

Smart kartelat, çka janë ato?

Dr. techn. Blerim REXHA
blerim.rexha@cse-ks.com

1 Hyrje

Smart kartela quhen të gjitha pajisjet që kanë një qark të integruar - Integrated Circuit (IC) që posedon një formë sa do të vogël të inteligjencës dhe që janë të ngjitura në një copë plastike. Prania e inteligjencës në kartela iu ka dhënë këtyre kartelave emrin “*smart*” – të meçme. Smart kartelat kanë lindur si nevojë për ti ruajtur dhe përpunuar shënimet në vend dhe formë të sigurt. Siguria e shënimeve në smart kartelë i bënë smart kartelat mbi të gjitha të jenë *smart*.

Smart kartelat janë paraqitur në treg në fillim të viteve të '70. Në vitin 1968 gjermanet Jürgen Dethloff dhe Helmut Grotrupp e kanë patentuar idenë që qarqet e integruara (IC) të ngjiten në një copë të plastikes. Në vitin 1970 japonezi Kunitake Arimura ka aplikuar për patentën e njëjtë në Japoni, ndërsa në vitin 1974 francezi Rokand Moreno e regjistroi patentën e njëjtë në Francë.

Paraardhëset e smart kartelave, kartelat me shirit magnetikë, në të cilin munden vetëm të ruhen shënimet (300-400 bajt) nuk kanë mundësi të përpunimit të shënimeve. Kartelat e para për qëllime pagesa janë paraqitur në treg nga Diners-Club në fillim të viteve të '50.

Smart kartelat sot janë shumë të përhapura: në telefonin tonë mobil si **Subscriber Identity Modul (SIM)**, smart kartelat për të telefonuar, kartelat e bankës, bonus kartelat e ndryshme, kartelat për hyrje/dalje në objekte të ndryshme etj. Numri i gjithmbarshëm i smart kartelave të prodhuara në vitin 1996 ka qenë 6 miliard dhe supozohet se ky numër në vitin 2001 është rritur në 9 miliard [1].

2 Llojet e smart kartelave

Smart kartelat mund të ndahen në grupe të ndryshme. Varësisht nga madhësia e plastikës, ku është ngjitur IC-ja smart kartelat ndahet në dy grupe të mëdha:

- smart kartela me madhësi të kartelave të bankës (ID-1 formati), dhe
- smart kartela me madhësi të kartelave të telefonave mobil (ID-001 formati), pra SIM kartela.

Varësisht prej kontaktit me lexuesin (shkruesin) e smart kartelave, smart kartelat ndahen në:

- smart kartela me kontakt dhe që janë të standardizuara përmes standardit International Standardization Organization (ISO) 7816, dhe
- smart kartela pa kontakt, komunikimi me lexuesin e smart kartelave bëhet përmes fushës magnetike dhe janë të standardizuara me anë të standardeve ISO10536 dhe ISO14443, shih Fig. 1. Smart kartelat pa kontakt me tutje ndahen në tri nëngrupe, varësisht nga largësia e smart kartelës prej antenës:
 - 2-3 mm “*close coupled*” smart kartela,
 - 2-3 cm “*proximity*” smart kartela, dhe
 - deri në 1 m largësi, “*vicinity*” smart kartela

- smart kartela me *dual interface* që komunikimin me lexuesin mund ta bëjnë në dy mënyra: përmes kontakteve dhe përmes fushës magnetike.

Varësisht prej procesimit të shënimeve në smart kartelë, smart kartelat mund të ndahen në:

- smart kartela që posedojnë mikroprocesorë për përpunimin e shënimeve, dhe
- smart kartela vetëm me memorie.

Në Fig. 1 janë paraqitur ndarjet e përshkruara më lartë dhe sipas standardeve të International Standardization Organization.

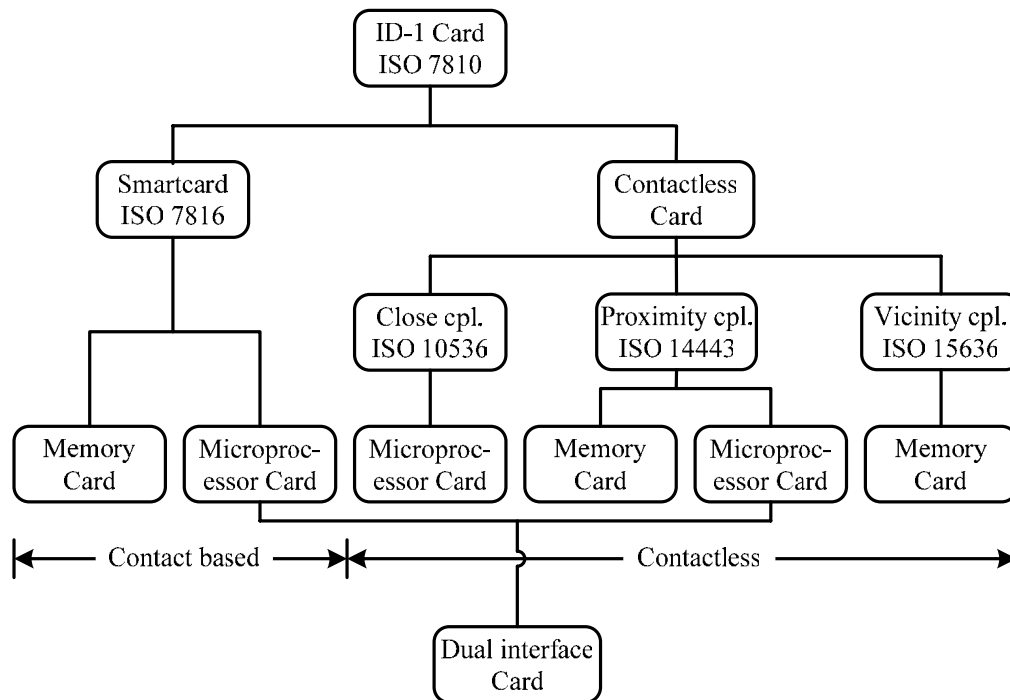


Fig. 1: Llojet e smart kartelave dhe ISO standardet

Smart kartelat mund të ndahen edhe sipas numrit të aplikacioneve që kanë, pra kemi smart kartela:

- që kanë vetëm një aplikacion, siç kanë qenë smart kartelat e para në treg, kartelat për telefonim nga kabinat publike, SIM kartela apo kartela e bankës,
- që kanë shumë aplikacione siç janë smart kartelat e kohës së fundit (Java smart kartela etj.).

Meqenëse siguria e shënimeve është roli primar i smart kartelave ato zbatimin më të gjerë e kanë gjetur në banka dhe në sigurimin e sistemit të pagesave.

3 Çka përmbajnë smart kartelat?

Mikroprocesori i smart kartelës është zakonisht 8 ose 16 bitësh. Sikurse kompjuterët e viteve '80-ta mikroprocesori i smart kartelës e ka njësinë për hyrje/dalje, memorien e përkohshme (**R**andom **A**ccess **M**emory - RAM), memorien e lexueshme (**R**ead **O**nly **M**emory - ROM), memorien përhershme dhe të ndryshueshme (**E**lectrically **E**rasable **P**rogrammable ROM – EEPROM), siç është paraqitur në Fig. 2.

Disa smart kartela me kërkesa të larta të sigurisë së shënimeve e përmbajnë edhe një krypto-procesor për operacione kriptografike.

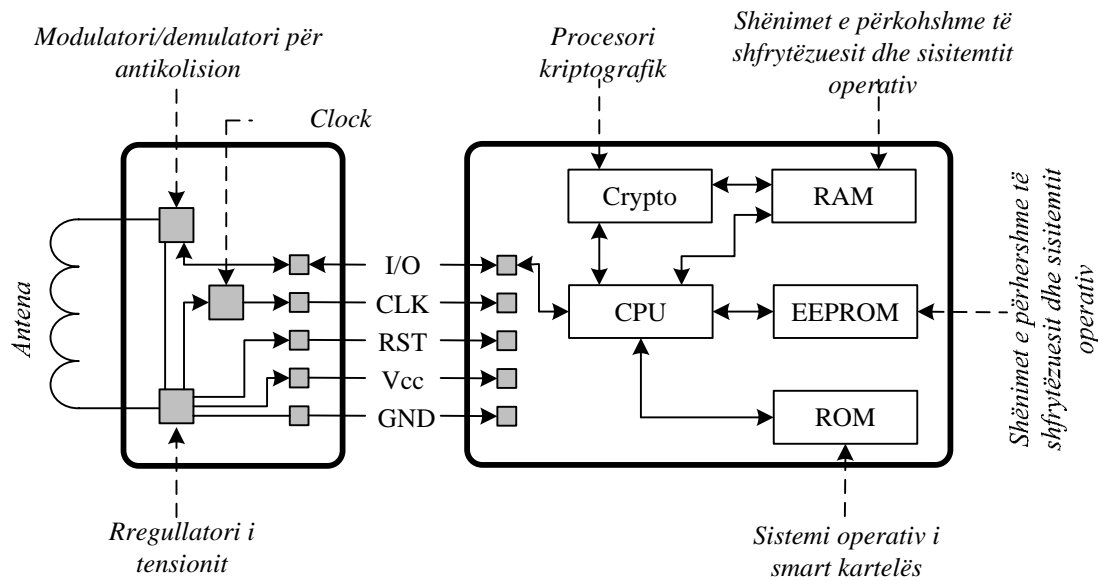


Fig. 2: Përmbajtja e smart kartelës

Në Fig. 2 është paraqitur përmbajtja simbolike e një smart kartela me kontakt dhe pa kontakt (me fushë elektromagnetike). Meqenëse smart kartela nuk përmban njësinë për furnizim ajo është gjithmonë pasive, duke pasur parasysh modelin *master-slave* smart kartela është gjithmonë slave, pra ajo vetëm përgjigjet në pyetjet nga ambienti jashtëm [2].

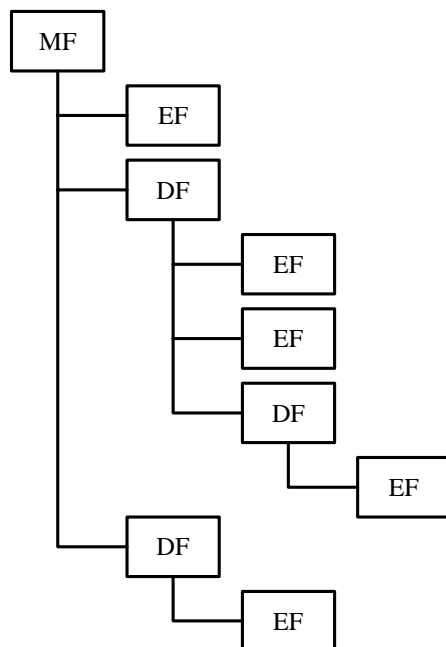


Fig. 3: Fajll sistemi i smart kartelave

Qasjet në shënime në memorien e përhershme, EEPROM mbrohen nga qasjet e paautorizuara me anë të ashtuquajturit “**Personal Identification Number**” (PIN). Vetëm pasi që pronari i smart kartelës e bënë prezantimin e suksesshëm të PIN-it smart kartela i lejon qasjen në shënime në EEPROM. PIN-i është i gjatë 4 deri në 8 shenja. Në rast se shfrytëzuesi e jep gabimisht PIN-in disa herë radhazi (zakonisht tri herë) smart kartela e bllokon plotësisht qasjen në EEPROM, me çka smart kartela shndërrohet në një plastikë të rëndomtë dhe të pavlerë.

Smart kartelat e kanë fajll sistemin në formën e pemës (tree), siç është paraqitur në Fig. 3. Rrënja e fajll sistemit quhet **Master File (MF)** dhe ka vlerën 3F00 heksadecimal dhe mund të përmbaj disa **Dedicated File-s (DF)** dhe **Elementary File-s (EF)**. Emrat e fajllave janë të normuar sipas ISO 7816-4 standardit. Secili fajll përbehet prej **File Identifier (FID)** të gjatë 2 bajt,

dhe që brenda një DF është unik [3]. Në disa smart kartela DF-at mund të referencohen edhe sipas emrit, i cili mund të jetë i gjatë deri në 16 bajt. Shënime të shfrytëzuesit, pronarit të smart kartelës ruhen në një EF.

4 Komunikimi me smart kartela

Smart kartela komunikon me lexuesin e smart kartelevë (apo terminalin siç quhet ndryshe) me shpejtësi deri në 115.200 bit për sekondë (bps). Komunikimi i terminalit me smart kartelën është gjysmë dupleks (half duplex), pra në kohën kur terminali dërgon shënime smart kartela duhet të jetë në gjendje pranimit, dhe kur smart kartela dërgon shënime terminali duhet të pranojë shënime, në rast të kundërt vjen deri të kolizioni në kanal transmetues. Komandat dhe shënimet që i merr smart kartela nga terminal i ruan në RAM dhe meqenëse sasia e RAM në smart kartela është shumë e kufizuar (disa qindra bajt) komandat që i dërgohen smart kartelës duhet të copëtohen në paketa më të vogla se 255 bajt dhe të dërgohen në formë sekeunciale.

Sa herë që smart kartelës i vendoset tensioni i furnizimit, ajo i përgjigjet terminalit me të ashtuquajturën **Answer To Reset (ATR)** përgjigje. Në ATR janë të koduar shënime mbi aftësitë komunikuese të smart kartelës, prodhuesit, versionit të sistemit operativ etj. ATR mund të jetë i gjatë deri në 33 bajt.

Dy protokollet më të përhapura për komunikim me smart kartela janë: protokollit T=0 dhe T=1. Duke pasur parasysh **Open System Interconnection (OSI)** modelin shtatë shtresor, për protokollet T=0 dhe T=1 mund të thuhet se janë në shtresën 2, në “data link”. Pas vendosjes së lidhjes në nivelin 2, protokollet në nivelin e aplikacionet në lexues dhe smart kartelë mund ti shkëmbejnë informatat, siç është paraqitur në Fig. 4.

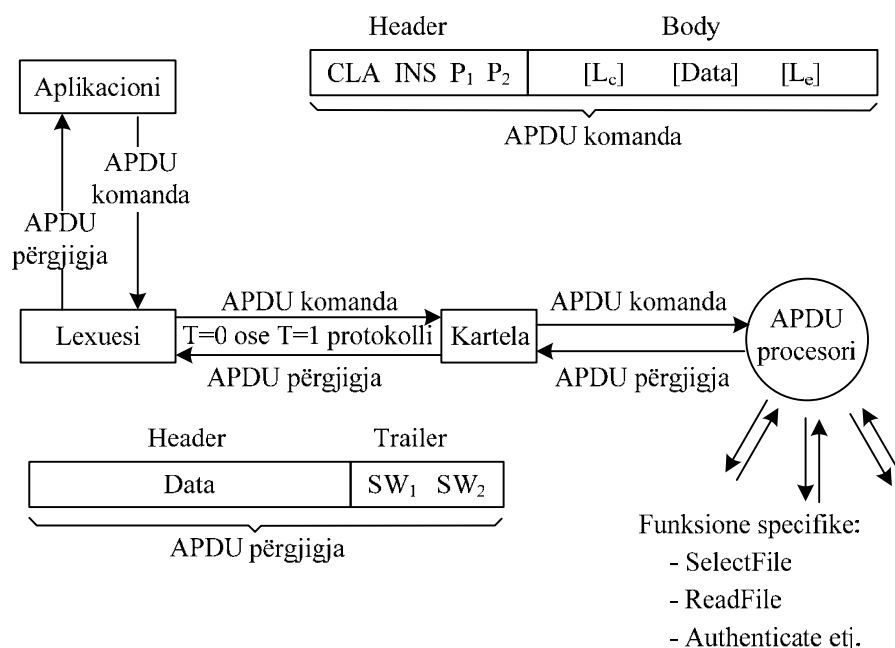


Fig. 4: Komunikimi me smart kartelë

Aplikacioni i shkëmbejnë informatat me smart kartelën në formë të strukturave të shënimeve që quhen **Application Protocol Data Unit (APDU)**. Aplikacioni i dërgon një APDU komandë smart kartelës dhe smart kartela i dërgon aplikacionit një APDU përgjigje, shih Fig. 4. APDU komandat dhe përgjigjet janë të normuar me ISO 7816-4 standardin.

APDU komanda përbehet prej header-it (kokës) dhe body (trupit). Header-i përbehet prej 4 bajtëve: klasa (class **CLA**), instruksioni (**INS**), parametri i parë (**P₁**) dhe parametri i dytë (**P₂**). Header-i APDU komandës është obligativ. Trupi i APDU komandës mund të përmbajë shënime, gjatësia e të cilave përcaktohet me anë të

parametrit L_c (Length of command). Me anë të parametrit L_e (expected Length), i terminali i bënë me dije smart kartelës se pret përgjigjeje me gjatësi L_e bajt. Trupi i APDU komandës mund ti ketë katër forma:

- nuk as shënime për në smart kartelë as përgjigje nga smart kartela,
- nuk as shënime për në smart kartelë por ka përgjigje prej smart kartelës, pra ekziston një vlerë për L_e parametrin,
- ka shënime për në smart kartelë (L_c është e ndryshme prej zero) dhe nuk përgjigje nga smart kartela, dhe
- ka shënime për në smart kartelë dhe ka përgjigje nga smart kartela (L_c dhe L_e janë të ndryshëm nga zero, shih Fig. 4.).

APDU përgjigja përbehet nga trupi dhe status fjala (**Status Word** - SW) prej 2 bajtëve, shih Fig. 4. Trupi i APDU përgjigjes mundet të mungoj, në rastin kur smart kartela nuk ka shënime për lexuesin e smart kartelës, ndërsa status fjala është gjithmonë prezent. Nëse ekzekutimi i komandës është bërë me sukses smart kartela i përgjigjet terminalit me përgjigjen 9000 në formë heksadecimale.

APDU komanda për selektimin e MF (Master File) do të dukej:

CLA	INS	P_1	P_2	L_c	Data	L_e	
00	A4	00	00	02	3F 00	00 (1)

Përgjigja korrekte nga smart kartela do të dukej:

SW ₁	SW ₂	
90	00 (2)

Komandat e zakonshme siç janë: selektimi, leximi dhe shkruarja e një fajlli, verifikimi i PIN-it janë të standardizuar me ISO7816-4 standardin [3].

Me paraqitjen e Personal Computer Smart Card (PC/SC) standardit në vitin 1997 smart kartelat dhe lexuesit e smart kartelave janë bërë pajisje standarde të kompjuterëve personal. Shërbimi (service-i), programi për komunikim me smart kartela është pjesë përbërë e çdo sistemi operativ modern.

5 Aplikacionet me smart kartela

Smart kartelat e para janë përdorur në kabina të telefonave publik për ti zëvendësuar monedhat metalike. Këto smart kartela kanë një numërues, i cili mundet vetëm të zvogëlohet dhe gjate thirrjes telefonike ky numërues zvogëlohet në proporcion me impulset e harxhuara. Kur numëruesi e arrin vlerën zero, pra kartela është zbratur ajo mund të hidhet si e pavlerë. Logjika e vetme që këto kartela e kanë është aftësia e “zvogëlimit të sigurt e numëruesit” dhe në disa raste edhe autentifikimi aparatit telefonik në kabinë.

Kartelat e bankës pothuajse në gjithë boten janë të pajisura me qark të integruar (çip). Në EEPROM, më saktësisht në një EF ruhen shënimet e pronarit të kartelës, xhiro llogarisë si dhe transaksionet e fundit të bëra me kartelë. Të gjitha kartelat e bankës janë të afta të bëjnë edhe llogaritje kriptografike (simetrike ose/dhe asimetrike). Pra çdo transaksion ta nënshkruajnë në formë digjitale ose ta sigurojnë me një **Message Authentication Code** (MAC). Të gjitha llogaritjet kriptografike që i bëjnë kartelat e bankave sot bazohen në enkriptimin simetrik dhe në çelësa të

derivuar. PIN-i i kartelës së bankës ruhen në një EF të veçantë në smart kartelë. Autentifikimi me PIN bazohet në enkriptimin simetrik, çelësa të derivuar dhe numrin serik të smart kartelës.

Smart kartelat e kohëve të fundit po pajisen me mikroprocesor të fuqishëm, me çka mundësohet që në smart kartelë të zhvillohen operacione kriptografike siç janë: gjenerimi i çelësave privat dhe publik, krijimi i nënshkrimit digjital si dhe dekriptimi me çelësin privat. Smart kartelat paraqesin mediumin më të sigurt për ruajtjen e shënimeve private si xhiro llogaritë bankare dhe transaksionet tjera financiare. Pagesat e sigurta me smart kartela dhe përmes Internetit bazohen pikërisht në vetit kriptografike të smart kartelave.

6 Përmbledhje

Smart kartelat sot konsiderohen si pajisje me të sigurta për ruajtjen dhe përpunimin e shënimeve private. Komunikimi me smart kartela është i standardizuar, gjë që ka shkaktuar që smart kartelat të konsiderohen si pjesë standarde të kompjuterëve personal. Qasja në shënime në smart kartelë, bëhet vetëm pasi të bëhet autentifikimi i suksesshëm me PIN-in e smart kartelës. PIN-i i smart kartelës është i njohur vetëm pronarit të smart kartelës. Nëse pronari i smart kartelës e harron PIN-in ose e jep atë disa herë radhazi gabimisht smart kartela e bllokon qasjen në shënimet në EEPROM dhe smart kartela shndërrohet në plastike të pavlerë.

Referencat

- [1] CardLogix, http://www.cardlogix.com/corporate_press_factoids.asp, 3.10.2005
- [2] Scott B. Guthery & Timoty M. Jurgensen, Smart Card Development Kit, ISBN=1-57870-027-2, 1998,
- [3] Wolfgang Rankl & Wolfgang Effing: Handbuch der Chipkarten – Aufbau Funktionsweise Einsatz von Smart Cards, ISBN=3-446-21115-2, 1999