Sistemi elektronskog plaćanja

Sistemi elektronskog plaćanja

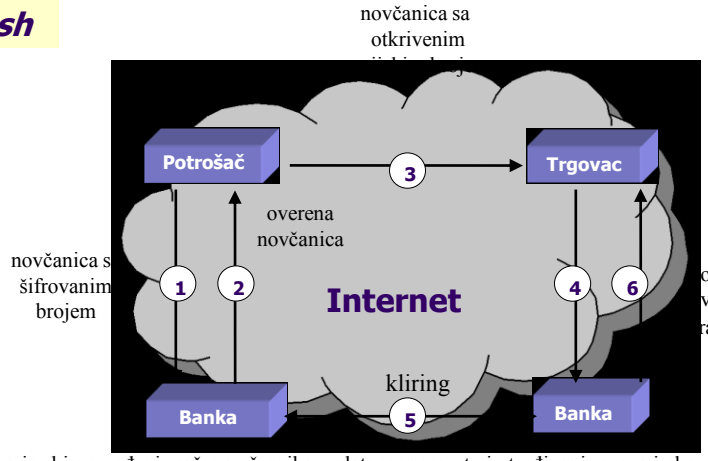
- elektronski novac - vrednost niza cifara u digitalnoj memoriji
  - brojevi su unikatni
  - potpuna anonimnost kupca
  - lakši za rukovanje od papirnog novca
  - troškovi transfera preko Interneta znatno su manji
- problem u vezi s nominalnom vrednošću
  - sistem morao biti sposoban da "vrati kusur" ili digitalne novčanice sa odgovarajućom vrednošću
- problem oporezivanja transakcija na Internetu
- mehanizmi za prepoznavanje i prevenciju ponovljenih plaćanja istim digitalnim novčanicama

2

Online plaćanja elektronskim novcem

- Najpoznatiji sistemi su: ***E-Cash***, ***DigiCash*** **i** ***NetCash***

E-cash



Kliring je zbirno vođenje računa učesnika u platnom prometu i utvrđivanje prava i obaveza po osnovu hartija od vrednosti i novčanih sredstava

Online plaćanja elektronskim novcem

E-cash

- **Bezbednost E-cash-a**:
  - asimetrični kriptografski algoritam
  - dopuna - pristup računa dodatno zaštićen ličnim lozinkama
- **Mane E-cash-a**:
  - veliki troškovi provere autentičnosti
  - nepogodnost za mikro plaćanja
  - potpuna anonimnost - ukinuta bilo kakva mogućnost praćenja transakcija

4

Online plaćanja elektronskim novcem

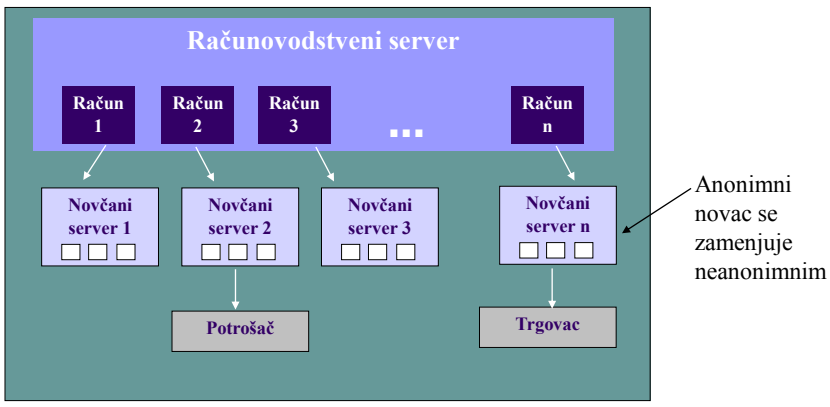
NetCash

- Razvijen na Univerzitetu Južne Kalifornije u SAD
- Upotreba postojećih računovodstvenih sistema i procedura u finansijskim institucijama – smanjenje početnih investicija
- Decentralizovan – lakše rešavanje problema velikog broja novčanica i učesnika
- Delimična anonimnost, kooperacija svih finansijskih institucija
- Bezbednost – pomoću kriptografskih alata
- Efikasniji za mikro plaćanja

5

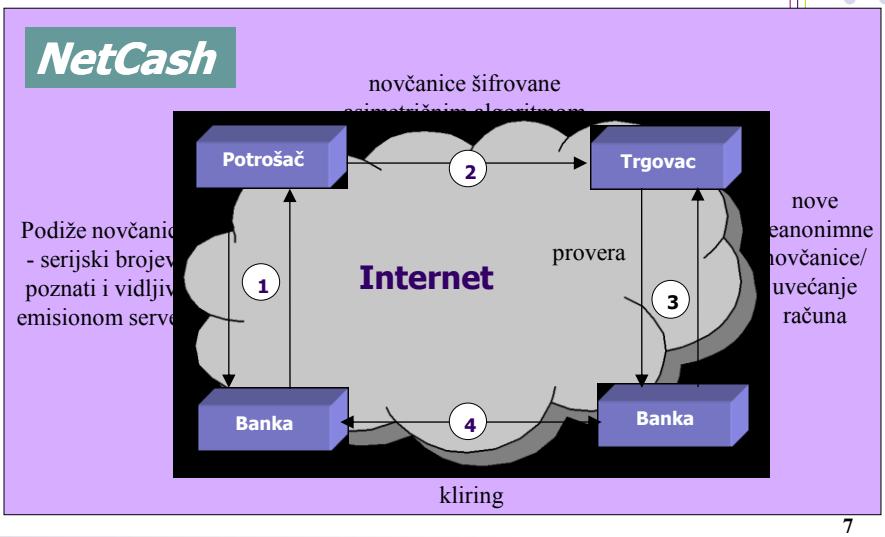
Online plaćanja elektronskim novcem

NetCash



6

Online plaćanja elektronskim novcem



7

Mikro plaćanja

- Elektronska plaćanja male vrednosti (u rasponu od nekoliko dolara do nekoliko centi, pa i manje)
- Specijalno dizajnirana za elektronsku trgovinu na Internetu
- Mali broj funkcionalnih sistema:
  - ***MilliCent*** - kupovine u iznosima od jednog centa, pa čak i manjim, ne nudi anonimnost plaćanja
  - ***CyberCoin*** - transfer novca sa potrošačevog privremenog računa na trgovčev privremeni račun koji su, posebno za tu namenu, kreirani u CyberCash banci u Virdžiniji
  - ***NetBill*** - proveru autentičnosti, upravlja računima, vrši obradu transakcija, fakturisanje i informisanje klijenata i korisnika u mreži

8

Mehanizmi i instrumenti elektronskog plaćanja

- ***Elektronski prenos novčanih sredstava (EFT – Electronic Fund Transfer)***
- Ostvaruje se korišćenjem sopstvene računarske mreže banaka ili integracijom sopstvene mreže u jednu veliku mrežu koja služi korisnicima mnogih banaka i finansijskih institucija
- Pre nego što se EFT mreža instalira potrebno je rešiti probleme zaštite:
  - Prihvaćeno je korišćenje tajnog ličnog identifikacionog broja (*Personal Identification Number* – PIN) zajedno sa bankarskom karticom koja nosi ostale informacije potrebne za pokretanje transakcija
- PIN treba da zna samo legitimni vlasnik kartice

9

Mehanizmi i instrumenti elektronskog plaćanja

Dužina PIN-ova treba da bude dovoljno velika da je mogućnost pogađanja prihvatljivo mala

Dužina PIN-ova treba da bude dovoljno kratka da bi vlasnici kartice mogli da ih zapamte

→ Dužina PIN-ova 4 do 8 decimalnih cifara

10

Realizacija EFT sistema sa PIN-om i tajnim ključem

- Pretpostavimo da su terminali bezbedni
  - tačnost inicijalizacije obrade zavisi od bezbednosti PIN-ova i kartica
- Za povećanje zaštite EFT sistema:
  - produžiti PIN-ove
    - povećava se broj pogrešnih pokušaja inicijalizacije (teško zapamtiti) i/ili
  - uvesti kartice čije je dupliciranje teško i skupo
- Dva rešenja:

1. Dve utisnute poruke: broj računa PAN (*Primary Account Number*) i lični ključ (*Personal Key – PK*)
2. Tri poruke: PAN i PK i kod za ličnu autentifikaciju (*Personal Authentication Code – PAC*)

11

Zahtevi u pogledu PIN brojeva

Za identifikaciju korisnika baziranih na PIN-ovima i bankarskim karticama:

- ✓ PIN mora da se čuva u tajnosti sve vreme,
- ✓ PIN ne sme biti zapisan na kartici,
- ✓ kartica treba da sadrži jedinstven broj (PAN) koji odgovara PIN-u vlasnika kartice,
- ✓ ako kartica sadrži kod za ličnu autentifikaciju (PAC), on mora da zavisi od PIN-a ali otkrivanje PIN-a iz osnove PAC-a mora da bude nepraktično,
- ✓ proces identifikacije mora biti vremenski zavisan (da spreči ponovni napad)

12

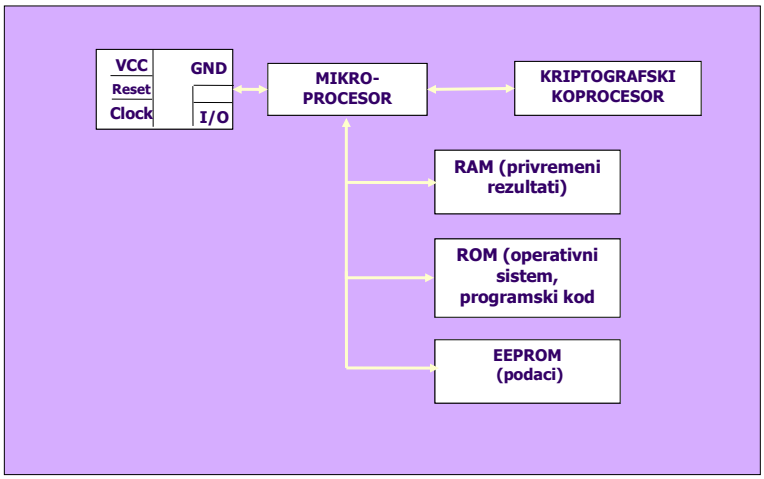
Inteligentne (SMART) kartice

SMART k-ce su sledeći korak za povećanje bezbednosti EFT sistema.

- SMART k-ca je personalni računar u malom koji uključuje:
  - **Procesor (CPU)** - pomoću koga se vrše razna izračunavanja,
  - ***Read-Only Memory* (ROM)** – memoriju na kojoj se nalazi operativni sistem,
  - ***Random Access Memory* (RAM)** – memoriju koja se koristi za privremeno skladištenje prilikom rada procesora i
  - ***Electronically Erasable and Programmable Read Only Memory* (EEPROM)** – memoriju u kojoj su smešteni podaci od interesa
- Ne poseduje tastaturu niti bilo kakav displej - funkcioniše tek u kombinaciji sa odgovarajućim uređajem za čitanje smart kartica – CAD (*Card Acceptance Device*)

13

Struktura inteligentne kartice



14

Životni ciklus inteligentnih kartica

- **Faza proizvodnje** – u čip se utiskuje tzv. ključ proizvođača, jedinstven za svaku smart karticu.
- **Faza pre-personalizacije** – čip se postavlja na karticu i testira, a ključ proizvođača se zamenjuje tzv. ličnim ključem, i nadalje se zabranjuje fizički pristup memoriji, a dopušta se isključivo logički.
- **Faza personalizacije** – na karticu se upisuju podaci o korisniku, upisuju se PIN i deblokirajući PIN. Upisuju se aplikacije i ostali podaci od interesa.
- **Faza korišćenja** – korisnik u ovoj fazi redovno koristi karticu, a prava pristupa pojedinim podacima reguliše aktivna aplikacija koja je pod kontrolom operativnog sistema.
- **Faza blokiranja** – kartica se poništava kada prestane potreba za njenim korišćenjem, jer se iz tehničkih, ali i bezbednosnih razloga ne preporučuje da pređe u ruke drugog vlasnika.

15

Bezbednost smart kartica

U EEPROM-u se nalaze lični podaci o vlasniku kartice, broj tekućeg računa, certifikati → od velikog interesa je da ovi podaci ne budu izloženi zloupotrebi

- Identifikacija pomoću PIN-a višestruko je bezbednija od bilo kog drugog načina identifikovanja:
  - ✓ PIN nikada ne putuje mrežom i otporan je na napade
  - ✓ polise koje regulišu dužinu i učestanost promene PIN-a mogu biti manje restriktivne od onih za *password*
  - ✓ izbegava se ugrožavanje bezbednosti sistema od strane osoblja zapisivanjem identifikacionih kodova na papire ili u datoteke
- Generisanja:
  - otiska prsta korisnika na čipu kartice
  - elektronske fotografije korisnika na plastičnoj podlozi same kartice

16

Primene inteligentne kartice

- **Finansije** - univerzalna platna kartica
- **Identifikacija** - za autorizaciju, odnosno, kontrolu pristupa objektima, kao vozačka dozvola, studentska iskaznica - univerzalna legitimacija
- **Telefonija** - bezbedno iniciranje poziva, identifikacija korisnika u GSM sistemu
- **Zdravstvo** - zdravstvena knjižica i zdravstveni karton
- **Saobraćaj** - elektronske karte i vaučeri za rezervisanje mesta, predaju prtljaga ili pri naplati putarine, parkinga
- **Informacione tehnologije** - kontrola pristupa računarima i računarskim mrežama

17