Synthesis
International Scientific Conference of IT and Business-Related Research

BEZBEDNOSNI ASPEKTI ELEKTRONSKIH LIČNIH IDENTIFIKACIONIH DOKUMENATA NOVE GENERACIJE

SECURITY ASPECTS OF THE NEW-GENERATION ELECTRONIC IDENTIFICATION DOCUMENTS

Andreja Samčović[1], Svetlana Čičević[1], Milkica Nešić[2]
[1]Univerzitet u Beogradu, Saobraćajni fakultet, Vojvode Stepe 305, Beograd, Srbija
[2]Univerzitet u Nišu, Medicinski fakultet, Bulevar dr Zorana Đinđića 81, Niš, Srbija

Apstrakt:
U ovom radu su prikazane osnove koncepta elektronskog identifikacionog dokumenta, zasnovanog na tehnologiji pametnih kartica. Ova tehnologija pruža minimum uslova za izdavanje bezbednog i pouzdanog dokumenta za identifikaciju, kako u realnom tako i u digitalnom svetu. Pametna kartica sa biometrijskim podacima vlasnika poseduje infrastrukturu javnih ključeva. S tim u vezi, razmotrena su tehnološka pitanja prilikom implementacije zaštićenih personalnih identifikacionih kartica. Predstavljena je *Sm@rtCafe* aplikacija za upravljanje pametnim karticama.

Ključne reči:
pametna kartica, identifikacioni dokument, informacione tehnologije, autentifikacija, Sm@rtCafe aplikacija.

Abstract:
This paper presents the fundamentals of the concept of electronic identification document, based on the smart card technology. This technology provides minimum requirements for issuing secure and reliable identification documents, both in the real and digital world. Smart cards with biometric data have the Public Key Infrastructure (PKI). Hence, technological issues in implementation of protected personal identification cards are considered. *Sm@rtCafe* application for smart cards management is introduced.

Key words:
smart card, identification document, information technologies, authentication, Sm@rtCafe application.

Napomena.
Ovaj rad je podržan i finansiran od strane Ministarstva prosvete i nauke Republike Srbije (Projekti br. 32025, 32048, 36022, 36006 i 179002).

1. UVOD

Sa smanjenjem cene, rastućom računarskom snagom i memorijskim kapacitetima, pametne kartice su postale jedan od mogućih izbora za elektronsku autentifikaciju. Stotine miliona pametnih kartica se danas koriste u hiljadama aplikacija koje uključuju identifikaciju, elektronsko plaćanje, kontrolu pristupa, memorisanje medicinskih informacija, mobilnu telefoniju, itd. Pametne kartice se, po pravilu, koriste za izvršavanje kriptografskih informacija pod kontrolom tajnih ključeva ugrađenih u njihovoj zaštićenoj memoriji (Stallings, 2010). Sa druge strane, cilj potencijalnog napadača na sistem jeste da izvuče tajne ključeve iz fizički zaštićene kartice, u cilju modifikacije sadržaja kartice, kreiranja duplikata kartice, ili generisanja neautorizovane transakcije.

Pametne kartice su, po pravilu jeftine, pogodne za korišćenje, sa malom količinom memorije, nekim osnovnim računarskim mogućnostima i određenim ulazno/izlaznim portovima preko kojih se dobijaju napajanje i sinhronizacioni impulsi. Pokazalo se da tehnologija pametnih kartica pruža relativno bezbednu platformu za identifikaciju pojedinaca. Sistem baziran na pametnim karticama obezbeđuje vrlo isplativo rešenje koje odgovara zahtevima državne uprave i poslovnim zahtevima za bezbednu i preciznu proveru identiteta, dok sa druge strane omogućuje zaštitu privatnosti informacija o pojedincu.

Pametne kartice su korisne u oblasti zaštite ličnih podataka. Mogu da se koriste za autentifikaciju i bezbedan pristup informacionim sistemima koji zahtevaju visok nivo bezbednosti (Samčović & Turan, 2007). Podaci smešteni u pametnoj kartici su prenosivi. Pametne kartice sadrže bezbednosni sistem sa mehanizmima protiv falsifikovanja i neovlašćenog očitavanja i upisivanja podataka. Naime, sadrže bezbednosni kriptoprocesor, bezbednni fajl sistem i optički čitljive podatke. Uz to, poseduju sposobnost za čuvanje poverljivih podataka u svojoj memoriji.

Identifikacioni dokumenti (ID), kao što su lične karte, koje se upotrebljavaju u Republici Srbiji, su zasnovani upravo na tehnologiji pametnih kartica. Stari tip ličnih karata je bio baziran na *Apollo* operativnom sistemu. To je tzv. *proprietary* operativni sistem (OS), i nije univerzalan kao Java OS. Takođe, *Apollo* operativni sistem nije otvoren za javnost, za razliku od Jave. Međutim, novi tip ličnih karata izdatih u Republici Srbiji, se zasniva na Java operativnom sistemu, i usklađen je sa svim specifikacijama standarda za bezbednost kriptografskih uređaja.

2. ARHITEKTURA ELEKTRONSKE LIČNE KARTE

Elektronske lične karte koriste *Infineon* SLE66CX322P čip (PC/SC Workgroup, 2014), *Module type* M 5.1. To je 16-bitni mikrokontroler urađen u 0,22 μm CMOS tehnologiji. Sadrži 136 kB ROM-a, 5052 bajtova RAM-a i 32 kB *EEPROM*-a. Ima integrisanu jedinicu za upravljanje i zaštitu memorije, 1100-bitni *Advanced Crypto Engine* (ACE) za RSA kriptografske operacije i 112-bitni/192-bitni DDES-EC2 akcelerator (za DES/DES3 i kriptografske operacije sa eliptičkim krivama). Baziran je na 8051 mikrokontroleru, samo što je dosta unapređen u odnosu na njegovu osnovnu verziju.

Čip moduli su vrlo bezbedni, predstavljaju vrhunski domet u toj oblasti i napredovali su u pogledu zaštite. Čip ima nekoliko senzora za detekciju zloupotrebe i manipulacije silicijuma kao što su senzor visokog i niskog napona napajanja, glič senzor,

E-mail: andrej@sf.bg.ac.rs
DOI: 10.15308/Synthesis-2015-101-106

svetlosni senzor, senzor temperature, *on-chip* samotestiranje, zaštita memorije za RAM, EEPROM i ROM, hardverski merni brojači za SPA (*Simple Power Analysis*), DPA (*Differential Power Analysis* - diferencijalna analiza napajanja), i DFA (*Differential Fault Analysis* - diferencijalna analiza grešaka), kao i aktivnu zaštitu od probnih signala. Senzori su u mogućnosti da daju evidenciju bilo koje vrste ometanja.

Telo kartice sa zaštitnim obeležjima i moduli čipova su otporni na elektromagnetno zračenje i elektrostatičko pražnjenje. Mikroprocesor je u skladu sa ISO/IEC 10373 standardom u pogledu zadržavanja x-zraka i elektrostatičkog pražnjenja. Modul je zaštićen od elektrostatičkog pražnjenja od 6 kV.

Kartica je čitljiva kada se ubaci u standardni PC/SC čitač (Security & Chip Card, 2002). Čipovi su u skladu sa komunikacionim protokolima T=0 i T=1, prema ISO 7816-3. Mogu da komuniciraju sa svakim od čitača kartica koji odgovara standardu ISO 7816-3. ID kartica može da se čita pomoću personalnih računara (PC) korišćenjem odgovarajućih PC/SC ili CT-API čitača kartica.

Čip SLE66CX322P obezbeđuje hardverski generator slučajnih brojeva, hardverski kripto kontroler za brzo generisanje RSA potpisa i hardverski DES procesor za brzo grupno (*bulk*) kriptovanje. Čip podržava RSA do 2048 bita. Proveren je shodno zajedničkim kriterijumima EAL 5 uvećano, što uključuje i procenu ranjivosti. On je tako otporan na poznate hardverske napade kao što su SPA, DPA, DFA, mikro-probing, i ostale.

3. ZAŠTITNI ELEMENTI NA ELEKTRONSKIM LIČNIM KARTAMA

Elementi softversko-elektronske zaštite na ID dokumentima se po svojoj funkcionalnosti mogu grupisati u sledeće celine:

- Hardversko-operativna zaštita pametne kartice;
- Sistemska zaštita pametne kartice;
- Zaštita pristupa podacima pametne kartice;
- Zaštita podataka pametne kartice;
- Bezbednosna formatizacija pametne kartice.

Hardversko-operativna zaštita pametne kartice se odnosi na elemente zaštite koji predstavljaju protivmeru analizi čipa kartice (sadržaja memorije i protoka podataka koji se unutar čipa vrše), dopunjenu sa zaštitnim mogućnostima koje pruža sam operativni sistem kartice.

Sistemska zaštita pametne kartice se odnosi na postupke koji se koriste pri instaliranju aplikacije na pametnoj kartici i na radnoj stanici. Aplikaciju pametne kartice čine odgovarajući aplet (za *Java* kartice), i podaci kartice sa definisanim pravima pristupa. Prilikom punjenja apleta ili kreiranja fajl strukture koriste se sistemski ključevi kartice. Ovi ključevi imaju svoje definisane fabričke vrednosti. U toku pripreme podataka i personalizacije kartica, radi se izmena vrednosti ovih ključeva čime je onemogućena svaka neovlašćena izmena aplikacija na personalizovanim dokumentima. Za uspešnu verifikaciju podataka pametne kartice neophodno je na radnim stanicama instalirati određene CA (*Certification Authority*) sertifikate koji omogućavaju provere svih potrebnih lanaca sertifikata.

Zaštita pristupa podacima pametne kartice se odnosi na prava i načine pristupa pojedinim podacima pametne kartice. Podaci koji se nalaze na pametnim karticama su definisani u odgovarajućim tabelama (*Data Prepatation Tables*, DPT) za svaki tip dokumenta.

Podaci na pametnoj kartici se mogu podeliti na vidljive i nevidljive. Nevidljivi, elektronski podaci upisani u čip, mogu biti javni ili zaštićeni PIN (*Personal Identification Number*) kodom, šifrovani ili nešifrovani (otvoreni), kao i promenljivi ili nepromenljivi. Za pristup pojedinim podacima kartice zahteva se odgovarajući PIN kôd, dok se nekim javnim podacima može pristupiti bez ograničenja. Postoje tri različita PIN koda na svakoj kartici: korisnički PIN kôd (*User PIN*), službeni PIN kôd (*Official PIN*) i administratorski PIN kôd (*Administration PIN*). Svi PIN kodovi se generišu u toku pripreme podataka, kao slučajan niz dužine 8 alfanumeričkih bajtova. Podaci zaštićeni PIN-om zahtevaju dodatnu autentifikacionu proveru osobe ili aplikacije koja pokušava da pristupi njihovom sadržaju.

Postoje dve grupe podataka zaštićenih PIN-om na ID dokumentima: podaci građanina za e-upravu (ovi podaci su zaštićeni pomoću korisničkog PIN koda) i podaci za službene namene kojima pristupaju samo ovlašćeni službenici Ministarstva unutrašnjih poslova (MUP).

Kada su podaci građanina za e-upravu u pitanju, ID kartice su dizajnirane na takav način da mogu da podrže aplikacije e-uprave. Iz ovog razloga se kreira dodatni skup podataka koji će biti korišćen u budućim aplikacijama sa razmenom elektronskih podataka između građana i vlade. Ovi podaci se odnose na dva asimetrična para ključeva (u stvari: dva sertifikata i dva odgovarajuća privatna ključa).

Prvi asimetrični par ključeva služi za identifikaciju građanina i digitalne koverte. Prvi digitalni sertifikat se koristi za identifikaciju građanina i za formiranje poruke sa digitalnom kovertom za ovog građanina. Drugi asimetrični par ključeva služi za digitalno potpisivanje i generiše se u proceduri dodatne personalizacije, koja se izvršava na ovlašćenom registracionom mestu. Drugi par ključeva se generiše direktno na hardveru pametne kartice ID dokumenta. Drugi privatni ključ će biti korišćen za generisanje kvalifikovanog elektronskog potpisa u budućim aplikacijama e-uprave. Čuva se samo na pametnoj kartici (nije kriptovan, ali se ne može ni pročitati ni menjati). Drugi sertifikat je upisan u karticu.

Rezultat kompletne procedure je da na kartici postoje dva privatna i dva javna ključa građanina koji se čuvaju u odgovarajućim digitalnim sertifikatima. Da bi pristupio ovim podacima u budućim aplikacijama e-uprave, građanin mora da se autentifikuje na karticu korišćenjem korisničkog PIN koda.

Razvijena je specifična odgovarajuća procedura koja koristi kombinaciju korisničkog imena i lozinke umesto PIN koda i zbog toga se korisničko ime i lozinka štampaju na PIN nosiocu i predaju vlasniku kartice nakon njene personalizacije. Znači, korisnički PIN se posebnom transformacijom izvodi iz korisničkog imena i lozinke, koje korisnik unosi u aplikaciju za rad sa karticom.

Korisnički PIN kôd je potreban za odgovarajuće podatke kojima može da pristupi samo korisnik pametne kartice koji ga zna. Ovo se odnosi na one podatke i funkcije kartice sa kojima radi sam korisnik (npr. prijava na karticu, digitalno potpisivanje, itd.). Ukoliko se tri puta za redom pogreši u unosu imena i lozinke, izračunati PIN kôd će biti neispravan i kartica će se blokirati, čime će biti onemogućen pristup njenim zaštićenim podacima. U tom slučaju potrebno je deblokirati karticu, za šta je potrebno obratiti se odgovarajućoj službi. Postupak deblokiranja korisničkog PIN koda zahteva poznavanje administratorskog PIN koda kartice.

Što se podataka za službene namene kojima pristupaju samo ovlašćeni službenici MUP-a tiče, neki podaci zahtevaju odgovarajuću autentifikaciju (ili aplikacije verifikacionog uređaja) da bi bili pročitani sa kartice. S druge strane, promenljivi podaci sa kartice mogu da budu promenjeni samo posle odgovarajuće autentifikacije službenika MUP-a. Ovim se sprečava da ti podaci mogu da budu pročitani/ažurirani od strane bilo koga osim autorizovanih službenika MUP-a, korišćenjem odgovarajućih verifikacionih aplikacija MUP-a.

DOI: 10.15308/Synthesis-2015-101-106

Podaci za službene namene su zaštićeni specijalnim PIN kodom – službenim PIN kodom, koji se upisuje u ID dokument u postupku personalizacije kartice. Imajući u vidu da službeni PIN kôd mora da bude jedinstven za svaki ID dokument i da nije moguće da službenik MUP-a zna PIN kôd za svakog građanina, obavlja se automatska procedura za generisanje službenog PIN koda.

Službeni PIN kôd se automatski generiše na osnovu master PIN koda MUP-a, nekih jedinstvenih podataka građanina upisanih na karticu i specifične PCG procedure (PCG – *PIN Code Generation*). PCG procedura se izvršava u hardverskom uređaju otpornom na ometanja u kome se master PIN kôd MUP-a takođe bezbedno čuva. Ovaj uređaj može da bude službena kartica MUP-a ili specifični SAM (*Secure Application Module*) modul integrisan u verifikacionom uređaju.

Službeni PIN kôd je potreban za podatke (minucije) kojima može da pristupi samo ovlašćeni službenik ministarstva. Za određivanje službenog PIN koda koristi se administratorski PIN kôd i SAM modul. Ukoliko se tri puta za redom pogreši u određivanju, PIN kôd će biti blokiran, čime će biti onemogućen pristup službenim podacima. U tom slučaju potrebno je deblokirati PIN, za šta je potrebno obratiti se odgovarajućoj službi. Administratorski PIN kôd se koristi za deblokiranje kartice. Deblokiranje administratorskog PIN koda nije predviđeno. Sva tri PIN koda su upisana u ID kartice sa takvim statusom da se ne mogu pročitati. Njihova promena je zaštićena PIN-om i kodovi nisu kriptovani.

Zaštita podataka pametne kartice podrazumeva da su neki podaci na pametnoj kartici upisani u šifrovanom obliku. To se odnosi na osetljive podatke (prvi privatni ključ, simetrični ključ, minucije, definisano u DPT tabelama), čija se bezbednost želi unaprediti. Tada se pored zahtevanog PIN koda za pristup, podaci dodatno šifruju u toku njihove pripreme i digitalno potpisuju.

Na kartici postoje tri digitalna potpisa: digitalni potpis nepromenljivih otvorenih podataka, digitalni potpis nepromenljivih šifrovanih podataka i digitalni potpis promenljivih otvorenih podataka. Digitalno potpisani nepromenljivi podaci se ne menjaju u toku životnog veka ID dokumenta (npr. registracioni broj, tip dokumenta, prezime, ime, lični registracioni broj, itd.). Ovi podaci su digitalno potpisani privatnim ključem MUP-a. Nepromenljivi podaci na ID dokumentima, koji su potpisani i šifrovani, su biometrijski podaci građanina koji se neće menjati u toku životnog veka ID dokumenta (redukovani portret, otisak prsta). Ovi podaci su digitalno potpisani pomoću privatnog ključa MUP-a, a zatim šifrovani.

Promenljivi otvoreni podaci na ID dokumentima su podaci građana koji bi mogli da budu menjani u toku životnog veka ID dokumenta (npr. nacionalnost, adresa, itd.). Ovi podaci su inicijalno digitalno potpisani korišćenjem privatnog ključa MUP-a, poput nepromenljivih podataka kartice. Međutim, u životnom veku ID dokumenta, ovi podaci bi mogli da budu povremeno menjani. U takvim slučajevima, podaci su digitalno potpisani pomoću privatnog ključa ovlašćenog službenika MUP-a, a to je, u stvari, drugi privatni ključ sa službene kartice tog službenika.

Šifrovanje se izvršava korišćenjem specijalnog simetričnog kriptografskog algoritma koji je posebno dizajniran za MUP i koji zadovoljava sve zahteve za korišćenje u vladinim institucijama. Bezbednosna formatizacija je postupak kojim se proveravaju određeni sistemski podaci pametne kartice i ujedno ima za cilj da detektuje pokušaj kopiranja sadržaja pametne kartice. U osnovi ovog postupka je da se proveri digitalni potpis formatizacionog bloka podataka na kartici. Podaci u bloku su jedinstveni za svaku karticu (izvedeni na osnovu serijskog broja kartice) i u slučaju da su upisani na drugu karticu digitalni potpis će se razlikovati. Na ovaj način bi se detektovao pokušaj kopiranja sadržaja pametne kartice, jer bi se na kopiranoj kartici nalazio drugi serijski broj, i verifikacija digitalnog potpisa ne bi uspela. Za uspešnu proveru bezbednosne formatizacije potrebno je na verifikaconim radnim stanicama instalirati odgovarajući lanac sertifikata, kao i sertifikat za formatizaciju.

4. PREDNOSTI ELEKTRONSKIH LIČNIH KARATA

Postavlja se pitanje koje su prednosti elektronskih ličnih karata u poređenju sa ličnim kartama bez čipa. Provera identiteta se najčešće obavlja putem dokumenta sa fotografijom (lične isprave, putne isprave ili vozačke dozvole). Tradicionalne metode izdavanja dokumenata i provere identiteta nisu dovoljno pouzdane da spreče zloupotrebe. Zloupotreba identiteta je krivično delo koje je sve zastupljenije u svetu. Porast krivičnih dela zloupotrebe identiteta objašnjava se slabošću u postupku izdavanja identifikacionih dokumenata i postupku provere identiteta pojedinaca zasnovanom na tako izdatom dokumentu. Slabost u sistemu utvrđivanja i provere identiteta osoba uopšte, a posebno na graničnim prelazima i aerodromima može jednu zemlju učiniti potencijalno atraktivnom metom terorističkih grupa.

Upravo strah od terorističkih napada uticao je na pojavu trenda uvođenja obaveznih identifikacionih dokumenata, kao i putnih isprava sa biometrijskim podacima vlasnika. Takav izbor je logičan, jer se biometrijski identitet ne može falsifikovati ili kopirati. Nova tehnologija sigurno može da pomogne u uspostavljanju pouzdanog sistema identifikacije lica i zaštite identifikacionih dokumenata koji će, na prvom mestu, povećati njihovu upotrebljivost i pouzdanost, i samim tim dalje doprineti smanjenju zloupotreba.

Pametna kartica sa biometrijskim podacima vlasnika (digitalna fotografija, otisak prsta, analiza irisa oka ili DNK analiza) i infrastrukturom javnih ključeva (*Public Key Infrastructure*, PKI), koja štiti podatke u čipu kartice, i elektronskim transakcijama tako što omogućava pouzdanu autentifikaciju, tajnost, integritet i raspoloživost podataka, nameću se kao prirodno rešenje za pouzdan ID kako u realnom, tako i u svetu digitalne komunikacije. Kod lične karte (LK) sa čipom identitet se vizuelno i elektronski verifikuje (sa ili bez biometrijskih podataka), dok se kod lične karte bez čipa verifikuje samo vizuelno. Kod LK bez čipa su svi podaci vidljivi jer su odštampani na njoj, dok se kod LK sa čipom neki podaci (npr. adresa) nalaze samo u čipu i za promenu adrese je dovoljno samo prepisati stare podatke novim u memoriji čipa, što se obavlja u MUP-u od strane ovlašćenog lica. Podaci o licu se mogu očitavati iz čipa u drugim aplikacijama, dok se kod LK bez čipa moraju ručno unositi za korišćenje u drugim aplikacijama. Lične karte sa čipom još poseduju mogućnost elektronskog potpisa, mogućnost korišćenja javnih servisa, kao i dodatne zaštitne elemente.

Strategija državne uprave u Republici Srbiji promoviše kao jedan od osnovnih principa reforme princip modernizacije primenom dostignuća savremenih informacionih tehnologija (IT). Cilj modernizacije državne uprave je da se uvođenjem IT u rad državnih organa, kako na centralnom, tako i na lokalnom nivou, omogući građanima dostupnost najrazličitijih servisa elektronskim putem.

Očekivani rezultati primene za građane su humanija i jednostavnija procedura izdavanja primarnog i kasnije sekundarnih dokumenata (pasoša, vozačke dozvole, saobraćajne dozvole, ...), brza i laka promena podataka na primarnom dokumentu (npr. adrese) i upotreba dokumenta u servisima buduće e-uprave. Za

DOI: 10.15308/Synthesis-2015-101-106

MUP Republike Srbije, očekivani rezultati primene su efikasna i pouzdana identifikacija osoba, unapređen značaj i ugled institucije, kao i uštede u troškovima korišćenja i prenosa informacija. Konačno, za društvo, očekivani rezultati primene su osnova za e-upravu, efikasnost državnih institucija u pružanju usluga građanima i LK po svetskim standardima koji omogućavaju integraciju u Evropsku Uniju (EU).

5. UPOTREBA APLIKACIJE *SM@RTCAFE*

Najvažniji standard za mikrokontrolerski bazirane pametne kartice je ISO/IEC 7816. Njegov četvrti deo, ISO/IEC 7816-4, sadrži organizaciju, bezbednosnu arhitekturu, *secure messaging*, APDU komande (*Application Programming Data Unit*) i slično, tako da je upravo ovaj deo standarda od najvećeg značaja (ISO/IEC, 2013). Ideja standarda je da se definiše set komandi koje svaki operativni sistem za pametne kartice - SCOS (*Smart Card Operating System*) treba da ima, kao i da ima istu APDU komandu za jednu naredbu, npr. za operaciju čitanja fajla (*read file*). Kod svakog operativnog sistema ta operacija, kao i druge, treba da ima istu APDU komandu, odnosno isti niz bajtova koji se šalju kartici kao komanda. Operativni sistemi kartica se tako i prave. Zahvaljujući tome, mogućnosti pametnih kartica različitih proizvođača, kao i različitih tipova kartica, su slične i barem jednim delom je sličan i način njihovog programiranja.

Open Platform (ili *Global Platform*) (Markantonakis & Mayes, 2003) je internacionalni industrijski standard za multiaplikativne kartice (što su pre svega Java kartice). Opisuje organizacionu i bezbednosnu arhitekturu multiaplikativnih pametnih kartica, što uključuje arhitekturu kartica i koncept bezbednosti, koncept životnog ciklusa kartica i aplikacija, kao i interfejs, nezavisno od tehnologije provajdera servisa.

Java Card koncept, generisan od strane *Java Card* foruma i publikovan od strane *Sun Microsystems*-a, definiše primenu Java platforme na pametnim karticama. Njegova specifikacija sadrži tri dela: *Virtual Machine Specification, Java Card Runtime Environment Specification* i *Java Card API* (Smart Card Technology, 2009).

U ovom radu je predstavljen kôd urađen u okruženju *Sm@rtCafe* (Reference Manual, 2009) koji će na jednostavnom primeru približiti programiranje pametnih kartica. Kôd će biti detaljno objašnjen i potkrepljen postupnom ilustracijom. Po pokretanju programa *Sm@rtCafe* kreiraćemo novi projekat na način koji je prikazan na Slici 1.

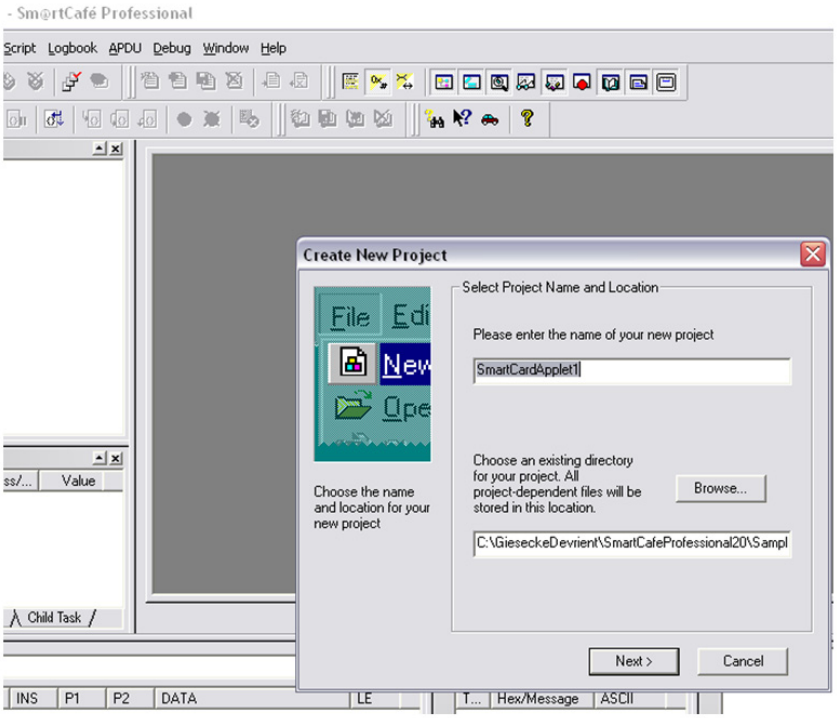
U sledećem koraku je potrebno odabrati odgovarajući *card template*, kao na Slici 2, pri čemu se mora odabrati jedna od dve ponuđene opcije, a to je u ovom slučaju *Sm@rtCafe* simulacija.

Na Slici 3 se može videti u potpunosti pokrenut program u *Win XP* operativnom sistemu. Ovo okruženje još uvek nije u potpunosti operabilno, jer sledi još par koraka. U zavisnosti da li je neki deo koda već napisan ili je potrebno iz početka raditi na njemu, u paleti *File* se odabira *open* ili *new*.

Na samom početku je definisana određena biblioteka koja će se koristiti, a to je *javacard.framework*. Zadatak programera je da kreira klasu koja se može proizvoljno nazvati, a to je u ovom slučaju *MyFirst*. Sledeći korak je zapisivanje varijabli koje će se koristiti u ovoj klasi. Kao što se iz apleta vidi one su uglavnom proglašene za *final static*. Rezervisana reč *final* podrazumeva nepromenjivost, dok *static* predstavlja jedan vid statičnosti, i to u slučaju da se novostvorena vrednost promenljive ne može vratiti na prethodno stanje.

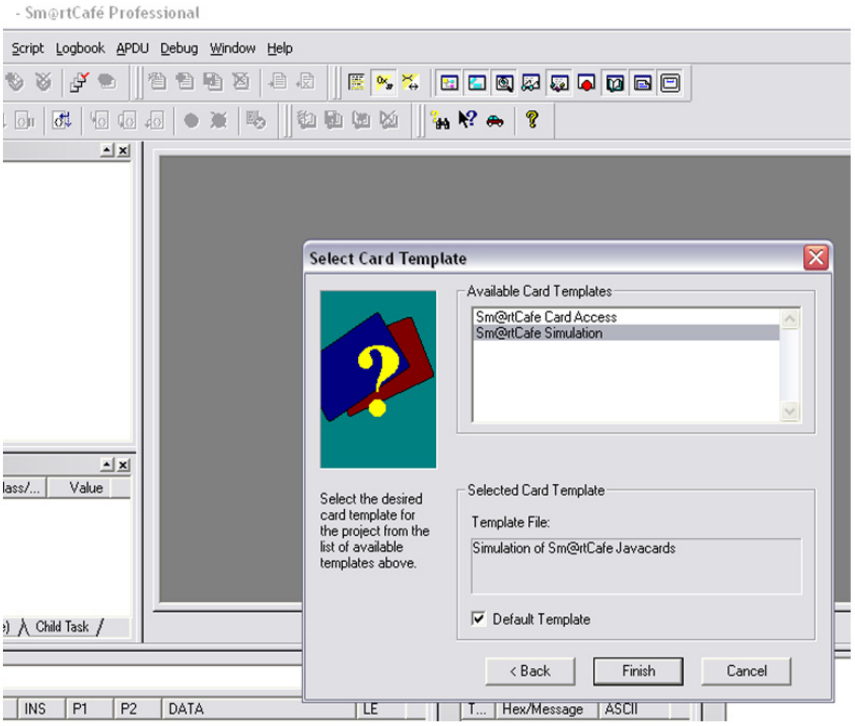
Na samom početku je definisana određena biblioteka koja će se koristiti, a to je *javacard.framework*. Zadatak programera je da kreira klasu koja se može proizvoljno nazvati, a to je u ovom slučaju *MyFirst*. Sledeći korak je zapisivanje varijabli koje će se koristiti u ovoj klasi. Kao što se iz apleta vidi one su uglavnom proglašene za *final static*. Rezervisana reč *final* podrazumeva nepromenjivost, dok *static* predstavlja jedan vid statičnosti, i to u slučaju da se novostvorena vrednost promenljive ne može vratiti na prethodno stanje.

Aplet se kreira samo jednom, i to u procesu instalacije, pozivom statičke metode *Install*. Metoda *install* unutar *DATA* u APDU nizu bajtova je predstavljena sa AID (*Application Identifier*). To je jedinstveni identifikator aplikacije, dužine od 5 do 16 bajtova i predstavljen je u heksadecimalnom sistemu. Poziva se od strane JCRE (*Java Card Runtime Environment*), prilikom instalacije apleta. U procesu instalacije je neophodno pozvati

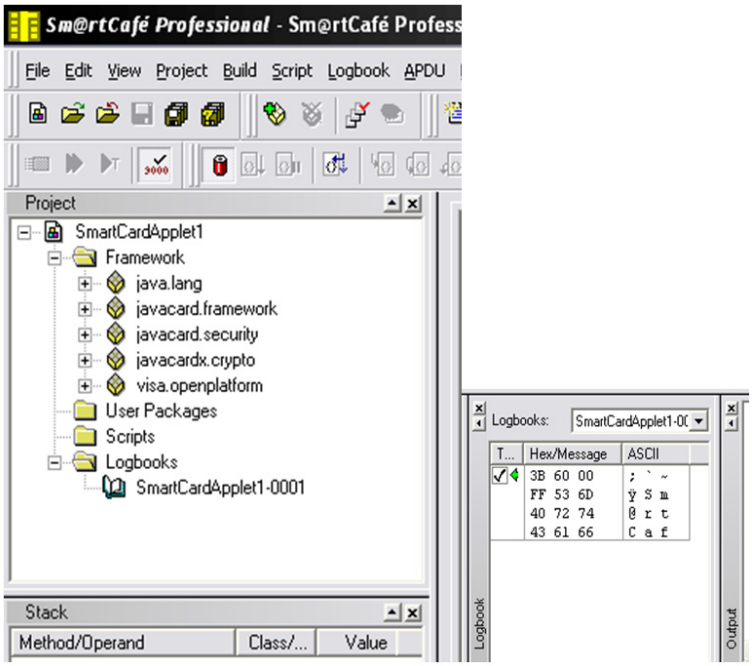


Slika 1. Kreiranje novog projekta

DOI: 10.15308/Synthesis-2015-101-106



Slika 2. *Sm@rtCafe* simulacija



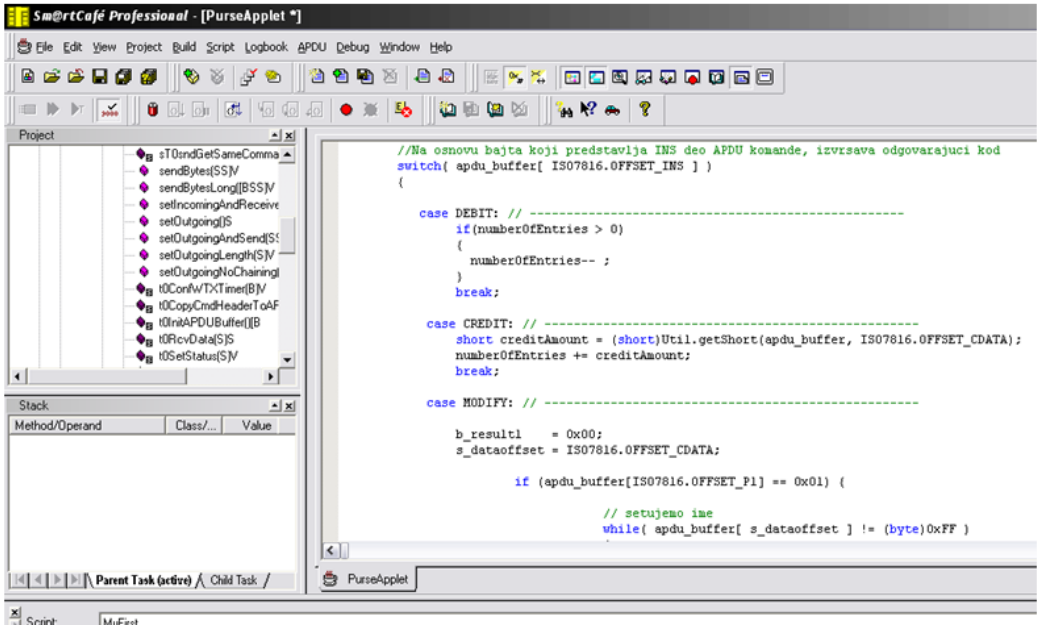
Slika 3. Inicijalizacija *Sm@rtCafe* aplikacije

metodu *register*() koja registruje aplet na nivou kartice, tj. *Card Manager*-a (*OPEN*). Unutar konstruktora se odvaja prostor u memoriji za podatke o korisniku: *userdata, id_userdata* i *numberOfEntries*. Ideja je da u prvih 30 bajtova smeštamo ime korisnika, a u preostalih 30 prezime. Kao oznaka za kraj imena, kao i prezimena, biće bajt FF, koji predstavlja 0. U *id_userdata* se odvaja prostor u memoriji za podatak o ID korinika, jer ovo je jedinstveni podatak o korisniku, prezime i ime nisu jedinstveni. *NumberOfEntries* govori o početnom broju dozvoljenih unosa, i to deset.

Sledeće je uvođenje *Process* metode koja radi (upravlja) sa APDU komandama. APDU o_apdu predstavlja klasu definisanu u *javacard.famework*-u koja sadrži funkcije za rad sa APDU komandama sa dodeljenim nazivom o_apdu. Linija koda *byte[] apdu_buffer = o_apdu.getBuffer()* znači da sa funkcijom *getBuffer* od APDU komande pravi niz bajtova. APDU komande su predstavljene kao niz bajtova u *scipt editoru*. *Byte*[] predstavlja indeksiranje kako bi se moglo pristupiti svakom članu niza.

Switch naredbom je pozvan standard ISO7816 uz OFFSET_INS, po kome se tačno zna na kom mestu u APDU komandi prevedenoj u bajtove se nalazi član sa instrukcijom. Zapaža se na Sl. 4, zaglavlje komande koje predstavlja prva četiri bajta. Zaglavlje je obavezno. Prvi bajt, CLA , određuje klasu instrukcije. Drugi bajt, INS, određuje samu instrukciju. Bajtovi P1 i P2 su parametri instrukcije. Forma zaglavlja je ista za sve komande APDU tipa. Polja *Lc*, *Data* i *Le* su opciona. Bajt *Lc* označava dužinu *Data* polja u komandi, tj. broj bajtova koji se prenose u smeru ka kartici. Polje *Data* čine podaci koji se prenose u

DOI: 10.15308/Synthesis-2015-101-106



Slika 4. Zaglavlje komande

pametnu karticu. Dužina *Data* polja, *Lc*, može biti od jednog do 255 bajtova. Bajt *Le* predstavlja očekivanu dužinu odgovora u bajtovima, i obično iznosi od 1 do 255, s tim što, ako se za *Le* stavi vrednost 00h, onda se smatra da je *Le*=256.

U *switch-case* naredbi su definisana tri slučaja: *debit, credit* i *modify*. *Debit* je u APDU komandama označen sa 30 što vidimo iz INS polja. Nema parametara P1 i P2, znači naredbom *if* je određeno da se za slučaj provlačenja kartice, kada je broj ulazaka veći od nule, skine jedan kredit. Na kraju svakog slučaja se nalazi *break*, što znači da je pronađen odgovarajući slučaj i da tada izlazi iz *switch*-a.

Credit slučaj naredbom *get short* kaže "uzmi" iz niza bajtova *apdu_buffer*, iz polja DATA(ISO7816.OFFSET_CDATA), određeni broj kredita. Treći slučaj je *modify,* koji predstavlja naredbu koja radi bilo koji upis. Postoje dve ovakve naredbe. Jedna je kada je parametar P1=1, dok je druga za parametar P2=1. Za P1=1 se vrši upis imena i prezimena korisnika, s tim da treba imati u vidu da je od 60 odvojenih bajtova 30 rezervisano za ime i 30 za prezime. Mesta koja ostanu nepopunjena posle ovih 30 se popunjavaju *space*_ovima, što je uređeno ASCII kodom. Druga naredba je za setovanje ID, što aplet prepoznaje pročitavši da je P2=1. Takođe se ostatak nepopunjenog rezervisanog prostora po ASCII kodu popunjava razmacima.

Imajući ovo u vidu, kroz praktičan rad prikazan je primer verifikacije pametnih kartica u *Sm@rtCafe* okruženju. Predstavljen je deo koji čini komunikaciju aplikacije sa pametnom karticom, kao i korišćenje dobijenih resursa za upravljanje pametnim karticama. Nadogradnjom i slobodnom izmenom koda prikazani primer se može prilagoditi i za druge načine upotrebe kartice npr. za digitalni potpis.

6. REZIME

Razvojem i primenom novih informacionih tehnologija, pre svega tehnologije pametnih kartica i biometrijske tehnologije, u utvrđivanju i proveri identiteta lica, dobija se identifikacioni dokument koji pruža široku osnovu za pouzdanu identifikaciju kako u svakodnevnom životu, tako i u svim oblastima gde su zastupljene elektronske transakcije. Zbog porasta krivičnih dela zloupotrebe identiteta, među donosiocima odluka u vladama i poslovnim organizacijama, sve je manje podeljenih mišljenja u shvatanju važnosti i ozbiljnosti pitanja bezbednog i pouzdanog utvrđivanja identiteta. Identifikacioni dokument baziran na tehnologiji pametnih kartica i biometrijskoj tehnologiji, učiniće da svet neizbežno postane mnogo komplikovaniji osobama koje se bave zloupotrebom identiteta.

Cilj uvođenja elektronskih ličnih dokumenata je da komunikacija građana sa državom postane kvalitetnija, jednostavnija i jeftinija, što podrazumeva korišćenje elektronske komunikacije. Takođe se očekuje da se ta komunikacija odvija u normativnim i tehničkim uslovima koji su potrebni i podobni da eliminišu ili barem na najmanji stepen svedu mogućnost ugrožavanja prava na zaštitu podataka o ličnosti i svakog drugog ljudskog prava.

LITERATURA

Giesecke & Devrient. (1999). Reference Manual Sm@rtCafe 1.1 Card. Preuzeto 28.03.2015. sa http://www.jstic.com/java/smartcafe/Smartcafe.pdf

ISO/IEC 7816-4. (2013). International Standard: Identification cards - Integrated circuit cards— Part 4: Organization, security and commands for interchange. Geneva, Switzerland.

Markantonakis, K., & Mayes, K. (2003). An overview of the Global Platform smart card specification. *Information Security Technical Report*, 8(1), 17-29.

PC/SC Workgroup. (2014). *PC/SC Workgroup Specification Version 2.01.14.* Preuzeto 28.03.2015. sa http://www.pcscworkgroup.com/specifications.

Samčović, A., & Turan, J. (2007). Multimedia data hiding: techniques and modeling. XXV Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju - PosTel 2007, 11-12. Decembar 2007 (str. 91 -100). Beograd : Saobraćajni fakultet.

Security & Chip Card ICs - SLE 66CX322P. (2002). Infineon Technologies AG, Munich, Germany.

Smart Card Alliance. (2009). Smart Card Technology and Application Glossary. Princeton Junction, NJ: Smart Card Alliance.

Stallings, W. (2010). *Cryptography and network security: Principles and practice*. Upper Saddle River, N.J: Prentice Hall.

DOI: 10.15308/Synthesis-2015-101-106