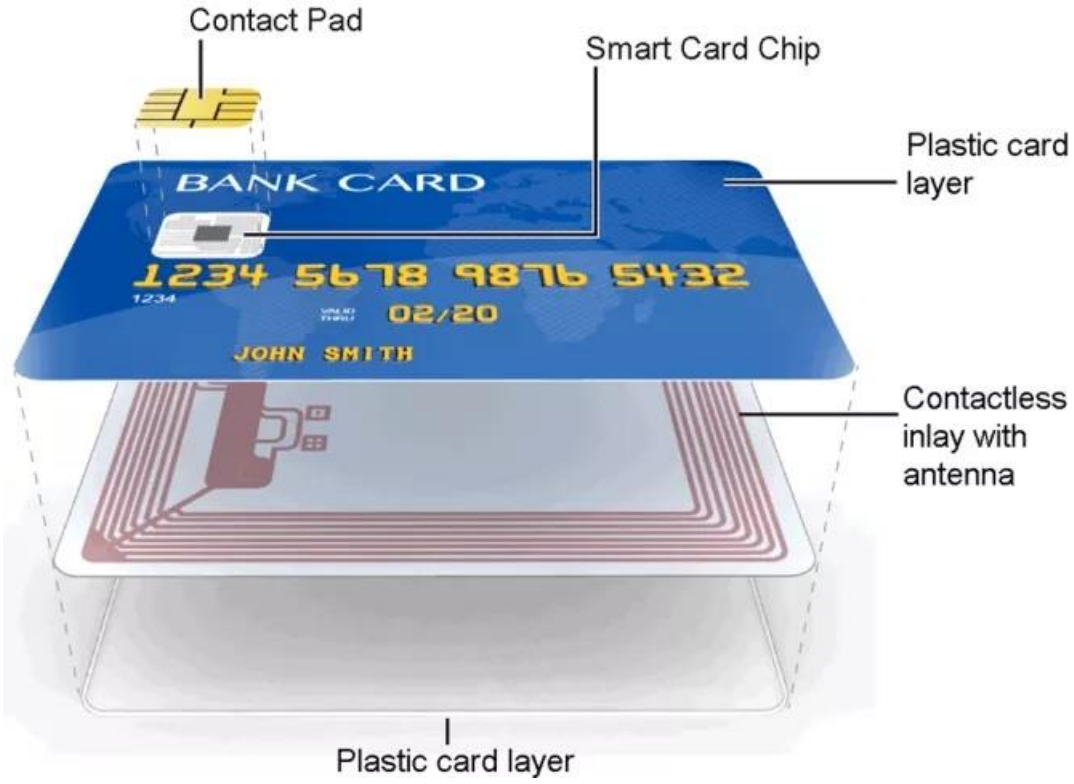
2.3 Smartcard-uri fără contact (wireless)

Chiar dacă un card inteligent de contact CPU este mai sigur decât un card de memorie, nu pot fi potrivite pentru toate tipurile de aplicații, în special pentru cazul în care sunt implicate operațiuni

masive, cum ar fi cele de transport de date transport sau a aplicațiilor din domeniul transportului auto, naval sau aerian. Pentru că în utilizările de transport-public, datele cu caracter personal nu pot fi capturate de către cititor într-o perioadă scurtă de timp (prin introducere într-un cititor de carduri), se realizează un contact de la distanță în timp real. Acest lucru se realizează prin utilizarea de frecvențe radio, Smartcardul poate transmite datele utilizatorului de la o distanță destul de mare într-o perioadă scurtă de activare (timp). Titularul de card nu ar trebui să introducă cardul în cititor. Procesul de tranzacție întreg ar putea fi efectuat fără a scoate cardul din portofelul utilizatorului.

Cardurile inteligente fără contact „*contactless*" utilizează o tehnologie care permite cititorilor de carduri să furnizeze energie pentru tranzacții și comunicații fără a face contact fizic cu cardurile. De obicei, semnalul electromagnetic este utilizat pentru comunicarea între card și cititor. Puterea necesară pentru a rula cipul de pe card ar putea fi furnizată de bateria încorporată în card sau transmisă la frecvențele de tip microunde din citire-ER de pe card.

Smartcardurile „*contactless*" sunt foarte potrivite pentru un transfer mare de date. Cu toate acestea, Smartcardul „*contactless*" nu a fost standardizat. Există aproximativ 16 tehnologii diferite de carduri contactless. Fiecare dintre aceste tehnologii au avantajele sale specifice, dar ele nu pot fi compatibile între ele. Cu toate acestea, din cauza costurilor de producție ridicate și a faptului că tehnologia este relativ nouă, aceste tipuri de carduri nu au fost adoptate, încă, pe scară largă.



2.4 Smartcard-uri Combi

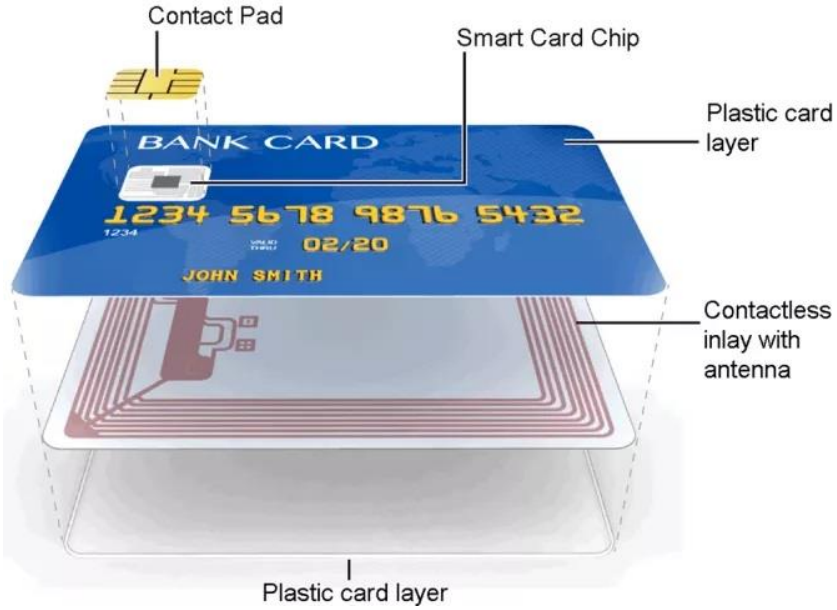
În stadiul actual, cardurile inteligente de contact și contactless folosesc două protocoale de comunicare și procese de dezvoltare diferite. Ambele carduri au avantajele și dezavantajele lor. Cardurile de contact inteligente au un nivel mai ridicat de securitate și o infrastructură disponibilă, în timp ce cardurile inteligente contactless asigură un mediu de tranzacție mai eficient și mai convenabil.

În scopul de a oferi clienților avantajele celor două tipuri de carduri s-au aplicat două metode:

- prima metodă este de a construi un cititor de carduri hibrid, care ar putea înțelege protocoalele de pe ambele tipuri de carduri;
- a doua metodă este de a crea un smartcard care combină funcțiile cardului cu contact cu funcțiile celui contactless.

Deoarece costul de fabricație al cititorului hibrid este foarte scump, soluția a doua a fost preferată. Uneori, termenul „*Smartcard Combi*” este utilizat în mod abuziv de către producători.

Ambele tipuri de tehnologii „*contact / contactless*” au încorporate elementele fizice specifice fiecărei tehnologii. Cu toate acestea cardul hibrid de contact IC elementele componente sunt asamblate separat, nefiind integrate într-un singur cip.

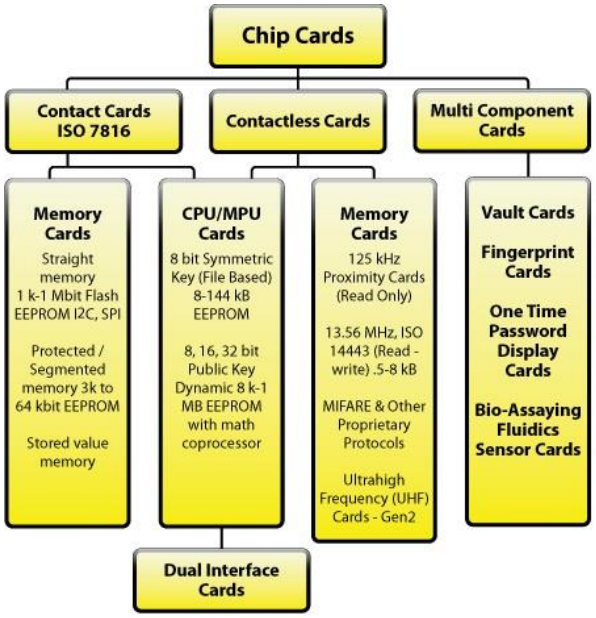


Între cele două tehnologii implementate pe același suport de plastic nu există conexiuni electrice pentru comunicarea între cele două cipuri. Aceste două module pot fi considerate cipuri separate, dar coexistente pe același card.

Pe „*Smartcard Combi*” „*contact / contactless*” cipurile ar putea comunica între ele, dând astfel „*Smartcard-ului Combi*” capacitatea de a vorbi cu mediul extern, fie prin metoda contactului direct fie prin metoda contactless.

„*Smartcardul Combi*” dispune de avantajele ambelor carduri „*contact / contactless*”, singurul motiv pentru care împiedică acceptarea sa este costul.

În cazul în care costurile și obstacolele tehnice sunt depășite, cardurile „*combi*” vor deveni din ce în ce mai utilizate.



3. APLICAȚII ALE SMARTCARD-urilor

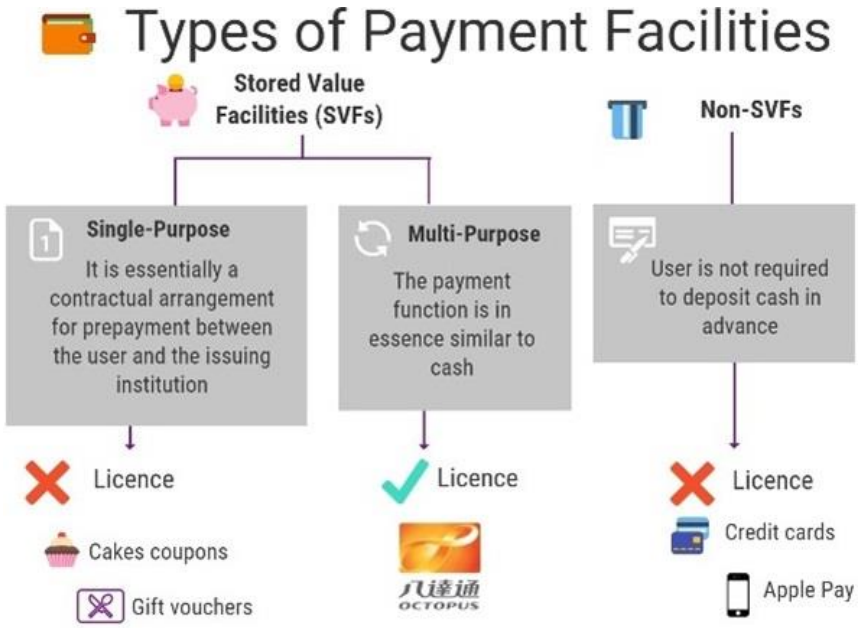
Odată cu expansiunea rapidă a tehnologiei de pe Internet și a comerțului electronic, cardurile inteligente sunt acum mult mai acceptate în piața comercială în funcție de calitate, de valoare stocată și de siguranță. De asemenea, au început să fie utilizate ca o carte de identitate. De exemplu, în City University din Hong Kong, vechile cartele elev/personal au fost înlocuite cu cărțile de identitate pe bază de hibrid-card. Acest card de identitate poate fi folosit pentru accesul normal, precum și de a efectua o plată electronică. Cardul a fost, de asemenea, utilizat în transportul comun, cum ar fi cardul Octopus, care a înlocuit vechiul card cu bandă magnetică. Rezultatele medicale pot fi, de asemenea, stocate pe un smartcard. Acest lucru permite stocarea de informații despre pacient, astfel încât, să poată fi preluate de fiecare dată când este necesar. Cu ajutorul tehnologiei smartcard, multe date sigure, cum ar fi numele de utilizator și parola calculator poate fi, de asemenea, păstrate, astfel încât utilizatorul nu trebuie să țină minte un număr mare de parole. În capitolul următor, se descriu pe scurt unele aplicații curente de carduri inteligente. Aceste aplicații pot fi clasificate în 6 categorii principale:

- plăți electronice;
- securitate și autentificare;
- transport;
- telecomunicații;
- program loialitate;
- carduri de sănătate.

3.1 Smart Cards applications worlwide

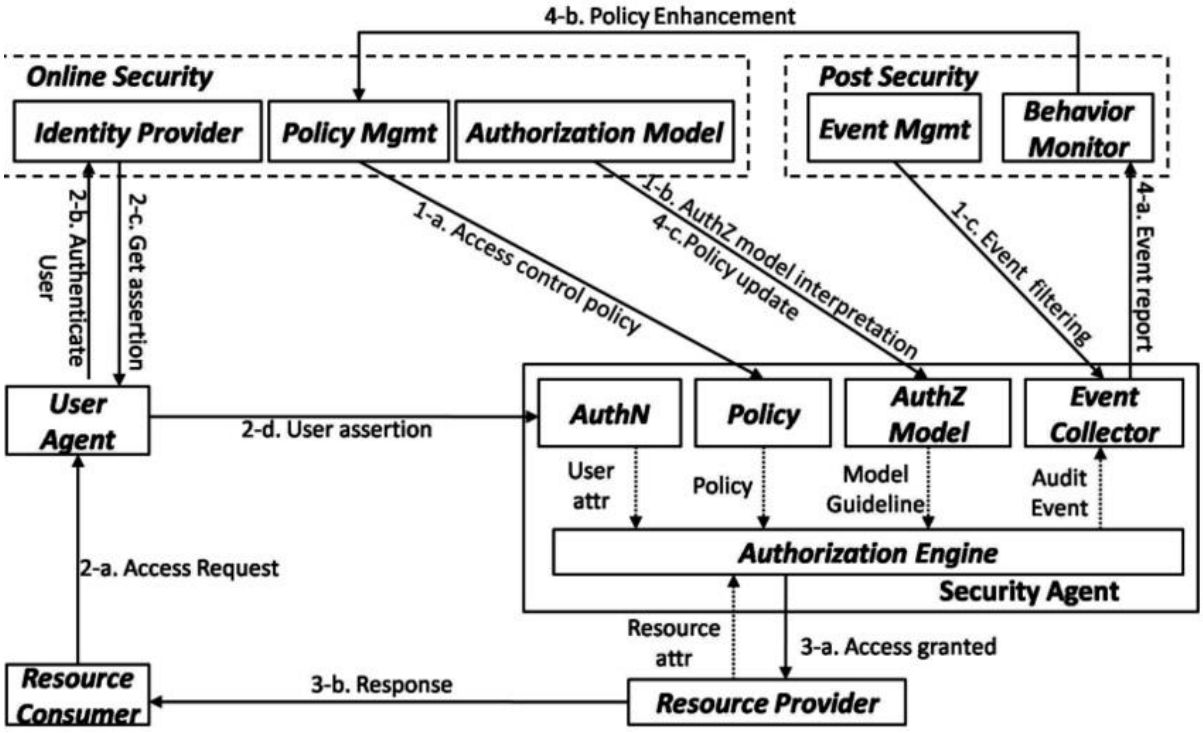
3.1.1 Electronic payment Applications. Stored Value Cards

Un smartcard poate funcționa ca un înlocuitor de numerar prin organizarea unei valori, care este redusă de fiecare dată când cardul este prezentat pentru a obține bunuri sau servicii. Acestea sunt cardurile de valoare stocată „*Stored Value Cards*”. Furnizorul de servicii ține o evidență a tranzacțiilor, iar procesul de rambursare se efectuează la intervale regulate de către controlerul de sistem. Furnizorul de servicii nu trebuie să cunoască identitatea titularului cardului. Cardurile pot fi de unică folosință sau reîncărcabile. Cardurile reîncărcabile pot fi completate prin plata în numerar la ghișeu sau prin transferul de fonduri de la o bancă. Există, de asemenea, sisteme de carduri care permit un sistem automat de încărcare cu fonduri în cazul în care valoarea în card ajunge la o sumă minimă specificată.



Detalii privind tranzacțiile recente sunt înregistrate în memoria cardului. Portmoneele electronice au potențialul de a funcționa pur și simplu ca un substitut pentru bani, permițând tranzacții complet anonime, cu condiția ca informațiile despre titularul cardului sau despre card (cum ar fi un număr de serie) să nu fie transferate de pe cardul respectiv. Cu toate acestea, introducerea unui portofel electronic care permite titularului cardului să efectueze transferul de bani de pe card pe un alt cont bancar, reduce potențialul anonimatului din motive de securitate (Lokan, CWI CAFE, Dawson, Gaskell, Mewett & Russell).

O altă utilizare a cardurilor inteligente în comerțul electronic este utilizarea lui sub forma unui jeton electronic. Acesta este un exemplu al cartelei cu valoare stocată. Principiul este că unele memorii de pe Smartcard sunt rezervate pentru a stoca semnale electronice sau bilete electronice. Un smartcard poate stoca jetoane pentru diferite servicii și fiecare dintre jetoanele respective pot fi reumplute, în funcție de tipurile de card de memorie. Acest lucru permite costurilor să fie distribuite pe un număr de servicii și pentru o durata de viață mult mai mare. De exemplu, cardul ar putea fi folosit pentru a plăti utilitățile, precum electricitate, gaz telefonie etc. și acest lucru în mod automat. Consumatorii încărcați în modul debitării automate pe Smartcard permite operarea fără probleme. Avantajul acestui tip de tranzacții este că nu mai este necesară alimentarea card-ului, extragerea fiind efectuată direct din bancă. De asemenea se pot monitoriza tiparele de consum și de a reveni cu noi informații despre comercianți, sau chiar de a introduce produse derivate (McCrindle1990).



3.1.2 Security and Authentication Applications

i. Utilizarea criptografiei

Din punct-de-vedere al operatorului de servicii și de sistem, cerința principală a aproape tuturor sistemelor de carduri este că trebuie să poată fi citite automat și de a se asigura că respectivul card este valabil și titularul cardului este într-adevăr persoana îndreptățită să folosească cardul. Pentru a verifica identitatea posesorului de card, utilizatorii trebuie să introducă codul PIN (Personal Identification Number). Acest cod PIN este păstrat pe card, mai degrabă decât pe terminalele sau mașinile gazdă. Procedurile de identificare și autentificare au loc la terminalul de card. Una dintre probleme este de a asigura că cip-ul furnizează date ce pot fi citite automat, pentru îndeplinirea criteriului de autenticitate. Acest lucru poate fi rezolvat prin utilizarea comunicațiilor criptate între card și terminal. Este bine

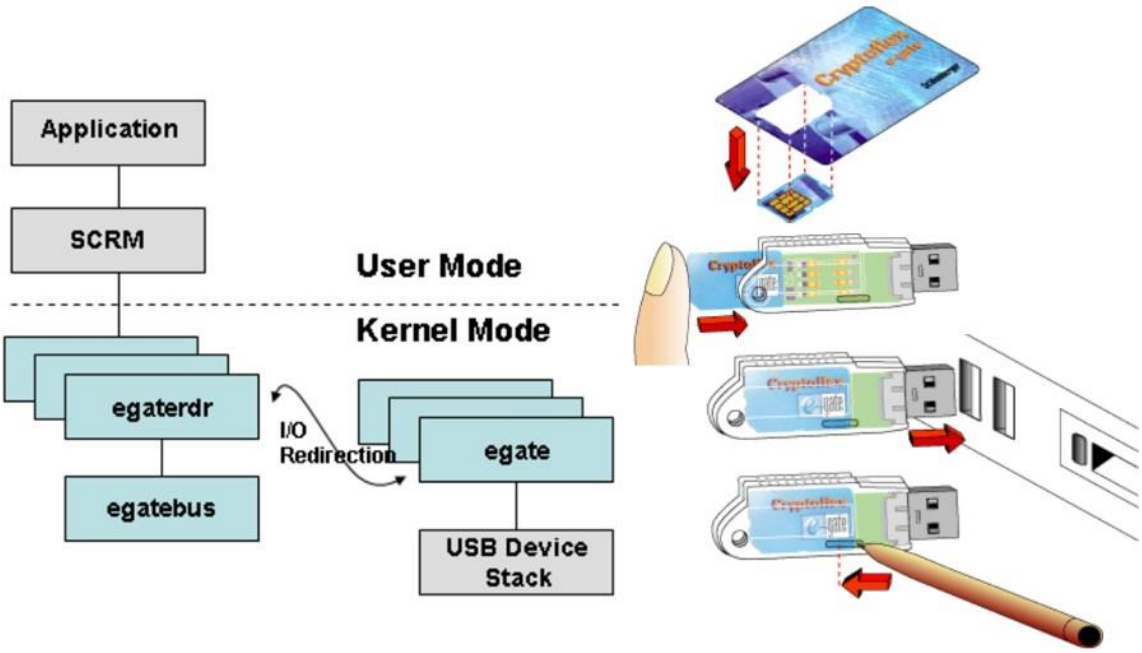
cunoscut faptul că pentru a asigura secretul de mesaje trimise și, de asemenea, pentru autentificarea mesajelor se utilizează criptarea. În scopul de a efectua procedura de criptare, Smartcard-urile trebuie să aibă următoarele proprietăți:

- cardurile trebuie să aibă suficientă putere de calcul pentru a rula algoritmi criptografici;
- algoritmii de criptare trebuie să fie teoretic siguri, acest lucru înseamnă că nu este posibilă obținerea cheii secrete din textele corespunzătoare;
- cardurile inteligente trebuie să fie sigure fizic, fiind imposibilă extragerea cheii secrete din memoria cardului.

Dacă aceste condiții sunt îndeplinite, și cu progresele tehnologice pentru microcontroler, cardul inteligent pe bază de microprocesor poate fi realizat pentru a satisface nivelul de securitate necesar (Chaum1989).

De exemplu, Verisign și Schlumberger[2] au dezvoltat utilizarea de smart card Cryptoflex pentru realizarea unui act de identitate Verisign Clasa 1 digitala (Verisign 9701). Cardul Cryptoflex este primul card inteligent criptografic în industrie, care este conceput pe baza specificațiilor PC / SC. Acest lucru permite utilizarea de smart card pentru acces la Internet portabil cu Microsoft Internet Explorer 3.0 la toate site-urile accepta Verisign Digital ID-uri.

În Universitatea Michigan, cardul Cyberflex a fost folosit pentru stocarea chei Kerberos într-un proiect de autentificare securizat (Michigan 9701).



ii. Identity card

Identificarea unei persoane este una dintre cele mai complexe procese în domeniul tehnologiei informației. Este nevoie atât ca individul să se identifice și sistemul să recunoască conexiunea de intrare care este generată de un utilizator legal. Sistemul acceptă apoi responsabilitatea pentru a permite toate acțiunile ulterioare, fiind în cunoștință de cauză faptul că utilizatorul are autorizarea de a face tot ce solicită sistemul. Dacă se utilizează un card inteligent, informațiile stocate pe card pot fi verificate pe plan local având o „*password / PIN*” care se aplică mai înainte de conexiune. Acest lucru previne ca parola de a fi sustrasă de către „*hackeri*”. Unele dintre cardurile inteligente vor avea datele personale stocate pe card. De exemplu, titularul cardului: numele, numărul de identificare, precum și data nașterii (Devargas 1992).

[2] https://www.yumpu.com/en/document/read/34395264/cryptoflex-cards-programmers-guide-serwer-galeraiipwedupl

iii. Access control card

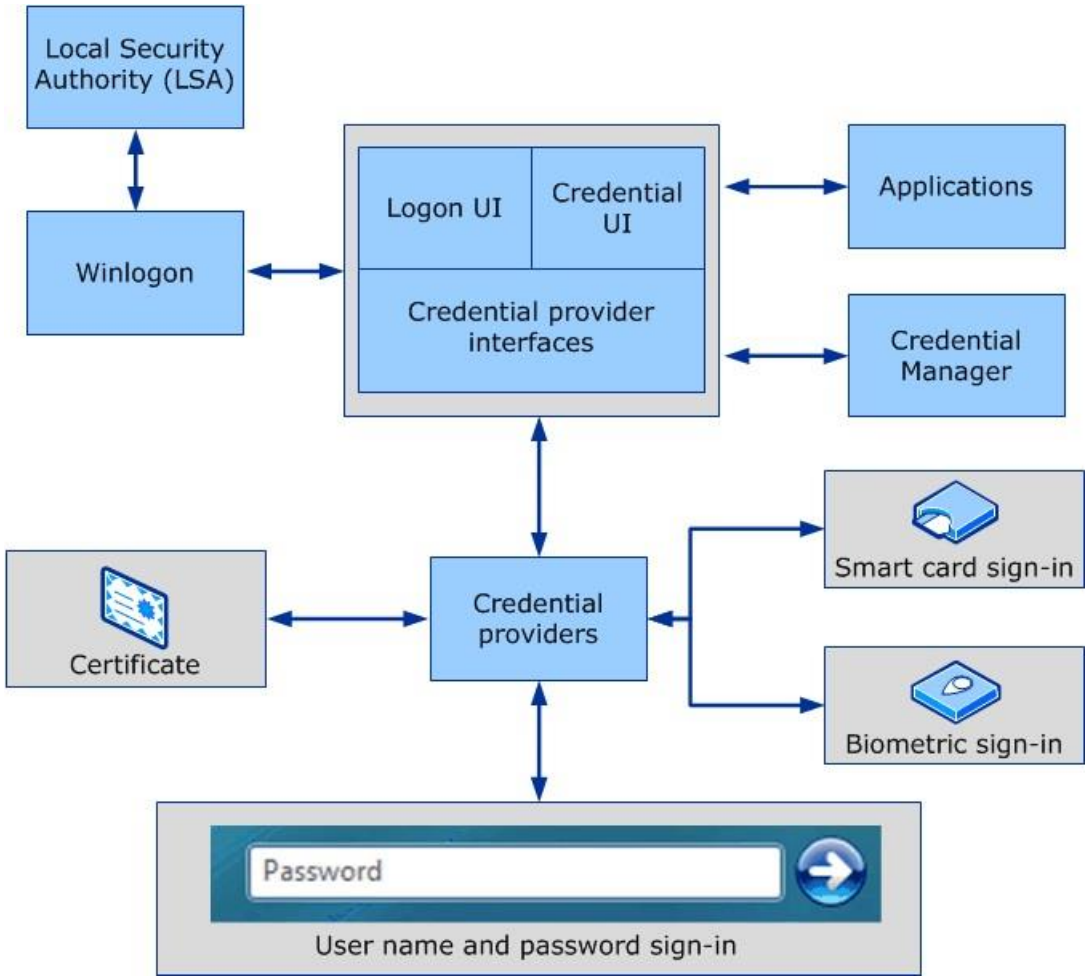
Cele mai frecvente dispozitive utilizate pentru a controla accesul sunt chei, jetoane și carduri magnetice. Acestea toate au aceleași dezavantaje de bază: pot fi ușor copiate și furate, acestea putând fi decriptate de către o persoană neautorizată. Smartcard-ul depășește aceste deficiențe, fiind foarte greu de reprodus și capabil să stocheze caracteristici personale digitizate. Cu echipamentele de verificare corespunzătoare, aceste date pot fi folosite la punctul de intrare în vederea identificării utilizatorului dacă este sau nu titularul cardului autorizat. Cardul poate fi, de asemenea, personalizat pentru a permite accesul la facilități, în funcție de nivelul de securitate al titularului. Un jurnal privind acțiunile titularului, printr-un sistem de securitate, pot fi stocate pe card ca o pistă de audit de securitate (McCrindle 1990). Cardul ar putea conține informații privind privilegiile utilizatorului (de exemplu, accesul pentru a asigura zone ale clădirii, identificarea automată a vehiculului la intrările în parcurile auto ale companiei, etc.) și restricții de timp. Toate informațiile sunt verificate pe card. Accesul la diferite zone ale clădirii pot fi distinse prin diferite coduri PIN. Mai mult, poate urmări, de asemenea, mișcarea utilizatorului în jurul clădirii (Devargas1992).

iv. Computer login/logout

Accesul la sala de calculatoare și a serviciilor sale pot fi controlate de către smartcard. În ceea ce privește accesul la rețea, Smartcard-ul poate autentifica utilizatorul. În plus, în funcție de mediul protejat cardul de acces la rețea poate efectua, de asemenea, următoarele funcții:

- manipularea, pentru diferite:
  - moduri de autentificare;
  - niveluri de securitate;
- utilizarea tehnicilor biometrice ca o măsură de siguranță suplimentară;
- păstrarea unei piste de audit pentru prevenirea eșecurilor și a tentativelor de încălcare a diferitelor protocoale.

Între timp, în ceea ce privește accesul la sala de calculatoare, verificarea PIN-ului se poate face de pe card fără a fi nevoie de cabluri în punctele de acces la un calculator central. Identificarea unui utilizator se face de obicei prin intermediul unui PIN. PIN-ul este verificat de microcomputerul cardului cu PIN-ul stocat în memoria RAM. În cazul în care comparația este negativă, procesorul va refuza să funcționeze. Cipul păstrează, de asemenea câte încercări consecutive au fost greșite la introducerea (sau recunoașterea) codului PIN. În cazul în care acest număr atinge un prag prestabilit, card-ul este blocat pentru a nu mai putea fi utilizat în continuare.



3.1.3 Transportation uses

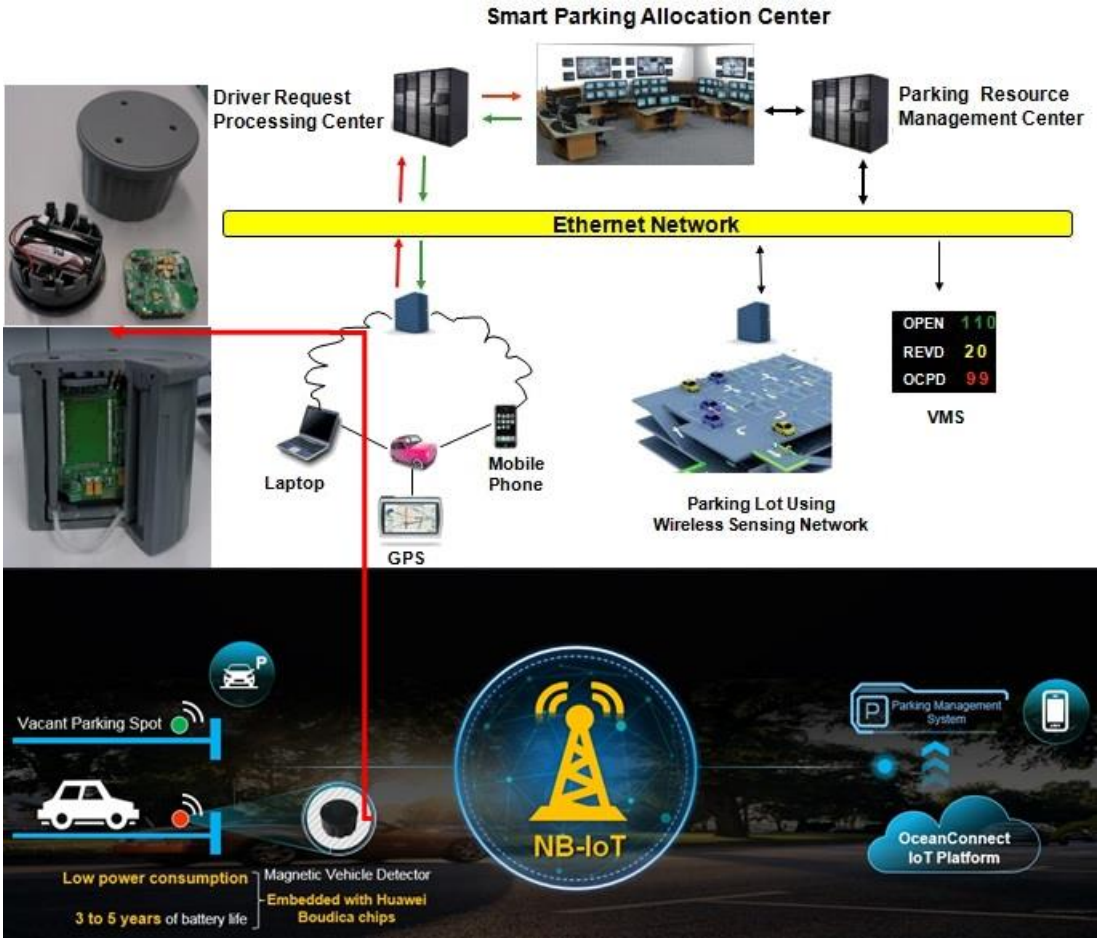
Sisteme cu taxare și emitere de bilete în mod automat:

Australia - Melbourne

Cardul poate acționa și în sistemele de taxare pentru parcare, pentru bilete sau ca monedă electronică pentru conducătorii auto care ar avea nevoie să plătească o taxă înainte de a putea utiliza un drum sau tunel. Spre exemplu în Melbourne există sistemul SMARTPARK - un sistem de taxe de

parcare pentru parcările din ansamblurile de business sau mall-uri. Se poate stabili astfel taxa de parcare auto, poate decela informațiile privind efectuarea cumpărăturilor etc.. Introdus în 1993, sistemul SMARTPARK, funcționează pe baza unui card inteligent EPROM în care datele sunt stocate până când tranzacția este finalizată, moment în care datele sunt șterse, iar cardul este re-emis pentru un alt conducător auto. SMARTPARK funcționează astfel:

- mașina intră în parcul auto în cazul în care conducătorul auto are emis un card inteligent și o broșură care explică modul în care funcționează sistemul SMARTPARK;
- cardul înregistrează punctul de intrare pentru mașină, ora și data intrării;
- șoferul intră apoi Shopping Centre sau Business Centre;
- de fiecare dată când consumatorul face o achiziție la unul dintre punctele de vânzare cu amănuntul în Centrul Melbourne înaintează cardul inteligent către comerciant. Acesta utilizează un cititor pentru a înregistra ora, data și marfa cumpărată pe smartcard-ul șoferului;
- la ieșirea din parcul comercial, șoferul predă card-ul personalului desemnat cu introducerea card-ului în cititoarele aferente. Se calculează taxa de parcare în funcție de suma de bani cheltuită de către conducătorul auto în centrul comercial și timpul petrecut în parcare. În final cardul este reținut de către reprezentantul care se ocupă de parcare;
- informațiile asupra a ceea ce s-a cumpărat din centrul comercial sunt anonime și se descarcă doar în baza de date a centrului comercial, mai înainte de a fi șterse de pe card. Apoi este remis pentru un nou client.



O trăsătură centrală a sistemului SMARTPARK este că nu este identificat consumatorul în mod individual sau prin înmatricularea autovehiculelor. Cu toate acestea, obiceiurile de cumpărare ale consumatorului sunt înregistrate doar pentru a permite gestionarea Centrului Comercial de a lua decizii cu privire la amplasarea de magazine, orarul etc.. Designerii sistemului estimează că un

asemenea card poate fi remis de până la 10.000, ceea ce îl face mai rentabil decât alte card-uri similare.

Sistemul SMARTPARK este un exemplu de un sistem smartcard anonim în care informațiile personale despre consumator nu sunt cunoscute. La nici o etapă în timpul tranzacției nu apare numele consumatorului și nici detalii referitoare la înregistrarea automobilului sau informații despre persoană (vârstă, sex etc). Cu toate acestea, având în vedere că există stimulente comerciale de colectare și stocare a acestor informații, în special în cazul în care poate fi legat de obiceiurile cumpărătorilor, sistemul ar putea fi extins treptat pentru a include programe de loialitate sau alte aplicații care identifică un individ.

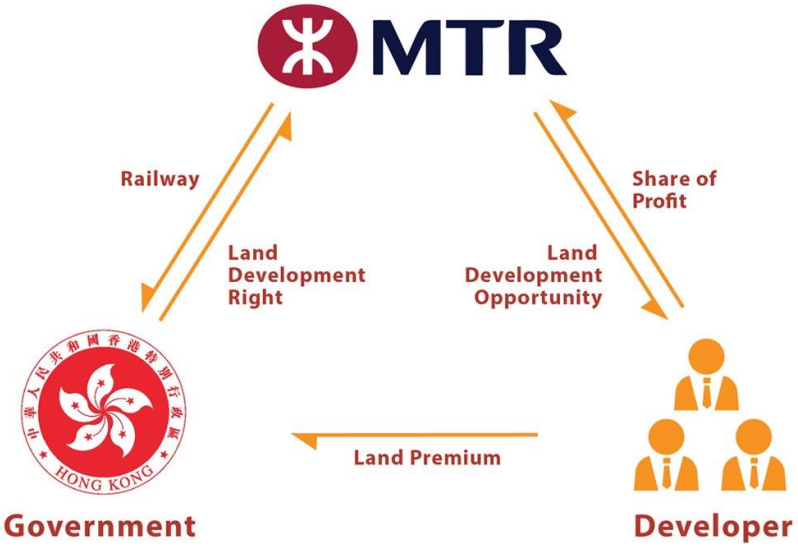
Hong Kong

Un consorțiu din Hong Kong numit Creative Star a realizat un sistem de ticketing pentru sistemul de transport public al orașului, care include trenuri, autobuze, tramvaie și feriboturi. Cardul fără contact (contactless) permite navetiștilor să treacă prin punctele de taxare fără a fi nevoie de a introduce cartela într-un cititor. În schimb, în afara acestor puncte incluse în sistem, card-ul trebuie apropiat sau introdus în cititoare. Utilizatorii sistemului trebuie să alimenteze card-ul, astfel:

- se introduce cardul într-o fereastră Mass Transit Railway Corporation și se plătește în numerar;
- se stabilește un acord de debitare directă cu un cont de economii, astfel încât atunci când mașina ajunge la un anumit nivel minim, fonduri suplimentare sunt adăugate pe cardul;

sau:

- se introduce cardul într-un bancomat (ATM) și se efectuează transferul de fonduri dorit;
- utilizatorii vor avea opțiunea de a utiliza un card anonim sau un card personalizat care va conține detalii cu privire la nume, data nașterii, numărul de identificare și de eligibilitate pentru reduceri (ca elev, student, etc).

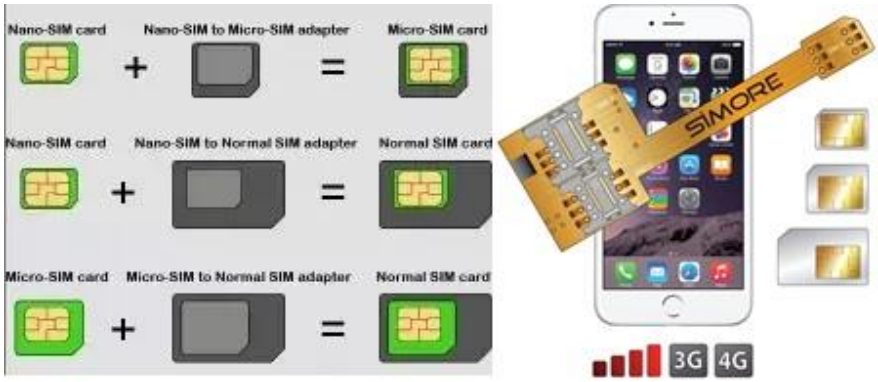


Singapore

Un studiu care implică carduri inteligente fără contact se desfășoară în Singapore pentru a înlocui taxarea automată la intrarea pe autostrăzi. Un smartcard montat pe parbrizul mașinii este debitat automat de cititoare de carduri montate pe drumul pe care mașina circulă și trece printr-o stație de taxare la viteze de până la 120 de kilometri pe oră. Soldul rămas pe card este vizibil conducătorului auto printr-un ecran cu cristale lichide încorporat în card. Spre deosebire de multe dintre modelele din Europa, sistemul Singapore nu identifică mașinile individuale sau șoferul. Sensibilitatea informațiilor despre deplasarea persoanelor a fost ilustrat în Hong Kong, unde a fost propus un sistem care să identifice mașinile, astfel încât proprietarii să fie tarifați lunar, tip abonament. Temerile consumatorilor cu privire invadarea vieții private, precum și a costurilor anticipate, au condus la abandonarea proiectului.

3.1.4 Aplicații în telecomunicații

Sistemele de telecomunicații sunt unele dintre cele mai mari piețe pentru aplicațiile Smartcard. În 1997, cardurile telefonice ocupau cea mai mare parte a pieței de Smartcard. Peste 70% din Smartcard-uri sunt emise ca și carduri telefonice (Card-Tech 1997), iar acest lucru va continua să reprezinte și în următorii 3 ani cea mai mare piață. Din 1988, Smartcard a devenit o componentă esențială în sistemele de telefonie celulară. Date privind rețeaua, informații referitoare la abonați și toate datele critice ale rețelei de telefonie mobilă sunt păstrate în interiorul cardului. Cu acest card, abonații ar putea face apeluri de la orice telefon portabil. Mai mult decât atât, prin intermediul cardului IC, apelurile prin telefonul mobil ar putea fi criptate, și să asigure, astfel, intimitate. În viitor, tot mai multe servicii cu valoare adăugată, cum ar fi serviciile bancare electronice, ar putea fi susținute prin folosirea acestui card cu microprocesor.



3.1.5 Loyality Applications

Programul de loialitate este o altă aplicație importantă a cardurilor inteligente în cazul efectuării de cumpărături. Statutul de client este preferat să fie încărcat cu informații detaliate privind obiceiurile de cumpărături și care sunt stocate și procesate pe smartcard.

Cu aceste informații, comercianții ar putea deriva mai bine tipul de cumpărături sau a profilurilor de cumpărături ale unui client personalizat. În plus, acest profil al cumpărăturilor este păstrat pe cardul clientului. Prin urmare, cumpărăturile ar putea fi păstrate ca și date confidențiale împotriva accesului neautorizat. Ca o extensie a aplicației de loialitate, ar putea fi adăugate (și stocate) funcții cu valoare predefinită. În sistemele de televiziune cu plata la zi, preferințele utilizatorilor sunt păstrate împreună cu schema de plată electronică. Utilizatorii nu ar trebui să fie setați în funcție de preferințele lor de fiecare dată când folosesc sistemul de televiziune.

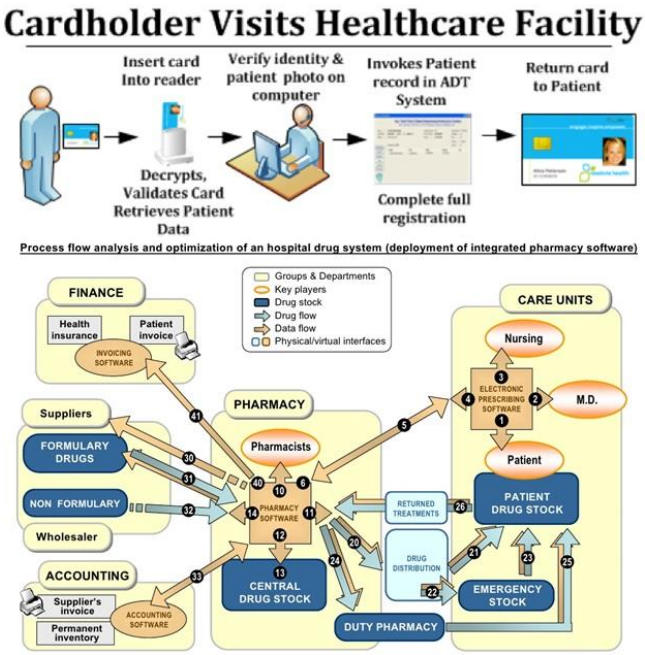
Acest card va fi, de asemenea, utilizat ca o cheie de deschidere a programelor TV, utilizatori având accesul restricționat în funcție de plata sau neplata abonamentului.

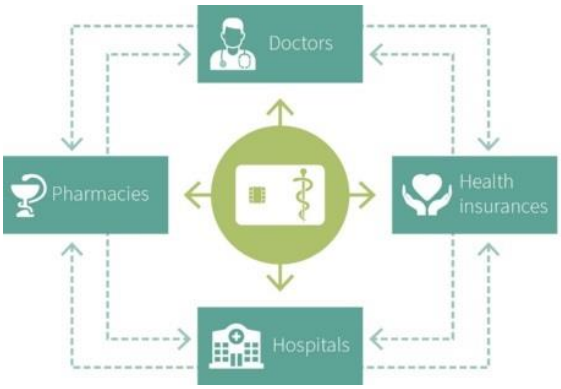
3.1.6 HealthCare Applications

Datorită nivelului de securitate prevăzut pentru stocarea de date, cardurile inteligente oferă o nouă perspectivă pentru aplicațiile medicale. Aplicații medicale care pot extrage date necesare privind starea pacientului direct de pe cardurile inteligente. Acestea pot stoca informații: date cu caracter personal, polița de asigurare, informații medicale de urgență, date de admitere în spital și dosarele medicale recente. Numeroase spitale naționale din Franța, Germania și chiar Hong Kong au început deja să pună în aplicare acest tip de card de sănătate. Cu un microcontroler încapsulat, cardurile inteligente ar putea fi utilizate pentru gestionarea nivelurilor de informare autorizate pentru utilizatori diferiți, similare cu un sistem de control al unui flux de producție. Medicii ar putea accesa dosarul medical de pe cardul pacientului, în timp ce personal specializat ar putea face uz de informații pentru a emite noi prescripții medicale și care urmează a fi stocate pe card, în urma stabilirii unui tratament medical. Date de urgență privind starea unui pacient sunt păstrate pe card: identitatea posesorului de card, persoanele de contact în caz de accident și detalii speciale asupra unor afecțiuni, care pot fi folosite pentru salvarea vieții pacientului. În unele țări, este necesară o asigurare medicală pentru plata spitalului. Cu înregistrările de asigurare stocate în cardul pacientului, procedurile administrative sunt simplificate.

Health-Passport

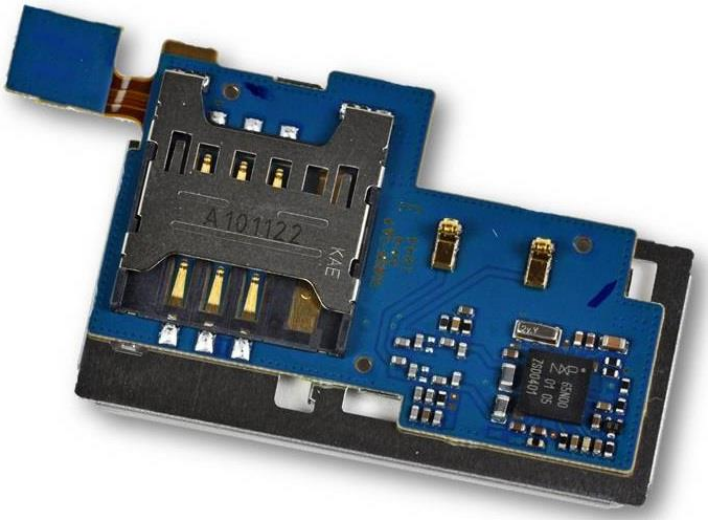
Pașaportul de sănătate este un smartcard, care deține informații importante legate de sănătate și care sunt la îndemâna părinților, tutorilor și copiilor, pentru a putea beneficia de programe de sănătate. Informațiile pentru mai mulți furnizori diferiți de asistență medicală sunt păstrate în siguranță, într-un loc și pot fi citite numai în cazul în care titularul cardului autorizează utilizarea acestuia. Acest lucru va permite accesarea într-un timp record a datelor necesare unei intervenții ulterioare. Pașaportul de sănătate permite posesorilor de carduri pentru a urmări informații importante, cum ar fi rezultatele recente ale examenelor medicale, ale contactelor cu anumite persoane (din punct de vedere al unor afecțiuni ce se pot transmite), înregistrări privind imunizările etc.. Se stochează informații personale actuale și exacte cum ar fi: adresa și numărul de telefon, informații de contact cum ar fi furnizorii de sănătate, date antropometrice etc.. Aceste informații ajută la evitarea repetării testelor și înregistrărilor. Participanții pot utiliza, de asemenea, cardul pentru a ține evidența numirii și sesizării altor servicii de sănătate publică eligibile. Informațiile privind cardul pot fi citite sau actualizate prin utilizarea de cititoare de carduri aflate în custodia prestatorilor de servicii medicale. Deținătorii de carduri pot citi, de asemenea, cardurile lor la chioșcurile destinate acestui scop și care se găsesc pe întreg arealul UE.





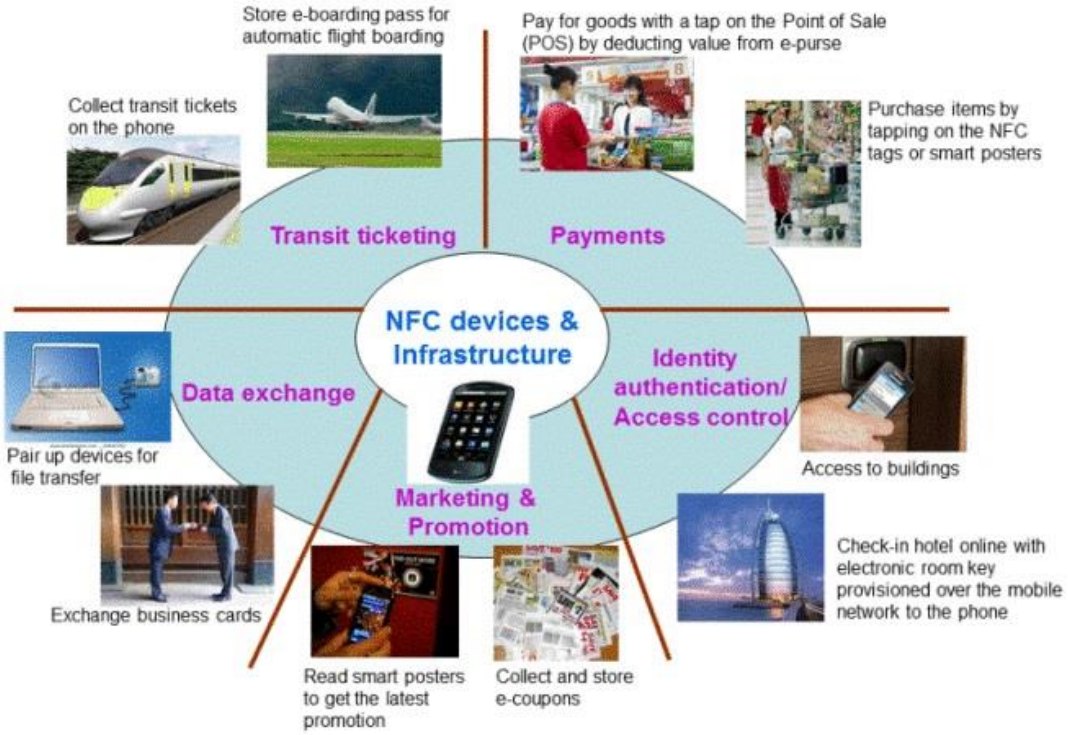
4. TEHNOLOGII NFC

Dezvoltarea tehnologică în domeniul NFC (Near-Field-Communication) presupune o centrare pe chipset-ul pregătit pentru a sprijini protocolul, atunci când se utilizează UICC PCB ca element securizat.



NXP PN65 utilizat în telefonia mobilă[3]

Comerțul deja se găsește în faza e-commerce. Comerțul electronic are loc prin internet. O altă aplicație este aceea de e-banking în care trecerea de la utilizarea de carduri de credit s-a transferat către domeniul tranzacțiilor pe internet, lucru valabil și pentru transferul de bani.
Acesta a fost momentul în care tranzacțiile trebuie să fie securizate și a determinat apariția Smartcard-ului, a cărui origine este Europa.



Possibilities for using NFC technology in our daily lives are numerous

[3] https://www.ifixit.com/Teardown/Nexus+S+Teardown/4365

NFC este un set de tehnologii wireless cu rază scurtă, care necesită de obicei o distanță de 10 [cm] sau mai puțin. NFC operează la 13,56 [MHz] pe ISO / IEC 18000-3 interfață aer și la rate variind de la 106÷424 [kbit/s].

NFC implică întotdeauna un inițiator și un obiectiv; inițiatorul generează în mod activ un câmp RF care poate alimenta o țintă pasiv. Acest lucru permite obiectivelor NFC de a lucra cu factori de formă foarte simplă, cum ar fi etichete, autocolante, brelocuri, sau carduri care nu necesită baterii. Este posibilă comunicarea NFC peer-to-peer, cu condiția ca ambele dispozitive să fie alimentate. Deja există licențe brevetate, pentru NFC, de către Agenția de Brevete din Franța, care vin în completare la fondul de brevete creat în 2011. În continuare această tehnologie este în cercetare de dezvoltare al Via Licensing Corporation, o filială independentă de Dolby Laboratories, încheiat în mai 2012. De asemenea există biblioteci publice independente de platforma NFC distribuite sub GNU în mod gratuit. NFC conține date, doar pentru citire, dar poate fi și rewriteable. Acestea pot fi personalizate, codificate de către producătorii lor sau de specificațiile oferite de Forumul NFC, o asociație însărcinată cu promovarea tehnologiei și stabilirea standardelor cheie. Tag-urile NFC pot stoca în siguranță, date cu caracter personal, cum ar fi informații de debit și carduri de credit, date program de fidelitate, PIN și contacte în rețea, printre alte informații. NFC Forum definește patru tipuri de etichete care oferă diferite viteze de comunicare și capacități în ceea ce privește configurabilitate, memorie, securitate, păstrarea datelor si rezistenta scriere.

Speed	Active device	Passive device
424 kbit/s	Man, 10% ASK	Man, 10% ASK
212 kbit/s	Man, 10% ASK	Man, 10% ASK
106 kbit/s	Modified Miller, 100% ASK	Man, 10% ASK

Ca și în tehnologia cardurilor de proximitate, NFC produce o inducție magnetică între două antene tip buclă situate în câmpul de contact, formând în mod eficient un transformator. Acesta funcționează în cadrul frecvențelor radio de bandă ISM disponibil la nivel global și fără licență pentru frecvența de 13,56 MHz. Cea mai mare parte a energiei RF este concentrată în gama de lățime de bandă ± 7 [kHz], dar pachetul spectral complet poate fi la fel de mare ca 1,8 [kHz], atunci când se utilizează ASK modulare.

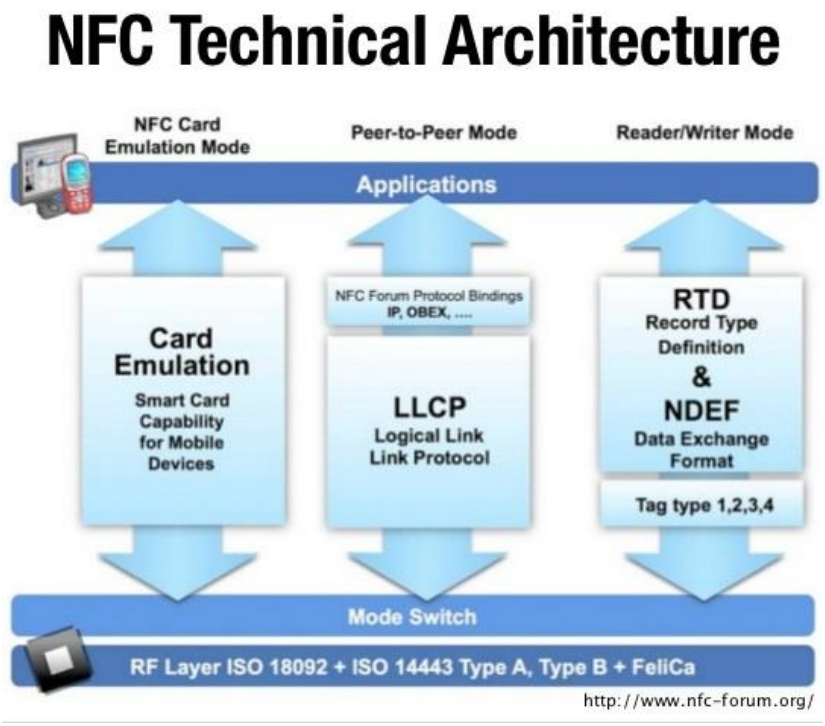
Distanța teoretică de lucru cu antene standard, compact: până la 20 [cm], distanța de lucru practică este de aproximativ 4 [cm], cu rate de transfer de date: 106÷212÷424 de [kbit/s] (rata de biți 848 kbit / s nu este în conformitate cu standardul ISO / IEC 18092).

Există două moduri:

Modul de comunicare pasivă: Dispozitivul inițiator oferă un câmp purtător și primește răspunsuri de la dispozitivul țintă prin modularea domeniului existent. În acest mod, aparatul țintă poate obține puterea de funcționare

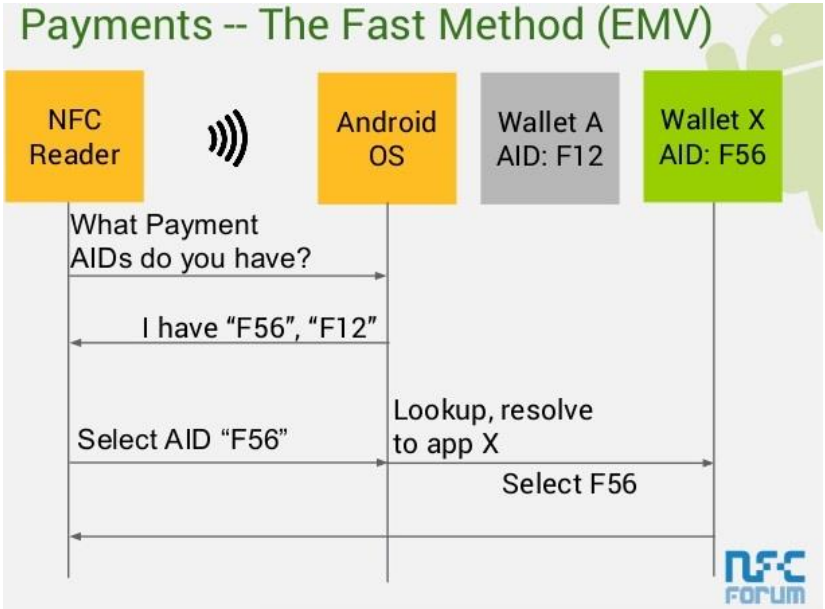
de la câmpul electromagnetic furnizat de inițiator, transformând astfel dispozitivul țintă într-un transponder.

Modul de comunicare activă: Atât inițiatorul cât și dispozitivul țintă comunică prin generarea alternativă a domeniilor de lucru. Un dispozitiv dezactivează domeniul său RF în timp ce așteaptă să primească date. În acest mod, ambele dispozitive au de obicei surse de alimentare.



4.1 Standarde NFC

Standardele NFC acoperă protocoale de comunicații privind schimbul de date, și se bazează pe standardele existente de identificare prin radiofrecvență (RFID), inclusiv ISO / IEC 14443 și FeliCa. Standardele includ ISO / IEC 18092 și cele definite de Forumul NFC, care a fost fondat în 2004 de către Nokia, Philips Semiconductors (devenit NXP Semiconductors din 2006) și Sony, și are în prezent mai mult de 160 de membri.



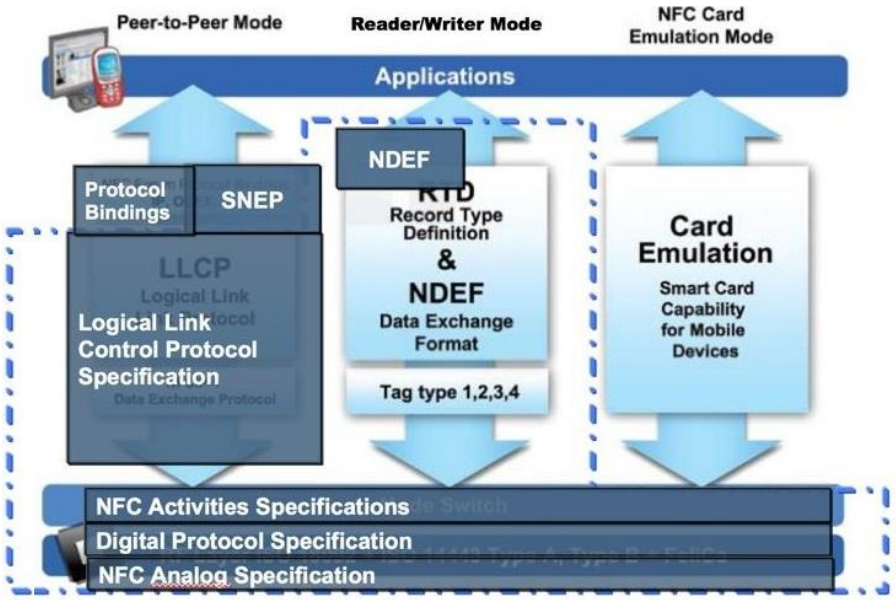
Forum-NFC promovează, de asemenea, NFC și certifică respectarea dispozitivului și dacă se potrivesc criteriilor pentru a fi considerat o rețea personală. În plus față de Forumul NFC, GSMA a lucrat pentru a defini o platformă pentru implementarea de „*standarde GSMA NFC*” în telefonia mobilă. Eforturile GSMA includ „Servicii de încredere Manager”, protocoale, testare și certificare, „*elemente securizate*”. Standardele GSMA privind protocoalele NFC, pentru telefonia mobilă nu sunt nici exclusive, nici universal acceptate. De exemplu, implementarea Google de tip card-gazdă se realizează pe principiul emulării pe Android KitKat, care prevede un control de software de radio universal. În acest „*HCE Implementation Android*”, protocolul NFC este ca un efect de pârghie fără standarde GSMA.

4.1.1 ISO/IEC

NFC este standardizată în ECMA-340 și ISO/IEC18092. Aceste standarde specifică schemele de modulare, codificare, vitezele de transfer și formatul cadru al interfeței RF de dispozitive NFC, precum și schemele de inițializare și condițiile necesare pentru coliziunea datelor de control la inițializare pentru ambele moduri NFC: ***pasive*** și ***active***. Mai mult decât atât, ele definesc, de asemenea, protocolul de transport, inclusiv activarea protocoalelor și metodelor de schimb de date. Interfața de transmisie wireless pentru NFC este standardizată în:

- ISO/IEC18092/ECMA-340: NFC Interface și Protocolul-1 (NFCIP-1);
- ISO/IEC21481/ECMA-352: NFC Interface și Protocolul-2 (NFCIP-2).

NFC include o varietate de standarde existente, inclusiv ISO/IEC 14443, atât de tip A, tip B, și FeliCa. Telefoanele pot utiliza NFC la un nivel de bază, cu sistemele de citire existente. În „*modul de emulare*” NFC lucrează ca un dispozitiv ce transmite, cel puțin, un număr unic de identificare al unui cititor existent. În plus, Forumul NFC a definit un format de date comun numit NFC Format pentru Schimbul de Date NDEF (NFC Data Exchange Format), care poate stoca și transporta diferite tipuri de articole, de la orice obiect MIME-dactilografiate la ultra-scurt CDT-documente, cum ar fi adrese URL. NFC Forum a adăugat și Protocolul de Liber Schimb NDEF SNEP (Simple NDEF Exchange Protocol), care permite transmiterea și primirea de mesaje între două dispozitive NFC.




```
import nfc
import nfc.snep

class DefaultSnepServer(nfc.snep.SnepServer):
   def __init__(self, llc):
      nfc.snep.SnepServer.__init__(self, llc, "urn:nfc:sn:snep")

   def put(self, ndef_message):
```

```
        print "client has put an NDEF message"
        print ndef_message.pretty()
        return nfc.snep.Success

def startup(llc):
    global my_snep_server
    my_snep_server = DefaultSnepServer(llc)
    return llc

def connected(llc):
    my_snep_server.start()
    return True

my_snep_server = None
clf = nfc.ContactlessFrontend("usb")
clf.connect(llcp={'on-startup': startup, 'on-connect': connected})

class DefaultSnepServer(nfc.snep.SnepServer):
    def __init__(self, llc):
        nfc.snep.SnepServer.__init__(self, llc, "urn:nfc:sn:snep", 10*1024)

import nfc
import nfc.snep
import threading

def send_ndef_message(llc):
    sp = nfc.ndef.SmartPosterRecord('http://nfcpy.org', title='nfcpy home')
    snep = nfc.snep.SnepClient(llc)
    snep.put( nfc.ndef.Message(sp) )

def connected(llc):
    threading.Thread(target=send_ndef_message, args=(llc,)).start()
    return True

clf = nfc.ContactlessFrontend("usb")
clf.connect(llcp={'on-connect': connected})

import nfc
import nfc.snep
import threading

server = None

def send_ndef_message(llc):
    sp = nfc.ndef.SmartPosterRecord('http://nfcpy.org', title='nfcpy home')
    snep = nfc.snep.SnepClient(llc)
    snep.put( nfc.ndef.Message(sp) )

def startup(clf, llc):
    global server
    server = nfc.snep.SnepServer(llc, "urn:nfc:sn:snep")
    return llc

def connected(llc):
    server.start()
    threading.Thread(target=send_ndef_message, args=(llc,)).start()
    return True
```

```
clf = nfc.ContactlessFrontend("usb")
clf.connect(llcp={'on-startup': startup, 'on-connect': connected})

import nfc
import nfc.snep

class PrivateSnepServer(nfc.snep.SnepServer):
    def __init__(self, llc):
        self.ndef_message = nfc.ndef.Message(nfc.ndef.Record())
        service_name = "urn:nfc:xsn:nfcpy.org:x-snep"
        nfc.snep.SnepServer.__init__(self, llc, service_name, 2048)

    def put(self, ndef_message):
        print "client has put an NDEF message"
        self.ndef_message = ndef_message
        return nfc.snep.Success

    def get(self, acceptable_length, ndef_message):
        print "client requests an NDEF message"
        if ((ndef_message.type == '' and ndef_message.name == '') or
            ((ndef_message.type == self.ndef_message.type) and
             (ndef_message.name == self.ndef_message.name))):
            if len(str(self.ndef_message)) > acceptable_length:
                return nfc.snep.ExcessData
            return self.ndef_message
        return nfc.snep.NotFound

def startup(clf, llc):
    global my_snep_server
    my_snep_server = PrivateSnepServer(llc)
    return llc

def connected(llc):
    my_snep_server.start()
    return True

my_snep_server = None
clf = nfc.ContactlessFrontend("usb")
clf.connect(llcp={'on-startup': startup, 'on-connect': connected})

import nfc
import nfc.snep
import threading

def send_ndef_message(llc):
    sp = nfc.ndef.SmartPosterRecord('http://nfcpy.org', title='nfcpy home')
    snep = nfc.snep.SnepClient(llc, max_ndef_msg_recv_size=2048)
    snep.connect("urn:nfc:xsn:nfcpy.org:x-snep")
    snep.put( nfc.ndef.Message(sp) )

    print "*** get whatever the server has ***"
    print snep.get().pretty()

    print "*** get a smart poster with no name ***"
    r = nfc.ndef.Record(record_type="urn:nfc:wkt:Sp", record_name="")
    print snep.get( nfc.ndef.Message(r) ).pretty()
```

```
    print "*** get something that isn't there ***"
    r = nfc.ndef.Record(record_type="urn:nfc:wkt:Uri")
    try:
        snep.get( nfc.ndef.Message(r) )
    except nfc.snep.SnepError as error:
        print repr(error)

def connected(llc):
    threading.Thread(target=send_ndef_message, args=(llc,)).start()
    return True

clf = nfc.ContactlessFrontend("usb")
clf.connect(llcp={'on-connect': connected})
```

4.1.2 GSMA

Asociația GSM (GSMA) este asociația comerțului mondial, reprezentând aproape 800 de operatori de telefonie mobilă și mai mult de 200 de produse și servicii pentru companii din 219[4] de țări. Mulți dintre membrii săi au condus studii NFC în lume și se pregătesc acum de servicii pentru lansarea comercială.

Setarea standard: GSMA este în curs de dezvoltare pentru certificare și testare în baza standardelor pentru a asigura interoperabilitatea globală a serviciilor NFC.

Pay-Buy-Mobile: urmărește să definească o abordare globală comună pentru a utiliza NFC, este o tehnologie pentru a lega dispozitive mobile cu sistemele de plăți și contactless. AT & T, Verizon si T-Mobile au lansat o companie mixtă, care intenționează să dezvolte o platformă unică bazată pe NFC, caietul de sarcini poate fi utilizat de către clienții acestei companii pentru a face plăți prin telefonul mobil. Noua societate, cunoscută sub numele de Isis Mobile Wallet sau ca Softcard, se ocupă de implementarea la scară largă a tehnologiei NFC, care permite telefoanelor mobile NFC să funcționeze în mod similar cu cardurile de credit.

4.1.3 StolPaN

StoLPaN (Store Logistics and Payment with NFC) este un consorțiu pan-european susținut de programul Information Society Technologies al Comisiei Europene. StoLPaN va examina potențialul încă neexploatat pentru noul tip de interfață wireless locale, NFC și comunicații mobile.

4.1.4 NFC Forum

NFC Forum este o asociație non-profit fondată pe 18 martie 2004, prin NXP Semiconductors, Sony și Nokia, cu scopul de a avansa utilizarea de NFC cu rază scurtă de interacțiune fără fir pentru industria de electronice, dispozitive mobile și PC-uri. NFC Forum promovează punerea în aplicare și standardizarea tehnologiei NFC pentru a asigura interoperabilitatea între dispozitive și servicii. Din iunie 2013, Forumul NFC are peste 190 de companii membre.

4.1.5 ETSI/SCP (Inteligent Platforma Card)

Se ocupă cu realizarea de interfețe specifice între cartela SIM și chipset-ul NFC.

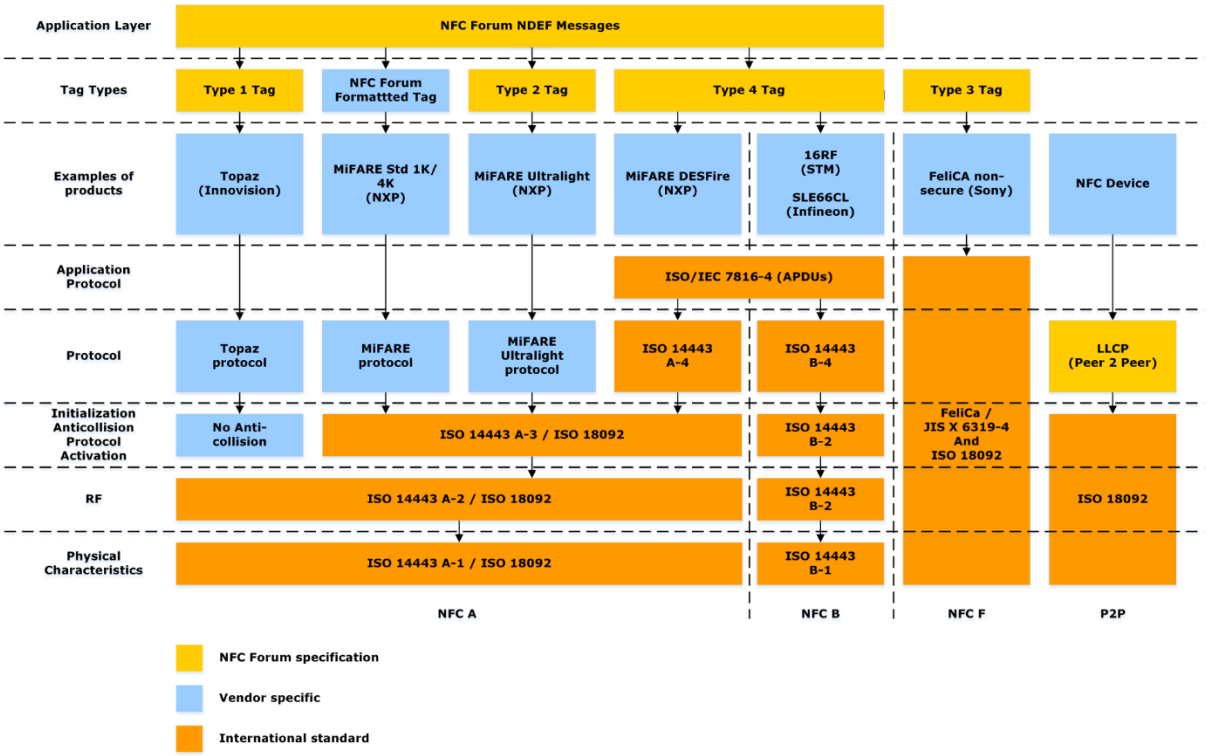
4.1.6 GlobalPlatform

Se ocupă de realizarea unei arhitecturi multi-aplicație a elementelor de siguranță.

4.1.7 EMVCo

Studiază impactul asupra cererilor de plată EMV

[4] https://dan-caragea.ro/blog/2015/09/17/cate-tari-sunt-in-lume/


Application Layer
NFC Forum NDEF Messages
Tag Types
Type 1 Tag
NFC Forum Formattted Tag
Type 2 Tag
Type 4 Tag
Type 3 Tag
Examples of products
Topaz (Innovision)
MiFARE Std 1K/ 4K (NXP)
MiFARE Ultralight (NXP)
MiFARE DESFire (NXP)
16RF (STM)
SLE66CL (Infineon)
FeliCA non-secure (Sony)
NFC Device
Application Protocol
ISO/IEC 7816-4 (APDUs)
Protocol
Topaz protocol
MiFARE protocol
MiFARE Ultralight protocol
ISO 14443 A-4
ISO 14443 B-4
LLCP (Peer 2 Peer)
Initialization Anticollision Protocol Activation
No Anti-collision
ISO 14443 A-3 / ISO 18092
ISO 14443 B-2
FeliCa / JIS X 6319-4 And ISO 18092
RF
ISO 14443 A-2 / ISO 18092
ISO 14443 B-2
ISO 18092
Physical Characteristics
ISO 14443 A-1 / ISO 18092
ISO 14443 B-1
NFC A
NFC B
NFC F
P2P
NFC Forum specification
Vendor specific
International standard

5. TEHNOLOGIA SMARTCARD: afaceri și consum, aspecte în cadrul UE

5.1 Smartcard

Cardurile inteligente[5] sunt setate sa revoluționeze sistemele tranzacționale în următorii câțiva ani. Oferind sisteme sigure, de încredere pentru cetățenii europeni sub a cărui protecție va fi stimulat comerțul electronic și mobil.

Viziunea e-Europe este de a face cu adevărat o societate informațională reală și inițiativa Europeană privind cardurile inteligente joacă un rol important. Activitatea europeană care urmărește să promoveze dezvoltarea Smartcard, este structurată în jurul a cinci aspecte-cheie:

- Legislație;
- interoperabilitate/standardizare/certificare;
- comerț electronic;
- probleme de consum;
- îmbunătățirea serviciilor publice.

Până nu demult, efortul de a dezvolta o legislație care să reglementeze dezvoltarea și gestionarea sistemelor de carduri inteligente nu a fost un efort concertat. Cadrul relevant de reglementare în UE constă din directivele e-Signature, e-Commerce, e-Copyright, e-Money, privind protecția datelor, jurisdicția și legislația aplicabilă, considerații privind impozitarea indirectă și problemele de Servicii financiare.

Un organism impresionant de cercetare-dezvoltare și de consultare a fost realizat în Europa, care va facilita procesele de standardizare Smartcard, interoperabilitate și certificare. În cadrul acestei mișcări principale de dezvoltare pentru Smartcard se vor identifica și propune: procese de identificare, carduri multifuncționale inteligente, dezvoltarea unui cititor de carduri generic pentru a fi utilizat de către toate sistemele și tehnologia contactless.

Principala activitate se învârte în jurul dezvoltatorului e-Europa SmartCard (TB):

- identitate publică (TB1);
- identificare și autentificare (TB2);
- protecția, certificarea și securitatea fiecărui profil în parte (TB3);
- card reader (TB4);
- e-payment și m-payment (TB5);
- cardurile inteligente contactless (TB6);
- sistemul Multi-Application (TB7);
- cerințele de utilizare (TB8);
- transportul public (TB9);
- e-Guvernare (TB10);
- e-Sănătate (TB11)
- semnătura electronică avansată (TB12).

Toate acestea reprezintă preocupări destinate dezvoltării de soluții pentru e-identity, e-autentification, e-signature și e-certification.

Activitatea acestor deschizători de drumuri este legată de semnătura electronică EESSI (European Electronic Signature Standardisation Initiative).

Un proiect european important legat de aceste deschideri este EUROSMART. Un alt proiect care este în curs de dezvoltare este un modul de autentificare NAME.ES, pentru care până în prezent au fost realizate deja un număr mare de standarde. Un interes major îl reprezintă CWA 141172, care oferă îndrumări cu privire la modul de a facilita standardizarea semnăturilor electronice.

[5] http://www.lindamacaulay.com/upload/resource/7_4smartcardtechconsumerissuesfull.pdf

Infrastructura pentru cheile publice va juca un rol hotărâtor în viitor, drept pentru care se generează permanent proceduri de identificare și de certificare.

Generalizarea Card Reader (TB4) se referă la dezvoltarea, standardizarea și punerea în aplicare a unui sistem generic, interoperabil de SmartCard.

În principiu proiectul dezvoltatorilor este FINREAD, ale cărui specificații de dezvoltare sunt în lucru pentru un FINREAD multi-canal care să asigure citirea de carduri inteligente.

Cele trei părți principale ale acestui proiect FINREAD se referă la: înglobare, nivel de încredere și portofoliu. FINREAD este bine dezvoltată și a fost dezvoltat un CWA 14174 care definește caracteristicile cheie ale unui cititor de carduri generice inteligente care acoperă cerințele utilizatorilor, compatibilitate, standardizare și preț de cost.

Cardurile inteligente (TB6) fără contact sunt în continuare în proces de dezvoltare și interoperabilitate contact tehnologie SmartCard. Proiectul științific Eurosmart își propune să faciliteze punerea în aplicare pe scară largă de carduri inteligente fără contact.

CLUB (the Contactless Users Board) acționează ca un forum important pentru promovarea adoptării tehnologiei fără contact. Multe dintre proiectele de transport public vizualizează carduri inteligente fără contact ca element cheie de astfel de servicii. Un număr de standarde au fost produse de către ISO/IEC JTC SC17 cu privire la tehnologia fără contact (ISO/IEC 14443, 15693, 10373).

Sistemul Multi-Application (TB7) este un dezvoltator extrem de important de investigare al aspectelor tehnice, de afaceri și a consumatorilor legați de detașarea de carduri inteligente multi-aplicație, reprezentând următoarea generație de inovații SmartCard.

Platforma ETSI inteligent Card, Card de Forumul Java, Platforma Global, MULTOS, EMV Co. și workshop-PC/SC sunt jucători importanți în dezvoltarea și interoperabilitatea cardurilor inteligente multi-aplicație (și-au dezvoltat propriile standarde).

Proiectul SmartCities reprezintă o punere în aplicare a unui proiect pilot cheie a unui SmartCard multifuncțional proiectat pentru a îmbunătăți calitatea serviciilor pentru cetățeni și de a utiliza capacitățile de colectare a datelor de pe cardurile inteligente pentru modernizarea și îmbunătățirea serviciilor existente conform nevoilor utilizatorilor.

Cardurile inteligente pot oferi dimensiunile Europene asupra dezvoltării e/m-commerce. Cu toate acestea, există o serie de provocări cu care se confruntă organizațiile care doresc să facă e/m-commerce.

Căutarea de un model de afaceri de succes a indicat necesitatea unei abordări pro active care să cuprindă tehnologia la un nivel strategic, mai degrabă decât ca un sistem reactiv. Un model de succes va fi construit pe o bună înțelegere a consumatorului, furnizarea de un serviciu complet, atenție la imagine și branding, dezvoltare de interfața cu utilizatorul-sistem, educația și dezvoltarea de tehnologii de consum pentru a satisface nevoile consumatorilor.

Este necesar să se evalueze receptivitatea pieței la tehnologia SmartCard, atât în termeni de receptivitate a consumatorilor și starea de tehnologie și infrastructură pentru a sprijini noi inovații existente. O abordare iterativă este indicată, de exemplu, prin introducerea de e-bag în scopul de a asigura o tranziție lină a cardurilor Multi-Funcționale.

În cadrul e/m-commerce băncile se confruntă cu o concurență mai mare din partea altor furnizori de servicii, așa-numitele non-bănci, care poate utiliza o strategie go-it oferind singure atât servicii de telecomunicații cât și servicii de plată.

Cu toate acestea, modelele de afaceri de succes sunt susceptibile de a fi bazate pe alianțe strategice între non-bănci și bănci - utilizând punctele forte ale fiecărui. Cu toate acestea, o analiză atentă trebuie acordată problemelor de gestionare a cardurilor în astfel de alianțe. În afară de aceste probleme, este necesar de a promova interoperabilitatea între sistemele e/m-commerce; în caz contrar ele nu sunt susceptibile de a răspunde așteptărilor și nevoilor consumatorilor.

e-payment și m-payment (TB5) este o inițiativă majoră de lucru în vederea promovării de e/m-commerce. Forumul Mobey se ocupă de tranzacțiile electronice mobile (TEP), care împreună cu Platforma ETSI inteligent Card reprezintă cea mai importantă alianță din acest punct de vedere. Ea poate genera specificații pentru standardizarea e/m-commerce și dezvoltarea unor modele de afaceri conexe.

Este necesară o bună înțelegere a problemelor majore de consum (persoane fizice și comercianți), care joacă un rol în adoptarea inovațiilor cardurilor inteligente, pentru dezvoltarea unui model bazat pe perspective multi-grup.

Inovațiile în domeniul SmartCard trebuie să adauge valoare procesului tranzacțional, inclusiv comoditate, beneficii economice și opțiuni de personalizare. Mai mult, este necesar de a înțelege filozofiile de gestionare a banilor consumatorilor și modul în care această gestionare ar putea afecta adoptarea de către aceștia a cardurilor inteligente. O înțelegere a acestor probleme poate ține de marketing pentru a îmbunătăți imaginea SmartCard pentru grupuri diverse.

Caracteristicile de punere în aplicare a Smart Card necesită o analiză atentă, deoarece acestea pot afecta masa critică. Implementatorii ar putea dori să utilizeze aspecte de învățare sociale în scopul de a contribui la atingerea masei critice. O înțelegere a culturilor de plată predominante vor fi de asemenea utile în a înțelege ce obstacole trebuie prevăzute în programele de punere în aplicare SmartCard.

Au fost identificate mai multe bariere în calea utilizării NFC: securitatea vieții private, încredere, costuri tranzacționale, calitatea serviciilor și cerințele utilizatorilor din interfața cu utilizatorul-sistem.

Cerințele de utilizare (TB8) se concentrează pe cerințele utilizatorilor la interfața cu utilizatorul-sistem. Acesta a identificat un model de comportament al utilizatorilor într-o încercare de a înțelege cum interacționează consumatorul cu sistemul smartcard. SATURN, la workshop-ul CEN/ISS pentru User Related Information (URI) și ETSI Human Factors Committee (ETSI TC/HF) sunt proiecte majore pentru acest nou început.

SATURN a identificat cerințele utilizatorilor grupurilor vârstnice și cu handicap, în scopul de a informa proiectanții de smartcard să adapteze tehnologia smartcard. Într-adevăr, tehnologia smartcard va avea cel mai mare impact asupra calității vieții acestor grupuri.

Proiectul URI lucrează la elaborarea de standarde pentru cartele inteligente multi-aplicație în ceea ce privește informațiile legate de utilizator. ETSI TC/HF este preocupat de păstrarea abilități de manipulare în conformitate cu tehnologia emergentă și are în prezent în curs de dezvoltare cinci standarde (STF 180-184). Design-ul este conceput, astfel încât, să fie accesibil tuturor utilizatorilor. e-Europa încearcă să utilizeze carduri inteligente pentru a îmbunătăți serviciile publice pentru toți cetățenii europeni.

Accentul principal până în prezent a fost pe dezvoltarea de aplicații smartcard în transportul public (TB9), care este privit ca un motiv cheie de depunere a datelor pentru dezvoltarea de smart card tehnologic. CALYPSO, are o evoluție în cadrul acestui sistem nou de deschidere de drumuri.

e-Guvernare (TB10) are ca scop modernizarea serviciilor publice locale și naționale să promoveze legăturile între statele membre.

În special, Sănătate (TB11) are ca scop dezvoltarea de servicii de administrare și cărți de identitate de sănătate.

Începând cu anul 2003 la nivel European s-a demarat implementarea masivă de smartcarduri. Provocarea va fi de a combina rezultatele într-un întreg coerent care va informa următoarea generație de aplicațiile specifice smartcard-urilor.

5.2 NFC – Near Field Communication – noi deschideri[6]

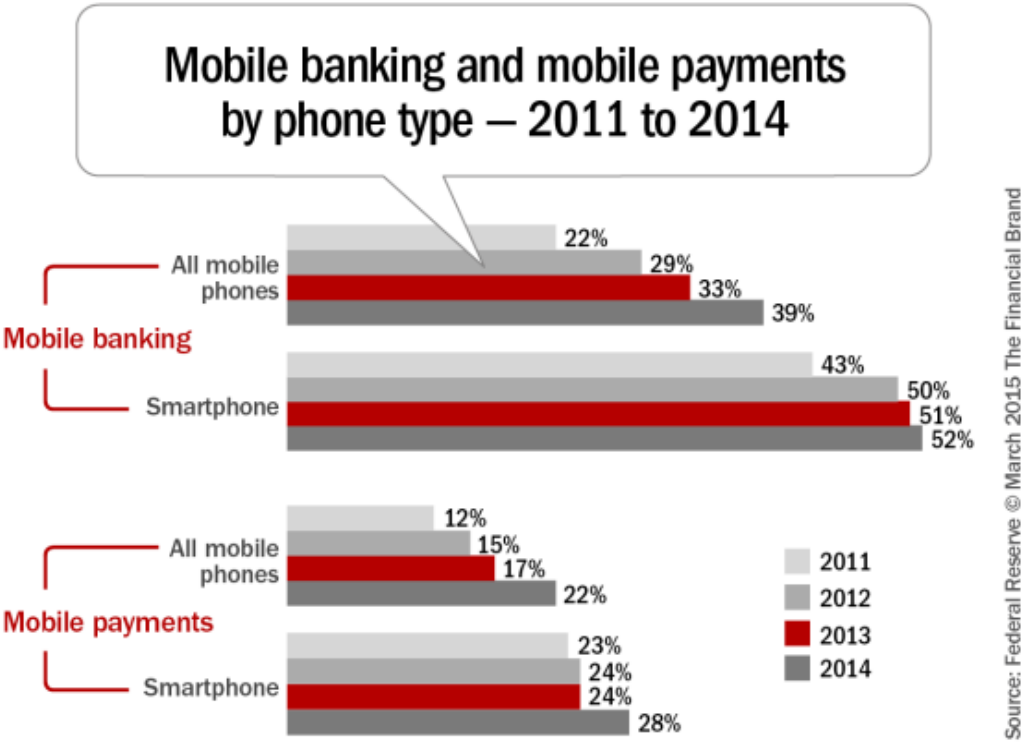
Parteneriatul **Vengo și Signal360**[7] introduce noi compatibilități mobile iBeacon™ și extind capabilitățile automatelor de a efectua tranzacții cu consumatorii. Automatele Vengo sunt în prezent în primele loc în New York, Chicago, Boston și cu planuri de a extinde rețeaua de alte 3 orașe în următoarele 6 luni, automatele utilizate de către birouri, baruri și mall-uri,. Acest parteneriat marchează introducerea primelor automate iBeacon™ și Sonic capabile să suporte o conectivitate mobilă și interactivitate atunci când un utilizator este în imediata apropiere a unui automat Vengo.

[6] *Copyright 2015. NFC Bootcamp. All rights reserved.*, https://www.nfcbootcamp.com/industry/
[7] http://www.prweb.com/releases/2015/04/prweb12633393.htm

OneSwipe[8] este un instrument nou pentru securizarea NFC făcând parolele inutile: Un smartphone va avea acces, în loc de parole lungi, prin soluții de autentificare de tip SecurEnvoy. Noul instrument de autentificare OneSwipe NFC-based, este construit pe noul sistem de comunicare de câmp apropiat (NFC) sub platforma Windows 10, care va permite utilizatorilor să se autentifice doar prin atingerea smartphone-urilor, în loc de a scrie parole lungi. Principiul de funcționare este următorul: se selectează contul pe care doresc să-l activeze, apoi se introduce un cod PIN de patru cifre și apoi OK la smartphone-ul pentru a activa contul pentru Windows 10 al tabletei sau PC-ului.

Procesul va lansa automat URL-ul ales în browser și automat jurnalele în cont. Tehnologia OneSwipe utilizează un cod QR, care este generat la fiecare treizeci secunde pe dispozitivul utilizatorului, și în loc de NFC, utilizatorii trebuie să arate codul camerei de pe alculator pentru a avea acces la cont.

Utilizarea Mobile Banking și-a atins gradul de saturație (maturare)?[9]: Un raport Federal Reserve arată că o creștere a plăților e-Banking și prin intermediul telefoniei mobile a crescut semnificativ în corelație cu dreptul de proprietate a smartphone-urilor. Nivelul de confort cu mobile banking este de asemenea în creștere, datorită capacităților extinse oferite prin intermediul unui dispozitiv mobil. Dar utilizarea de e-Banking și-a atins nivelul maxim? Conform Rezervei Federale 2015 s-a realizat următorul grafic.



MobiKwik[10]**,** societatea de portofele mobile a investit aproape de $ 25M în finanțarea seriei B: Tree line Asia, Sequoia, Cisco, Amex. Compania a declarat ca va utiliza fondurile pentru investiții în tehnologia de analiză date, construirea unui nou brand și o creștere a rețelei de utilizatori și comercianți. Investițiile American Express și Cisco par în conformitate cu promovarea obiectivelor de stimulare a ritmului de creștere a plăților mobile din India și cu un accent pe mobilitate și IO.

Revoluția treptată a serviciilor digitale[11]: *THE MEDIA YEARBOOK*: apariția tehnologiei digitale a "revoluționat" la nivel internațional OOH (out of home) industria mass-media, în

[8] http://www.cbronline.com/news/cybersecurity/physical/oneswipe-and-youre-in-new-securenvoy-nfc-tool-makes-passwords-useless-4548566
[9] http://thefinancialbrand.com/51255/mobile-banking-usage-report-fed/
[10] http://yourstory.com/2015/04/mobikwik-series_b-funding/
[11] http://themediaonline.co.za/2015/04/29642/

conformitate cu Nancy Fletcher, președinta și directoarea executivă a Asociației de Publicitate pentru Exteriorul Americii (OAAA) a precizat că:

- „*eforturile în acest sens vor înregistra o creștere mai mare în 2015*";
- „*există premisele ca în viitorul apropriat să apară mult mai multe instalații OOH digitale ale căror utilizări să fie influențate de conexiunile din sociale mass-media, care să permită deservirea consumatorilor, cum ar fi stațiile de autobuz*".

Publicité EXTERIEURE (FEPE), organismul internațional al industriei OOH, a declarat că 2015 va aduce mai multe panouri publicitare digitale și utilizarea tehnologiei fără fir în sensul de a valorifica sinergia cu telefonia mobilă. El spune că ar putea fi mai mult utilizată NFC – cu o rază scurtă de conexiune wireless low-power, care va putea transfera cantități mici de date între două dispozitive - dacă Apple va permite cip NFC în noul iPhone pentru a folosi mai mult sistemul lor de plată. Pe măsură ce societatea noastră devine mai dependentă de telefonia mobilă, industria OOH, SUA va oferi consumatorilor mai multe moduri de a se angaja cu brandurile prin intermediul social media.

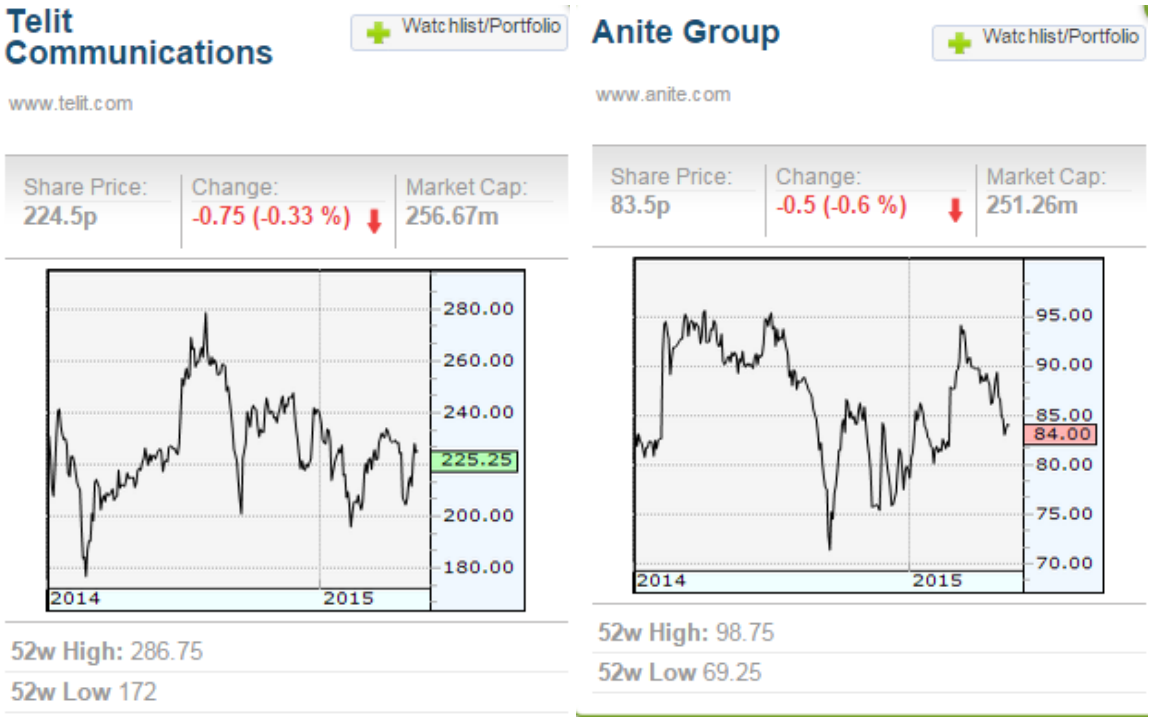
Revoluția mobilă ... 5G, IO, NFC, M2M[12]: Asistăm la o luptă pentru lățimea de bandă:

- 3G - a treia generație de tehnologii wireless - este încă puternică, oferind o lățime de bandă de transfer rapid de date, audio și video streaming și video-conferințe;
- 4G, cum s-ar aștepta, sunt mai rapide decât rețelele 3G și pot transporta mai multe date;
- 5G, în cazul în care vorbim despre „*tehnologia de rețea inteligentă*", care pare a gestiona traficul dar și pachete de prioritizare a datelor.

Conectarea la o rețea a cât mai multor mașini, vor crea probleme privind calitatea transmiterii.

Apariția 5G promite să accelereze dezvoltarea pieței de comunicare machine-to-machine (M2M), care este o veste bună pentru Telit Communications (LON: TCM), unul dintre liderii mondiali în acest domeniu. "Telit are ca scop creșterea conectivității, detectarea și automatizarea prin intermediul modulelor și serviciilor din domeniile: asistenței medicale, telematică, contorizarea inteligentă auto și alte sectoare speciale din zona serviciilor publice.

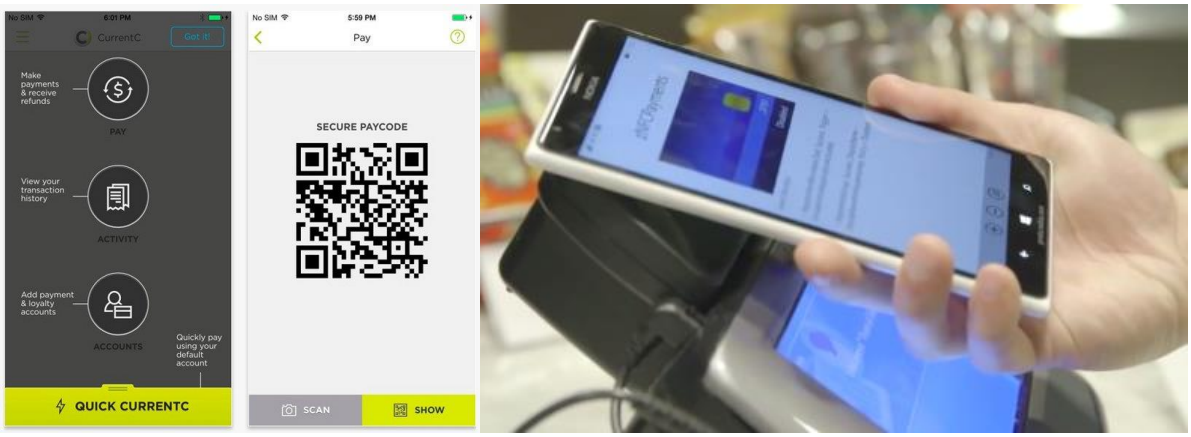
De asemenea un alt beneficiar care va avea de câștigat este Anite (LON: AIE), furnizor de soluii de testare și măsurare pentru industria wireless internațională.



[12] http://www.proactiveinvestors.co.uk/companies/news/78999/goin-mobile-5g-iot-nfc-m2m-and-other-buzzwords-of-the-modern-age-78999.html

Raport privind piața SmartCard ca portofel mobil până în 2020 - aplicații industriale, dimensiunea pieței, segmentarea, cota de companie[13]: utilizarea tot mai mare de smartphone-uri este, de asemenea, un factor de propulsie pentru piața portofelelor mobile. Progresele continue în NFC și metodele de plată sigure sunt factorii de așteptat pentru a alimenta și mai mult piața mondială cu portofele mobile. Plata cu ajutorul portofelului mobil pe baza obiectivelor de tranzacție este împărțită în plăți: persoană⇔persoană (P2P) și client⇔afaceri (C2B).

Apple a Pay - CurrentC[14]: iPhone Apple folosește în spațiul plăți prin telefonul mobil ca soluție MCX în consorțiul CurrentC. Potrivit unui raport de la MacWorld, CurrentC va fi lansat oficial pe piață în SUA. Spre deosebire de Apple, care completează operațiunile pe bază de carduri de credit și de debit prin intermediul tehnologiei NFC touchless, CurrentC se bazează pe ceea ce consideră unii a fi un mijloc mai puțin sigur de procesare a plăților. Cu tehnologia CurrentC un client folosește smartphone-ul făcând o fotografie la un cod QR, care odată generat la un punct-de-vânzare este preluat de terminale MCX. Suma de plată este dedusă direct din contul bancar al unui utilizator, care este legat de CurrentC pe banking.



Microsoft se pregătește să ofere propriul serviciu de plată mobil[15]: pentru plata cu smartphone-uri echipate cu Windows. Microsoft a reușit să intre în baza de date NMLS pentru a avea licență de a transmite bani. Obținerea acestor licențe se numără printre pașii cheie care trebuie efectuați.

Intel, Broadcom și Securitatea Plăților IO[16]: Intel și Broadcom pun accent pe facilitarea plăților sigure și mobile, IO (internetul obiectelor) continuă să crească. Intel și Ingenico Group au realizat un parteneriat pentru a dezvolta o tabletă care va sprijini NFC, Eurocard, MasterCard și Visa prin metode EMV de implementare a cipurilor pe Smartcard-urile de plată în avans, astfel încât băncile să aibă un mijloc eficient de a contracara frauda prin cardurile de credit. Broadcom a dezvoltat noi microcontrolere MCU cu suport integrat NFC pentru a permite o gamă largă de dispozitive, inclusiv conectarea celor care alcătuiesc internetul obiectelor (IO), precum și PC-uri ca punct de vânzare - terminale POS - pentru a accepta plăți prin telefonul mobil în siguranță. Noua familie BCM58100 de MCU este o extindere a portofoliului Broadcom StrataGX de chips. Cisco Systems estimează că numărul de dispozitive: sisteme și senzori de la electrocasnice, autovehicule, mașini pentru smartphone-uri, notebook-uri, sisteme industriale, echipamente medicale și tehnologii inteligente care-city care sunt conectate la Internet - va crește de la 25 de miliarde anul trecut, la peste 50 de miliarde până în 2020.

---

13 http://www.whatech.com/market-research-reports/press-release/consumer/52273-latest-report-on-mobile-wallet-market-to-2020-industry-applications-market-size-segmentation-company-share

14 http://appleinsider.com/articles/15/04/06/apple-pay-to-face-mobile-payments-competitor-currentc-in-mid-2015

15 http://www.geekwire.com/2015/regulatory-approval-shows-microsoft-gearing-up-to-offer-its-own-mobile-payment-service/

16 http://www.eweek.com/security/intel-broadcom-look-to-secure-iot-payments.html

Microcontrolere sigure cu NFC integrat[17]: Broadcom Corporation a anunțat extinderea portofoliului de StrataGX cu o nouă familie de microcontrolere extrem de sigure, care oferă o securitate avansată, performanță de neegalat și NFC integrat pentru o varietate de dispozitive conectate. Familia BCM58100 este concepută pentru terminale mPOS, calculatoare personale și alte aplicații, inclusiv produse IO. BCM58100 oferă cel mai înalt nivel de securitate pentru a proteja datele sensibile de amenințările la adresa din stratul de fizic și la cea de rețea în timp ce s-au realizat simplificări în proiectarea sistemului, reducerea amprentei și scăderea costurilor pentru producătorii de echipamente originale (OEM). Arhitectura BroadSAFE oferă protecție împotriva sabotajului sistemului de criptare, precum stocarea sigură și prelucrarea informațiilor tip date și utilizarea datelor biometrice: amprente digitale, iris, template facial. BCM58100 este în conformitate cu Standardul Federal Information Processing FIPS (Federal Information Processing Standard) și de asemenea se asigură că produsele finite respectă standardele Industriale Stricte de Plăți cu Cardul PCI DSS (Payment Card Industry Data Security Standard) și Europay, MasterCard certificări, și Visa EMV.

Sistem fizic de compensare a dispersiei electronice de 28 10^{-9} [m] - EDC

[17] https://en.ctimes.com.tw/DispProduct.asp?O=HJZ428KGBCISAA00PJ