Elektronsko Bankarstvo:

Lekcija 2: Bezbednost transakcija

zima 2018/2019

Branimir M. Trenkić

Bezbednost transakcija na Internetu

- ***Nedostatak*** široko prihvaćenog ***sistema za bezbedna*** elektronska plaćanja - ***glavna prepreka*** porastu ***trgovine preko Interneta***
- ***Strah*** od ***davanja finansijskih informacija*** preko Interneta
- ***Od suštinske važnosti*** – ***obezbeđenje sigurnosti podataka*** koji se šalju preko Internetu
  - Npr. podaci sa platne kartice
- Iako postoji opasnost – ona je ***precenjena***
  - Gubitak ili krađa platne kartice u realnom svetu

Bezbednost transakcija na Internetu

- Da ***zaključimo***:
- Široko prihvaćeni ***bezbedni sistem plaćanja***
  1. Trenutno ***ne postoji***
  2. Predstavljao bi ***krupan korak u evoluciji*** Interneta

Bezbednost transakcija na Internetu

- ***Zahtevi*** koje je neophodno zadovoljiti da bi elektronske ***transakcije bile bezbedne***:

A) Obezbeđivanje ***privatnosti komunikacije***

- Zaštita ***tajnosti i poverljivosti*** podataka
- Zaštita osetljivih i ličnih informacija od namernog i nenamernog otkrivanja

B) Obezbeđivanje ***integriteta podataka***

- Detekcija ***neovlašćene izmene*** podataka u prenosu

Bezbednost transakcija na Internetu

C) ***Autentifikacija***

- ***Postupak provere identiteta korisnika*** (osoba, aplikacija ili uređaj) koji zahteva pristup sistemu ili mreži

D) ***Autorizacija***

- Postupak provere da li je osoba ili entitet legalno ***ovlašćen za prava*** koja zahteva

E) ***Neporicanje transakcije***

- Eliminisanje mogućnosti da inicijator transakcije ***porekne slanje*** poruke

Tehnike autentifikacije korisnika

- Savremeni ***načini provere identiteta*** korisnika na Internetu:
- Na osnovu nečega ***što korisnik poznaje***
  - Lozinka (***password***) ili ***PIN*** - ***zajednička tajna*** koju poznaje korisnik i onaj ko vrši autentifikaciju
- Na osnovu nečega ***što korisnik ima***
  - ***(Security) Token*** ili ***smart kartica*** - moguće neautorizovano korišćenje u slučaju gubitka
- Na osnovu nečega ***što korisnik jeste***
  - ***Biometrijske*** karakteristike (otisak prsta, glas,...)

Tehnike autentifikacije korisnika

Lozinka (password)

- ***Sprečava neautorizovan pristup*** informacijama, softveru ili nekom računaru
- ***Niz karaktera*** i ***simbola*** koje je ***potrebno uneti***

Tehnike autentifikacije korisnika

Lozinka (password)

- ***Efikasna*** lozinka
  - Mora da bude ***dovoljno dugačka*** - teška za pogađanje
  - Poželjno je da se ***često menja***

Tehnike autentifikacije korisnika

Lozinka (password)

- Prilikom unosa, obično se ***ograničava***:
  - ***Broj pokušaja*** i
  - ***Vreme unošenja*** ispravne lozinke

a) ***Statičke*** lozinke i

b) Lozinke za ***jednokratnu upotrebu***

Tehnike autentifikacije korisnika

(Security) Tokeni

- Fizički (***hardverski***) ***uređaji*** **– *tri tipa***:
  1. ***USB tokeni***
  2. ***Smart kartice***
  3. ***Tokeni koji generišu lozinku (password)***

Tehnike autentifikacije korisnika

Tokeni

USB tokeni

- ***Static password token***
- Relativno **sigurno sredstvo** za ***čuvanje osetljivih podataka***
- ***Otporni na falsifikovanje*** jer ih je ***teško kopirati***
- ***Jednostavni za rukovanje*** – direktno se ubacuju u USB port računara
- ***Ne zahtevaju instalaciju*** dodatnog specijalnog hardvera

Tehnike autentifikacije korisnika

Tokeni

Smart kartice

- ***Veličine platne kartice*** i ***sadrže procesor*** koji omogućuje ***skladištenje i obradu*** podataka
- ***Neophodno je*** na korisnikov računar ***instalirati kompatibilan čitač kartice***
- Kompletan proces autentifikacije:
  a) Čitač ***proveri validnost kartice***
  b) Nakon toga, ***unosi se PIN*** (drugi metod)

Tehnike autentifikacije korisnika

Tokeni

Smart kartice

- ***Prednost*** – interakcija između kartice i korisnika (čitača) se odvija ***direktno preko*** sopstvenog ***bezbednog interfejsa***
- ***Nedostatak*** – potrebna je ***instalacija posebnog hardverskog uređaja*** kao i odgovarajućeg softvera

Tehnike autentifikacije korisnika

Tokeni

Tokeni za generisanje lozinke

- ***Elektronski uređaj*** veličine kreditne kartice, izgleda slično kalkulatoru
- ***Sinhrono-dinamički*** *password* token (baziran na ***vremenu***)
- ***Asinhroni*** password token (baziran na ***događaju***)

Tehnike autentifikacije korisnika

Tokeni

Tokeni za generisanje lozinke

- Token ***generiše jednokratnu lozinku*** (***OTP***, *one time password*) koja se ispisuje na displej
- Nakon svakog uključenja (sesije autentifikacije) – ***nova lozinka***
- Lozinka ***traje samo 60 sekundi*** – time se sprečava zloupotreba

Tehnike autentifikacije korisnika

Tokeni

Asinhroni tokeni za generisanje lozinke

- ***Korisnik*** tipično izvršava ***peto-stepeni proces*** (CRAM) da autentifikuje svoj identitet i dobije slobodan pristup:
  1. ***Autentifikacioni server*** dodeli ***zahtev za upit korisniku*** (***challenge*** tekst)
  2. ***Korisnik*** unosi ***upit u*** njegov ***token uređaj***
  3. Token uređaj matematički izračuna ***tačan odgovor na upit*** autentifikacionog servera

Tehnike autentifikacije korisnika

Tokeni

Asinhroni tokeni za generisanje lozinke

- ***Korisnik*** tipično izvršava ***peto-stepeni proces*** da autentifikuje svoj identitet i dobije slobodan pristup:

  4. ***Korisnik*** unosi ***odgovor na upit*** zajedno sa korisničkim imenom ili *password*-om ili *PIN*-om

  5. ***Odgovor*** i korisničko ime ili *password* ili *PIN* ***se verifikuju od strane servera za autentičnost*** i, ako je sve u redu, pristup je dozvoljen

Tehnike autentifikacije korisnika

Tokeni

Sinhroni tokeni za generisanje lozinke

- ***Koristi vreme + tajni ključ*** u proračunavanju ***jednokratne lozinke***
- ***Vreme je sinhronizovano*** između ***token uređaja*** i ***autentifikacionog servera***
- Token ***koristi vreme*** na satu kao deo algoritma ***da generiše kod*** koji se periodično menja
- Tipičan sinhroni token pruža novi kod sastavljen od ***6 do 8 cifara*** svakih 60 sekundi; može raditi do 4 godine

Tehnike autentifikacije korisnika

Tokeni

Sinhroni tokeni za generisanje lozinke

- ***Ovaj kod*** se onda prikazuje korisniku i tada je on iskorišćen ***kao autentifikacioni kod*** ili
- ***kombinovan sa korisničkim imenom ili PIN-om*** formira ***autentifikacioni kod***, koji autentifikuje korisnika
  - U nekim implementacijama ***PIN se unosi u uređaj*** i onda biva iskorišćen kao deo algoritma za generaciju autentifikacionog koda

Tehnike autentifikacije korisnika

Tokeni

Sinhroni tokeni za generisanje lozinke

- Zahteva ***manje koraka za korisnika*** - da bi se izvršila autentifikacija mora uspešno proći sledeće:
  1. ***Korisnik čita vrednost sa*** njegovog ***token uređaja***
  2. ***Korisnik unosi vrednost*** sa token uređaja ***u log-in prozor*** zajedno sa njegovim *PIN*-om (korisn. imenom)
  3. ***Server za autentifikaciju izračuna svoju komparativnu vrednost*** baziranu na ***vrednosti sinhronizovanog vremena*** i **PIN-a** korisnika. Ako se komparativne vrednosti slažu, pristup je dozvoljen

Tehnike autentifikacije korisnika

Tokeni

Tokeni za generisanje lozinke

- ***Pristup korisnika*** nekom bankarskom servisu na Internetu (***jedna implementacija***):
  1. U odgovarajuću formu upiše ***identifikacioni broj tokena*** (***zajednička tajna*** korisnika i banke)
  2. Upiše generisanu lozinku sa displeja
- ***Server*** kada primi zahtev:
  1. Na osnovu identifikacionog broja tokena algoritamski ***generiše lozinku*** i
  2. Upoređuje je sa lozinkom koju je uneo korisnik

Tehnike autentifikacije korisnika

Biometrijske tehnologije

- Zasnivaju se ***na fizičkim ili psihološkim karakteristikama*** korisnika
- Omogućuju ***prevazilaženje manjkavosti*** standardnih sistema provere
- Prednosti biometrijskih sistema:
  - Znatno ***pouzdaniji sistemi provere*** – karakteristike tela ili ponašanja je ***teško falsifikovati***
  - Ne mogu biti ***zaboravljene*** (lozinka) ili ***izgubljene*** (token)
  - Zahtevaju prisustvo osobe koju treba autentifikovati

Tehnike autentifikacije korisnika

Biometrijske tehnologije

- ***Biometrijske karakteristike*** možemo podeliti u ***dve kategorije***:

1. ***Fiziološke karakteristike***
   - Vezane su za ***oblik tela***
   - ***Otisak prsta*** (korišćeno pre 100 godina)
   - Prepoznavanje rožnjače oka, oblik šake, lica,...
2. Osobine koje se odnose na ***ponašanje pojedinaca***
   - U široj upotrebi – ***svojeručni potpis***

Tehnike autentifikacije korisnika

- ***Višestruke*** metode autentifikacije
  - Znatno ***pouzdanije*** od korišćenja samo jedne metode
  - Korišćenje ***jedne metode*** – ***neadekvatno za visokorizične transakcije***
- ***Multi-faktorska*** autentifikacija
  - Koristi ***dva ili više faktora*** za verifikaciju identiteta
  - Izbor tehnike zavisi od procene rizika vezanog za određenu uslugu elektronskog bankarstva
  - Na primer, ***korišćenje bankomata***

Krađa finansijskih podataka

- ***Kako zaštititi podatke za autentifikaciju?***
- ***Kako neovlašćeno doći do podataka za autentifikaciju?***
- ***off-line*** i ***on-line krađe*** finansijskih podataka
- ***off-line*** krađe finansijskih podataka
  - Napadom na klijentov PC ***posredstvom malicioznog softvera*** (virusi, trojanski konji)
  - Navođenje klijenta da dobrovoljno otkrije svoje finansijske podatke – ***phishing***
  - ***pharming***

Phishing

- ***Lažni e-mailovi*** kao da su došli od *eBay*, *PayPal* il neke druge bankarske institucije
- Traži se da se ***klikne na link koji je u mail-u***, a potom da se ***unese korisničko ime i lozinka***

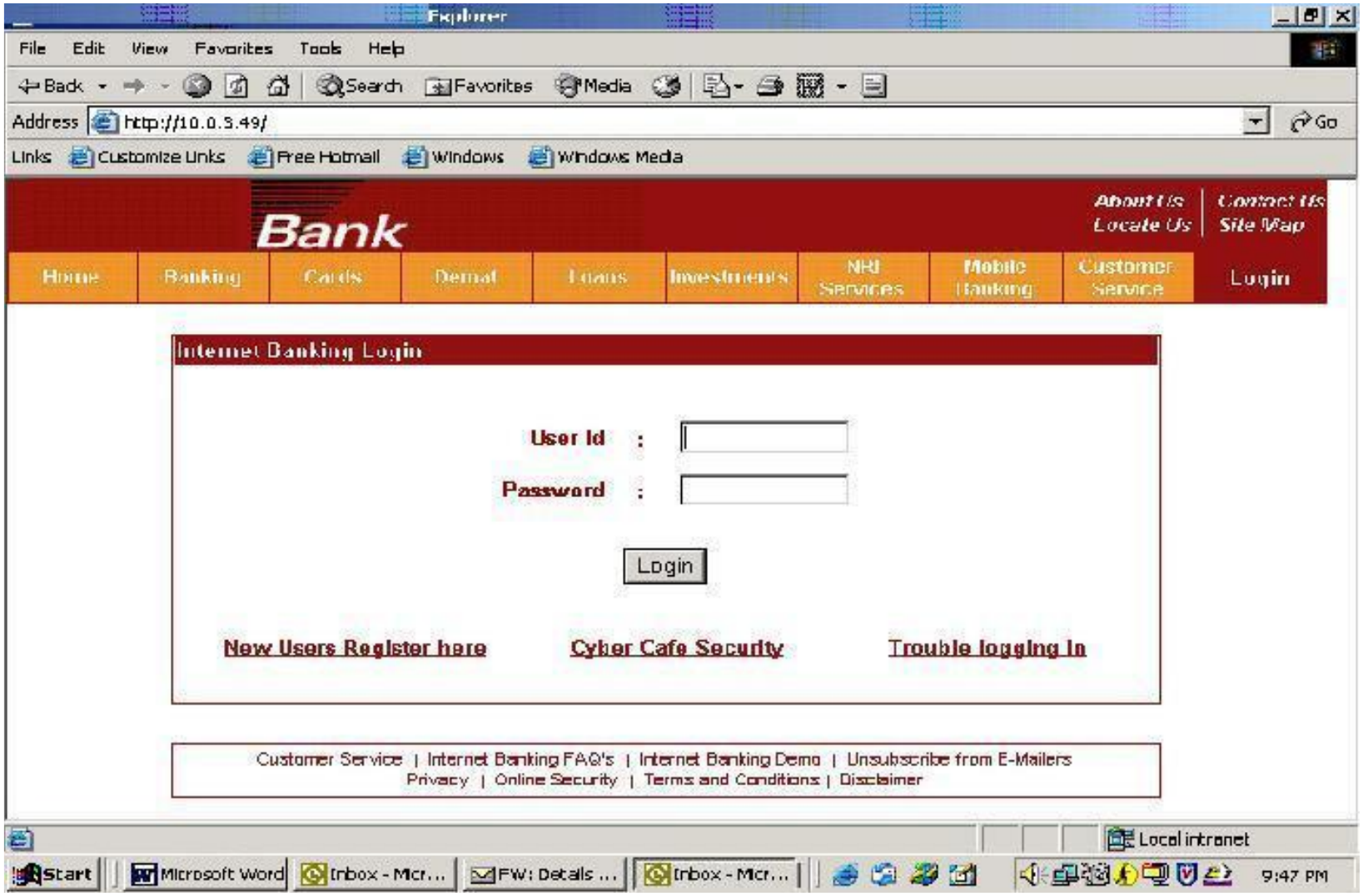
Phishing

- Ova vrsta prevare ***nije vezana*** striktno za Internet
- Može se realizovati ***i kontaktom telefonom***
  - ***višing*** (*Voice phishing*) što bi značilo pecanje putem glasa
  - Nakon pozivanja određenog broja uneti broj računa i svoj PIN
  - Prevaranti mogu koristiti **lažni *caller-ID***
- Može se realizovati ***i SMS porukama***
  - ***smišing*** - što bi značilo pecanje putem SMS-a

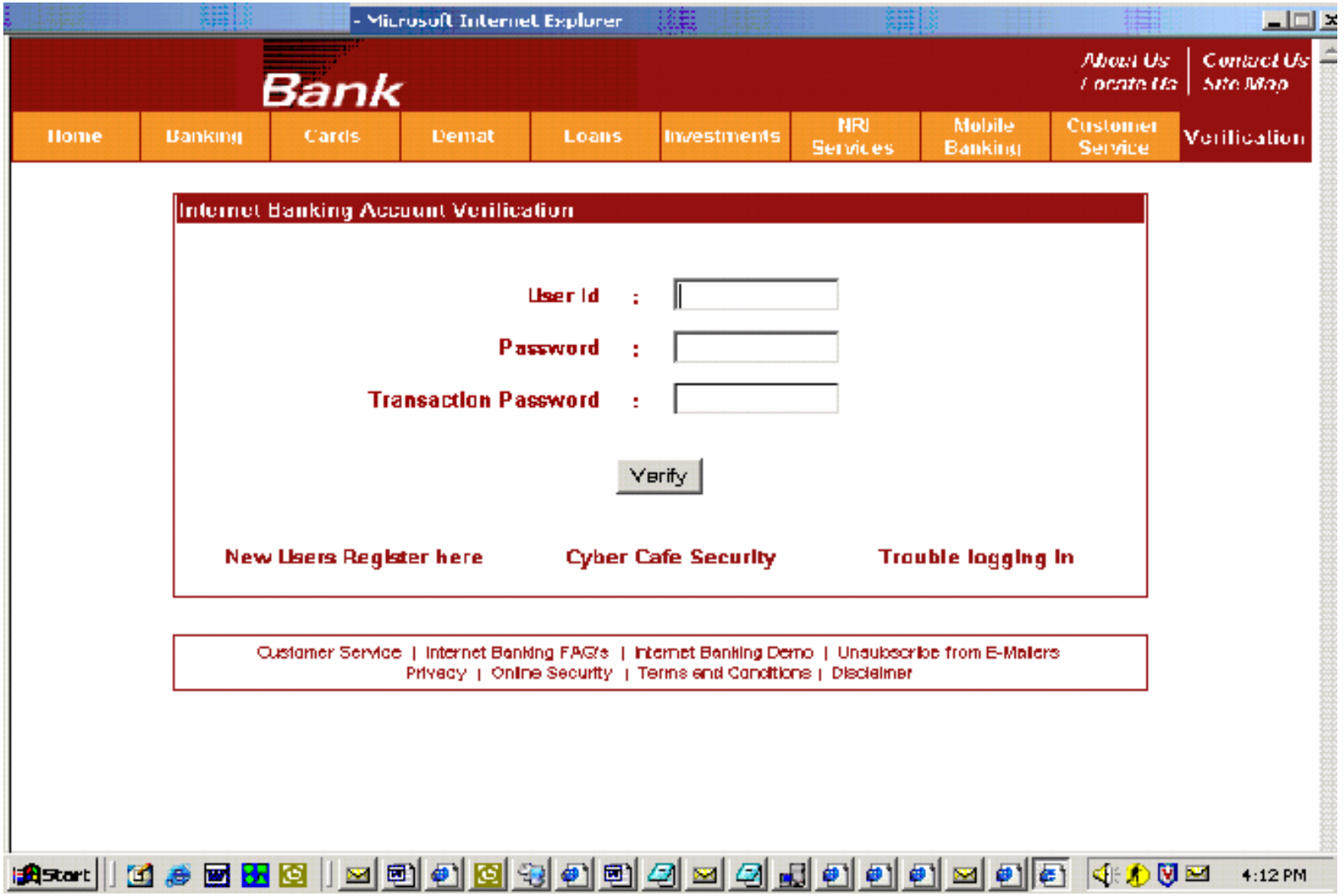
Phishing e-mail

From: *****Bank [mailto:support@****Bank.com]
Sent: 08 June 2004 03:25
To: India
Subject: Official information from ***** Bank
Dear valued ***** Bank Customer!
For security purposes your account has been randomly chosen for verification. To verify your account information we are asking you to provide us with all the data we are requesting. Otherwise we will not be able to verify your identity and access to your account will be denied. Please click on the link below to get to the bank secure page and verify your account details. Thank you.
https://infinity.*****bank.co.in/Verify.jsp
****** Bank Limited

Phishing – originalna stranica



Phishing – lažna stranica



Phishing

Phishing statistika:

- Od maja 2004. do maja 2005. ***oštećeno je preko 1.2 miliona korisnika*** u SAD što ukupno iznosi oko ***929 miliona $***
- ***2007***. se povećava ovakva aktivnost pa je zato ***3.6 miliona korisnika*** oštećeno sa ***3.2 milijardi $***

Strategije u borbi protiv *Phishing*-a

- ***Ne postoje*** klasični sistemi zaštite

1. ***Obuka korisnika***
2. ***Mere*** implementirane kao preference koje se ***uključuju u pretraživač***
   - ***Provera crne liste poznatih phishing sajtova*** i upozorenje korisniku kada se dođe na takav sajt
3. ***Spam filteri***
4. ***Bezbedni sistemi komunikacije***

Strategije u borbi protiv *Phishing*-a

- ***Obuka korisnika***
- ***Ne postoje*** klasični sistemi zaštite, ali se ***korisnici redovno upoznaju*** kako da prepoznaju ovakve napade kako ne bi bili oštećeni
- ***Najčešće*** se dešava da budu oštećeni oni ***korisnici koji u suštini veoma malo poznaju računar*** i onim kojima on služi samo za zabavu
- U suštini ***podizanje socijalne svesti*** o ovome može se stati na put e-pecanju

Strategije u borbi protiv *Phishing*-a

- ***Obuka korisnika* – *korisni saveti***
- ***Legalna komunikacija*** će uvek ***pozdraviti korisnika njegovim ličnim imenom*** a ne nekom generičkom formom kao ‘’*dear accountholder*’’
- Jedini način da se posumnja da je u pokušaju prevara je ako se ***kojim slučajem uoče nepravilnosti u gramatici***
- ***U legalnoj komunikaciji nikada se ne*** postavljaju pitanja o ***osetljivim i ličnim podacima***

Strategije u borbi protiv *Phishing*-a

- ***Obuka korisnika* – *korisni saveti***
- ***Manipulacija linkovima -*** Primer eBay:
- "***http://www.ebay.com***" i
- "***http://cgi3.ebay.com***" ***valjane Web adrese***, ali
- "***http://www.ebay.validate-info.com***" i
- "***http://ebay.login123.com***" su ***lažne adrese***

Strategije u borbi protiv *Phishing*-a

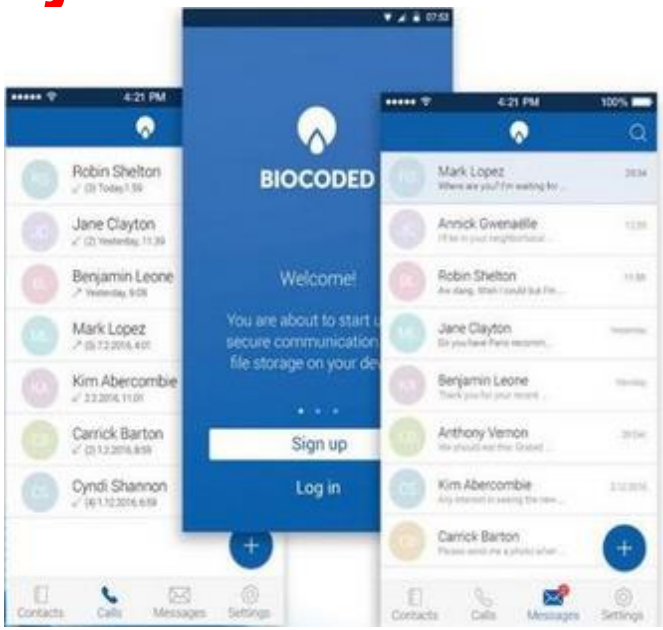
- ***Obuka korisnika* – *korisni saveti***
- ***Manipulacija linkovima***
- "***http//www.google.com@members.tripod.com/***"
- Kada se naiđe na ovakav link tada imamo ***zasigurno elektronsko pecanje***, jer u tom slučaju ***ne idete na google.com već na members.tripod.com*** gde će vaše ***šifre biti otkrivene i iskorišćene u loše svrhe***

Strategije u borbi protiv *Phishing*-a

- ***Biocoded*** je aplikacija koja vam omogućava ***trenutno najviši*** mogući ***stupanj zaštite*** tokom komunikacije
- Ova aplikacija poseduje

  dvostruki zaštitni protokol

  koji vam omogućava potpuno bezbednu komunikaciju



- ***Biocoded*** aplikacija je proverena i odobrena od strane nezavisnih bezbednosnih agencija.

Pharming

lažni Web sajt

Preko ***DNS*** ime i ***IP adresa***

DNS u ***lokanom kešu*** korisnika

e-mail “otruje” lokalni DNS keš

Još o off-line krađi finansijskih podataka

- ***Efikasnost off-line krađa*** finansijskih podataka
  - Kada se ***podaci skladište*** na potencijalno ***nesigurnim uređajima***
  - Kada se ***koriste statičke lozinke***
  - Kada je klijentov ***PC bez zaštite od virusa i trojanaca***
    - Mogu da skinu jednostavno sve podatke koji se unose tastaturom i periodično šalju na predefinisanu adresu

Tehnologija enkripcije

- ***Kriprografija*** je nauka koja se bavi ***metodama očuvanja tajnosti*** informacija
- ***Enkripcija*** je ***proces transformacije*** običnog teksta ili ***podataka u šifrovani tekst*** koji ne može da pročita niko drugi sem pošiljaoca i primaoca
- Svrha enkripcije je:
  - da zaštiti čuvane informacije,
  - da zaštiti prenos informacija
- Transformacija običnog u šifrirani tekst se vrši uz pomoć ***ključa (šifre)***

Tehnologija enkripcije

- Postoje ***dve vrste kripto-sistema*** za enkripciju podataka:
  - ***Simetrični*** kripto-sistem
  - ***Asimetrični*** kripto-sistem
- Kod enkripcije ***simetričnim ključem***, i pošiljalac i primalac koriste ***isti ključ*** za šifrovanje i dešifrovanje poruke
- Prethodno moraju da se dogovore u pogledu zajedničkog tajnog ključa

Tehnologija enkripcije

- ***Prednost*** ove metode je ***brzina enkripcije***
- ***Nedostatak*** je obezbeđivanje ***polovične bezbednosti*** (tajnost + integritet)
- Najpoznatiji simetrični algoritam je ***DES*** (*Data Encription Standard*)
  - 1977. godine razvio ***IBM***
  - Izvanredno dizajniran algoritam
  - Potrebno ***22 sata i 15 minuta*** za njegovo razbijanje (1999. godine, 100.000 PC u mreži)
- ***3DES algoritam*** – primenjuje DES tri puta

Tehnologija enkripcije

- *Whitfield Diffie* i *Martin Hellman* su ***1976. godine*** predložili ***novi način šifrovanja podataka*** nazvan ***asimetrična kriptografija*** ili ***kriptografija javnim ključem***
- Ovaj metod ***rešava problem razmene*** ključeva
- U ovoj metodi koriste se ***dva*** matematički ***povezana digitalna ključa***: ***javni*** i privatni (***tajni***)
- ***Privatni ključ*** čuva vlasnik i on ***je tajni***,
- ***Javni ključ*** se ***slobodno distribuira***

Tehnologija enkripcije

- ***Oba ključa*** mogu da se koriste i za ***šifrovanje*** i za ***dešifrovanje*** poruka
- ***Ključ*** kojim je ***izvršeno šifrovanje ne može*** se koristiti ***i za dešiforvanje*** iste poruke
- Kriptografija javnim ključem je zasnovana na ideji ***nepovratnih matematičkih funkcija***
  - Matematički algoritmi kojima se vrši šifriranje su ***jednosmerne funkcije*** i ulaz se ne može dobiti na osnovu poznavanja izlaza

Tehnologija enkripcije

- Ako pošiljalac ***koristi javni ključ*** za enkriptovanje poruke
  - ***Poverljivost poruke*** – jedino je primalac može dekodovati tajnim ključem
- Ako pošiljalac ***koristi tajni ključ*** za enkriptovanje poruke
  - Dokaz o ***autentičnosti pošiljaoca***
  - ***Nema garancije poverljivosti***!
- Najčešće korišćeni asimetrični algoritam je ***RSA*** (Rivest-Šamir-Ejdlman) - ključevi dužine ***1024 bita***

Hash i digitalni potpis

- Kako bi se obezbedila provera da poruka nije menjana u toku prenosa (***integritet poruke***) - koriste se ***hash funkcije***
- Tom prilikom se kreira ***otisak ili „digest“ poruke***
- Hash funkcija je algoritam kojim se na bazi sadržaja poruke dobija ***binarni broj fiksne dužine*** (128 bitova) i koji se naziva otisak poruke
- Otisak je ***jedinstven*** za svaku poruku
- Otisak se ***šalje primaocu***, zajedno ***sa porukom***

Hash i digitalni potpis

- Oba su ***zajedno šifrovana javnim ključem*** primaoca ***u jedinstvenu poruku***
- ***Po prijemu poruke*** (i dešifrovanja svojim tajnim ključem) – primalac:
  - ***Primenjuje hash funkciju*** na primljenu poruku i
  - ***Proverava*** da li je dobijeni rezultat ***identičan*** sa dešifrovanim otiskom
- Ako jeste, to znači da poruka nije menjana – ***ali nemamo dokaz o autentičnosti pošiljaoca!***

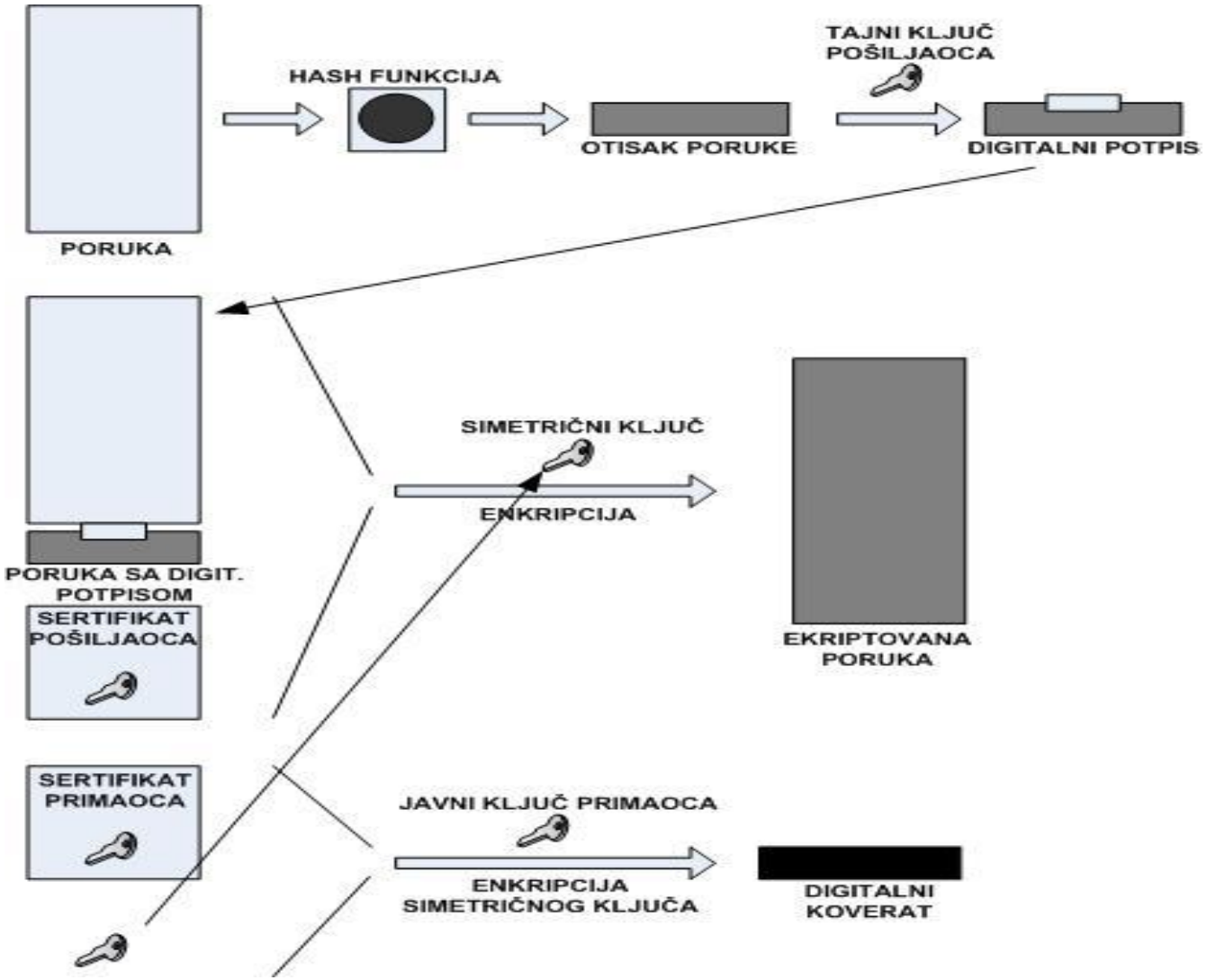
Hash i digitalni potpis

- Da bi ***obezbedila autentifikacija*** - pošiljalac ***šifruje otisak*** korišćenjem svog ***tajnog ključa***
- Ovim se dobija tzv. ***digitalni potpis*** (takođe se naziva i e-potpis), koji se kao takav ***"lepi" na kraj izvorne poruke***
- Digitalni potpis je blizak ručnom potpisu, jer je ***jedinstven***
- Trebalo bi da ***samo jedna osoba*** poseduje korišćeni tajni ključ

Hash i digitalni potpis

- Problem koji ***nije rešen*** korišćenjem digitalnog potpisa je ***problem tajnosti ili privatnosti***
- Ovaj problem ***može biti rešen dodatnim korišćenjem simetričnog algoritma*** za enkriptovanje same poruke

Postupak enkripcije



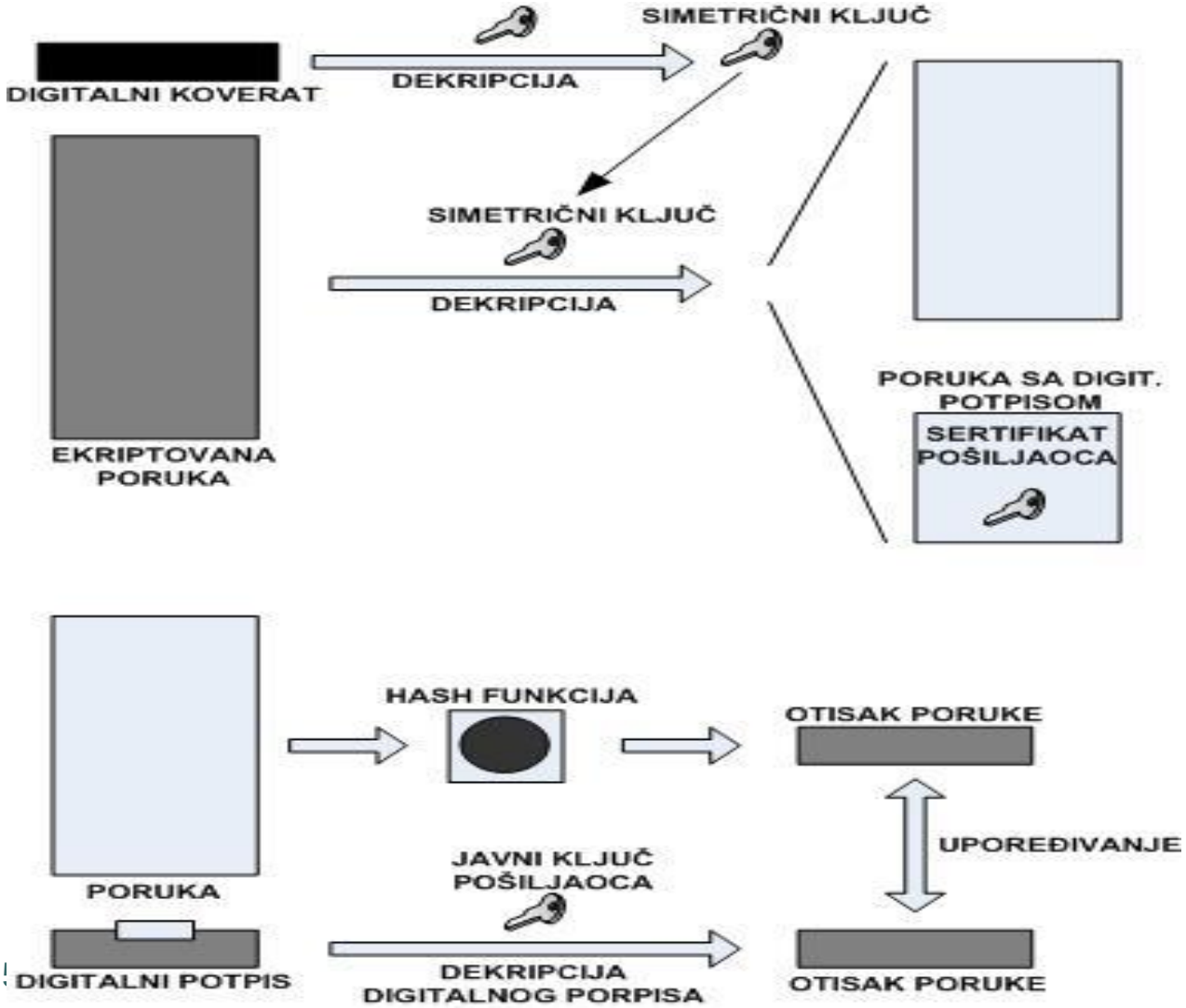
Postupak dekripcije

- ***Primalac*** pomoću svog ***tajnog ključa*** dešifruje ***digitalni koverat***
- Tako dolazi u ***posed simetričnog ključa*** – kojim dekriptuje poruku
- Dešifrovana ***poruka sadrži***:
  - ***Poruku***
  - ***Digitalni potpis***
  - ***Digitalni sertifikat*** pošiljaoca (sa ***njegovim javnim ključem***)
    - ***Javnim ključem pošiljaoca*** dešifruje se potpis i dobija otisak

Postupak dekripcije

- Zatim se ***koristi ista hash- funkcija*** kako bi se ***iz*** dobijene ***poruke izračunao otisak***
- Ako je izračunati otisak jednak primljenom otisku – primalac poruke može biti siguran
  - Da je ***digitalni potpis autentičan***
  - Da poruka ***nije neovlašćeno izmenjena***

Postupak dekripcije



Digitalni sertifikat

- Čitav ***sistem digitalnog potpisa*** oslanja se na mogućnost uspostavljanja ***veze između javnog ključa i njegovog vlasnika***
- ***Ključno pitanje***:
- Kako možemo biti sigurni da je ***veza*** između ***javnog ključa*** i predstavljenog ***identiteta vlasnika autentična (prava) – a ne lažna***?
- Problem je moguće rešiti korišćenjem ***digitalnog sertifikata***

Digitalni sertifikat

- Digitalni sertifikat predstavlja ***strukturu podataka*** koja ima za cilj ***pouzdano povezivanje*** ***javnog ključa*** sa ***podacima o njegovom nosiocu*** – obezbeđujući na taj način ***proveru identiteta*** prilikom digitalnog potpisivanja
  - ***Samopotpisani***
  - ***Kvalifikovani*** sertifikati
- Tehnički ***identični***
- Kvalifikovane sertifikate izdaje ***akreditovano sertifikaciono telo*** , ***CA*** (*Certificate Authority*)

Digitalni sertifikat

- ***Sertifikat*** je ***kolekcija informacija*** koje su ***digitalno potpisane*** od strane ***sertifikacionog tela***
  - Time ***izdavalac garantuje*** njegovu autentičnost
- ***Prvi korak*** pri izdavanju – ***generisanje para ključeva***
  - ***Tajni*** se koristi ***za potpisivanje***
  - ***Javni*** ide ***u sertifikat***
- ***Drugi korak*** – ***predaje se zahtev*** za izdavanje sertifikata ***i javni ključ***

Digitalni sertifikat

- ***Sertifikaciono telo*** ***proverava informacije*** i ako je sve u redu ***pravi sertifikat (potpisuje ga)*** i ***šalje ga podnosiocu zahteva***
- ***Podnosioc zahteva*** ga ***učitava u računar*** i ***počinje da ga koristi***

- ***Ceo ovaj sistem*** koji povezuje javni ključ sa identitetom korisnika posredstvom sertifikacionog tela naziva se ***PKI (Public Key Infrastructure)***

Digitalni sertifikat (banke)

- ***Banka*** obezbeđuje korisnike sa ***parom ključeva*** za koje je ***neko sertifikaciono telo*** od poverenja ***izdalo sertifikate***
- ***Tajni ključ*** i ***sertifikat*** ***uspostavljaju uzajamno autentifikovani SSL/TLS kanal*** između korisnikovog računara i servera banke – ***eliminišući mogućnost on-line napada*** na komunikacije
- Jedini kritični moment – ***zaštita tajnog ključa od malicioznog softvera***

Digitalni sertifikat

Verzija formata certifikata(*v3*) - x.509
Serijski broj certifikata
Identifikator algoritma kojim se vrši digitalni potpis
Naziv certifikacionog tela koje je izdalo certifikat
Rok važnosti certifikata
Vlasnik certifikata
Javni ključ vlasnika certifikata
Određeni specifični podaci koji se odnose na uslove korišćenja certifikata
Digitalni potpis certifikata tajnim ključem certifikactionog tela

Digitalni sertifikat – proces izdavanja

- Proces izdavanja ***započinje*** u ***ustanovi za registraciju RA*** (*Registration Authority*)
- Tu se ***predaje zahtev za izdavanje*** koji sadrži ***lične podatke podnosioca***
- ***RA*** vrši ***proveru*** podnetih ***podataka***
- ***Podnosilac*** na licu mesta ***dobija karticu*** (koja u sebi ne sadrži ni ključeve ni sertifikat) ***i odgovarajući softver***

Digitalni sertifikat – proces izdavanja

- ***Kod kuće***, uz pomoć dobijenog softvera ***korisnik:***
  1. ***Generiše par ključeva***, ***javni*** i ***tajni*** (***na kartici!***)
  2. ***Kompletira zvanični zahtev*** za izdavanje digitalnog sertifikata
- Zahtev se ***prosleđuje*** sertifikacionom telu
- Zadatak sertifikacionog tela je samo da ga ***potpiše*** (zahtev) svojim ***tajnim ključem***
- Time je formiran ***kompletan digitalni sertifikat*** koji se ***vraća korisniku***

Digitalni sertifikat – proces izdavanja

- ***Podnosilac zahteva prijemom*** potpisanog digitalnog sertifikata, korišćenjem posebnog softvera – ***smešta ga na svoju karticu***
- ***Tajni ključ*** – ***nikad ne napušta karticu!***

Digitalni sertifikat

- ***Javni ključevi*** značajnih sertifikacionih tela su verovatno ***već ugrađeni u veb- pretraživače***
- Na taj način, ***primalac*** sertifikata može da ***proveri digitalni potpis*** sertifikacionog tela
- Javni ključ sertifikacionih tela je ***česta meta hakerskih napada***
  - Veoma ***dugački*** ključevi
  - Česta ***promena*** ključeva

Digitalni sertifikat

- Odlaskom na **sajt koji je zaštićen** digitalnim sertifikatom
- U slučaju da ***pretraživač*** u svojoj listi ***nema podataka o izdavaocu*** tog sertifikata – dobija se ***automatsko obaveštenje***:
  - Izdavalac sertifikata nije poznat
  - Ne nalazi se na "***Trusted Publishers***" listi

Digitalni sertifikat

- ***Dobijanje digitalnog sertifikata*** je od ***ogromne važnosti*** za sve ***učesnike u transakcijama*** na Internetu
- Sadrže ***podatke za enkripciju*** što je ***preduslov za korišćenje*** nekog od ***bezbedonosnih protokola*** u obradi transakcije

Digitalni sertifikat

- ***Dve najveće kompanije*** registrovane za izdavanje digitalnih sertifikata
  - ***Norton Symantec***
  - ***TRUSTe***
- Sertifikaciona ***tela održavaju i obezbeđuju*** pristup ***listama za opoziv serifikata*** – ***CRL*** (*Certificate Revocation List*)
- Na osnovu tih listi se može ***utvrditi validnost sertifikata***

Digitalni sertifikat

- ***Pri svakoj upotrebi*** digitalnog sertifikata ***vrši se provera*** njegove ***ispravnosti***
- Proverava se ***rok važnosti***
  - Upisan u sam sertifikat
- Proveravaju se ***podaci o CA*** koje je izdalo digitalni sertifikat potpisniku
- Proverava se ***da li se sertifikat nalazi na CRL listi*** (opozvanih)
- ***CRL*** je izuzetno ***važan sigurnosni mehanizam***

Digitalni sertifikat

- Donošenjem ***Zakona o elektronskom potpisu*** (***2006.***) stvoreni su ***preduslovi za obrazovanje sertifikacionih tela u Srbiji*** koji će izdavati kvalifikovane digitalne sertifikate
  - Privredna komora Srbije
  - MUP Srbije
  - JP PTT
  - Halcom
  - Ministarstvo odbrane i Vojska Srbije
  - E-Smart Systems

Bezbedonosni Internet protokoli (standard)

- Iako je ***Internet nesiguran medij*** (zbog svoje decentralizovane prirode)
- Moguće je zaštititi podatke – korišćenjem standardizovanih ***bezbedonosnih protokola***
  - ***S-HTTP*** (*Secure HTTP*) i ***(HTTPS)***, ***bezbednost veb- transakcije***
  - ***SSL*** (*Secure Socket Layer*), ***bezbednost na transportnom nivou***
  - ***S/MIME*** (Više-namenska ekstenzija e- pošte)
  - ***SET*** (*Secure Electronic Transaction*), ***bezbednost elektronskih transakcija***

Bezbedonosni Internet protokoli (standard)

- ***Klasifikacija*** bezbedonosnih protokola:
- Obezbeđuju ***sigurnost veza*** (na transp. nivou)
  - ***SSL/TLS (Netscape/IETF, RFC2246)***
- Obezbeđuju ***sigurnost aplikacija*** (autentičnost i privatnost)
  - ***S-HTTP*** i ***S-MIME***
- ***SET*** ide dalje – obezbeđuje sigurnost elektronskih transakcija
- ***SSL*** i ***SET*** – koriste moć ***kriptografije*** i ***digitalnih sertifikata*** radi pouzdane autentifikacije

Bezbedonosni Internet protokoli (standard)

S-HTTP protokol

- Podržava bezbedno slanje podataka ***preko veb servisa (WWW)***
- ***Ne podržavaju ga*** svi ***veb*** pretraživači i serveri
- ***Rasprostranjenija tehnologija*** koja osigurava bezbednu komunikaciju preko WWW – ***HTTPS protokol (SSL)***
- Ova dva protokola su ***različito projektovana*** i imaju ***različite ciljeve***

Bezbedonosni Internet protokoli (standard)

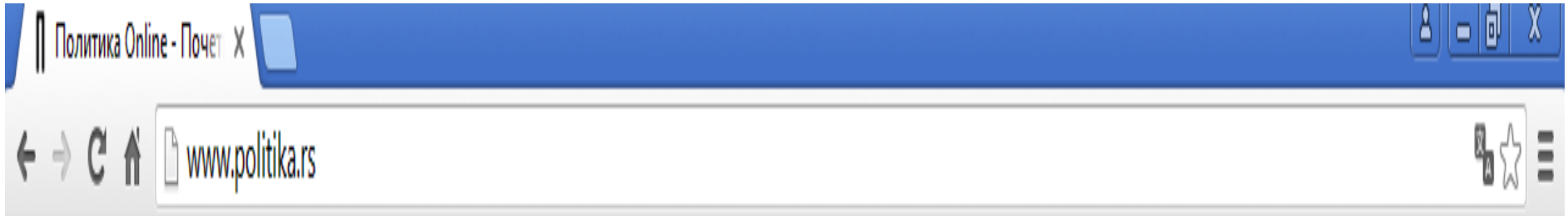
S-HTTP protokol

- ***HTTPS*** – korišćenjem SSL-a ***uspostavlja bezbednu vezu (komunikacioni kanal)*** između ***klijenta*** i ***servera***, koja omogućava bezbedan prenos ***bilo koje količine podataka***
- ***S-HTTP*** – omogućuje ***bezbedan prenos na nivou individualnih poruka***
- Razlog slabe rasprostranjenosti je ***neuspešan marketing*** koji ga je pratio, iako je tehnički zadovoljavao sve zahteve tržišta

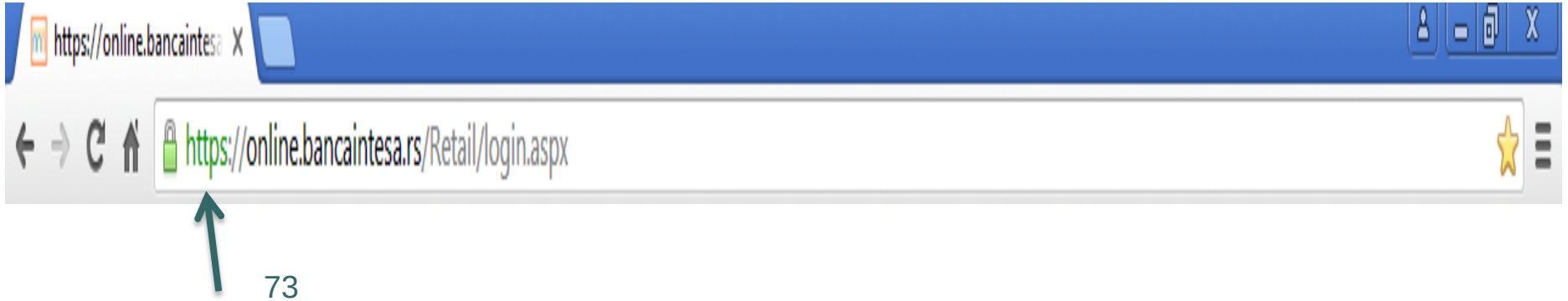
Bezbedonosni Internet protokoli (standard)

S-HTTP protokol

- Bez kontrole ***HTTPS*** –



- Pod kontrolom ***HTTPS*** –



Sigurnosni standardi na Internetu

SSL i TLS protokoli

- ***Kriptografski protokoli*** koji obezbeđuju sigurne komunikacije na Internetu
- Između ova dva protokola – ***neznatne razlike***
- Obezbeđuje ***sigurnost komunikacionog kanala*** kao dvosmernog toka podataka uspostavljenog ***između pretraživača i servera***
  - ***Privatnost***
  - ***Integritet***
  - ***Autentifikacija (Identitet)***

Bezbedonosni Internet protokoli (standard)

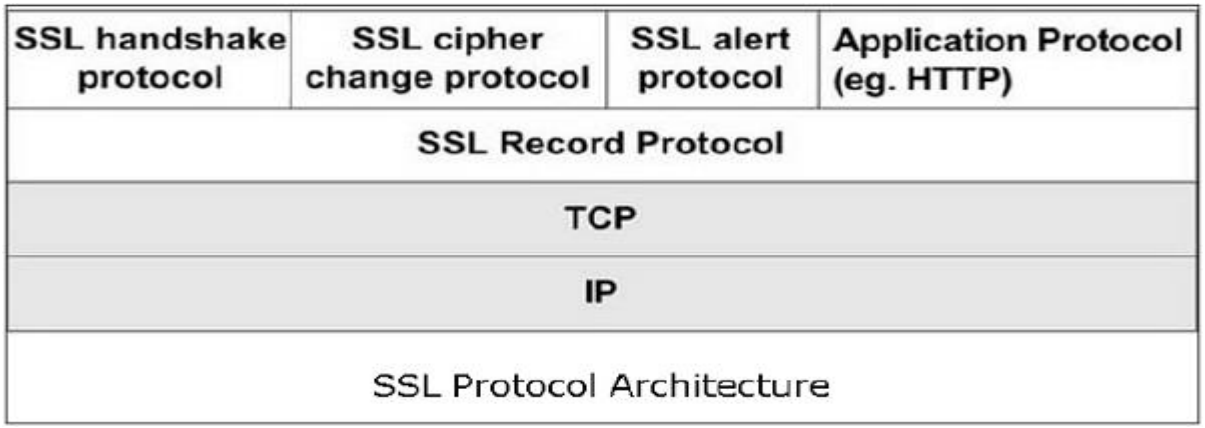
SSL i TLS protokoli

- ***Osnovna ideja*** – aplikaciju SSL protokola smestiti u ***novi sloj između aplikacionog i TCP sloja***
- Tu će se vršiti ***enkripcija podataka*** koji se šalju ka severu tako da samo server koji poseduje ključ može da dekriptuje poruku
- I klijent i server moraju imati ***ugrađen SSL sloj***
- ***Fleksibilnost*** u pogledu ***izbora***:
  - ***Simetričnog ključa***
  - ***Hash funkcije*** i ***metode autentifikacije***

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- SSL se sastoji iz ***dva pod-sloja***:



1. ***SSL Handshake Layer (uspostava bezbednog kanala)***
2. ***SSL Record Layer (korišćenje bezbednog kanala)***

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Record Layer*** – obezbeđuje
  - ***enkripciju i dekripciju*** osetljivih podataka ***i***
  - ***izračunavanje MAC-a*** (kriptografski *chechsum*)

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***MAC*** (*Message Authentication Code*) omogućuje:
  - ***Integritet podataka***
  - ***Autentifikaciju***
    - Za razliku od digitalnog potpisa dobija se ***simetričnim šifrovanjem***

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Handshake Layer*** – ***procedura***
- ***Korisnik*** kontaktira ***zaštićeni URL*** (***https:***) – obično zaštićena forma za prikupljanje ličnih podataka od kupca
- ***Pretraživač klijenta*** šalje ***clientHello*** poruku:
  - ***Verzija*** SSL ***protokola***
  - ***Lista kriptografskih tehnika*** (podržani ***algoritmi*** i ***hash*** funkcije) koje može koristiti
  - ***Slučajno generisani broj (Client_Random)***, metod kompresije (opciono)...

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Handshake Layer*** – ***procedura***
- ***Server*** šalje ***serverHello*** poruku
  - Izabrane ***algoritme*** i ***hash funkciju*** (najače) iz liste prethodno dobijene od pretraživača
  - Serverov ***digitalni sertifikat*** (javni ključ)
  - ***Slučajno generisani broj (Server_Random)***, izabrani metod kompresije
- ***Autentifikacija servera*** - ***Pretraživač klijenta proverava validnost*** digitalnog sertifikata servera

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Handshake Layer*** – ***procedura***
- Nakon ***uspešne autentifikacije***, koristeći podatke dobijene u ***Handshake postupku*** – pretraživač ***klijenta generiše*** - ***PreMasterSecret*** šifra sesije
- ***PreMasterSecret*** se ***enkriptuje javnim ključem servera*** (iz sertifikata trgovca)
- ***Klijent šalje serveru*** enkriptovani ***PreMasterSecret*** (u poruci ***Client Key Exchange***)

Bezbedonosni Internet protokoli (standard)

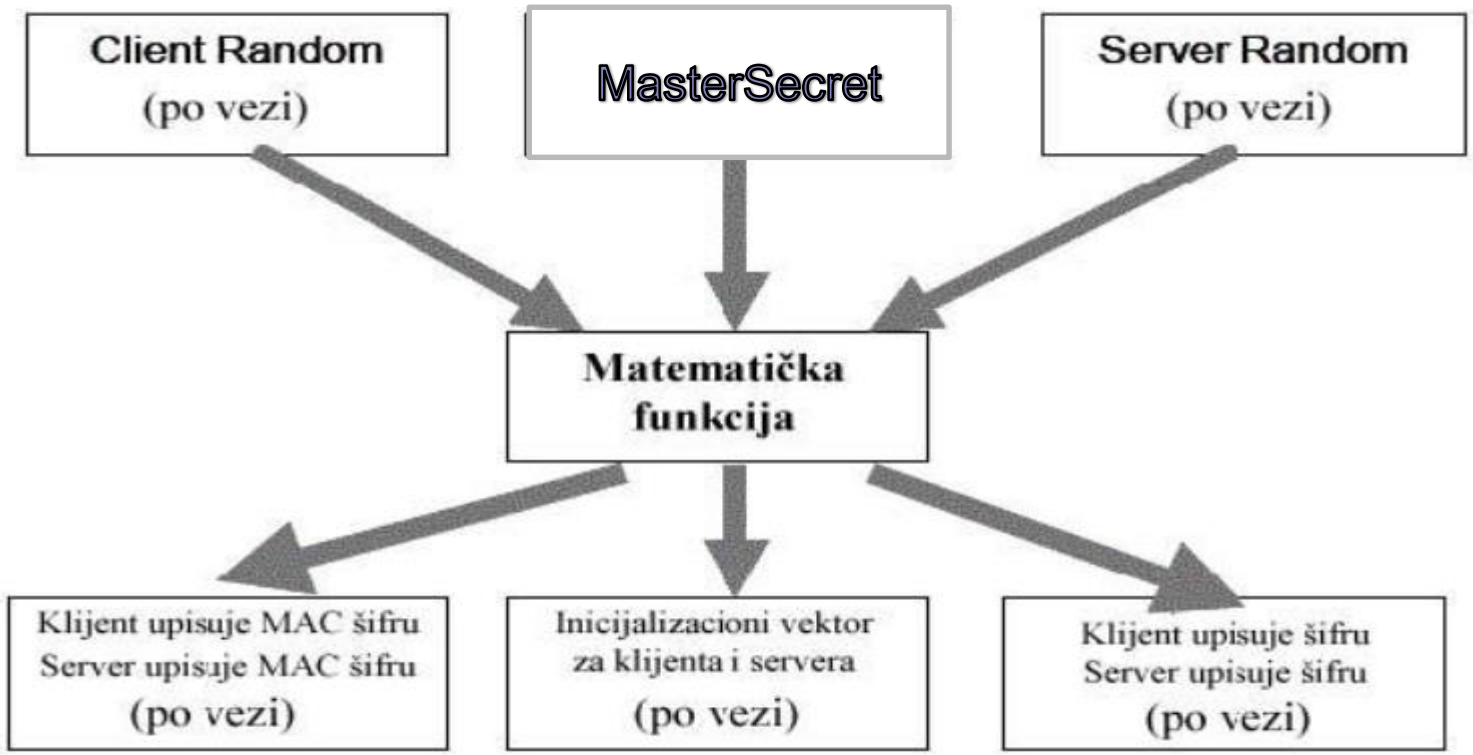
SSL i TLS protokoli

- ***Generisanje glavne šifre (ključa) po sesiji - MasterSecret***

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***Generisanje ključeva na početku svake sesije***

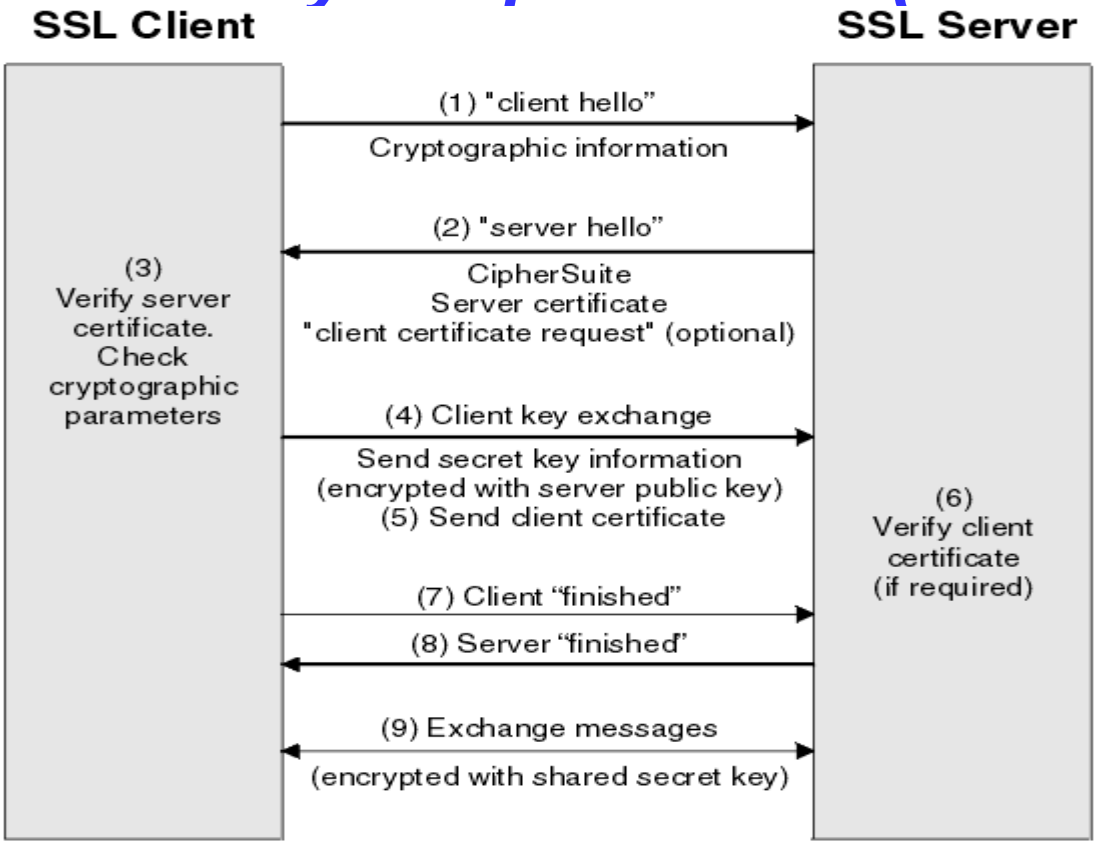


Simetrični ključevi

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Handshake Layer – procedura (blok dijagram)***



Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Record Layer***
- ***Nakon*** uspešno izvršenog ***SSL handshake-a***

Na strani klijenta

- ***Prihvata podatke*** od aplikacionog sloja,
- ***Fragmentira*** ih u blokove
- Opciono ***komprimuje*** podatke
- ***Izračunava MAC*** i zajedno sa porukom ga ***šifruje simetričnim ključem***

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Record Layer***

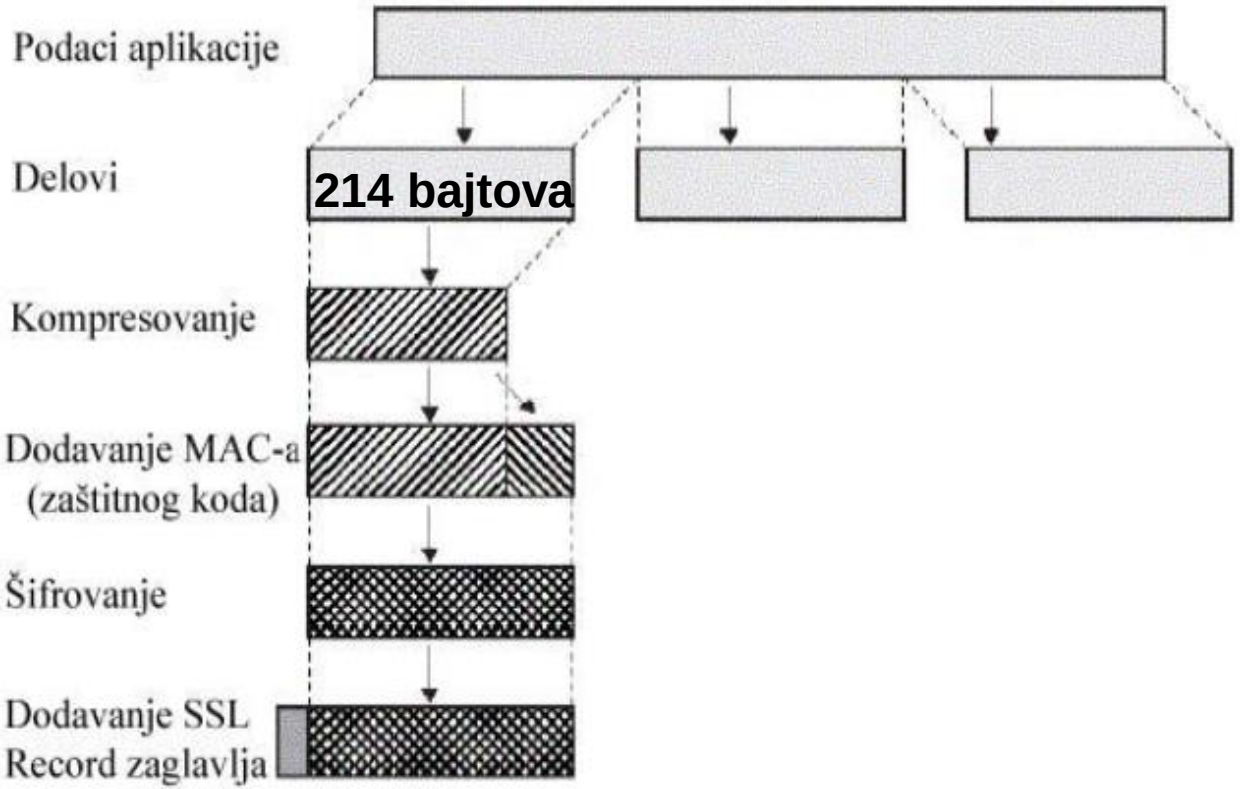
Na strani servera

- Vrši se verifikacija MAC-a, ako je ***verifikacija uspešna*** – prosleđuje se poruka ka aplikacionom sloju

Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Record Layer***



Bezbedonosni Internet protokoli (standard)

SSL i TLS protokoli

- ***SSL Record Layer***
- SSL ***koristi simetričnu enkripciju*** koja je dosta brža od asimetrične
  - Nakon završetka komunikacije – ***sesijski ključ se eliminiše***

Sigurnosni standardi na Internetu

SET protokol

- SSL je dovoljan za ***zaštitu poslovnih transakcija***
- Za ***zaštitu finansijskih transakcija*** potrebno je obezbediti ***snažnije mehanizme autentifikacije***
- U tom cilju – razvijen je ***SET protokol***
- Savršeniji ali zahteva instalaciju dodatnog softvera
- ***Cilj SSL*** je smanji verovatnoću ***presretanja***
- ***Cilj SET*** je da smanji verovatnoću ***prevare***
- Razvijen od strane ***VISA*** i ***MasterCard***

Sigurnosni standardi na Internetu

SET protokol

- Zasniva se na tehnologiji ***enkripcije*** i ***digitalnog sertifikata***
- Obezbeđuje:
  - ***Integritet*** poruke
  - ***Autentifikaciju*** svih aktera
  - ***Tajnost*** osetljivih podataka

Sigurnosni standardi na Internetu

SET protokol

- Poruka se enkriptuje ***slučajno generisanim ključem*** (***simetričan***) – koji se naknadno enkriptuje javnim ključem primaoca - ***digitalna koverta***
- ***Primalac*** (***Banka***) dešifruje digitalni koverat uz pomoć ***tajnog ključa*** – zatim ***koristi simetričan*** za dešifrovanje ***cele poruke***

Sigurnosni standardi na Internetu

SET protokol

- ***Autentifikacijom naručioca*** SET protokol ***štiti trgovca od*** potrošačevog ***poricanja***
- ***Potrošač je siguran*** jer trgovac ***nema pristupa informacijama*** sa njegove platne kartice
- SET omogućava i ***autentifikaciju vlasnika platne kartice***, odnosno, njegovog računa u banci
- Pored toga, koristeći ***digitalni potpis*** i ***sertifikat trgovca***, SET obezbeđuje i ***autentifikaciju trgovca***

Sigurnosni standardi na Internetu

SET protokol

- ***Najčešća primena SET protokola*** je u slučaju kada ***vlasnik platne kartice*** šalje ***poruku koja sadrži dva dela:***

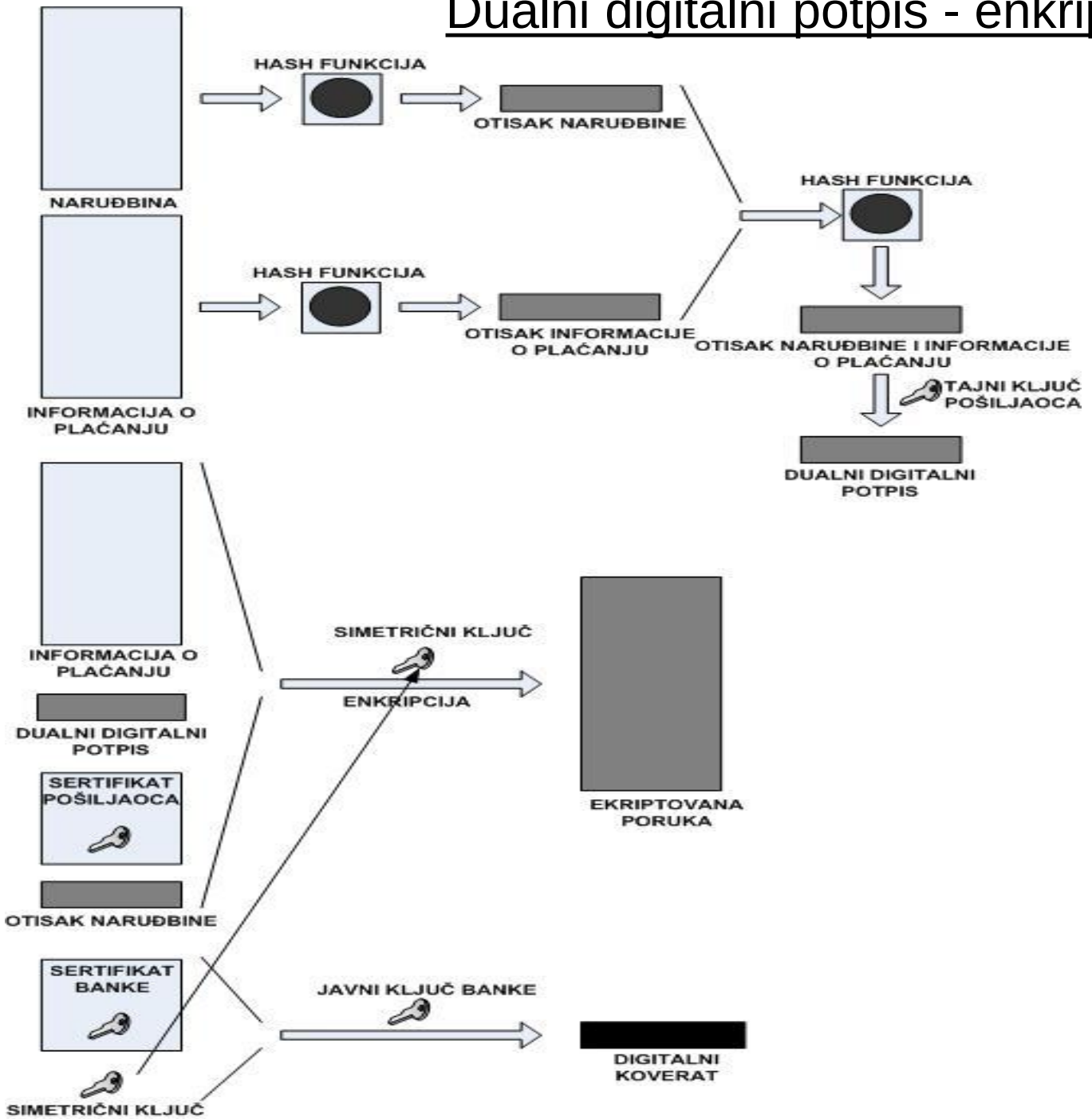
1. ***porudžbinu*** sa podacima o proizvodima koje naručuje kao i
2. ***finansijske podatke (za plaćanje)***

Sigurnosni standardi na Internetu

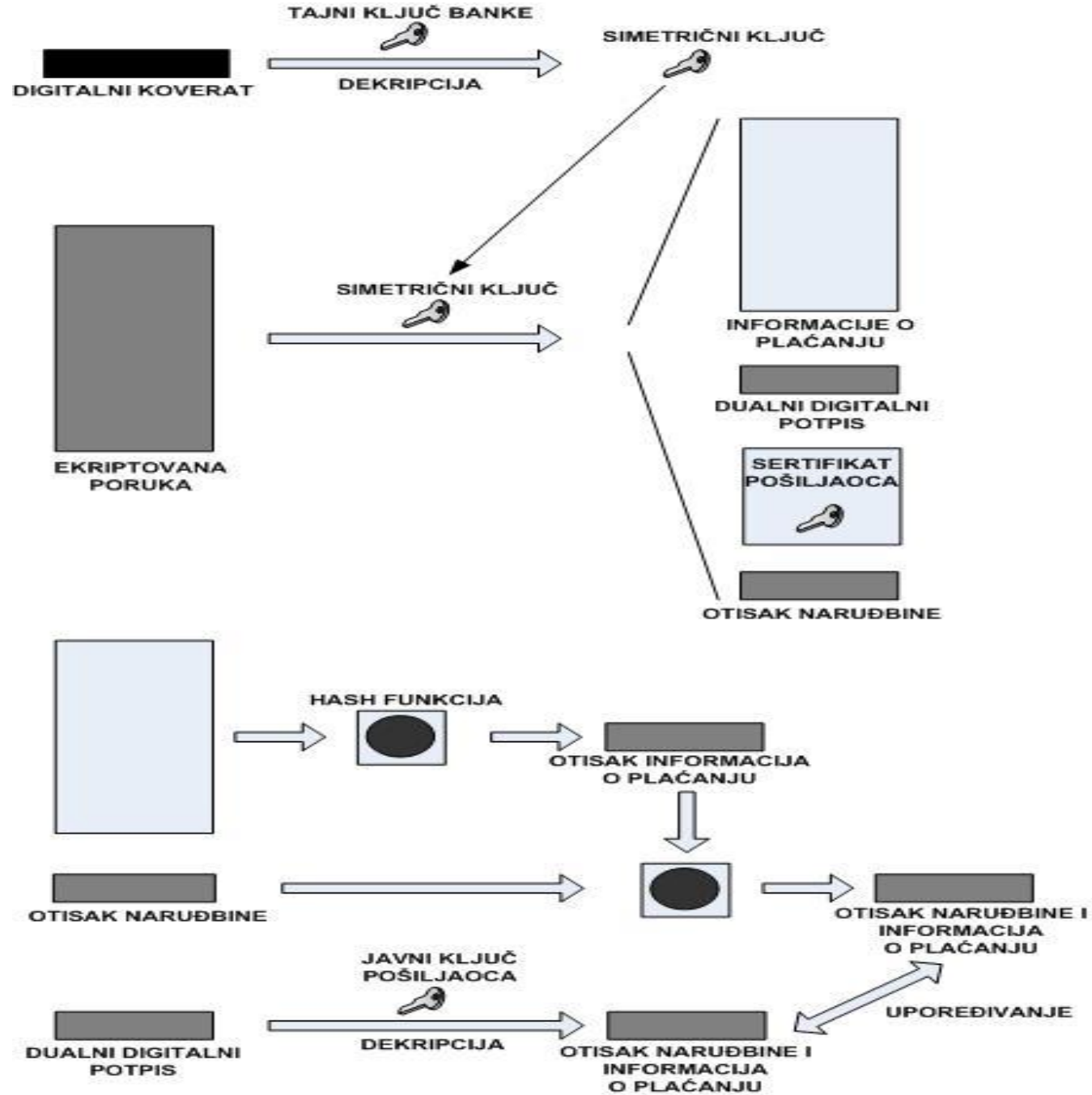
SET protokol

- ***Oba dela se šalju zajedno*** – ***trgovac je sprečen da vidi informacije o plaćanju***
- U ovom slučaju, SET koristi tehniku koja se zove ***dualni digitalni potpis***
- Slede šematski prikazi ***enkripcije*** i ***dekripcije*** primenom dualnog digitalnog potpisa

Dualni digitalni potpis - enkripcija



Dualni digitalni potpis - dekripcija



Sigurnosni standardi na Internetu

- Neke ***napomene***
- Bezbednost čitavog sistema ***zavisi od načina čuvanja tajnih ključeva***
  - Sistem je ugrožen čuvanjem najosetljivijih podataka ***na hard disku računara*** – gde su izloženi mogućim zloupotrebama
- Proces enkripcije i dekripcije se ***obavlja softverski*** – koji je ***podložan najrazličitijim bag-ovima*** i neotporan na napade
- ***Rešenje***: upotreba specijalizovanih hardverskih uređaja – ***smart kartica***