Autentifikacija platnih smart kartica

Emir Ugljanin, Milan Vidaković i Goran Sladić

***Sadržaj* — U ovom radu su izloženi osnovni pojmovi iz oblasti elektronskog plaćanja, kao i korišćenje platnih Smart kartica i tehnike autentifikacije smart kartica. Zbog ekspanzije korišćenja platnih kartica online i offline dolazi do problema oko sigurnosti autentifikacije i mogućim prevarama. Uvode se tehnike koje povećavaju sigurnost korišćenja smart kartica u transakcijama.**

***Ključne reči* — smart kartice, autentifikacija smart kartica, platne kartice, kartice sa čipom.**

I. UVOD

OSNOVNI cilj ovog rada je da prikaže tehnike autentifikacije platnih smart kartica u finansijskim transakcijama offline i online. Želi se istaći prednost u odnosu na magnetne kartice u vidu povećane sigrnosti finansijskih podataka kao i uspešnosti transakcija.

U radu su predstavljeni razlozi za uvođenje smart kartica kojima se ukazuje na prednost u odnosu na magnetne kartice. Prikazuje se organizacija fajl sistema smart kartica, kao i funkcije odgovarajućih fajlova. Na kraju je prikazano korišćenje simetričnog kriptografskog postupka i potom korišćenje simetričnog kriptografskog postupka.

II. RAZLOZI ZA UVOĐENJE SMART KARTICA

Razlog zabrinutosti u vezi nastavljanja korišćenja tehnologije magnetnih kartica je porast prevara i zloupotreba kartica sa magnetnim trakama širom sveta. Prevaranti imaju dosta informacija o dizajnu ovih kartica što im omogućava da identifikuju sigurnosne propuste koji im mogu omogućiti prevaru.

U face-to-face transakcijama falsifikovanje magnetnih traka je postala velika pretnja[1,2]. Ova pretnja kombinovana sa sofisticiranim metodama praćenja PIN-a vlasnika kartice uzrokuje veliku štetu finansijskim institucijama. Asocijacije i operatori platnih sistema su počeli sa radom na smanjenju broja prevara. U ovom kontekstu prelazak sa magnetne trake kao nosioca finansijskih podataka na čip je veliki napredak. Termin "Čip" označava integrisano električno kolo u plastičnu karticu. Ovakav čip je poznat kao vrlo siguran.

Smanjenje prevara je postalo moguće zbog sledećih razloga:

- Vrlo je teško klonirati ove čip kartice, naročito tajni kriptografski parametri koje oni sadrže ukoliko nije skinut zaštitni sloj.
- Kroz njegovu mogućnost procesuiranja, čip je aktivno uključen u upravljanje rizikom na mestu kupovine. On je predstavnik izdavača i može da pomogne u sprečavanju prevara u lokalnim transakcijama za terminalom kada ne postoji pristup internetu ili mreži.
- Čip unapređuje proces određivanja falsifikovanih kartica, koristeći metodu atutentifikacije sa dinamičnim mehanizmima. On takođe omogućava veću sigurnost vlasniku kartice tokom off-line verifikacije i korišćenja PIN-a.

Asocijacije i operatori platnih sistema su prihvatili nova operativna pravila za njihove čip proizvode, koji su motivisali izdavače i prihvatioce da izvrše čip migraciju. Politika smanjivanja takse razmene za prihvatioce koji ne adaptiraju svoje terminale da prihvate čip katrice može biti dobar razlog da prihvatioci implementiraju čip tehnologiju. U isto vreme, izdavači i prihvatioci mogu biti ohrabreni da prihvate čip kroz odgovarajuću politiku obaveza. Ova politika može usloviti da izdavači i prihvatioci koji nisu izvršili čip migraciju preuzmu kompletan rizik u slučaju prevare u toku transakcije.

Zbog bolje mogućnosti donošenja odluka uz pomoć čipa na mestu kupovine, moguće je smanjiti trošak kontrole autorizacije. Ovo znači da trošak komunikacije koji se odnosi na on-line autorizaciju [3] transakcije može biti smanjen u situacijama gde rizik uređivanja kartica zajedno sa uređivanjem rizika terminala odlučuje da autorizacija može biti dozvoljena lokalno.

Obzirom na to da čip ima mogućnost obrade, platna kartica postaje "smart" (pametna). Aplikacije kartice mogu ponuditi mnogo fleksibilnije finansijske servise i da bolje odgovore na brze promene u finansijskim sistemima. Jedan čip može imati više aplikacija, koje omogućavaju višeaplikacionu dimenziju čip kartica. Ovo omogućava izdavaču da smanji troškove ulaganja za aplikaciju i da bolje kombinuju nekoliko instrumenata plaćanja koje zadovoljavaju različite platne potrebe.

III. ORGANIZACIJA FAJL SISTEMA SMART KARTICA

Operativni sistem smart kartica pravlja fajl sistemom koji čuva podatke potrebne za svaku aplikaciju kartice. ISO/IEC 7816–4[4] podržava dve kategorije fajlova: posvećeni fajlovi (dedicated files - DFs) i elementarni fajlovi (elementary files - EFs). Oni su organizovani po sistemu stabla, sa DF kao granama i EF kao listovima. Tipična organizacija fajl sistema kartice je prikazana na slici Sl.1.

Ovaj rad delimično je finansiralo Ministarstvo nauke Republike Srbije, Projekat tehnološkog razvoja TR 13012.

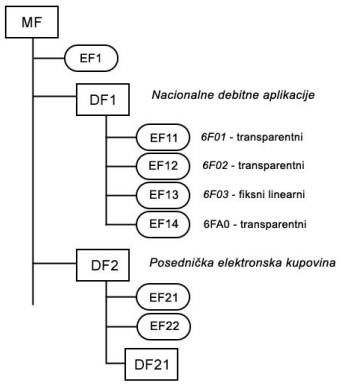
Emir Ugljanin, Univerzitet u Novom Pazaru, Srbija (e-mail: emirugljanin@gmail.com).

Milan Vidaković, Fakultet tehničkih nauka, Univerzitet u Novom Sadu, Srbija; (e-mail: minja@uns.ns.ac.yu).

Goran Sladić, Fakultet tehničkih nauka, Univerzitet u Novom Sadu, Srbija; (e-mail: sladicg@uns.ns.ac.yu).

A. *Master File i Dedicated File*

Najviši DF u hijerarhiji koji je koren drveta se naziva master file (MF), on je jedini obavezni DF u organizaciji fajlova. U primeru prikazanom na slici Sl.1., MF sadrži jedan list elementary file EF1 i dve grane dedicated file DF1 i DF2.



Sl.1. Organizacija fajl sistema smart kartica

Podaci koji se koriste za sve aplikacije u kartici (npr. administrativne i generalne bezbedonosne informacije kao što su ICC (integrated circuit card – kartica sa integrisanim kolom) serijski broj, ključevi kontrole pristupa, generalni PIN kartice kao i podaci koji se tiču upravljanja životnim ciklusom kartice) su snimljeni u elemntary file-u na MF nivou. Ova informacija može biti korišćenja od strane operativnog sistema za kreiranje novog DF-a na MF nivou.

Dedicated fajl DF1 sadrži 4 lista. Prva tri od njih (EF11, EF12 i EF13) su aktivni EF-ovi, dok je EF14 interni EF. Dedicated file DF2 sadrži samo dva lista, a to su aktivni elementary fajlovi EF21 i EF22. Svaki dedicated file može dalje sadržati druge niže po hijerarhiji dedicated fajlove. Na slici Sl.1. DF2 sadrži jedan pod-dedicated fajl DF21.

Dedicated fajl može biti predstavljen kao skladište podataka koji pripadaju jednoj aplikaciji kartice. Nekoliko elemenata podataka aplikacije kartice koji su semantički povezani, čuvaju se u istom elementary fajlu. Informacija kontrole aplikacije i finansijski podaci vlasnika kartice se čuvaju u elementary fajlu koji je sadržan i ustom DF-u. Svaki DF može da sadrži kriptografske ključeve za implementiranje raznih sigurnosnih usluga i svaki može imati PIN svoje aplikacije, koji može biti korišćen da unapredi mehanizam kontrole pristupa kartice sa više aplikacija.

B. *EF*

Elementi podataka aplikacije kartice su kodirani u elementary fajlu. Elementary file aplikacije kartice može biti podeljen u aktivne EF-ove i interne EF-ove:

- Aktivni EF čuva podatke koje aplikacija kartice ne prevodi, već ga pre koristi aplikacija terminala isključivo tokom izvršavanja protokola sa karticom.
- Interni EF čuva podatke kojima upravlja aplikacija kartice u svrhe menadžmenta i kontrole. Kriptografski parametri korišćeni za usluge sigurnosti obezbeđeni od strane kartice i PIN vlasnika kartice ili drugi verifikacioni kodovi vlasnika kartice (CHVs) se čuvaju u internoj EFs.

Zaglavlje fajla svakog EF-a čuva informacije o tipu EF strukture fajla i veličini fajla. On takođe čuva moguće akcije koje će se izvršiti na fajlu (čitanje, pisanje, poništavanje, povraćaj, uvećavanje) kao i uslov pristupa pod kojim aplikacija terminala može izvršiti tu akciju (generalni PIN kartice ili PIN aplikacije, autentifikacija sa simetričnim ključem, pristup uvek dozvoljen ili pristup nikad dozvoljen). [5]

IV. AUTENTIFIKACIJA KORIŠĆENJEM SIMETRIČNOG KRIPTOGRAFSKOG POSTUPKA

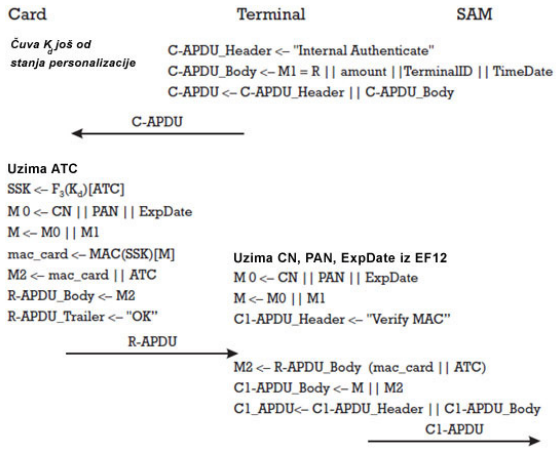
Jedina sigurnosna usluga predviđena u ovom profilu transakcije je autentifikacija kartice. Dinamička autentifikacija podataka bazirana na MAC-u (message authentication code) je sigurnosni mehanizam koji implementira ovu sigurnosnu uslugu.

Obzirom da je šema posednička, operator platnog sistema može lako da upravlja celim procesom glavnog menadžmenta za izdavača i prihvatioca u sistemu simetričkih kriptografskih tehnologija.

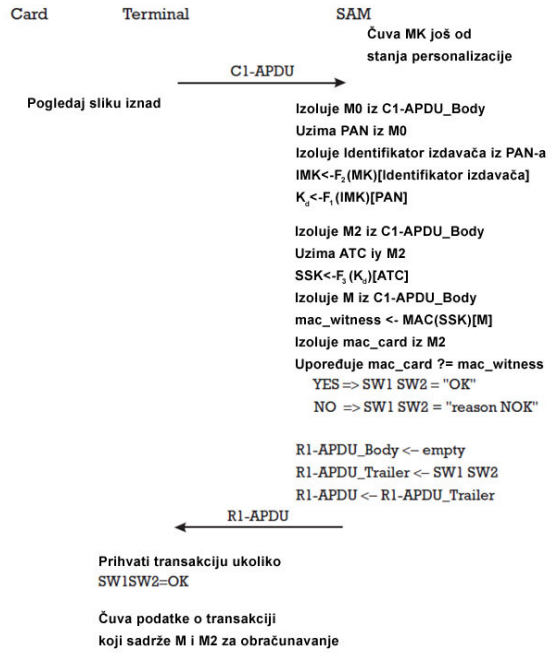
- Koristeći kanal distribucije sigurnosnih ključeva napravljenih unapred, svaki izdavač prima IMK (issuer master key). Operator platnog sistema izvodi izdavačkog master ključa (IMK) iz njegovog master ključa (MK). Identifikator izdavača služi kao informacija o razlikama *Diversification_Info* (npr. IMK=F_2 (MK) - identifikator izdavača) . Tokom faze personalizacije kartice, izdavač koristi IMK da bi napravio ključ K_d koji je simetrični ključ za računanje dinamičkog autentifikatora. Formula za računanje K_d je $K_d=F_1(IMK)[PAN]$. F_1 je jednoznačna funkcija, kao MAC koji je zasnovan na 64 bita dugačkom bloku cifara
- Operator platnog sistema obezbeđuje prihvatiocu sigurnosni aplikacioni modul (SAM) koji čuva MK. SAM je čip otporan na kvarove koji nije ugrađen u plastičnu karticu već je pre direktno ubačen u specijalizovani konektor unutar terminala. Primetimo da pošto ovaj čip sadrži MK, njegova otpornost na kvarove je osnovna pretpostavka za sigurnost operatora platnog sistema.

Fokusiraćemo se na procesiranje koje obavlja kartica da bi napravila dinamički autentifikator *MAC-card* kao i na njegovu verifikaciju od strane terminala, uz pomoć njegovog SAM, ukoliko je autorizacija obezbeđena offline. Slika Sl.2. i Sl.3 prikazuju računanje dinamičkog autentifikatora od strane aplikacije kartice.

Terminal priprema C-APDU sa zaglavljem (CLA, INS, P1 i P2) što odgovara internoj komandi autentifikaicje. Telo C-APDU sadrži poruku M1=R||*amount*||*TerminalID* ||*TimeDate*||. M1 je napravljen kao skupljanje sleva na desno nasumičnog broja R, iznos transakcije *amount,* identifikatora terminala *TerminalID*, i vremena/datuma kada je transakcija obavljena, *TimeDate*.



Sl.2. Računanje dinamičkog autentifikatora od strane aplikacije kartice



Sl. 3. Računanje dinamičkog autentifikatora od strane aplikacije kartice

Posle primanja ovog C-APDU aplikacija kartice obavlja sledeće obrade:

- Uzima trenutni Aplication transaction counter - ATC i koristi ga kao sredstvo odvajanja za dobijanje ključa sesije SSK iz jedinstvenog ključa kartice K_d(npr. SSK=$F_3(K_d)$[ATC]).
- Računa poruku M0=CN||PAN||ExpDate. Ova poruka je niz sleva na desno od imena vlasnika kartice (CN, PAN-a, i datuma isteka aplikacije kartice).
- Uzima poruku M1 iz C-APDU tela i pravi poruku M kao niz od M0 i M1 (npr. M=M0||M1)
- Računa dinamički autentifikator kao *mac_card*=MAC(SSK)[M]

Posle primanja R-APDU, terminal može da verifikuje offline tačnost dinamičkog autentifikatora *mac_card* primljenog od kartice, koristeći SAM. U ovom slučaju SAM se može tretirati kao udaljeni agent izdavača koji proverava dinamički autentifikator. Na kraju, terminal pravi M0 na isti način kao što je kartica koristeći elemente podataka CN, PAN i datum isteka aplikacije prethodno pročitan sa kartice. Terminal računa poruku M koja veže M0 i M1. Terminal priprema još jedan C1-APDU, ovog puta adresiran na SAM. Njegovo zaglavlje (CLA, INS, P1 i P2) odgovaraju *Verified MAC* komandi podržanoj od strane SAM. Telo ovog C1-APDU sadrži poruku M=M0||M1 spojene sa porukom M2=*MAC_card*||ATC.

Posle primanja C1-APDU, SAN obavlja verifikaciju dinamičkog autentifikatora *MAC_card*, prateći sledeće korake:

- Uzima PAN iz M0 i izoluje identifikator izdavača. Koristi ga kao sredstvo odvajanja da bi dobio IMK kao IMK=F_2(MK)[identifikator izdavača], gde je MK sačuvan u SAM-u još od njegove personalizacije.
- Koristeći PAN kao sredstvo odvajanja izvodi se jedinstveni ključ kartice K_d, korišćen za računanje dinamičkog autentifikatora, iz IMK (npr. K_d = F_i (IMK) [PAN]).
- Uzima ATC iz M2 i koristi ga kao sredstvo odvajanja za izdvajanje ključa sesije SSK iz jedinstvenog ključa kartice K_d (SSK=$F_3(K_d)$[ATC]).
- Računa dinamički autentifikator kao *mac_witness* = MAC (SSK) [M].
- Uzima dinamički autentifkator *mac_card* izračunato od strane kartice iz M2 i upoređuje ga sa ponovo izračunatom vrednošću *mac_witness*.
- Ukoliko su dve vrednosti jednake pozicija SW1 i SW statusnih reči u segmentu od R1-APDU kao OK. U drugom slučaju, pozicionira ih kao NOK. Vraća R1-APDU.

Posle primanja ishoda verifikacije dinamičkog autentifikatora u R1-APDU, terminal odlučuje da li će da odobri (SW1SW2=”OK”) ili odbije (SW1SW2=”NOK”) transakciju. Terminal čuva transakcione podatke (M, M2) u njegovu stalnu memoriju. Podaci će biti poslani prihvatiocu na proces obračunavanja.

Ukoliko terminal odluči da autorizacija obavljena online od strane IH, poruka zahteva aplikacije (1100) će prebaciti M=M0||M1 spojene sa porukom M2=*MAC_card*||ATC. Posle primanja ovih poruka sigurnosni modul IH će obaviti isto obračunavanje za verifikovanje dinamičkog autentifikatora kao obračunavanje opisano za SAM.

Kao što se može videti, u slučaju posedničkih latnih aplikacija koje mogu autorizovati offline transakcije uključujući male količine kriptografske tehnike simetričkog ključa su prikladne za implementiranje sigurnosnog mehanizma. U ovom slučaju operator platnog sistema kontroliše celokupno upravljanje ključem za izdavača i prihvatioca, što omogoćuava laku i niskobudžetnu operaciju kriptografskih algoritama simetričkog ključa. Neposredna posledicva je da kartica ne mora da implementira asimetričke kriptografske algoritme i stoga kriptografski koprocesor za duga aritmetička izračunavanja nije potreban u njegovoj hardverskoj arhitekturi. Ovo održava nisku cenu smart kartica. Korišćenje SAM u strukturi terminala dozvoljava offline verifikaciju dinamičkih autentifikatora zasnovanih na MAC-u. SAM uvećava cenu terminala, što je cena za

offline autorizaciju transakciju koje uključuju male količine. Ukoliko operator platnog sistema odluči da sve autorizacije moraju biti obavljene online nezavisno od količine transakcije, prisustvo SAM-a u terminalu nije više potrebno. U ovom slučaju, verifikacija dinamičkog autentifikatora se direktno obavlja od strane izdavača što uprošćava dizajn terminala i njegovu cenu.

Korišćenje kriptografije simetričkih ključeva je jeftino za obezbeđivanje vlasničkih platnih šema, bar sa tačke gledišta izdavača. Ovo ne znači da se tehnike kriptografije tajnog ključa više ne koriste za obezbeđivanje offline autorizacije transakcija u posedničkoj platnoj šemi. Sa dolaskom čip tehnologije može se predvideti da naglašavanje sigurnosnih izračunavanja pomeriti na čipove sa javnim ključem što će nepotrebno vartiti prisustvo SAM-a u hardverskoj strukturi terminala.

V. AUTENTIFIKACIJA KORIŠĆENJEM ASIMETRIČNOG KRIPTOGRAFSKOG POSTUPKA

Implementacijom offline usluge autentifikacije kartica koristeći simetrične kriptografske tehnologije potrebno je da svaki operator platnog sistema obezbedi prihvatioca sa posvećenim SAM-om. Ovo negativno utiče na kompleksnost terminal i proces uređivanja ključeva.

Otvorenost dizajna i međuoperabilnost uključuje korišćenje asimetričnih kriptografskih tehnika za implementiranje offline usluga autentifikacije kartica. Stoga, sa ciljem da se dokaže autentičnost finansijskih podataka personalizovanih u kartici, kao i činjenica da je kartica originalna, umesto korišćenja DDA (dynamic data authentication) mehanizma zasnovanog na MAC-u, neko mora koristiti digitalni potpis – baziran na DDA mehanizmu. U ovom slučaju nema potrebe za distribucijom osetljivih tajnih kriptografskih parametara od strane operatora platnog sistema, što je značajna korist. Prema ovome, hardverska struktura terminala je uprošćena upravljanje ključevima.

Smart kartice, svakako, moraju biti u stanju da proizvedu digitalni potpis, koji zahteva RSA operaciju u slučaju EMV™ čipova. Stoga, hardverska struktura čipa uključuje kriptografski koprocesor, za ubrzavanje računanja koje obavlja kartica. Šta više, nema više potrebe za EEPROM prostorom na čip karticama da čuva privatni ključ korišćen za generisanje potpisa kao i odgovarajući javni ključ sa pratećim sertifikatom izdavača da bude prosleđen terminalu za verifikaciju potpisa. Ove dodatne pogodnosti su skupe u pogledu snage računanja i stalnog prostora za skladištenje. Oni značajno uvećavaju cenu smart kartica koje podržavaju asimetričnu kriptografiju kada se uporedi sa čip karticama koje podržavaju samo simetričnu kriptografiju.

EMV⇔ nudi jeftino rešenje koje oslikava sigurnosnu zaštitu sa statičkim autentifikatorom, ali na međuoperativan način. Izdavač može ovog puta da računa statički autentifikator koristeći potpise bazirane na SDA mehanizmima. U ovom slučaju smart kartice neće ništa izračunati (nema potrebe za koprocesorom) već samo čuvaju više bajtova prema statičkim algoritmima zasnovanim na potpisima. Svakako, sigurnost je drastično smanjena ukoliko se EMV™ transakcija obavi offline i nikakva online pordška nije tražena od strane izdavača.

Statički autentifikator bi dokazao autentičnost finansijskih podataka personalizovanih u kartici, ali nebi obezbedio zaštitu od falsifikovanja. Postoji ubeđenje da je kloniranje javnih informacija smart kartica mnogo teže od kloniranja magnetne trake. Kloniranje javnih informacija, svakako, je još uvek moguće sa dobro opremljene hakere. Stoga, dok troši 400.000$ za čip kartice koje podržavaju simetričnu kriptografiju povrh troška implementacije magnetne trake, izdavač gubi korist visoke sigurnosti protiv prevara sa malim transakcijama obavljenim offline. Šta više, izdavač neće biti u mogućnosti da implementira metodu verifikacije asimetričnog kodiranog PIN-a vlasnika kartice.

Ova metoda bi unapredila sigurnost PIN-a vlasnika kartice na mestu kupovine, što je vrlo osetna prednost. Na kraju, izdavač nije u mogućnosti da implementira na višeaplikacionu čip karticu ostale "teške" kriptografske aplikacije kartice, kao međuoperativni elektronski novac CEPS, elektronsko brokerstvo, aplikaciju za elektronsku administraciju za plaćanje poreza. [6]

VI. ZAKLJUČAK

Analizom karakteristika zaključujemo da je bolje da se čip migracija obavi sa podrškom asimetričnog kriptografskog postupka nego sa podrškom simetričnog. Uz podršku asimetričkog kriptografskog postupka unapređuje se sigurnost PIN-a vlasnika kartice na mestu kupovine. Takođe uz to operator platnog sistema izbegava teret organizovanja i generisanja simetričnih ključeva i distributivnih procesa, i čini operativnom infrastrukturu javnog ključa.

LITERATURA

[1] Chan, E, "Fraud, a Common Virus in Asia," *Cards Now*, March/April 2001

[2] Stern, C., "Micro-Thief That 'Steals' Credit Cards," *Sunday Mirror Magazine*, January 28, 2001

[3] Cristian Radu "Implementing Electronic Card Payment Systems", poglavlje 3

[4] ISO/IEC 7816-4, "Identification Cards—Integrated Circuit(s) Cards with Contacts—Part 4: Interindustry Commands for Interchange," 1995.

[5] http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_5_basic_organizations.aspx

[6] Electronic Payment Systems for E-Commerce, Donal O.Mahony, Michael Peirce, Hitesh Tewari

ABSTRACT

This study examines basic concepts of electronic business as well as using payment Smart cards and techniques of authentication of smart cards. Because of expansion of using payment cards online and offline we have to deal with the issues of security of authentification and possible frauds. Techniques that increase safe use of smart cards in transactions are being introduced.

AUTHENTIFICATION SMART PAYMENT CARDS

Emir Ugljanin, Prof dr Milan Vidaković i Goran Sladić