PODSISTEM ZA ELEKTRONSKU PERSONALIZACIJU IDENTIFIKACIONIH DOKUMENATA ZASNOVANIH NA SMART KARTICAMA

Željko Škrnjug, Goran Pantelić, *NetSeT, Beograd*

Sadržaj – *U ovom radu opisana je implementacija jednog podsistema za elektronsku personalizaciju identifikacionih dokumenata zasnovanih na smart karticama. Predstavljeni su kriterijumi za izbor smart kartica, struktura podsistema i nekoliko faza razvoja sa stanovišta elektronske personalizacije. Postupci, predlozi i rešenja izneti u ovom radu mogu poslužiti kao osnova za realizaciju budućih sistema identifikacionih dokumenata, a takođe i bilo kojih sistema koji će koristiti smart kartice kao elektronske identifikacione medije.*

1. UVOD

Standardni načini čuvanja podataka na identifikacionim dokumentima (lična karta, zdravstvena knjižica, članske karte i sl.) su štampane informacije na papirnom ili plastičnom materijalu. Ovakva dokumenta predstavljaju medijum koji je čitljiv samo optički, neefikasnog načina promene podataka, malog kapaciteta vizuelnih memorijskih elemenata i slabe mogućnosti procesiranja.

Savremeniji način čuvanja podataka identifikacionih dokumenata zasnovan je na pametnim (*smart*) karticama - plastičnim karticama sa čipom i podržanom memorijsko-procesnom logikom. *Smart* kartice su jednostavne konstrukcije i funkcionalnosti, a pritom omogućavaju čuvanje vizuelnih i smeštanje i obradu elektronskih informacija. Karakteristike, operabilnost i način pristupa *smart* karticama definisani su međunarodnim standardima [1,2].

2. KARAKTERISTIKE SMART KARTICA

Nakon definisanja zahteva koje treba da ispune *smart* kartice u sistemima identifikacionih dokumenata, između ostalog potrebne količine i ciljne grupe kojoj su namenjene, potrebno je odabrati tip *smart* kartica. Osnovni kriterijumi su dimenzije, materijal za izradu tela kartice, vrsta i karakteristike čipa, protokoli komunikacije, operativni sistem kartice, kao i druge osobine poput načina programiranja, ugrađenih algoritama i slično [3].

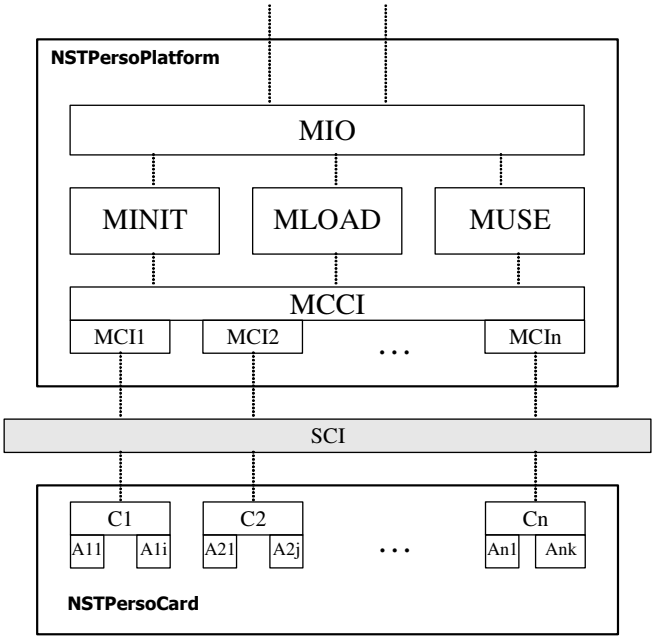
Međunarodnim standardima definisana su tri formata kartica, ID-000, ID-00 i ID-1. U Srbiji, od toga se u praksi koriste kartice tipa ID-000 (veličine SIM kartice u mobilnim telefonima) i ID-1, kartice kakve se viđaju u elektronskom bankarstvu. Matrijal za izradu tela kartica bira se prema svojoj trajnosti, kvalitetu temperaturne i mehaničke obrade, toleranciji, uticaju na životnu sredinu i ceni. Po vrsti čipa razlikuju se memorijske (sa sigurnosnom logikom i bez nje) i mikrokontrolerske kartice (sa koprocesorom i bez koprocesora). Karakteristike čipa podrazumevaju trajnost EEPROM memorije, otpornost na analize i sl. Po načinu komunikacije *smart* kartice mogu biti kontaktne, beskontaktne i dvointerfejne kartice (tj. ujedno i kontaktne i beskontaktne).

Izbor operativnog sistema kartice uslovljen je performansama, implementacionim karakteristikama i fleksibilnosti koju operativni sistem može da pruži. Postoji veliki broj operativnih sistema za *smart* kartice prema međunarodnim standardima. Među njima izdvajamo operativne sisteme koji podržavaju fajl-strukturu na kartici [1] i operativne sisteme sa podrškom za kompilirani/interpretirani programski kod [4,5]. U osnovi, kartice sa fajl-strukturom su brže, dok kartice sa programskim kodom pružaju veću fleksibilnost. Pored ovih, za specijalne namene moguće je prema posebnim specifikacijama praviti i sopstvena rešenja operativnih sistema koji se ugrađuju u ROM memoriju *smart* kartica.

3. OPIS

Kompletno rešenje sistema identifikacionih dokumenata sastoji se iz velikog broja podsistema, kao što su podsistemi za komunikaciju, prikupljanje i skladištenje podataka, proizvodnju kartica, vizuelnu i elektronsku personalizaciju, izdavanje dokumenata i dr.

U ovom radu pažnja je posvećena implementaciji podsistema za elektronsku personalizaciju *smart* kartica. Prikazana implementacija namenjena je stonim računarskim sistemima, ali se slična organizacija poslova može primeniti i za velike distribuirane proizvodne centre. Podsistem je podeljen u dva segmenta – *NSTPersoPlatform* koji čini skup programskih komponenti na stonom računaru i *NSTPersoCard* koji čine *smart* kartice i programska rešenja na *smart* karticama. Konfiguracija rešenja prikazana je na Sl.1.



Sl.1. *Podsistem elektronske personalizacije smart kartica*

Uloga *NSTPersoPlatform* je prijem i obrada podataka za personalizaciju, prikaz rezultata u vidu izveštaja i log fajlova (*Module Input Output - MIO*), inicijalizacija (*Module Initialization - MINIT*), punjenje (*Module Personalization - MLOAD*) i korišćenje (*Module Usage - MUSE*) *smart* kartica.

NSTPersoPlatform segment može da radi sa nekoliko vrsta *smart* kartica različitih proizvođača i različitih operativnih sistema za različite tipove dokumenata. Moguća je i upotreba više kartica za jedan tip dokumenta, ukoliko te kartice poseduju funkcionalnost koje zahteva identifikacioni dokument. Mana rešenja sa podrškom za veći broj kartica je bilo duže vreme implementacije i probemi prilikom usaglašavanja razlika, ali je prednost za korisnika sistema očigledna, jer se povećava nezavisnost od jednog proizvođača kartica i isporučioca operativnog sistema kartica. U proces elektronske personalizacije moguće je uvrstiti ili izbaciti podržane tipove kartica, u zavisnosti od željene konfiguracije sistema. Predviđena je i mogućnost proširenja novim modelima kartica, čime se korisnik dodatno obezbeđuje od zastarevanja ili problema u nabavci.

U *NSTPersoPlatform* implementiran je dvoslojni skup funkcija za komunikaciju sa *smart* karticama (*Module Card Common Interface - MCCI* i *Module Card Interface - MCIx*), koji koristi standardni protokol komunikacije spoljnog uređaja i smart kartice preko terminala (*Smart Card Interface - SCI*). U sloju *MCIx* se nalaze funkcije za pristup svakom pojedinom tipu smart kartica. *MCIx* čine programski moduli proizvođača smart kartica prema standardima kakav je PKCS#11 [6], kao i namenska/sopstvena rešenja [7] koja u sebi realizuju direktnu komunikaciju sa *smart* karticama. Drugi sloj, *MCCI*, čine moduli za objedinjavanje programskog pristupa karticama u jedan jedinstveni interfejs. *MCCI* interfejs je funkcionalna osnova nezavisno od vrste kartica i tipa kartičnog operativnog sistema.

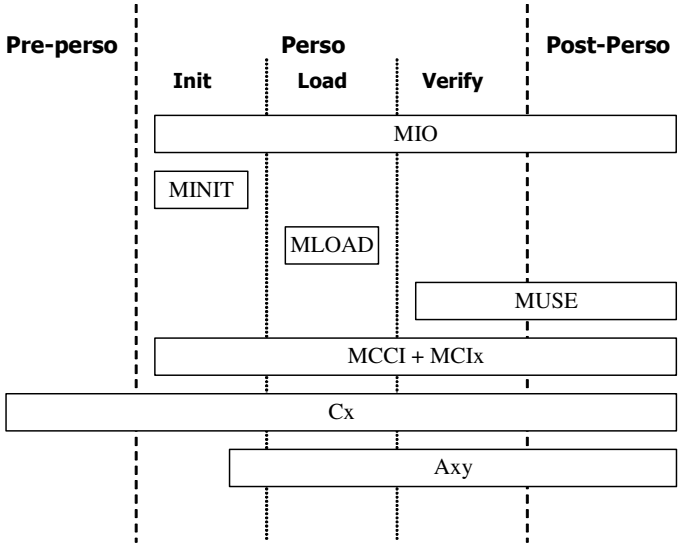
NSTPersoCard čine skup smart kartica (*Cx*) i aplikacija na *smart* karticama (*Axy*) koje podržavaju specificirani tip identifikacionog dokumenta. Ako je reč o smart karticama koje rade sa fajl strukturom, aplikacije predstavljaju skup organizovanih fajlova određenog sadržaja i privilegija. Kod *JavaCard* sistema aplikacije su posebni apleti koji se pišu u Java jeziku, a zatim se transformišu i učitaju u EEPROM memoriju kartica. Kod PKCS#11 sistema, aplikacije na kartici predstavljaju skup posebno definisanih PKCS#11 objekata grupisanih u odgovarajuće celine. Kao što je rečeno, tehnički je izvodljivo da isti tip dokumenta bude podržan od strane više kartica, jer su u *NSTPersoCard* podaci i programski kod organizovani na sličan način, bez obzira što se realizacija izvodi na različitim operativnim sistemima kartica.

Poseban segment u izradi *NSTPersoCard* predstavlja zaštita podataka u aplikacijama na kartici. Realizovana je sigurnosna logika i kombinovane metode autentikacije korisnika prema spoljnoj aplikaciji. Korišćena je enkripcija u domenu operativnog sistema kartice standardnim algoritmima i implementacijom namenskih algoritama na aplikativnom nivou. Postoje specijalne privilegije za promenu podataka.

Pri realizaciji *NSTPersoCard* segmenta velika pažnja je posvećena i performansama kartičnih aplikacija, pa je granulacija i grupisanje podataka izvršeno da se obezbedi što brži odziv. *NSTPersoCard* aplikacije su razvijane i testirane alatima na stonom računaru, a na karticu se smeštaju uz pomoć funkcija iz *NSTPersoPlatform*.

3. FAZE U ELEKTRONSKOJ PERSONALIZACIJI

Razvojne faze *smart* kartica sa stanovišta elektronske personalizacije mogu se podeliti na tri segmenta: pre-personalizaciju, personalizaciju i post-personalizaciju (Sl.2).



Sl.2. *Upotreba modula podsistema elektronske personalizacije po fazama*

Pre-personalizacija *smart* kartica podrazumeva proces proizvodnje kartice sve do ugradnje operativnog sistema. Ovakve kartice su spremne za prihvat aplikacija.

Personalizacija podrazumeva tri podfaze. U inicijalizaciji se pomoću modula *MINIT* vrši priprema smart kartice za punjenje, formiranjem aplikacije *Axy* (učitavanjem *JavaCard* apleta ili formiranjem fajl strukture na kartici). Ovim je kartica spremna za prihvat podataka. Punjenje *smart* kartica obavlja se modulom *MLOAD*. U zavisnosti od tipa identifikacionog dokumenta, informacije koje se smeštaju mogu biti lični podaci, medicinski podaci, podaci za nekretninu ili vozilo. Pored tekstualnih podataka (ime, prezime, adresa) i binarnih podataka (npr. fotografija), mogu se personalizovati i kriptografski elementi, kao što su parovi asimetričnih ključeva i digitalni certifikati, čije se generisanje može obavljati u procesu akvizicije podataka ili nezavisnim softverskim alatima [8]. Verifikacija kartice je poslednja podfaza personalizacije i treba da potvdi ispravnost procesa punjenja. Modul *MUSE* aplikaciji na kartici *Axy* šalje komande za čitanje i procesiranje ulaznog podatka. Ukoliko dođe do greške, operativni sistem kartice vraća odgovarajuću poruku. Modul *MUSE* može aplikativno proveriti da li je integritet podataka u redu. Modul *MIO* može se iskoristiti za formiranje izveštaja koji bi olakšali nalaženje uzroka grešaka i ispravljanje problema. *MIO* se može koristiti i u ostalim fazama kad je potrebno dobiti više informacija o protoku informacija u sistemu.

Post-personalizacija je faza u kojoj se kartica koristi. Aplikacija *Axy je* napunjena i operativna. Dodatno se može

smestiti neki podatak za koji je rezervisan prostor u fazi pre-personalizacije. U modulu *MUSE* realizovane su sve potrebne funkcije za korišćenje kartice – čitanje, upis, slanje podataka za obradu na kartici i dr.

Personalizovane *smart* kartice omogućavaju vlasniku da se jedinstveno identifikuje i koristi usluge savremenih sistema elektronskog poslovanja (elektronska trgovina, elektronsko plaćanje, elektronsko bankarstvo, elektronska vlada, elektronska medicina...). Takođe, svoju primenu identifikacione kartice nalaze i u sistemima kontrole pristupa i telekomunikacijama.

5. POSEBNI SAVETI

Na početku specifikacije sistema identifikacionih dokumenata često se postavlja pitanje koliko dokumenata treba da bude na jednoj smart kartici i koliko mesta predvideti za proširenja? Najekonomičnije rešenje sa stanovišta broja izdatih kartica i fleksibilnosti upotrebe bila bi kartica tipa »jedna za sve«. Međutim, dosta je teško usaglasiti realne mogućnosti kartica sa mogućim potrebama i varijantama izvedbi i dodataka. Prepreka predstavlja i neopstojanje jedinstvenog ili barem usaglašenog informacionog sistema za proces izdavanja i obrade dokumenata. U svakom slučaju, pri izradi sistema identifikacionih dokumenata poželjno je da se ostavi prostor za moguća proširenja koliko god to specifikacije dozvoljavaju.

Posebnu pažnju posvetiti beskompromisnoj zaštiti podataka u sistemima identifikacionih dokumenata. Koristiti savremene šifarske simetrične i asimetrične algoritme i PKI infrastrukturu [8] za postizanje maksimalne sigurnosti u prenosu i razmeni informacija.

6. ZAKLJUČAK

Primenom opisanog sistema za elektronsku personalizaciju elektronskih identifikacionih dokumenata u potpunosti se zadovoljavaju svi standardi u pogledu fleksibilnosti, upotrebljivosti i bezbednosti podataka. Segmenti *NSTPersoPlatform* i *NSTPersoCard* su adaptivni i lako se mogu prilagoditi svakom zahtevu za identifikacioni dokument, uz podršku *smart* kartica po izboru korisnika. Porastom memorijskih kapaciteta, brzine komunikacije i procesne moći *smart* kartica, ovi proizvodi će biti unapređivani da bi omogućili nove funkcionalnosti »na čipu«.

Prednosti *smart* kartica u odnosu na klasična identifikaciona dokumenta su velika i postaju sve značajnija razvojem društva u informatičkom smislu. Napredak će postati još očigledniji većom ponudom servisa koji će koristiti identifikaciona dokumenta.

Smart kartice predstavljaju novi medij za čuvanje identifikacionih podataka koji će u budućnosti zameniti klasične dokumente.

LITERATURA

[1] ISO/IEC 7816, *Identification Cards – Integrated Circuit(s) Cards with contacts, Part 1-4,* ISO, 1995-1999.

[2] ISO/IEC 14443, *Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards, Part 1-4,* ISO, 2000-2001.

[3] W.Rankl, W.Effing, *Smart Card Handbook, 3rd Edition,* John Wiley & Sons, 2003.

[4] Global Platform*, Card Specification 2.0.1', Card Specification 2.1.1*, 2000, 2003.

[5] Zhiqun Chen, *JavaCard Technology for Smart Cards*, Sun Microsystems, 2000

[6] RSA Laboratories., *PKCS #11 – Cryptography token interface standard v2.11, revision 1,* 2001.

[7] Ž.Škrnjug, G.Pantelić, *Kriptografski API – Softverski modul za zaštitu podataka,* XLVIII Konferencija ETRAN, Čačak, jun 2004.

[8] G.Pantelić, Ž.Škrnjug, *Certifikaciono telo u PKI sistemu zaštite podataka,* XLVIII Konferencija ETRAN, Čačak, jun 2004.

Abstract – In this paper the implementation of subsystem for electronic personalization of smart card based identity documents is described. Criteria for choosing smart cards, subsystem architecture and several phases in development of smart cards from electronic personalization view are presented. The acts, suggestions and solutions in this paper may be considered as basis for developing future identity document systems, as well as for any other systems which will use smart cards for electronic identity media.

SUBSYSTEM FOR ELECTRONIC PERSONALIZATION OF SMART CARD BASED IDENTITY DOCUMENTS

Željko Škrnjug, Goran Pantelić