



Elektronsko Bankarstvo: Lekcija 3: Platne kartice

zima 2019/2020

Branimir M. Trenkić

Platne kartice - Definicija

- **Osnovna komponenta** sistema elektronskog bankarstva

Definicija

- Specifičan **instrument bezgotovinskog plaćanja** **izdat** od strane finansijske, trgovinske ili specijalizovane organizacije koji **omogućava korisniku da izvrši svoju obavezu plaćanja** – jednostavnom **prezentacijom kartice**

Platne kartice - Istorijat

- Krajem 19. veka (1894) u SAD – Hotel Credit Letter Company izdaje svojim korisnicima kreditnu karticu za plaćanje hotelskih usluga
- 1914. godine, Western Union - izdaje svojim povlašćenim korisnicima karticu za odloženo plaćanje računa (“buy now pay later”)
- Između dva svetska rata – mnoge trgovačke, hotelske i naftne kompanije izdaju platne kartice koje omogućavaju plaćanje po povlašćenim cenama

Platne kartice - Istorijat

- Sve te **kartice** su bile **zatvorenog tipa** – mogle su se koristiti **samo u objektima kompanije** koja ih je **izdala**
- **1938. godine**, razne **kompanije počinju da prihvataju kartice drugih kompanija**
- Njihova upotreba značajno je povećana **posle II svetskog rata**



Platne kartice - Istorijat

- Prvu univerzalnu karticu –izdao je **Diners' Club** (**1950. godine**)
- Naplaćuje se korisnicima kartica **godišnja provizija**
- Njihovi računi se **zadužuju mesečno ili godišnje**
- **Trgovine** koje prihvataju plaćanje ovom karticom **plaćaju proviziju za usluge** Diners' Cluba od **4% do 7%** od iznosa računa



Platne kartice - Istorijat

- **Bankarski sistemi kreditnih kartica** podrazumevaju da:
- **Banka odobrava** račun **trgovca odmah** po prijemu računa o prodatoj robi,
- **Prikupljajući iznose** koji će biti ***zaračunati korisniku kartice* na kraju** ugovorenog perioda
- **Korisnik** ovaj iznos ***plaća banci*** u ***totalu*** ili u ***mesečnim ratama*** sa obračunatom kamatom

Platne kartice - Istorijat

- **1958. godine**, Bank of America kreira karticu **Bankamericard** koja je u početku važila **samo u Kaliforniji** ali se postepeno upotreba širila na teritoriju čitavih SAD
- Ovaj proizvod je kasnije evoluirao u VISA sistem
- **1966. godine**, grupa banaka je ustanovila karticu MasterCard
- Pretpostavlja se da je danas u upotrebi blizu dva triliona platnih kartica



Platne kartice – mesta korišćenja

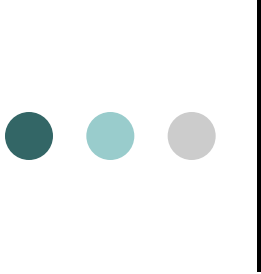
- Platne kartice se **primarno koriste na:**
- **Bankomatima** ili **ATM** (*Automatic Teller Machine*) **uređajima**
- **Šalteru** banke
- **POS** (*Point of Sale*) **terminalima**
- Neke kartice mogu biti korišćene i **za plaćanje preko Interneta, telefona ili faksa**

Platne kartice – sigurnost korišćenja

- Obezbeđuje se **putem** ličnog identifikacionog broja – **PIN** (*Personal Identification Number*)
 - Lična **tajna šifra** koju je banka izdavalac kartice prosledila korisniku kartice
- **Uručenje** platne kartice i PIN-a – **odvojeno!**
- **Korisnik** lično **unos** **PIN** preko **tastature** **ATM**-a ili **POS** terminala (ili svog **računara** – plaćanje preko Interneta)
 - **Najčešće** se koristi za **transakcije pomoću** **ATM**, **POS** terminala, sve više za plaćanje preko **Interneta**

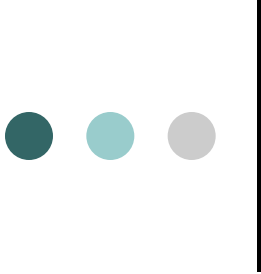
Platne kartice – sigurnost korišćenja

- **Neke banke** (radi sigurnosti plaćanja preko Interneta) – **pružaju mogućnost** da **umesto kucanja čitavog PIN broja** – izaberu iz padajućeg menija **dve cifre** koje se nalaze na određenim mestima u PIN kodu
- **PIN** najčešće **ima 4 cifre** – **10.000** mogućih **kombinacija**
- **Uz tri dozvoljena pokušaja** unosa – kradljivci kartice imaju **šansu 3/10.000** da pogode ispravan PIN pre nego se kartica blokira



Platne kartice – Prednosti za korisnika

- **Pojednostavljuje** se obavljanje **transakcija plaćanja**
- **Smanjuje rizik** koji proizvodi **nošenje gotovine**
- U slučaju **gubitka kartice**, korisnik **obaveštava izdavaoca** koji blokira njenu upotrebu – znatno **smanjuje mogućnost zloupotrebe**
- **Smanjuje troškove** obavljanja transakcija
- **Fleksibilnost** korišćenja
- Sistem plaćanja pomoću kartica – **ne poznaje nacionalne i valutne granice**



Platne kartice – koristi za banke

- ***Proširuje asortiman usluga*** koje pruža svojim korisnicima
- ***Smanjuju se troškovi poslovanja***
- Knjigovodstvo je ***jednostavnije***
- Banke **ostvaruju prihode od:**
 - **provizije** na ***plaćanja*** obavljena pomoću platne kartice,
 - **naplata troškova** održavanja,
 - **naplata troškova** gašenja,
 - ...¹²

Platne kartice – pravilo N°1

- **Napomena:** **banka** koja je izdala karticu je njen **vlasnik**, dok je **osoba koja poseduje** karticu – **korisnik**
- **Banka daje karticu** na korišćenje **pod uslovima navedenim u ugovoru** koji je sklopljen prilikom izdavanja kartice
- Kao vlasnik ona ima **pravo da je ukine**
- Kartica je **neprenosiva**



Platne kartice

- **Najveće (kartičarske) kompanije** koje posluju sa platnim karticama – organizovale su **vlastite elektronske obračunske sisteme**
- **MaserCard** i **VISA** - imaju **vlastite mreže za verifikaciju** svih transakcija koje se izvrše njihovim karticama
- VISA koristi **VisaNet sistem** – **tri računska centra**, jedan u Velikoj Britaniji i dva u SAD
- **Trgovci** koji prihvataju **plaćanja Visa karticom** – **povezani** su sa ovim računskim centrima



Podela platnih kartica – način izmirenja obaveza

- ***Način izmirivanja obaveza*** nastalih korišćenjem kartica, one se mogu ***podeliti na***:
 - ***Pre-paid kartice*** (*pay before*)
 - ***Debitne kartice*** (*pay now*) i
 - ***Kreditne kartice*** (*pay later*)



Pre-paid kartice

- Kartice sa *memorisanom monetarnom vrednošću*
 - Unapred *određen iznos* kojim korisnik raspolaže
- Pojavile su se *početkom 1970-ih na američkim univerzitetima* – unutar *zatvorene* univerzitetske mreže
- *1980-ih* pojava *telefonskih pre-paid kartica*



Pre-paid kartice

- *Dopuna monetarne vrednosti:*
 - **Jednokratne** ili
 - **Sa mogućnošću dopune**
- Ove kartice imaju
 - **veće provizije** i
 - **više kamatne stope**
- Pogodne za tinejdžere za kupovinu preko Interneta



Pre-paid kartice

- **Vrste** pre-paid kartica:

Gift kartice

- Prodaju ih **banke** ili **trgovci** **sa unapred uskladištenom vrednošću**
- Za jednokratnu upotrebu – uglavnom anonimne
- Mogu se koristiti **samo kod trgovca** koji ih je izdao

Teen kartice

- **Namenjene tinejdžerima** – dobar način da se najmlađi nauče da odgovorno **kontrolišu svoju potrošnju**



Pre-paid kartice

- *Vrste* pre-paid kartica:

Payroll kartice

- Služe **za uplaćivanje** mesečnih **plata**, **penzija** i **drugih primanja** za one **koji nemaju otvorene regularne račune**
- Ne glasi na radnika već na poslodavca – **vezana je za račun poslodavca**
- Radniku je **pomoću kartice omogućen pristup računu** koji je ustanovio **poslodavac**
- Mogu da se koriste **na bankomatima** i pojedinim prodavnicama pomoću **POS terminala**



Pre-paid kartice

- **Vrste** *pre-paid* kartica:

Trgovačke kartice (lojalnosti)

- Koriste se **u određenim trgovinama** ili **lancima prodavnica**
- Uglavnom daju odgovarajuće **popuste pri kupovini**

Internet kartice

- Koriste se samo **za plaćanje preko Interneta**
- Dobar način **sprečavanja zloupotreba** – na njoj je samo **vrednost potrebna za tekuću transakciju** (kupovinu)



Pre-paid kartice

- **Vrste** *pre-paid* kartica:

Kartice za prevoz

- Mogu biti **mesečne** ili se **po potrebi dopunjavaju**
- **Popularne** su kod putnika – **eliminišu potrebu preturanja po novčaniku** ili torbi u autobusu, železnici i slično

Kartice koje **izdaju univerziteti** svojim studentima

-



Pre-paid kartice

- Funkcionišu i ***u otvorenom*** i ***u zatvorenom*** sistemu
- U **zatvorenim** sistemima – ***izdavalac*** nudi kartice koje se mogu koristiti **samo za njegove proizvode** ili samo u određenim trgovinama
 - Primer
 - ***Kartice za prevoz***
 - ***Univerzitetske kartice***
- U **otvorenim** sistemima – mogu se koristiti **i van lokacija** koje pripadaju izdavaocu
 - Primer – ***payroll kartice***

Debitne kartice

- Direktno vezane za tekući račun
- Plaćanje – samo do iznosa pokrića na računu komitenta
 1. Plaćanje se vrši tek nakon autorizacije (provere stanja računa)
 2. Nakon toga automatski se zadužuje račun korisnika kartice
- Novijeg su datuma od kreditnih kartica
 - Mnoge debitne kartice su izdali Visa i MasterCard
 - Postoji i velik broj drugih kartica (uglavnom vezane za države, DinaCard)

Debitne kartice

- *Potreba veće kompatibilnosti i **prihvatanje evra kao nacionalne valute*** – uslovilo je njihovo **ujedinjenje** pod logom – **Maestro** (koji je deo MasterCard brenda)
- Neke kartice su **zadržale** **stari nacionalni brend** (**Solo** ili **Swatch** u Velikoj Britaniji)
- Ostale koriste **samo** logo Maestro
- **Banke** su počele da **izdaju debitne kartice 1980-ih** kako bi **smanjile korišćenje čekova**

Debitne kartice

- Akceptant – trgovac koji prihvata plaćanje određenom platnom karticom plaća proviziju za obavljenju transakciju
- Provizija – najčešće procenat od ukupnog iznosa transakcije
 - U Velikoj Britaniji – provizija kod plaćanja debitnom karticom je fiksna
 - Kod malih iznosa transakcija za trgovce je isplativije prihvatanje kreditnih kartica
 - U Nemačkoj i Belgiji slučaj je sasvim obrnut
 - ²⁵ Provizija za debitne kartice samo 0.3%



Debitne kartice

- **Provizija se deli** između
 1. **Banke izdavaoca** platne kartice
 2. **Banke prihvatioca** (koja je **sklopila ugovor sa akceptantom**)
- Obično **2/3 iznosa** ide **banci prihvatiocu**, a **1/3 banci koja je izdala** platnu karticu
- U nekim državama izdaju se samo **on-line debitne kartice**
- **Visa Electron** – izdaje se licima kojima ni u kom slučaju **nije dozvoljeno prekoračenje**

Debitne kartice - prednosti

- **Lako je može dobiti** i onaj ko nije dovoljno kreditno sposoban – pa ne može dobiti kreditnu
- **Korišćenje** debitne kartice je **limitirano iznosom** sredstava **na računu** – što korisnika sprečava da probije limit i preterano se zaduži
- Debitna kartica predstavlja **dobru zamenu za** papirne **čekove** – za razliku od čekova omogućuju **automatsku** finalizaciju transakcije
 - **Trgovac** u slučaju plaćanja čekovima **strahuje da li će mu iznos biti isplaćen**

Debitne kartice - nedostaci

- *U slučaju krađe*, odnos banke u slučaju *kreditne* kartice je *sasvim drugačiji* nego u slučaju *debitne*
- Iako su *debitne kartice* koje nose logo najvažnijih platnih kartica prihvaćene za gotovo sve transakcije kao i kreditne kartice – rentiranje automobila je jedan *izuzetak*

Kreditne kartice

- Omogućuje **korišćenje sredstava** kojim **banka izdavalac** kartice **kreditira korisnika** (**na osnovu** prethodno zaključenog **ugovora**)
- Omogućuje korisniku **da kupuje** i **podizē** **gotovinu** **do** prethodno utvrđenog **kreditnog limita**
- Odobreni kredit se može:
 - ***U celosti isplatiti*** na kraju **određenog perioda**
 - ***Isplaćivati u ratama***
- **Neizmireni dug** se smatra **odobrenim kreditom**



Kreditne kartice

- Prilikom **predaje zahteva za dobijanje** kreditne kartice – **procenjuje se kreditna sposobnost**
- **Podaci** na osnovu kojih se vrši procena:
 - I. Dobijeni **od samog korisnika**
 - Potrebno je **podneti dokaz o redovnim primanjima**
 - II. Uvidom u podatke koje **ima sama banka**
 - **Kreditni dosije** dužnika
 - III. Na osnovu **Izveštaja Kreditnog biroa**



Kreditne kartice

- Na osnovu Izveštaja **Kreditnog biroa**
- Formiran na nivou **Udruženja banaka**
- **Čuva podatke o kreditnim zaduženjima** i drugim dugovima bankama (i ne samo njima), **svakog građanina** koji se zaduživao kod ovih institucija u **poslednje tri godine**
- **Kako** korisnik kreditne kartice **otplaćuje svoj dug**
- Izveštaj Kreditnog biroa **ne može se dobiti** ukoliko se korisnik nije s time pismeno saglasio



Kreditne kartice

- Šira **primena** ovih kartica počinje **1950-ih godina**
- **Korisnik** kreditne kartice **daje** svoju **saglasnost za plaćanje** porudžbine:
 - **Potpisivanjem** računa
 - **Unošenjem** svog **PIN koda**

Kreditne kartice

- *Sistemi za elektronsku verifikaciju*
- *Omogućavaju trgovcu proveru ispravnosti **kartice** kao i **kreditnog limita korisnika** kartice za nekoliko sekundi **pomoću POS terminala***
 - ***Podaci** sa kartice **preizimaju se** sa **magnetne trake** ili sa **čipa***
- Prilikom naručivanja *preko Interneta* – kupac obično prosleđuje **dodatne podatke** – *bezbednosni kod* koji se nalazi **na poledini kartice**



Kreditne kartice

- ***Svakog meseca korisnik*** kreditne kartice ***dobija izveštaj*** koji sadrži:
 - ***Informacije o svim uplatama*** izvršenim preko računa
 - ***Naplaćenoj proviziji***
 - ***Preostalom zaduženju*** (na koje banka naplaćuje kamatu)



Kreditne kartice

- Postoje **razne varijacije kreditnih kartica**
Osigurane kreditne kartice
- Korisnik **polaže određeni iznos kao zalog**
- Banka **odobrava kredit do tog iznosa**
- Korisnik plaća banci kamatu za korišćenje svog novca!
- Izdaju se **korisnicima sa jako lošim** ili nepostojećim **kreditnim rejtingom**
- Nakon određenog perioda vremena – **dobija se ³⁵revolving kartica**



Kreditne kartice

- I na kraju...
- *Koja je razlika između odloženog plaćanja čekom i kreditnom karticom?*
- Kod plaćanja čekom prodavac *kreditira kupca* i *preuzima rizik*
- U slučaju kreditne kartice *kupca kreditira banka*
- **Trgovine** na svoju ruku *koriste kreditiranje čekom* jer im je skupa provizija koju plaćaju bankama za svaku transakciju karticom



Kreditne kartice

- ***Kreditne kartice*** mogu funkcionisati kao:
- **Charge kartice**
 - Korisnik je ***dužan da izmiri svoje obaveze u roku utvrđenom ugovorom*** sa bankom (30, 60 ili 90 dana)
- **Revolving kartice**
 - Odloženo plaćanje roba i usluga ***u neograničenom broju rata***
- **Installment kartice**
 - Izmirenje obaveza ***u jednakim ratama***



Charge kartice

- Kartica koja omogućava odloženo plaćanje
- Korisnik je dužan da **izmiri svoje obaveze u roku utvrđenom ugovorom**
- **Banka odobrava rok** od 30 do 90 dana – u toku kojih klijent troši novac
- **Po isteku tog roka** – banka ispostavlja račun po kome se plaća **celokupan** iskorišćeni **iznos** iz tog perioda

Revolving kartice

- Kao **forma revolving kredita**
 - **Revolving kredit** – kredit koji nema fiksni broj otplata (za razliku od *installment* kredita)
- **Složeni finansijski mehanizam** sa **različitim kamatnim stopama** za različite segmente dugovanja
- **Korisnik** može da **odluči** o broju i visini mesečnih rata prilikom otplaćivanja duga
- Korišćenje sredstava u visini **kreditnog limita**
- Limit se obnavlja nakon svake mesečne uplate



Revolving kartice

- Klijentu se pruža mogućnost da **samostalno izabere visinu mesečne obaveze**
- Postoji **minimalni procenat** mesečne obaveze
- **Do sredine 1990-ih** minimalna mesečna obaveza je iznosila **5%** od ukupnog **neotplaćenog duga**
- **Zbog konkurencije** danas je minimalan procenat **od 2% do 3%** od preostalog duga



Revolving kartice

- **Deo duga** koji **korisnik ne izmiri** – prenosi se u naredni mesec i na to zaduženje se dalje plaća kamata
- **Ukupno zaduženje** = **preneseno iz prethodnog meseca** + **novonastalo tokom meseca** – ne sme preći kreditni limit
- Ako pređe – zaračunava se **posebna kamata**



Revolving kartice

- ***Banke*** mogu ***revidirati kreditni limit***
- Kolika je ***konkurencija*** prisutna na tržištu bankarskih usluga
- Prilikom ***značajnih finansijskih događaja***
 - Novi posao
 - Preseljenje
 - Nastanak novog kredita ili likvidacija postojećeg



Revolving kartice

- Kreditnim institucijama je **preporučeno da u ugovore koje sklapaju** sa komitentima – **uključuje upozorenje**, kako bi ih **obeshrabrili da otplaćuju minimalni iznos**
- Većina banaka to **ignoriše** – ne objašnjavajući zašto to ne treba činiti
 - To može da rezultira **negativnom otplatom**
 $otplata < zaračnate kamate$
- Tako da preostali dug **neprekidno raste**



Revolving kartice

- **Od 2006.** u SAD – ***minimalna mesečna otplata*** mora da pokrije
 - ***zaračunate kamate*** i (+)
 - ***1% preostalog duga***



Installment kartice

- Kartica koja se može koristiti za ***izmirenje obaveza u jednakim ratama***
- Propisuje se ***kreditni limit***
- ***Svako plaćanje*** ovom karticom ***deli se*** na ***dogovoreni broj jednakih*** mesečnih ***rata***
- ***Prva rata*** se plaća ***na dan kupovine - bez kamate***
- Na ***ostale rate*** - koje se plaćaju u isti dan sledećih meseci - ***teče kamata***



Installment kartice

- Neke banke *ograničavaju broj transakcija* koje se *u toku jednog meseca* mogu obaviti ovakvom karticom
- *Banke* omogućavaju *beskamatnu kupovinu na rate* – kod *trgovaca* s kojima imaju ugovor
- Kad je reč *o kreditnom limitu* i prevremenoj otplati, *važi ono što je rečeno za revolving kartice*

Kreditne kartice - pogodnosti

- Omogućuju **veliku finansijsku fleksibilnost** i **dostupnost novca**
 - **Neodgovorno zaduživanje** uz visoke kamate može biti **veoma opasno**
 - **Prosečno američko domaćinstvo duguje 9.000 dolara** po revolving kreditnim karticama
- Omogućavaju korisnicima **druge pogodnosti** u zavisnosti od politike banke
 - **Odloženo plaćanje** ili **plaćanje na rate** bez kamate
 - Kupovinu **sa popustom**

Kreditne kartice - pogodnosti

- **Besplatno korišćenje** različitih usluga (osiguranje, tehnički pregled,...)
- Učešće u **programima lojalnosti** avio-kompanija ili trgovačkih i hotelskih lanaca
 - **Cash-back šema** – određeni procenat **potrošnje** (1%) **se vraća** kao kredit na mesečnom izvodu
 - **Grejs** (grace) **period** koji, zavisno od banke i tipa kreditne kartice, varira **između 20 i 30 dana**
 - **Ne zaračunava se kamata** ako se dug otplati u tom periodu

Kreditne kartice - pogodnosti

- **Za trgovca**, plaćanje pomoću kreditne kartice je **bezbednije od plaćanja pomoću čekova**
- **Banka** koja je izdala karticu **se obavezuje** da će isplatiti trgovcu u momentu kada je transakcija verifikovana – **bez obzira da li će korisnik kartice platiti svoj račun ili ne**



Kreditne kartice - pogodnosti

- Postoje i tzv. **sigurne kreditne kartice** (*safe credit card*) za koje je neophodno **položiti određeni depozit**
- Uobičajno je da **korisnik deponuje** između **100% i 200%** od iznosa željenog kredita

Kreditne kartice - problemi

- ***Veliki problem*** kod kreditnih kartica je njihova **bezbednost**
- Mogućnost ***krađe brojeva kreditnih kartica*** – postoji ***crno tržište brojeva*** kreditnih kartica
- ***Većina krađa preko Interneta*** – ***kopiranjem podataka*** od trgovca (*on-line* i *off-line*)
- Uvek ***kada su informacije*** sa kreditne kartice ***neekriptovane*** pre nego što se pošalju banci trgovca – **postoji bezbedonosni rizik**

Kreditne kartice - problemi

- Postoje slučajevi da **zaposleni u** legalnim **prodavnicama kopiraju brojeve** sa kreditnih kartica
- Koriste **male elektronske uređaje** kojima **čitaju podatke sa magnetne kartice**
- U slučaju krađe kartice – **lopov može da izvrši neautorizovane porudžbine** – sve dok korisnik ne **prijavi da mu je kartica nestala**
- Problem se može **rešiti korišćenjem PIN koda** koji korisnik treba da ukuca na tastaturi POS terminala ili računara ukoliko plaća preko Interneta

Kreditne kartice - problemi

- Da bi se **rešio problem kopiranja** kartica – izdaju se **kartice sa čipom** koje ne mogu biti kopirane
- U slučaju krađe kartice, **banka izdavalac refundira deo iznosa** koji je plaćen ukradenom karticom
- U nekim državama, **trgovac mora da plati štetu** ako nije tražio na uvid ličnu kartu što se obično zahteva
- Gubici zbog krađa kartica su veliki
 - Preko **500 miliona funti** u 2004. u GB
 - U SAD **4 milijarde dolara** u istoj godini

Kreditne kartice - problemi

- **Trgovac** (akceptant) **banci** (svojoj) **sa kojom ima ugovor** o prihvatanju kartica – **plaća proviziju**
- **Visina provizije zavisi** od dogovora sa bankom
- Obično iznosi **1-3%** za **veće porudžbine** i **3-6%** za **manje**
- **Deo provizije** se prosleđuje
 - **Banci izdavaocu** kartice i
 - **Odgovarajućoj asocijaciji** (**MasterCard/Visa**)
- **Banke izdavaoci** ostvaruju velike prihode od ovih provizija (**15% od ukupnog prihoda**)

Kreditne kartice - problemi

- Trgovac, takođe, mora da plati troškove za korišćenje POS terminala
- Ovi **dodatni troškovi** mogu da obeshrabe kupce da koriste kreditne kartice
- Banke sklapaju ugovore sa trgovcima koji onemogućuju da nude različite cene u zavisnosti od načina plaćanja (keš/platna kartica)
- Kako bi se **stimulisalo korišćenje** platnih kartica zakoni nekih zemalja zabranjuju davanje popusta za kupovinu pomoću keša

Kreditne kartice - problemi

- **Korisnici kreditnih kartica** takođe **plaćaju** neke **naknade**
 - Za **prekoračenje kreditnog limita**
 - Za **kašnjenje u otplati kredita**
 - Za **transakcije u inostranoj valuti**
 - Za **procesuiranje plaćanja** (npr., prilikom **naručivanja robe putem Interneta**)
 - **Mesečnu ili godišnju članarinu** (u nekim slučajevima kao procenat od kreditnog limita)

Kreditne kartice - problemi

- **Kreditne kartice** se mogu koristiti i za **podizanje gotovine** pomoću bankomata, do visine kreditnog limita
- **Banke** naplaćuju proviziju za ovu transakciju čak **iako ATM pripada banci** izdavaocu kreditne kartice
- **Kamata se zaračunava** od trenutka podizanja novca – **ne računajući grejs period** kao u slučaju korišćenja POS terminala

Kreditne kartice

- **Kreditne kartice** se ponekad koriste i za **pokretanje biznisa**
- Postoje priče da su *Sergej Brin* i *Lari Pejdž* pomoću kreditnih kartica **pokrenuli Google** kupujući potrebnu opremu
- **Tržištem** kreditnih kartica dominiraju **MasterCard** i **Visa**
- U udruženja koja predstavljaju ova dva najveća sistema **uključene su vodeće svetske banke** (*Bank of America, Wells Fargo,..*)



Podela platnih kartica – tehnologija izrade

- ***Prema tehnologiji izrade*** platne kartica možemo ***podeliti na:***
- ***Plastične kartice sa magnetnom trakom***
- ***“Pametne” (smart) kartice***



Kartice sa magnetnom trakom

- Kartice *sa digitalnim zapisom* podataka *na magnetnoj traci* (na poledini kartice)
- **Magnetna traka** – u to vreme, osnovni *medij za elektronsko memorisanje podataka*
- **Izum** kompanije **IBM** – ugovor sa vladom SAD za pravljenje ovog bezbedonosnog sistema
- **Osnovni problem** – *kako nalepiti magnetnu traku na plastičnu karticu?*



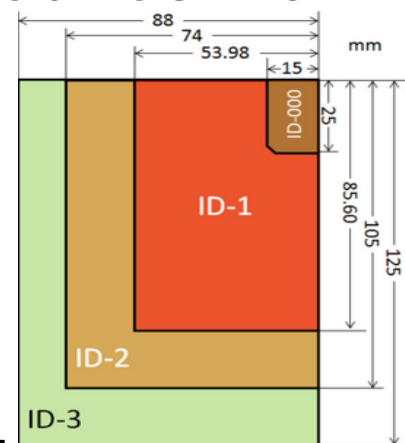
Kartice sa magnetnom trakom

- **Osnovna ideja** izumitelja:
- Magnetna traka bi trebala da:
 - Omogući ***skladištenje podataka u elektronskoj formi***
 - ***Minimizira korišćenje papira***
 - Obezbedi ***automatizaciju***

Kartice sa magnetnom trakom - Standardi

- Danas, **veliki broj ISO standarda** se odnosi na magnetne kartice

- **ISO/IEC 7810 - fizičke karakteristike**



- **ISO/IEC 7811 - tehnike snimanja** na karticu
- **ISO/IEC 7812 - identifikacija izdavača**
- **ISO/IEC 7813** - definiše **sadržaj finansijskih** kartica
- **ISO/IEC 8583 - razmena** (finansijskih) **poruka** nastalih korišćenjem kartica

Načini zapisa podataka

- Podaci su *utisnuti* (*embosirani*) na prednjoj strani i *zapisani* na magnetnoj traci koja je smeštena na pozadinu kartice
 - Kartice koje se mogu koristiti i uz pomoć *imprintera*
- Podaci *laserski ugravirani* ili odštampani na prednjoj strani
 - Upotreba isključivo *u elektronskim karticama*

Načini zapisa podataka

- Podaci odštampani *upotrebom bar koda na prednjoj strani*
 - *Ne koriste se* za finansijske kartice
- Podaci *isključivo na magnetnoj traci*
 - Hotelski “ključevi”

Klasične kartice sa magnetnom trakom - Sadržaj

- Podaci su *utisnuti* (**embosirani**) na prednjoj strani i *zapisani* na magnetnoj traci koja je smeštena na pozadinu kartice
- Na prednjoj strani se nalazi (prema ISO/IEC 7811):
 - **broj kreditne kartice** – identifikacioni broj (ISO/IEC 7812), koji se još zove i **PAN** (*Personal Account Number*)
 - **datum isticanja karte** (mesec i godina) posle kojeg kartica više nije validna
 - ⁶⁵**ime i prezime korisnika** (*cardholder*)

Klasične kartice sa magnetnom trakom - Sadržaj

- Na zadnjoj strani se nalazi:
 - **magnetni sloj**
 - moguće je čitati i pisati podatke
 - tri staze na magnetnom sloju
 - može se **oštetiti** (mehanički ili **razmagnetisati**)
 - **LoCo** (low-coercivity) i **HiCo** (high-coercivity)
 - **traka** (*tamper evident band*) **sa potpisom**
 - **Card Security Code (ili CVV2)**

Kartice sa magnetnom trakom

- Magnetna traka poseduje **3 staze za upis** određenih podataka
- Samo ***u stazi 1*** se može nalaziti ***alfabetски tekst*** (npr. ime korisnika kartice)

↑ 0.223" ↓	Track		Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	1	IATA	210	7 bits per character	79 alphanumeric characters
0.110"	2	ABA	75	5 bits per character	40 numeric characters
0.110"	3	THRIFT	210	5 bits per character	107 numeric characters



Kartice sa magnetnom trakom

Staza 3

- Praktično više *nije u upotrebi* kod većine svetskih kartica
- Obično se ni *fizički ne nalazi na kartici*

Kartice sa magnetnom trakom

Staza 1

- **Razvijena** od strane Međunarodne Asocijacije za Vazdušni Saobraćaj (**IATA**)

76 ALPHANUMERIC DATA CHARACTERS

SS	FC	PAN	FS	NAME	FS	ADDITIONAL DATA	DISCRETIONARY DATA	ES	LRC
		Primary Account No. (19 digits Max.)		Name (26 alphanumeric characters Max.)		No. of characters Expiration date [YYMM] 4 Service Code 3	No. of characters * PVKI 1 * PVV or Offset 4 * CVV or * CVC 3 Some or all of the above fields may be found with the discretionary data		
SS		Start Sentinel	%	FC		Format Code			
FS		Field Separator	^	LRC		Longitudinal Redundancy Check character			
ES		End Sentinel	?						

*(PVKI) PIN Verification Key Indicator
*(PVV) PIN Verification Value
*(CVV) Card Verification Value
*(CVC) Card Validation Code

Kartice sa magnetnom trakom

Staza 1

- **PAN** (*Primary Account Number*) – *broj (kartice) računa*

PAN	FS	NAME	FS	ADDITIONAL DATA
Primary Account No. (19 digits Max.)		Name (26 alphanumeric characters Max.)		No. of characters Expiration date [YYMM] 4 Service Code 3

- *Ime i prezime* korisnika kartice
- **Dodatni podaci**
 - *Rok isticanja važnosti* kartice
 - *Šifarnik usluga* (Service Code)
- ⁷⁰**Diskrecioni podaci**

Kartice sa magnetnom trakom

Staza 1

○ *Diskrecioni podaci*

DISCRETIONARY DATA	
	No. of characters
*PVKI	1
*PVV or Offset	4
*CVV or *CVC	3
Some or all of the above fields may be found with the discretionary data	

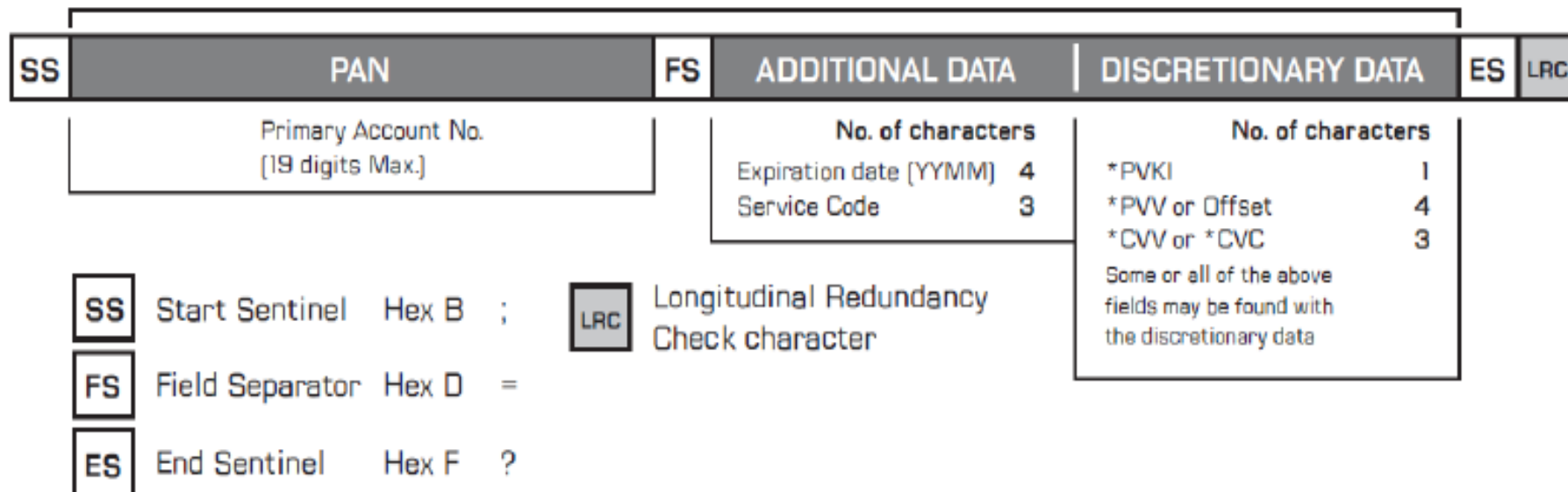
- **PVKI** (*PIN Verification Key Identifier*) – služi **za identifikaciju DES ključa pri verifikaciji PIN koda**
- **PVV** (*PIN Verification Value*) – služi **za verifikaciju PIN koda**
- **CVV** (*Card Verification Value*) – služi **za verifikaciju broja kartice**

Kartice sa magnetnom trakom

Staza 2

- **Razvijena** od strane Američke Bankarske Asocijacije (**ABA**)

37 NUMERIC DATA CHARACTERS





Kartice sa magnetnom trakom

Staza 2

- **PAN**
- **Rok isticanja** važnosti kartice
- **Šifarnik usluga** (Service Code)
- **PVKI (identifikator ključa)** i **PVV** i **CVV**



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)
 - Sadrži maksimalno **19 cifara (ISO/IEC 7812)**
 - Sastoji se **iz tri dela:**
 - 1. Identifikacioni broj (banke) izdavaoca (IIN)**
 - 2. Broj kartice** (*Card Number*)
 - 3. Kontrolna cifra** (*Checksum*)



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)

- 1. Identifikacioni broj (banke) izdavaoca (IIN)**

- **IIN** – *Issuer Identifier Number*
 - Zauzima prvih 6 cifara na magnetnoj traci
 - Započinje jednom cifrom - **MII** (*Major Industry Identifier*)
 - Pokazuje koja je **banka izdavalac kartice**
 - Ranije se zvalo **Bank Identification Number (BIN)**



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)

- 3. Kontrolna cifra** (*Checksum*)

- Poslednja cifra
 - Sračunava se **Luhn**-ovim (mod 10) algoritmom
 - Sprečavanje stvaranja lažnih brojeva (PAN-ova)

- 2. Broj kartice** (*Card Number*)

- Sve cifre između prvog dela (IIN) i kontrolne cifre (**9 do 12 cifara**)



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)
- Banke algoritamski definišu **validne PAN brojeve dodavanjem kontrolne cifre** (po **Luhn**-ovom algoritmu)

Primer: Neka je dat *account number* (**IIN** + **Card Number**) –

“7992739871”

Kompletirati PAN (Dodati validnu kontrolnu cifru)

Kartice sa magnetnom trakom

○ **PAN** (*Primary Account Number*)

Rešenje: Dakle, PAN će biti u formi **7992739871x**

Izračinati validnu kontrolnu cifru (x) primenom Luhn-ovog algoritma:

PAN	7	9	9	2	7	3	9	8	7	1	x
Dupliranje svake druge	7	18	9	4	7	6	9	16	7	2	x
Zbir cifara	7	9	9	4	7	6	9	7	7	2	x

Zbir cifara ⁷⁸**67+x**, zaključujemo **x = 3**, PAN = **79927398713**



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)
 - **MII** (*Major Industry Identifier*)

Vrednost	Vrsta
0	ISO/TC 68 and other industry assignments
1	Airlines
2	Airlines and other industry assignments
3	Travel and entertainment
4	Banking and financial
5	Banking and financial
6	Merchandising and banking
7	Petroleum
8	Telecommunications and other industry assignments
9	National assignment

Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)
 - **IIN** (*Issuer Identifier Number*) - **Prefiks**

Vrsta	IIN	Dužina
Visa	4xxxxx	16, 13
MasterCard	51xxxx-55xxxx	16
Visa Elektron (deb)	417500,4917xx,4913xx,4508xx,4844xx	16
Maestro (deb)	5020xx,5038xx,6304xx,6759xx,6761xx	16, 18
AmericanExpress	34xxxx, 37xxxx	15
Discover	6011xx	16



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)

Postupak validacije PAN-a

Broj kreditne kartice je **validan** ako je **broj** sračunat po **Luhn**-ovoj formuli - **deljiv sa deset**



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)
- Luhn-ov algoritam za validaciju:
 - **svaku drugu cifru** počev od druge cifre sa desna **pomnožiti sa dva**; sabrati cifre dobijenog broja i dodati na sumu
 - (**trik**: zbir cifara dvocifrenog broja **manjeg od 20** == **broj – 9**)
 - ostale cifre dodati na sumu
 - ako je dobijena suma deljiva sa 10, **broj je validan**



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)

Primer:

- **Proveriti validnost računa:**

49927398716



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)

- **Proveriti validnost računa:**

49927398716

Svaka druga cifra pomnožena sa 2:

- $(1 \times 2) = 2, (8 \times 2) = 16, (3 \times 2) = 6, (2 \times 2) = 4, (9 \times 2) = 18$

Suma svih cifara:

- $6 + (2) + 7 + (1 + 6) + 9 + (6) + 7 + (4) + 9 + (1 + 8) + 4 = 70$

Deljivost sa 10:

- $70 \% 10 = 0$



Kartice sa magnetnom trakom

- **PAN** (*Primary Account Number*)
 - **Prilikom transakcije** proverava se da li je PAN **iz prve staze** jednak onom koji se **nalazi u drugoj stazi**



Kartice sa magnetnom trakom

- **Rok isticanja** važnosti kartice
 - Zauzima **4 cifre** iza PAN broja ***i u prvoj i u drugoj stazi***
 - Formata je **yy.mm** (2 cifre za godinu i 2 za mesec)



Kartice sa magnetnom trakom

- **Šifarnik usluga** (Service code)
 - Nalazi se ***u obe staze***
 - **Sadrži tri cifre** koje označavaju ***koje usluge pruža kartica***
 - ***Prva cifra*** – **geografsko područje korišćenja + da li kartica podržava čip tehnologiju**
 - Kod ***Visa kartice***
 - ***Prva cifra = 1*** – radi se o internacionalnoj čip kartici
 - ***Prva cifra = 5*** – kartica je samo za lokalnu (nacionalnu) upotrebu



Kartice sa magnetnom trakom

- **Šifarnik usluga** (Service code)
 - **Druća cifra** - koja **vrsta obrade autorizacije** je obavezna
 - off-line
 - **on-line**
 - **Treća cifra** – (I) **vrste servisa** koje su na raspolaganju, kao i (II) **način verifikacije** vlasnika
 - Na primer:
 - **gotovina isključivo/PIN obavezan**
 - **bez ograničenja/PIN obavezan**



Kartice sa magnetnom trakom

- **Šifarnik usluga** (Service code)
 - Treća cifra - **vrste servisa** koje su na raspolaganju, kao i **način verifikacije** vlasnika

0 - bez restrikcija i PIN je obavezan

1 - bez restrikcija

2 - samo dobra i usluge (bez gotovine)

3 - samo ATM i pin obavezan

4 - samo gotovina

5 - samo dobra i usluge (bez gotovine) i PIN je obavezan

6 - bez ograničenja i PIN je obavezan kada je to izvodljivo

7 - samo dobra i usluge (bez gotovine) i PIN je obavezan kada je to izvodljivo

Kartice sa magnetnom trakom

- **PVKI** (*PIN Verification Key Indicator*)
 - Nalazi se u okviru **diskrecionih** podataka **u obe staze**
 - Može imati vrednost **1 - 6** – u zavisnosti od ove vrednosti **selektuje se odgovarajući DES ključ**

DISCRETIONARY DATA	
	No. of characters
*PVKI	1
*PVV or Offset	4
*CVV or *CVC	3
Some or all of the above fields may be found with the discretionary data	

Kartice sa magnetnom trakom

○ *PVV*

- *VISA verifikacioni metod i IBM-3624 sa ofsetom*
- Naziva se još i offset (IBM-3624)
- Zauzima *sledeće 4 cifre*
- Koristi se za proveru PIN koda kojeg je korisnik uneo prilikom obavljanja transakcije

DISCRETIONARY DATA	
	No. of characters
*PVKI	1
*PVV or Offset	4
*CVV or *CVC	3
Some or all of the above fields may be found with the discretionary data	



Kartice sa magnetnom trakom

Autentifikacija vlasnika preko PIN koda (IBM-3624)

○ *Tri PIN koda:*

- *prirodni* (natural) *PIN* – sračunava se *na osnovu PAN-a*
 - *Nigde se ne čuva!*
 - *Enkrijpcijom PAN-a namenski generisanim ključem – PGK (PIN Generation Key)*
 - *IBM 3624 metod verifikacije*
 - *Ne može biti korisnički selektovam – vezan za PAN*
- *vlasnikov PIN* (customer PIN)
 - ⁹² *zna samo vlasnik! – nigde nije zapisan*



Kartice sa magnetnom trakom

Autentifikacija vlasnika preko PIN koda (IBM-3624 sa offsetom)

○ *Tri PIN koda:*

- *offset* (offset)

- sračunava se na osnovu predhodna dva PIN-a (vlasnikov PIN – prirodni PIN)
- *upisan u kartici* i zove se *Pin Verification Value*
- *čuva se i na serveru banke!*
- služi pri verifikaciji PIN-a - *dodaje se na prirodni PIN* (bez prenosa) da bi se dobio vlasnikov PIN

Kartice sa magnetnom trakom

o IBM-3624 sa ofsetom verifikacioni algoritam:

PAN: 1234567890123445hex ulaz za DES algoritam

PIN simetrični DES ključ: 0123456789ABCDEF

Kriptovani PAN: 9A466AD30DFE0381hex (izlaz iz DES algoritma)

- prve četiri cifre su decimalizovane (A = 0, B = 1, ...)

Prirodni PIN: 9046

Offset: 2298 (zapisan na kartici)

Customer PIN: 1234

Provera (prirodni PIN + offset, bez prenosa)

Provera:

2298
+9046

1234



Kartice sa magnetnom trakom

- **VISA PIN Verifikacioni postupak**
- Postupak **izdavanja** + Postupak **verifikacije**
- Postupak se bazira na:
 - **DES** kriptografskom **algoritmu**
 - **Paru DES ključeva**
 - **PVK** (Pin Verification Keys)
 - Svaki izdavač kreira svoje vlastite PVK-ove koji se koriste samo u ovom postupku
 - Maksimalno 6 parova PVK-ova – **Tabela PVK ključeva**



Kartice sa magnetnom trakom

○ *Visa postupak izdavanja PIN-a:*

- **Slučajno** se generiše **PIN**
- Formira se blok podataka: $TSP = PAN + PVKI + PIN$
 - TCP (64bit) – Transformed Security Parameter
 - 11 krajnje desnih cifara **PAN**-a bez Kontrolne cifre
 - Ako **PIN** ima više od 4 cifre za postupak se uzimaju krajnje leve 4 cifre
 - **PVKI** – 1 cifra koja predstavlja indeks selektovanog para PVK-ova iz Tabele PVK ključeva



Kartice sa magnetnom trakom

- *Visa postupak izdavanja PIN-a:*

- Primer generisanog TCP-a:

- PAN = 4839 1234 5678 9019

- PVKI = 3

- PIN = 387283

TSP = 1234567890133872



Kartice sa magnetnom trakom

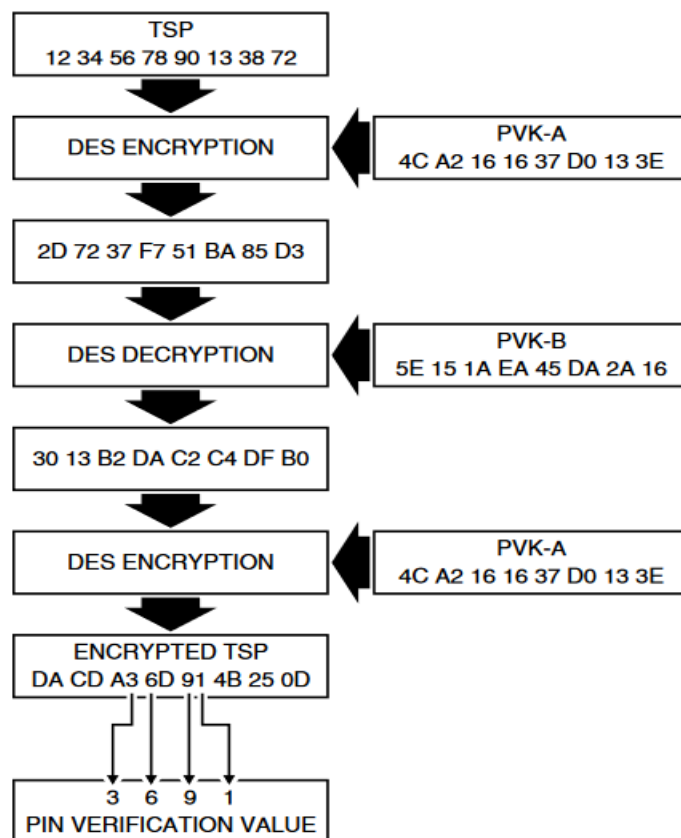
- *Visa postupak izdavanja PIN-a:*

- *Skeniranje enkriptovanih TCP-a:*

- Skeniranje s leva na desno izdvajajući cifre koje su manje ili jednake 9 dok se ne nađe 4 takvih cifara
 - Te 4 cifre predstavljaju – **PVV**
 - Proces skeniranja se završava.
 - Ako je broj takvih cifara manji od 4 – ponavlja se postupak skeniranja ali ovog puta samo cifara većih od 9 – svaka takva **cifra se decimalizuje**
 - Dopunom do 4 cifre proces skeniranja se završava

Kartice sa magnetnom trakom

- *Visa postupak izdavanja PIN-a:*
 - *Skeniranje enkriptovanih TCP-a:*





Kartice sa magnetnom trakom

- **Visa postupak izdavanja PIN-a:**
 - Iz rezultata 3DES enkripcije – **Referentni PVV (+ PVKI)**
 - **Referentni PVV + PVKI** se memoriše (kartica/BP banke)
 - PIN se automatski štampa u PIN pismo
 - Radna memorija je briše (resetuje na 0!)

Iz PVV se ne može rekonstruisati PIN!

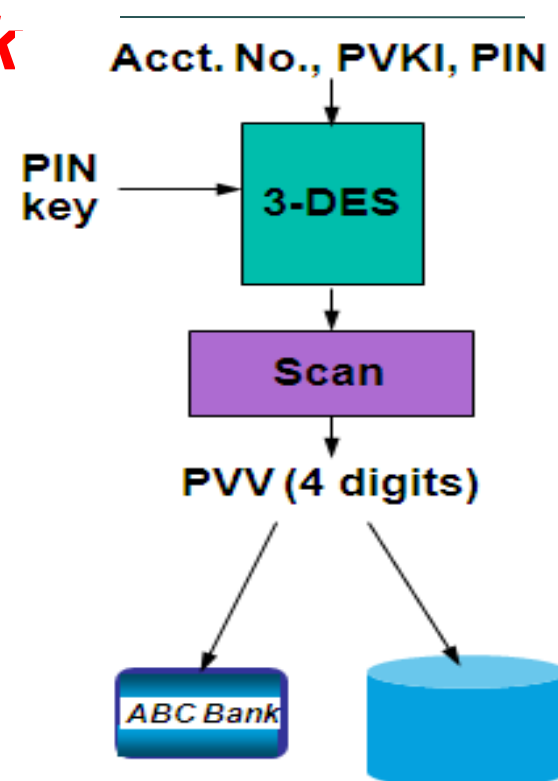
Kartice sa magnetnom trakom

VISA PIN Verifikacioni postupak

- Kada korisnik platne kartice ukuca PIN – na mestu verifikacije se izračunava

Transakcioni PVV

transformed security parameter
TSP



- Ako je **Referentni PVV = Transakcioni PVV**
 - Verifikacija je uspešna!



Kartice sa magnetnom trakom

- **CVV** (*Card Verification Value*)
 - Naziva se još **CVC** (*Card Verification Code*) ili **CSC** (*Card Security Code*)
 - Sadrži **3 cifre**
 - Koristi se **za proveru broja kartice** – poređenjem **podataka na traci** sa **podacima u bazi** podataka
 - Postoje **dva bezbedonosna koda**
 - **CVV1** (*transaction in person*)
 - **CVV2** (*card not present*)

Kartice sa magnetnom trakom

- **CVV** (*Card Verification Value*)
 - *Prvi* bezbedonosni kod
 - **CVV1** – *nalazi se šifriran na traci (čeksum podataka na magnetnom sloju)*, koristi se u transakcijama koje se obavljaju *uz prisustvo korisnika* (*transaction in person*)

DISCRETIONARY DATA	
No. of characters	
*PVKI	1
*PVV or Offset	4
*CVV or *CVC	3
Some or all of the above fields may be found with the discretionary data	



Kartice sa magnetnom trakom

- **CVV** (*Card Verification Value*)
 - **Drugi** bezbedonosni kod
 - **CVV2** – koristi se u **transakcijama** u kojima **kartica nije prisutna** (**card not present**)
 - Lokacija (Visa i MasterCard)
 - **Na poledini kartice**, **desno od potpisa** nalazi se broj – **poslednje tri cifre** su **CVV2** (Credit Card ID, **CCID**)
 - Lokacija (American Express)
 - **Na licu kartice** kao **odštampan broj** – **sadrži 4 cifre**

Kartice sa magnetnom trakom

- **CVV** (Card Verification Value)
 - **Lokacija CVV2 koda** na platnoj kartici





Kartice sa magnetnom trakom

- **CVV2** - Za *plaćanje preko Interneta*
 - Za plaćanje preko Interneta – *potrebno je poslati*
 - **CVV2**
 - **PAN broj**
 - **Rok isticanja važnosti kartice**
 - Zbog učestalih pokušaja krađa kartica i podataka sa njih – postalo je **obavezno slanje ovog bezbedonosnog koda** za sva plaćanja koja se obavljaju **bez prisustva korisnika**
 - Ovaj broj **ne treba mešati** sa **standardnim brojem računa** (**embosirane cifre** na licu kartice)



Kartice sa magnetnom trakom

- **CVV2** - Za *plaćanje preko Interneta*

- *Generiše se:*

- *Prilikom izdavanja kartice*
- Ekriptovanjem *tajnim ključem banke:*

- *Broj* kartice
- *Rok* isticanja važnosti
- *Šifarnik* usluga

- *Prilikom* obavljanja *transakcija* potrebno je *poslati ovaj broj* – kako bi se proverilo *da li kupac stvarno poseduje tu karticu*



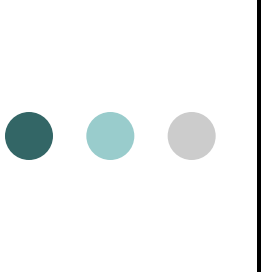
Kartice sa magnetnom trakom

- **CVV2** - Za *plaćanje preko Interneta*
 - Kako se **CVV2 kod ne nalazi na magnetnoj stazi** – uglavnom se koristi za transakcije koje se obavljaju *bez prisustva korisnika kartice*
 - Neki **trgovci** od nedavno *zahtevaju unos ovog koda* i kada se transakcija obavlja uz prisustvo korisnika CVV2 koda
 - Počev **od 2005.** ovo je *stalna praksa u nekim zemljama EU* (Engleska, Irska,...) kada se radi o *Amerikan Express* kartici



Kartice sa magnetnom trakom

- **CVV2** - Za *plaćanje preko Interneta*
 - *Korišćenje* ovog koda je i dalje *opciono*
 - *Transakcije* koje se obavljaju *bez ovog koda* pružaju *veću mogućnost zlonamernog otkrivanja podataka* sa kreditne kartice



Kartice sa magnetnom trakom - nedostaci

- Podaci koji se nalaze na njoj mogu biti *jednostavno pročitani i modifikovani*
- **Skimovanje** (*Card skimming*) – proces **čitanja podataka sa kartice**
- Uređaji koji to omogućuju - **skimeri**
- **Kloniranje kartice** – **pravljenja duplikata kopiranjem skimovanih podataka na drugu karticu**



Kartice sa magnetnom trakom - nedostaci

- To je razlog zbog čega se na kartici - ***ne mogu nalaziti poverljive informacije*** (lozinka, PIN)
- Prilikom transakcije ***ATM ili POS moraju on-line da proveriti PIN***, što ***zahteva vreme***
- Ovaj problem **može biti rešen** – ***smart karticom***



Smart kartice

- Termin SmartCard (*pametna kartica*) - u širem smislu
- Kartica koja ima *mogućnost da dovede u vezu informaciju(e) sa određenom aplikacijom*
 - *magnetna,*
 - *optička,*
 - *memorijska i*
 - *mikroprocesorska kartica*



Smart kartice

- ***U užem smisli***, smart karticama se smatraju:
 - ***Memorijske*** kartice i
 - ***Mikroprocesorske*** kartice



Smart kartice

- ***Sredinom 70-tih*** prošlog veka ***u Francuskoj*** – ***koncept kartice sa procesorom***
- ***Osnovna novina*** – ***poseduje algoritamsku zaštitu pristupa*** podacima
- Faktička ***primena u*** francuskim ***bankama*** - ***1992.***
- Najzastupljenija ***u Evropi***
- ***Predviđa se eksponencijalni rast tržišta*** smart kartica u narednih nekoliko godina



Smart kartice

- Postoje **dve osnovne kategorije** (u užem smislu) smart kartica

1. Memorijske kartice

- **kartica sa integrisanim kolom – ICC**
- **Optičke memorijske** kartice

2. Mikroprocesorske (čip-) kartice

- **Kartica sa procesorom**



Smart kartice

Memorijske kartice

- Sadrže samo memoriju i integrirano kolo sa ograničenim brojem **memorijskih funkcija**
- Ali ne i procesor za manipulaciju (obradu)
- Za **obradu** se koristi čitač kartice
- **Jednostavna tehnologija** izrade – **jeftina proizvodnja** (oko **1 dolar**)



Smart kartice

Memorijske kartice

○ Sadržaj:

● ***EEPROM (E²PROM)***

- electrically erasable programmable read-only memory
- Poseban oblik trajne memorije
- Kapacitet od nekoliko stotina bajtova do 8 KB

● ***ROM***

● ***Adresnu logiku*** i

● ***Primitivnu sigurnosnu logiku***



Smart kartice

Memorijske kartice

- Široka primena:
 - U segmentu **telefonskih kartica (pre-paid)**
 - U segmentu **kartica zdravstvenog osiguranja**
 - Kartice **za transport**
 - Pre-paid **kartice za parkiranje**
 - **Programi lojalnosti**



Smart kartice

Optičke memorijske kartice

- Izgledaju kao kartice na koje je **nalepljen deo CDROM-a**
- Mogu da uskladište **preko 4MB** podataka
- Jednom **uneti** podaci – **ne mogu se** više menjati
- Idealna za **čuvanje zapisa** – medicinski fajlovi, podaci sa vozačke dozvole
- Ove kartice **nemaju ugrađen procesor** – ali se može očekivati u budućnosti
- Cena¹¹⁹ izrade – **cena čitača** (nestandardni)



Smart kartice

Mikroprocesorske (čip) kartice

- Nude **veće mogućnosti skladištenja i sigurnosti podataka** – u odnosu na magnetne kartice
- Omogućavaju i **obradu podataka** koji se nalaze **na kartici**
- Koriste se u mnogim aplikacijama – naročito onim sa **ugrađenom kriptografijom**
 - Osnovna platforma **za čuvanje digitalnog identiteta**



Smart kartice

Mikroprocesorske (čip) kartice

○ Primeri ovih kartica:

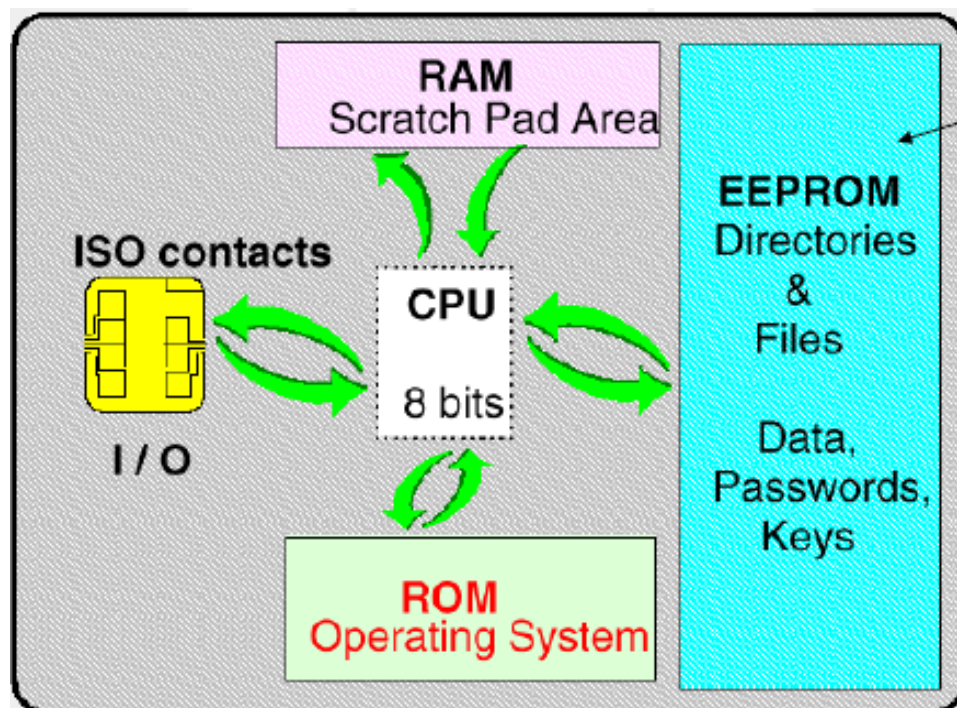
- Kartice sa ***uskladištenom monetarnom vrednošću, debitne, kreditne kartice***
- Kartice za držanje novčanih ekvivalenata – ***affinity kartice***
- Kartice koje omogućavaju ***bezbedan pristup*** mrežama
- Kartice koje se koriste ***u mobilnim telefonima***

Smart kartice

Mikroprocesorske (čip) kartice

○ Mikroprocesorska kartica sadrži:

- *Mikroprocesor*
- *Memoriju*
- *Ulazno/izlazni sklop*



Smart kartice

Mikroprocesorske (čip) kartice

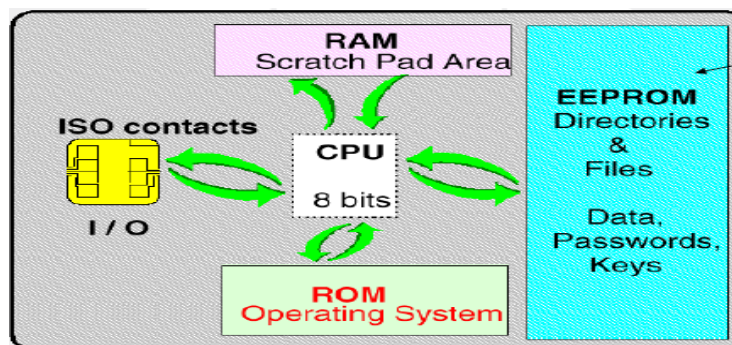
○ Mikroprocesorska kartica sadrži:

● **Mikroprocesor** – CPU

- Na njemu se *izvršavaju različite instrukcije* projektovane da
 - **Ograniče pristup** uskladištenim podacima
 - Onemoguće **neautorizovan pristup**

● **Memoriju**

- RAM
- ROM
- ¹²³EEPROM





Smart kartice

Mikroprocesorske (čip) kartice

EEPROM memorija

- Omogućava ***izmenu postojećih podataka***
- Podaci u njoj ***mogu biti zaključani*** – moguće im je pristupiti samo ***unošenjem PIN koda***
- ***Svaka transakcija*** se ***memoriše na*** samoj ***kartici***
- Kartica poseduje i ***ulazno/izlazni sklop*** preko koga se ***komunicira sa okolinom*** (čitačem)



Smart kartice

Mikroprocesorske (čip) kartice

- Sa pojavom smart kartica proširuju se aplikativne mogućnosti platnih kartica – kao rezultat:
 - a) Uvođenja autonomnosti obrade podataka na kartici u odnosu na sistem
 - b) Porasta kapaciteta memorije
- Primenom smart kartice moguće je sprečiti napade na lične podatke
 - Algoritamska zaštita pristupa
 - Bilateralna provera autentičnosti



Smart kartice

Mikroprocesorske (čip) kartice

- **Tipična** smart kartica:
 - 8-bitni procesor brzine **5 MHz**
 - **256KB – 1024KB** RAM-a
 - **6KB – 32KB** ROM-a
 - **2KB – 32KB** EEPROM-a
 - Operativni sistem – **JavaCard**, **MULTOS**
 - Najpoznatiji protokoli za upotrebu smart kartica – **SSL**, **SET**, EMV protokoli



Smart kartice

Mikroprocesorske (čip) kartice

- Smart kartice **mogu da sadrže** i **digitalni sertifikat** sa svim podacima o vlasniku kartice



Smart kartica kao platna kartica - pogodnosti

- Kartica se odnosi na lični račun koji korisnik ima u banci – a može da sadrži i informacije o potrošačkim preferencijama
 - Pristupa im se **klikom miša umesto popunjavanja** odgovarajućih **formi** na sajtu
- Omogućava **upravljanje** i **kontrolu troškova**
 - Automatski limiti i **izveštaji**
- **Programi lojalnosti** na Internetu – kartica služi za bezbedno centralno skladištenje bodova i nagrada
- **Mikro plaćanja** preko Interneta bez provizije



Prednosti smart kartice

A) Čuvanje ***mnogo veće količine podataka*** nego na magnetnoj traci

- Omogućuju ***svim učesnicima u transakciji uskladištenje dodatnih podataka na kartici***
- Tehnološka ***ograničenja magnetne kartice*** su bila ***očigledna***
 - ***Limitirani kapacitet*** za skladištenje podataka i ***nedostatak bezbedonosne logike*** – čini ih ***pasivnim uređajem***
- Brz porast snage i kapaciteta + smanjenje troškova izrade¹²⁹ – najbolja ***alternativa*** magnetnoj kartici

Prednosti smart kartice

A) Čuvanje *mного veće količine podataka* nego na magnetnoj traci

Tip kartice	Kapacitet podataka	Mogućnost procesiranja	Cena kartice	Cena čitača POS
Kartica sa magnetnom trakom	140 byte	nema	0,20 - 0,75 \$	750 \$
Memorijska kartica sa integrisanim kolom	1 Kbyte	nema	1 - 2,50 \$	500 \$
Kartica sa mikroprocesorom	8 Kbyte	8 -bit cpu 16 ili 32 bit	7 - 15 \$	500 \$
Optička memorijska kartica	4,9 Mbyte	nema za sada	7 -12 \$	3500 - 4000 \$

Prednosti smart kartice

B) Zaštita od neautorizovanog pristupa

- Na kartici je moguće **čuvati poverljive podatke (PIN)**
- Trgovac **ne mora** svaki put **on-line da obavlja autentifikaciju** korisnika
- Omogućavaju **čuvanje podataka** kao što su tajni ključevi i sertifikati nezavisno od računara – gde su podložni napadima virusa
 - Smart kartice imaju prednost u odnosu na **sofverska rešenja** bezbedonosnih problema (na PC-u)– **uređaj otporan na falsifikovanje**

Prednosti smart kartice

- C) Mnoštvo aplikacija** – više-namenski instrument
- Jedna kartica može da služi kao **pasoš**, **vozačka dozvola**, **identifikaciona** kartica, **finansijska (platna)** kartica ...
 - Na početku, **većina** smart kartica su **obavljale samo osnovnu kriptografsku obradu** – verifikacija digitalnog sertifikata
 - **Nove verzije** smart kartica - u stanju da čuvaju i izvršavaju **veliki broj aplikacija**
 - *Sun Microsystems Inc.* – **JavaCard API**
 - ¹³² Omogućuje **učitavanje različitih aplikacija** u karticu



Prednosti smart kartice

C) Mnoštvo aplikacija

- **Tipična** smart aplikacija treba da omogući:
 - **Upravljanje kešom**
 - **Pristup** finansijskim **servisima**
 - **Medicinske informacije**
 - **Javni prevoz**
 - Da obezbedi **funkcionalnost** koju već poseduje **platna kartica**



Prednosti smart kartice

D) Ne može biti jednostavno **kopirana** kao u slučaju magnetne kartice

- **Veliki broj krađa** magnetnih platnih kartica
- Potreba za ***naprednim mehanizmima autentifikacije*** – pronalaženje najbolje alternative – ***smart kartice***
- ***U Francuskoj***, uvođenjem smart kartica – ***krađe svedene gotovo na nulu***

Prednosti smart kartice

- E) Troškovi** obavljanja transakcija **su smanjeni**
- **Transakcije** koje **iziskuju** **vreme bankarskog službenika** i rad sa papirima – sada se **obavlja elektronski**
 - Omogućuje **plaćanje** **bez potrebe** ostvarenja **komunikacije** između trgovca i izdavaoca kartice
 - **Izbegavaju** visoke **troškove** **obrade čekova**
 - **Prednost u odnosu** na **keš** – mogućnost ostvarivanja **kamata na novac uskladišten na kartici**

EMV standard

- **Smart kartice** su uglavnom usaglašene sa EMV standardom
- Europay, MasterCard, Visa – 1993. godine zajedno rade na razvoju standarda i specifikacija za korišćenje smart kartice
- **EMV standardi** definišu **interakcije** na
 - fizičkom,
 - informacionom i
 - aplikativnom nivou **između**
- smart kartice i uređaja za procesuiranje transakcija



EMV standard

- *Dve* najpoznatije *implementacije saglasne EMV standardu:*
 - **VSDC** (**Visa**) *i*
 - **M/Chip** (**MasterCard**) *i* (M/Chip Fast)



EMV standard

- **Cilj i svrha standarda** – da omogući **interoperabilnost** između **smart kartica** zasnovanih na EMV i **terminala** širom sveta koji prihvataju plaćanje ovim karticama
- **Poboljšana** **bezbednost** **finansijskih transakcija** uz smanjenje krađe
- **Smart kartice** koje **nisu zasnovane na EMV** standardu imaju **sopstvenu kriptu zaštitu** koja je zasnovana na **lokalnim** privatnim **standardima**

EMV standard

- **Procesuiranje** transakcija pomoću smart kartica je sporije u odnosu na magnetne kartice
 - **Dodatna kriptografija**
 - Vreme potrebno za **prenos podataka** između kartice i terminala
- **Za potvrdu identiteta** uglavnom se koristi PIN kod a ređe potpisivanje računa
- U budućnosti će se verovatno koristiti **savremeniji sistemi za autentifikaciju** kao što su biometrijski
- Za sada **nedovoljno ekonomični**



EMV standard

- **EMV sesija** može biti podeljena u **5 faza**:
 1. Inicijalizacija: selektovanje aplikacije na smart kartici i čitanje odgovarajućih podataka;
 2. (opciona) Verifikacija kartice, SDA, DDA ili CDA;
 3. (opciona) Verifikacija korisnika kartice, pomoću PIN-a ili svojeručnog potpisa;
 4. Transakcija
 5. (opciona) Ažuriranje sadržaja kartice od strane izdavaoca, omogućuje izdavaocu da ažurira podatke na kartici neposredno nakon transakcije



EMV standard

Inicijalizacija

- U prvoj fazi EMV sesije, ***terminal dobija***:
 - Osnovne ***podatke o platnoj kartici*** (broj kartice, datum isteka važenja)
 - Informacije o ***funkcijama koje kartica podržava***
 - ***Informacije o konfiguracijama*** podržanih funkcija
- ***Opciono***, u ovoj fazi i kartica može da zatraži neke ***podatke od terminala***



EMV standard

Inicijalizacija

- Sesija započinje **selektovanjem određene aplikacije** (plaćanja)
- Nakon **razmene i usaglašavanja podataka** što se tiče selektovane aplikacije, prelazi se na sledeću fazu



EMV standard

Verifikacija kartice

- ◉ EMV sistemi koriste različite protokole **za proveru** da li je kartice koja se koristi – **legitimna**

- ◉ **Online**

- Zahteva **Internet konekciju** kako bi terminal mogao podatke za verifikaciju da pošalje **izdavaocu kartice** na proveru

- Slično proveru u slučaju magnetne kartice (CVV) – samo **mного bezbednije**

- ◉ **Offline**(SDA), **SDA** – Statička autentifikacija kartice

- ◉ **Offline**(DDA), **DDA** – Dinamička autentifikacija kartice



EMV standard

Verifikacija kartice

- **SDA** – Statička autentifikacija kartice
- Offline verifikacija kartice se vrši **bez Internet konekcije** sa izdavaocem kartice
- U EMV kartice su prilikom formiranja učitani:
 - Digitalno-potpisan sertifikat (od strane izdavaoca) i
 - Ključevi
- **Terminali** poseduju **javne ključeve** svih sistema plaćanja koji su prihvaćeni u toku njihovog konfigurisanja



EMV standard

Verifikacija kartice

- **SDA** – Statička autentifikacija kartice
- Procedura verifikacije ***započinje slanjem sertifikata*** kartice terminalu
- Terminal koristi odgovarajući javni ključ kako bi ***verifikovao sertifikat*** kartice
- Ako je verifikacija uspešna, ***preuzima javni ključ*** iz sertifikata (javni ključ kartice) i njega koristi u nastavku procedure verifikacije



EMV standard

Verifikacija kartice

- **SDA** – Statička autentifikacija kartice
- Kartica šalje **digitalno potpisane podatke** (uključujući **broj kartice+datum isticanja**) kako bi se verifikovala na terminalu
- Verifikacija je omogućena jer **terminal poseduje javni ključ** kartice
- Međutim na ovaj način verifikacije se ne otklanja mogućnost kloniranja kartice



EMV standard

Verifikacija kartice

- **DDA** – Dinamička autentifikacija podataka
- Slično SDA samo što se koriste **jedinstveni podaci** vezani za svaku transakciju
- Nudi **veći stepen sigurnosti**
- Asimetrična kriptografija (**tajni/javni ključ**) i
- Mehanizam **teksta izazova** (challenge-response mehanizam)



EMV standard

Verifikacija korisnika kartice

- **CVM** - *Cardholder Verification Method*
- Može biti ostvarena **na nekoliko načina**:
 - **Korišćenjem PIN-a**
 - Svojeručnim **potpisom**
 - **Nije potrebna** verifikacija
- Kartica šalji listu podržanih metoda verifikacije (**CVM Rules**) terminalu koja specificira pod kojim uslovima su koje CVM metode prihvatljive (sortirane po jačini)
- **Terminal selektuje metod** koji će se koristiti



EMV standard

Verifikacija korisnika kartice

- Ako je selektovana metoda **verifikacije pomoću PIN-a**, to je moguće realizovati **na tri načina**:
 - **Online PIN verifikacija**
 - U ovom slučaju banka izdavaoc vrši proveru PIN-a
 - **Offline tekstualni (izvorni) PIN verifikacija**
 - **Offline ekriptovani PIN verifikacija**



EMV standard

Verifikacija korisnika kartice

Offline tekstualni PIN verifikacija

- U ovom slučaju procesor na kartici proverava PIN
- PIN je prenet na karticu ***u izvornom obliku*** (plain text)

T→C: VERIFY(pin)

C→T: Success/ (PINfailed, tries_left) /Failed

tries_left – neuspešna verifikacija, preostali broj pokušaja¹⁵⁰ pre blokiranja kartice



EMV standard

Verifikacija korisnika kartice

Offline ekriptovani PIN verifikacija

- U ovom slučaju procesor na kartici proverava PIN
- PIN je prenet na karticu ***u enkriptovanom obliku***

T→C: GETCHALLENGE

C→T: nonce

T→C: VERIFY(encrypt(pin, nonce))

C→T: Success/ (PIN_failed, tries_left) /Failed

nonce – tekst izazova (slučajni broj koji može biti korišćen¹⁵¹ samo jednom u kriptografskoj komunikaciji)



Klasifikacija smart kartica

- U zavisnosti od metoda ***komunikacije*** i ***transfera podataka*** sa ***uređajima za čitanje*** smart kartice možemo podeliti na:
 - ***Kontaktne***
 - ***Beskontaktne***
 - ***Hibridne*** (kombinovane) kartice

Kontaktna smart kartica

- Standardna ili **kontaktna** smart kartica – istih **dimenzija kao** konvencionalne **plastične kartice**

- Pored toga,

ugrađena memorija + procesor

- Za njeno korišćenje potrebno je uspostaviti (fizički) kontakt sa

- Čitačem kartice (*card reader*) ili
- Terminalom



kako bi se priključila na naponski izvor

Kontaktna smart kartica

Čitač kartice

- **Snabdeva** integrisano kolo na smart kartici električnim naponom
 - **Čitanje** podataka sa kartice
 - **Upis** podataka u karticu
- Digitalni **ulazno-izlazni uređaj** koji **komunicira sa računarom (back-end)** u oba smera



Terminal

- Zaseban uređaj koji se **preko telekomun. mreže** spreže **sa centralnim računarom**
- Sadrži **SW/HW interfejs** za čitanje i upis na karticu



Kontaktna smart kartica

○ Čitači mogu biti

- **Samostalni** uređaji sa **LCD ekranom** i numeričkom **tastaturom**
- **Povezani** sa **personalnim računarom**
- **Integrirani** u
 - ATM uređaje,
 - POS terminale,
 - mobilne telefone.....



Kontaktna smart kartica

- **Memorija** i **centralni procesor** se mogu nalaziti:
- Na **posebnim čipovima**
 - Jedan čip – **procesor** i **operativna memorija**
 - Drugi čip – **sekundarna memorija**
- Na **istom čipu**
 - **Skuplje** rešenje
 - **Bezbednije** rešenje



Kontaktna smart kartica - nedostaci

- **Elektro-statičko pražnjenje** usled **lošeg kontakta** – može da **ošteti integrisano kolo** na kartici
- Ponekad korisnik **izvuče karticu** iz čitača **pre** nego što se **transakcija kompletira** – nije dobro za karticu (*Card Tearing*)



Kontaktna smart kartica

- Procesor kod kontaktnih smart kartica može biti **korišćen za autentifikaciju korisnika bez potrebe direktne on-line veze** sa centralnim računarom banke

Beskontaktna smart kartica

- **Beskontaktna kartice** (tzv. *Proximity* Cards) sadrže antenu kojom se prihvataju signali emitovani sa čitača
- Nije potreban direktan kontakt sa čitačem ili terminalom
- Kao i kontaktne – **ne sadrže bateriju**
- Koriste ugrađeni induktor koji hvata **radio signale** i koristi ih za napajanje elektronike u smart kartici
- Udaljenost od nekoliko santimetra **do pola metra**

Beskontaktna smart kartica

- **Nije potreban** fizički **kontakt** – time rešeni svi problemi vezani za kontaktne kartice
- Koriste se uglavnom kada je potrebno **transakciju izvršiti veoma brzo**
- Skuplje su u odnosu na kontaktne ali su i **dugovečnije**



Beskontaktna smart kartica - prednosti

- Za kupce – **komfornost** prilikom **plaćanja**, nije potrebno potpisivati račun ili unositi PIN kod
 - **Smanjenje vremena** za obavljanje **plaćanja**
- Za trgovce – **povećava** se **obim prodaje**, a nisu potrebne velike investicije za implementaciju ove tehnologije
 - Dovoljno je **postojećem POS** terminalu dodati RF čitač
- Za banke – **veći prihodi** od naplate provizija usled povećanog broja transakcija

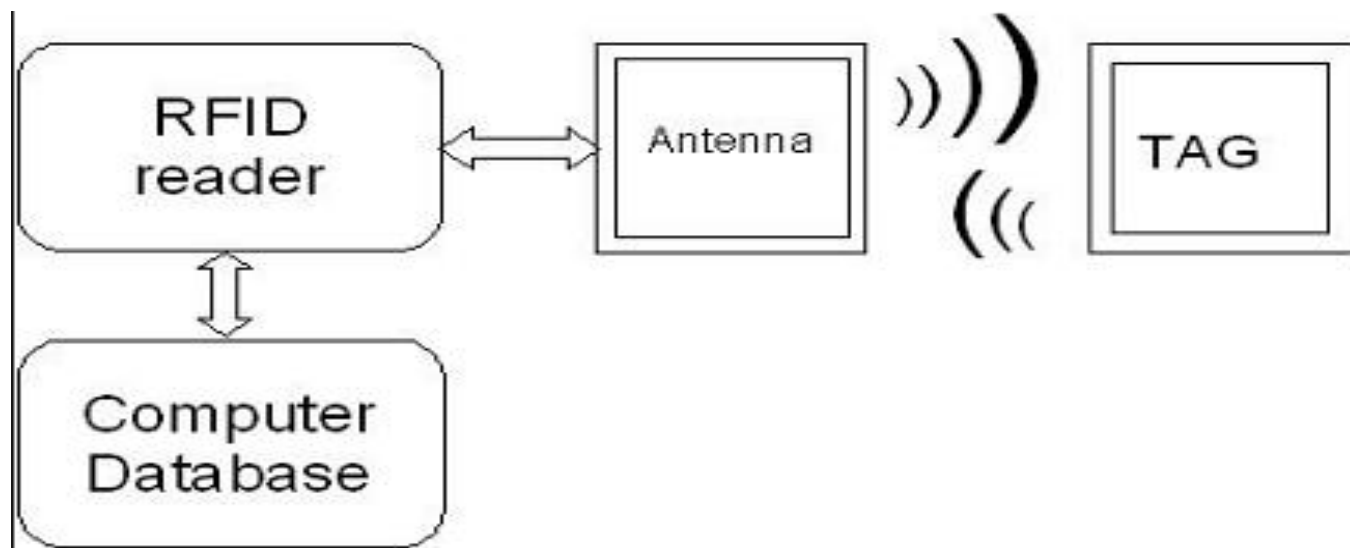


Hibridna smart kartica

- Imaju **moгуćnost komunikiranja** i **direktnim kontaktom** (u čitač kartica) kao i **pomoću RF signala**
- **Beskontaktni čip** se koristi kada je **potrebno brzo obaviti transakciju**
- **Kontaktni čip** se koristi za aplikacije koje zahtevaju **veću bezbednost**

RFID tehnologija

- **Identifikacija pomoću radio frekvencije – RFID**
(Radio-frequency identification)
 - **Koristi tehniku radio talasa za razmenjivanje podataka između čitača (reader) i uređaja koji se zove transmitter (tag) /transponder**



RFID tehnologija

- **Identifikacija pomoću radio frekvencije – RFID**
(*Radio-frequency identification*)
 - **RFID tag** – inkorporiran **u čip** koji se nalazi na smart kartici



RFID tehnologija

○ *Identifikacija pomoću radio frekvencije – RFID* (Radio-frequency identification)

- Sastoje se iz dva dela:

- *Prvi deo:*

- *Integrisano kolo (procesor)*

- Koje skladišti i obrađuje podatke
 - Modulacija i demodulacija RF signala

- *Drugi deo:*

- *Antena*

- Koja prima i šalje signale



RFID tehnologija

- *Identifikacija pomoću radio frekvencije – **RFID***
(Radio-frequency identification)
 - **Pasivni RFID**
 - ***Uključivanjem čitača*** on počinje ***emitovati signal*** određene frekvencije. Stvoreno elektro-magnetno polje daje energiju (struju) integrisanom kolu da bi se **RFID tag** (procesor) pokrenuo
 - **Aktivni RFID**
 - Sadrži ***sopstveno napajanje*** – bateriju
 - Neprekidno emituje signal (lokator)



RFID tehnologija

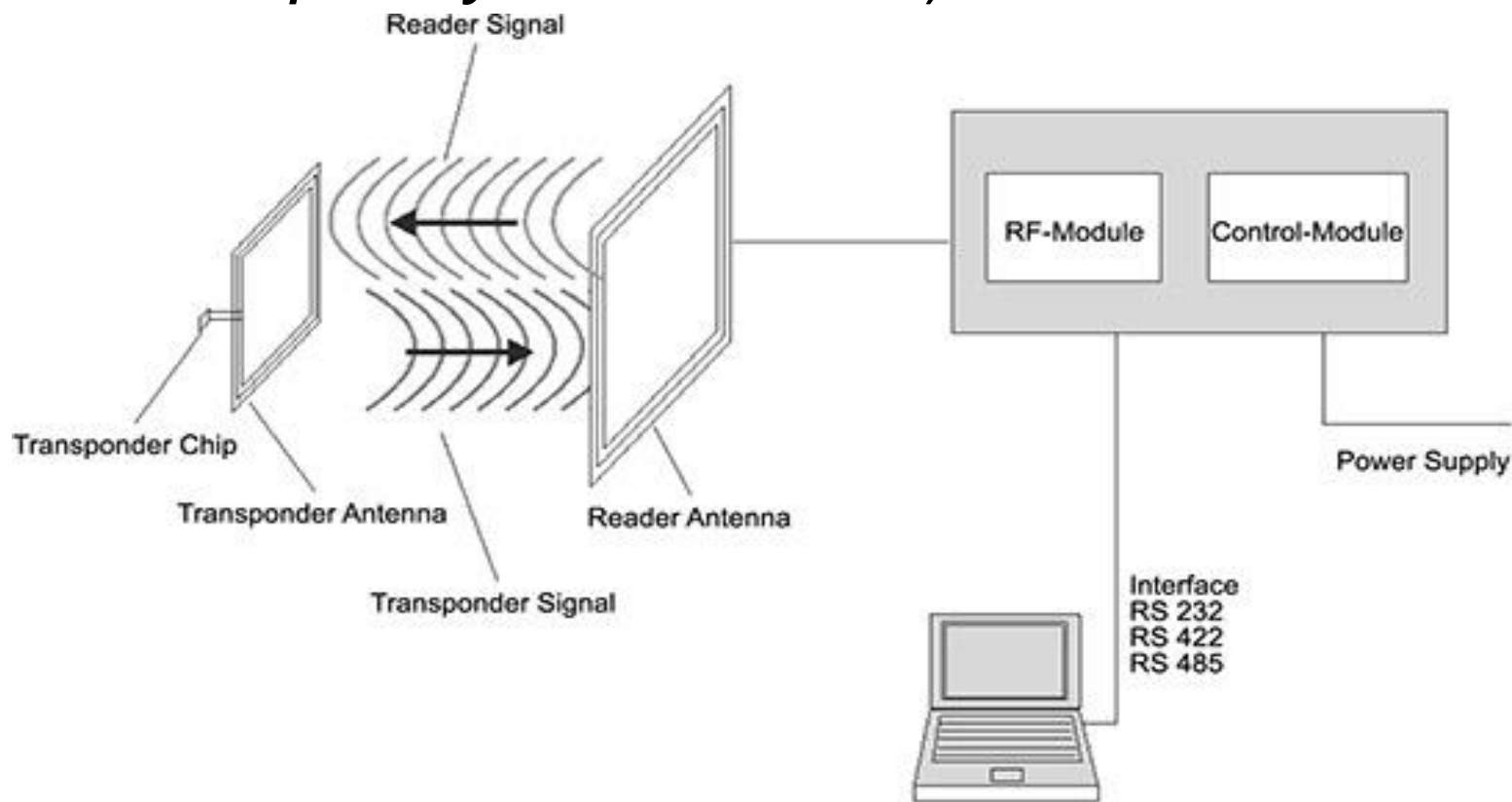
- ***Identifikacija pomoću radio frekvencije – RFID***
(*Radio-frequency identification*)
 - ***Polu-aktivni RFID***
 - Sadrži ***sopstveno napajanje*** – bateriju
 - Očekuje iniciranje od strane čitača

RFID tehnologija

- **Identifikacija pomoću radio frekvencije – RFID**
(Radio-frequency identification)
 - Metod **automatske identifikacije** - zasnovan na skladištenju i daljinskom očitavanju podataka pomoću – RFID tagova
 - U tag je **upisan jedinstveni identifikacioni broj (ID)** koji se putem radio talasa **emituje do prijemnika**
 - Prijemnik ga **prosleđuje u autorizacioni centar** gde se **ID vezuje za broj računa** u banci i vrši plaćanje

RFID tehnologija

- *Identifikacija pomoću radio frekvencije – RFID*
(Radio-frequency identification)





RFID tehnologija

- **Identifikacija pomoću radio frekvencije – RFID**
(*Radio-frequency identification*)
 - Mogu se **implementirati** u **životinje** ili **ljude** radi **identifikacije (praćenja)** (*aktivni RFID*)
 - Mogu se **automatski pročitati** (*pasivni RFID*)
 - Na njih se uglavnom gleda kao **zameni za bar kodove**



RFID tehnologija

- Identifikacija pomoću radio frekvencije – RFID
(*Radio-frequency identification*)

Primena

- RFID tagovi se koriste i za pasoše (**e-pasoši**)
- Prvi RFID pasoš je **izdat** u Maleziji **1998. godine**
- Sadrže **digitalnu fotografiju korisnika**, i **podatke o istoriji svih putovanja** – datumi ulaska i izlaska iz svih zemalja koje su posećene

RFID tehnologija - problemi

- **Nekompatibilnost frekvencija** koje se koriste za RFID u **Evropi** i **SAD** (još uvek **ne postoji standard**)
- **RFID čipovi** unutar RFID smart kartice mogu biti **podložni fizičkom uništenju** u slučaju jačeg udara
- **Glavni problem** koji nosi upotreba RFID tehnologije **je privatnost**
- Rešenje?

RFID tehnologija - problemi

- **Moguće je sprečiti napajanje presretanjem** elektro-magnetnih **signala**
- Na ovaj način se može **sprečiti čitanje podataka** na RFID kartici
- To se može preduprediti korišćenjem **anti-statičkog omotača** (aluminijumske folije) – **Faradejev kavez**

RFID tehnologija - problemi

- Kompanija Chase Corporation je **2007. godine** razvila **novi proizvod** – Paper Tyger za **zaštitu ličnih podataka** koji se nalaze na beskontaktnoj kartici
- Ovaj **RFID oklop** sadrži **sigurnosnu barijeru** za obezbeđivanje osetljivih podataka

