Smart Card

Prof.dr. Floarea NĂSTASE
Catedra de Informatică Economică, A.S.E. Bucureşti

Reforms in electronic business have presented new opportunities to use smart card technology as an enabling tool. The network-centric applications, where resources are located throughout the Internet and access to them is possible from any location, require authenticated access and secured transactions. Smart cards represent an ideal solution: they offers an additional layer of electronic security and information assurance for user authentication, confidentiality, non-repudiation, information integrity, physical access control to facilities, and logical access control to an computer systems.
***Keywords**: smart card, ICC.*

Ce este un Smart Card?

Smart cardul este un dispositiv, de mărimea unei cărți de credit, care poate conține unul sau mai multe circuite integrate. Deoarece termenul de smart card este uneori ambiguu, fiind utilizat în diverse situații, ISO (Inter-national Organization for Standardization) foloseşte denumirea de card cu circuit integrat (ICC - Integrated Circuit Card). Circuitul integrat încapsulat pe smart card poate acționa ca un suport pentru memorarea datelor, ca un controller sau ca un calculator propriu-zis. La modul general, smart cardul este considerat un obiect funcțional constituit din hardware şi software şi proiectat pentru a fi utilizat pe o platformă specifică. Figura 1 prezintă arhitectura frecvent utilizată, prin care smart cardurile sunt acceptate pe un sistem desktop.

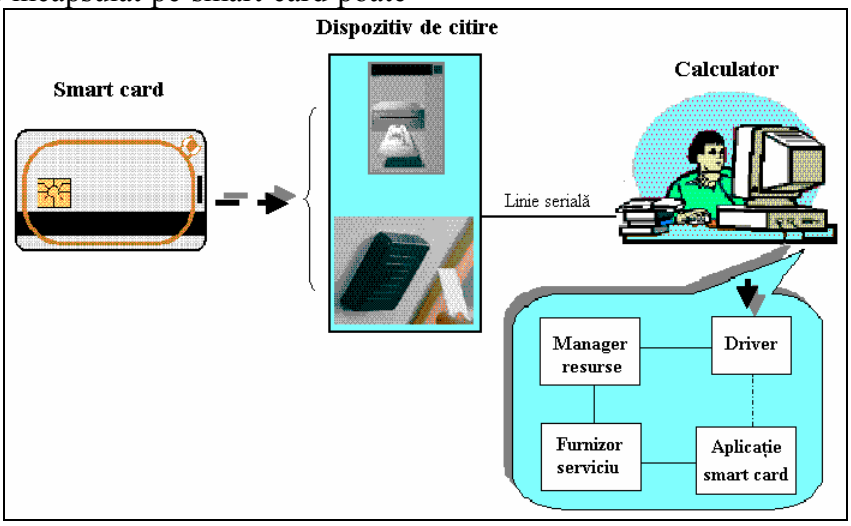

Fig.1. Arhitectura unui sistem care acceptă smart card

Cele trei componente principale suportate de o aplicație smart card sunt: furnizorul de serviciu, managerul resurselor şi driverul pentru cititorul de card.
Comunicația între aplicație şi driver se realizează, în mod indirect, prin furnizorul de serviciu care utilizează o interfață standardizată pentru managerul de resurse. În mod similar, managerul de resurse utilizează o interfață standard pentru comunicarea cu driverul. Driverul este dependent de caracteristicile cititorului de smart card, iar furnizorul de serviciu este strâns legat de caracteristicile smart cardului. Separare funcțională permite aplicației să utilizeze orice smart card cu orice cititor de card, dar să respecte condițiile disponibile pe calculatorul gazdă (impuse prin furnizorul de serviciu şi driver).

Un circuit integrat tipic de smart card conţine următoarele componente hardware şi software (figura 2):

- *componentele fizice* ale circuitului integrat sunt: unitatea centrală de procesare care poate opera pe 8 până la 32 biţi, memoria volatilă (RAM) se utilizează pentru stocarea temporară a datelor, memoria nevolatilă (ROM sau memoria flash) conţine sistemul de operare şi software de aplicaţie, spaţiu suplimentar de memorie nevolatilă care se foloseşte pentru stocarea datelor (de exemplu, memorie EEPROM - Electrically Erasable Programmable Read Only Memory), porturile de intrare/ieşire (I/E) şi logica de securitate;
- *software dedicat*, cunoscut sub denumirea de *firmware*, este deseori utilizat pentru testarea circuitului integrat, dar poate include şi servicii suplimentare;
- *sistemul de operare* include drivere de I/E şi drivere hardware, proceduri şi protocoale de I/E, proceduri pentru administrarea fişierelor şi memoriei, motor de criptare (suport pentru DES, 3DES, RSA, ECC) şi servicii care se găsesc în bibliotecă;
- *aplicaţiile native*, dacă există, au acces direct la sistemul de operare - ele pot fi instalate de fabricantul circuitului integrat sau, pot fi integrate mai târziu, în faza de personalizare a cardului;
- *interfaţa de sistem a aplicaţiilor* instalate poate conţine un încărcător, una sau mai multe maşini virtuale, manager de context;
- *aplicaţiile încărcate* realizează funcţii specializate.

Tipuri de carduri

De-a lungul timpului s-au folosit mai multe tipuri de carduri. Se poate face o scurtă clasificare a cardurilor luând în considerare anumite criterii, cum ar fi: tehnologia utilizată în fabricare, numărul aplicaţiilor care pot fi accesate, operaţiile de plată pe care le îndeplinesc, suprafaţa geografică pe care pot fi folosite etc.

Din punct de vedere *tehnologic* s-au remarcat următoarele trei categorii de carduri: cu bandă magnetică, cu circuit integrat şi optice.

Cardurile cu bandă magnetică sunt aseamănătoare cardurilor de credit folosite în prezent. Banda magnetică de pe card stochează aproximativ 130 de caractere care reprezintă informaţii privind contul şi deţinătorul de card (numele deţinătorului, numărul şi data de expirare a cardului etc.). Printr-un cititor adecvat poate fi accesată informaţia stocată pe card.

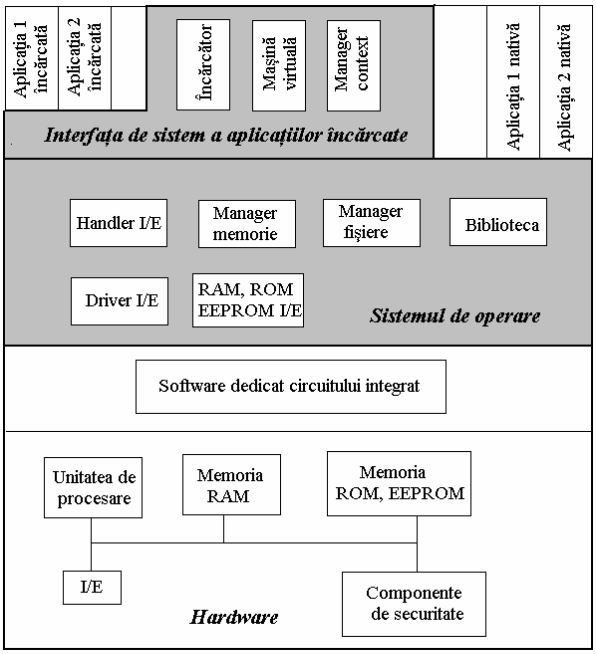

Fig.2. Componentele unui smart card

Cardurile cu circuit integrat. În funcţie de *conţinutul circuitului integrat* se identifică mai multe tipuri de carduri: numai cu memorie/cu memorie şi logică de securitate; cu memorie şi unitate centrală de prelucrare.

- *Cardurile numai cu memorie* sunt utilizate pentru aplicaţii simple, cum ar fi plata în avans a serviciilor telefonice. Un card cu memorie conţine un circuit integrat capabil să stocheze date. Cardurile cu memorie uneori necesită o baterie pe placă, pentru păstrarea datele memorate. Acest tip de card este utilizat pentru accesul deţinătorului în anumite zone restricţionate (cum ar fi accesul la locul de muncă, în biblioteci, în cluburi etc). În cazul unui card de plată electronică, o anumită valoare este stocată pe card şi acesta va putea fi utilizat până la epuizarea sumei, după care poate fi aruncat. Cardul cu memorie EEPROM are un cip care conţine informaţii ce pot fi scrise şi citite de mai multe ori. În cazul circuitelor integrate cu memorie şi lo-

gică de securitate, accesul la datele stocate este controlat.

• *Cardul inteligent (smart card)* conține un circuit integrat capabil să stocheze şi să proceseze date. Microprocesorul încorporat controlează toată informația de pe card. Un astfel de card, operează sub controlul unui sistem de operare, care este de obicei unic, fiind folosit numai de către producătorul acelui tip de card. Cardul cu microprocesor măreşte protecția împotriva fraudei şi poate fi folosit în aplicații care implică valori mari sau care necesită o securitate sporită. O aplicație, de exemplu, ar putea fi stocarea de chei criptografice, iar cardul cu cip ar putea funcționa ca un dispozitiv hardware sigur.

• *Cardul super-inteligent* (Super Smart Card) este termenul dat cardului care include tastatură, ecran LCD, baterie şi, evident, un circuit integrat capabil să stocheze şi să prelucreze date. Cardul super-inteligent, în mod normal, conține programe specializate, memorate în ROM, pentru diverse aplicații specifice, cum ar fi tranzacțiile bancare şi generarea de parole.

După modul de *activare a transferului* datelor de pe un card cu circuit integrat se diferențiază:

- *Cardurile prin contact*: pentru transmiterea datele stocate pe card este necesar ca între dispozitivul de citire şi terminalele circuitului integrat de pe card să existe contact fizic; cardurile de acest tip sunt frecvent utilizate în instituțiile financiare.

- *Cardurile fără contact* au în dotare o antenă încapsulată. Pentru transmiterea datelor cardul trebuie să fie trecut prin apropierea unui cititor de card. Cardurile fără contact sunt utilizate în mod obişnuit pentru controlul accesului şi în aplicațiile utilizate în tranzit.

- *Cardurile combinate* încapsulează două circuite integrate şi o antenă. Unul din circuitele integrate va funcționa prin contact şi cel de al doilea fără contact. Circuitele integrate nu sunt conectate între ele. Cipul care se activează prin contact va fi utilizat pentru aplicațiile care cer un grad mare de securitate. Al doilea cip se va utiliza pentru aplicațiile care solicită tranzacții rapide, cum ar fi plata taxei de autostradă.

Dacă se are în vedere *numărul aplicațiilor instalate* pe un card cu circuit integrat, există carduri cu o *singură aplicație* şi carduri cu mai *multe aplicații*. Dacă mai multe aplicații coexistă pe un acelaşi card, ele trebuie să fie compatibile. Aplicațiile care pot fi încărcate pe un smart card fac parte din următoarele categorii: credit/debit pentru afaceri bancare şi financiare, portofel electronic (valoarea fiind stocată pe card) şi programe pentru comerț electronic; procesarea tranzacțiilor din rețele, cum ar fi rețeaua de telefonie mobilă (cardurile SIM GSM), plata TV (carduri pentru abonament şi carduri de tipul "vezi-ce-plăteşti"), comunicarea virtuală (procesarea tranzacțiilor şi acces la Internet); cardurile pentru controlul accesului; carduri guvernamentale (pentru a înlocui cartea de identitate, carnetul de conducere, carnetul de sănătate etc.); comerț multimedia şi protecția drepturilor de proprietate intelectuală.

• ***Cardul hibrid*** (dual card) conține atât bandă magnetică, cât şi circuit integrat şi permite efectuarea unor operațiuni combinate, specifice fiecărui tip de card.

• ***Cardurile optice,*** denumite carduri laser, au dimensiunile standard ale cardurilor de credit. Materialul pentru card este alcătuit din mai multe straturi care reacționează când o lumină laser este direcționată către el. Suportul este scris o singură dată şi citit de mai multe ori (WORM - write-once-read-many). Informațiile stocate pe un card optic sunt: numele, adresa şi alte date personale ale deținătorului de card, fotografia şi semnătura deținătorului de card, date şi imagini medicale, informații pentru securizare etc.

Dacă se are în vedere *aspectul funcțional* al sistemului de plată prin card, diversele carduri pot fi incluse în una dintre următoarele categorii:

• ***Cardul de credit*** este cardul prin intermediul căruia deținătorul dispune de disponibilități băneşti ale emitentului, oferite sub forma unei linii de credit, care îi permit acestuia efectuarea operațiunilor de plată, retragere de numerar sau transfer de fonduri, în limita unui plafon stabilit în prealabil. În mod normal, aceste carduri au o valoare limitată, sta-

bilită de emitentul cardului, precum şi o rată a dobânzii care se aplică pentru creditul acordat. Rata dobânzii pentru sumele neachitate este de obicei de câteva ori mai mare decât rata dobânzii de bază.

• ***Cardul de credit cu depozit*** - posesorul cardului de credit depune un depozit cu o valoare între 100% şi 200% din suma dorită pentru creditare. Depozitul este păstrat într-un cont special, de economisire. Posesorul trebuie, şi în acest caz, să achite ratele împrumutului, ca şi pentru un card de credit obişnuit. Dar, dacă se întârzie cu plata, emitentul preia sumele restante din depozit, fără a mări dobânda.

• ***Cardurile de cheltuieli*** sunt similare cardurilor de credit fiind asociate unui cont special. Principala diferenţă constă în aceea că plăţile efectuate pe acest tip de card trebuie acoperite la sfârşitul unei perioade stabilite de banca emitentă.

• ***Cardurile de călătorie*** sunt carduri de cheltuiali care pot fi folosite pentru achiziţionarea de servicii de la companii aeriene, hoteluri, restaurante, companii de închiriat autovehicule etc.

• ***Cardul de debit*** este cardul prin intermediul căruia deţinătorul dispune doar de disponibilităţile băneşti proprii existente într-un cont deschis la emitent pentru efectuarea operaţiunilor de plată, retragere de numerar sau transfer de fonduri. Există două tipuri de carduri de debit: *on-line* şi *off-line*. *Cardurile de debit on-line* sunt carduri pentru ATM-uri. Ele folosesc sistemul de autentificare cu PIN (Personal Identification Number), iar debitele sunt actualizate imediat în contul posesorului. *Cardurile de debit off-line* au o limită de timp (câteva zile) sau/şi o sumă limită maximă de extragere, corespunzătoare sumei existente în cont. Pot fi relativ uşor fraudate prin falsificarea semnăturii. Tranzacţiile cu acest tip de carduri sunt reflectate în contul posesorului cu o întârziere de 2-3 zile.

• ***Cardul de debit cu facilitate de overdraft*** este cardul prin intermediul căruia deţinătorul poate dispune, pe lângă disponibilităţile băneşti proprii existente într-un cont deschis la emitent, şi de o anumita sumă, asimilată unui credit, în limita unui plafon predeterminat, acordată, de regulă, în situaţia în care drepturile băneşti ale deţinătorului (de exemplu salariul) sunt virate regulat în contul de card pentru efectuarea operaţiunilor bancare (plată, retragere de numerar sau transfer).

• ***Cardul de numerar*** este utilizabil doar la ATM sau la dispozitivele pentru retragere de numerar.

• ***Cardul de garantare a cecurilor*** este emis ca parte a unui sistem de garantare care, la prezentare alături de un cec completat şi semnat de către deţinătorul cardului, garantează că orice cec emis până la incidenţa valorii de garantare a cardului va fi onorat de banca emitentă a cecului.

• ***Cardul specific unei companii*** sau ***cardul de comerciant*** este emis de un comerciant clientului sau ori de un grup de comercianţi clienţilor lor, pentru a permite sau a facilita plăţi în vederea achiziţionării de bunuri sau servicii exclusiv de la comercianţii emitenţi sau de la cei care acceptă cardul pe bază de contract, fără a acorda accesul la un cont bancar.

• ***Cardul co-branded*** este emis de o bancă împreună cu o entitate care, de regulă, are ca obiect principal de activitate comerţul sau prestările de servicii.

Ciclul de viaţă al unui smart card

Ciclul de viaţă al unui smart card include cele cinci etape principale (figura 3):

• *fabricarea* şi testarea circuitului integrat: se adăugată cipului o cheie unică de producţie, pentru a-l proteja de modificări frauduloase până la asamblarea în materialul de plastic; sunt scrise în circuitul integrat datele de fabricaţie;

• *pre-personalizarea*: fabricantul cardului montează circuitul integrat pe suportul care poate avea inscripţionat un logo al furnizorului aplicaţiei; are loc testarea cardului; este înlocuită cheia de fabricaţie cu o cheie personalizată; nu sunt disponibile instrucţiunile de acces la memorie;

• *personalizarea*: emitentul cardului înregistrează pe card fişierele de date şi datele aplicaţiei; sunt memorate informaţiile despre identitatea deţinătorului de card, PIN-ul şi PIN-ul pentru deblocare;

• *utilizarea*: sunt activate aplicaţiile şi con-

trolul accesului la fişiere de către deţinătorul de card; accesul la informaţia de pe card este limitat prin politicile de securitatea ale aplicaţiei; furnizorul de aplicaţii poate instala pe acelaşi card mai multe aplicaţii;

• *finalul ciclului de viaţă* se atinge prin una din cele două metode:

- o aplicaţie scrie o cheie invalidă într-un fişier individual sau într-un fişier master; toate operaţiile lansate prin sistemul de operare vor fi blocate; pentru a putea face o analiză a evenimentului rămân active numai instrucţiunile de citire;
- sistemul de control blochează în mod ireversibil accesul, atât PIN-ul cât şi PIN-ul de deblocare sunt zăvorâte; toate operaţiile vor fi blocate.

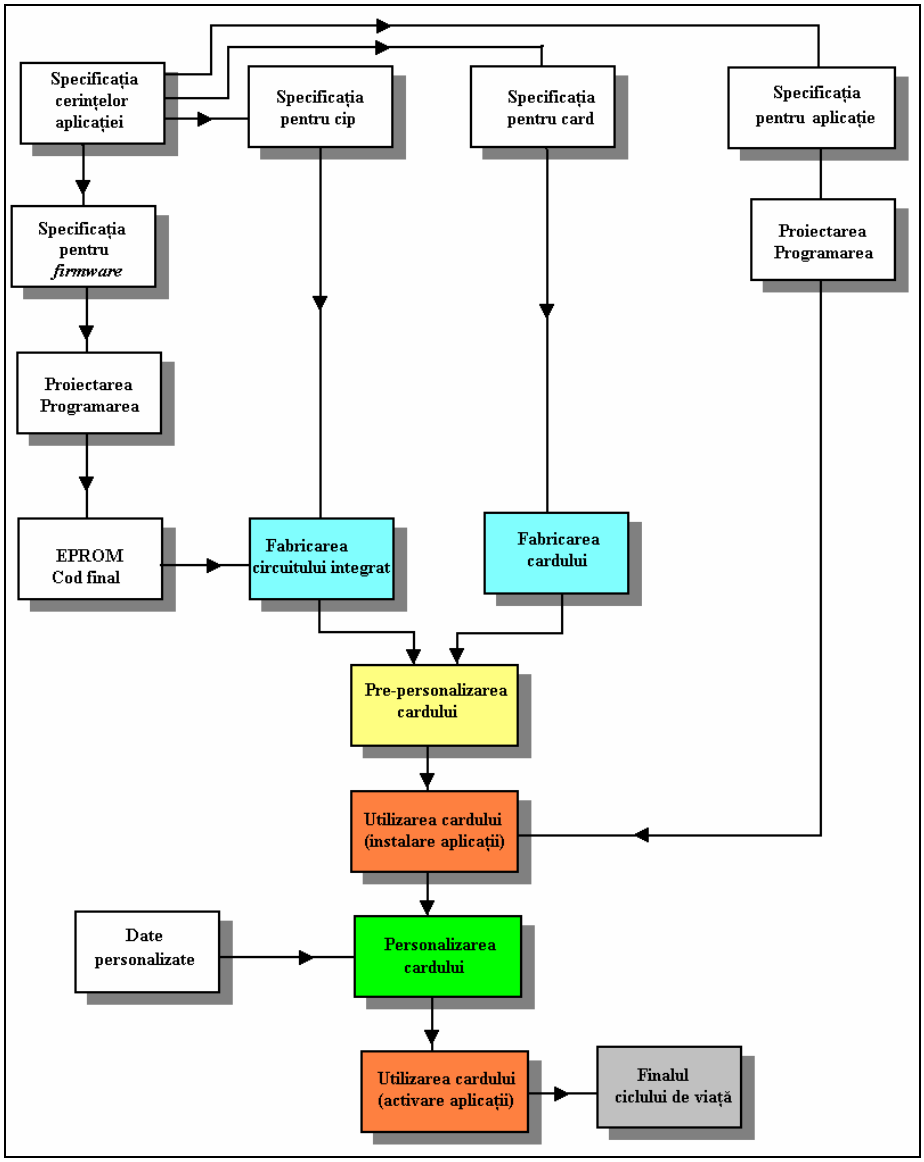

Fig. 3. Ciclul de viaţă al unui smart card

Utilizarea smart cardurilor

Tehnologia smart cardurilor oferă un set de rutine, pentru îmbunătăţirea capabilităţilor de identificare şi pot fi folosite ca instrumente în realizarea unor funcţii, cum ar fi:

Instrumente pentru controlul accesului - prin facilităţile de securitate, cardurile operează ca un token de autentificare a accesului logic la terminale şi reţele sau a accesului fizic în clădiri, camere, parcări etc.

Instrumente de plată - cardurile, prin aplicaţiile instalate, permit realizarea unor operaţii specifice unui sistem de plată, cum ar fi: creditarea, debitarea, stocarea de valori moneta-

re, accesul la conturile bancare şi transferul de fonduri între conturi.

Instrumente pentru management şi stocare a informaţiei - în funcţie de capacitatea memoriei circuitului integrat de pe card, datele sunt stocate şi utilizate pentru execuţia diverselor aplicaţii. De exemplu, informaţiile medicale de pe un smart card pot fi accesate rapid de către personalul medical autorizat, într-o situaţie de urgenţă sau la o vizită medicală de rutină. În acest fel, se reduce foarte mult timpul pentru obţinerea informaţiilor necesare în luarea unor decizii.

Instrumente pentru îmbunătăţirea capabilităţilor de acces securizat prin utilizarea unor tehnologii complexe, cum ar fi tehnologiile biometrice şi infrastructura de chei publice, pentru verificarea identităţii pentru accesul logic şi fizic. De exemplu, sistemul PKI utilizează chei publice şi private pentru semnătura digitală şi criptarea/decriptarea mesajelor de poştă electronică. Dacă la recepţionarea unui mesaj este verificată semnătura digitală a expeditorului, utilizându-se cheia lui publică, va rezulta că mesajul a fost semnat chiar de cel care pretinde că l-a trimis. Biometria utilizează caracteristicile fizice (cum ar fi: amprentarea, scanarea irisului, geometria mâinii, recunoaşterea vocii/feţei) pentru autentificarea identităţii unei persoane. PKI şi/sau biometria pot fi utilizate pentru autentificarea mai sigură a unei persoane.

Concluzie

Smart cardurile, care uneori sunt mai puternic decât primele calculatoare desktop, au şi vor avea un rol tot mai important în dezvoltarea aplicaţiilor distribuite în reţele, în special în cele mobile, care solicită acces autentificat şi tranzacţii securizate.

Bibliografie

- http://www.eurosmart.com/ - *Protection Profile Smart Card IC with Multi-Application Secure Platform*, noiembrie 2000
- http://wwws2.visa.com/nt/chip/ - Visa Integrated Card Specification: *Application Overview, Card Specification, and Terminal Specification*
- EMV Integrated Circuit Card Specification for Payment Systems: *Application Independent ICC to Terminal Interface Requirements*, Mai 2004
- EMV Integrated Circuit Card Specification for Payment Systems: *Security and Key Management,* Decembrie 2000
- FIPS PUB 186-3 - *Digital Signature Standard (DSS*), martie 2006
- CEPSCO - *Common Electronic Purse Specifications*, martie 2001
- Grant CNCSIS cod 1064/2005, Cercetări privind securitatea afacerilor electronice - *Sisteme de plăţi în afacerile electronice*, raport de cercetare
- I. Roşca, ş.a., *Comerţul electronic*, Ed. Economică, 2004
- http://www.opencard.org/
- http://www.cyberflex.slb.com/