Akademija tehničko-vaspitačkih strukovnih studija

odsek NIŠ

Katedra za Informaciono-komunikacione tehnologije

Predmet: **Elektronsko poslovanje**

Prof. dr Zoran Veličković, dipl. inž. el.

2019/20.

Prof. dr Zoran Veličković, dipl. inž. el.

Elektronsko poslovanje

Bezbednost - važna komponenta e-poslovanja (12)

Sadržaj

Bezbednost e-poslovanja

- Pod pojmom **BEZBEDNOST e-POSLOVANJA** se podrazumeva **SKUP SPECIJALNIH POSTUPAKA I PROCEDURA** u cilju zaštite **POVERLJIVIH INFORMACIJA** od **NEAUTORIZOVANOG** pristupa, korišćenja i destrukcije.
- Generalno, bezbednost e-poslovanja se može podeliti na **DVE** komponente:
  1. Bezbednost ELEKTRONSKIH KOMUNIKACIJA, označava zaštitu informacija ZA VREME PRENOSA iz jednog informacionog sistema u drugi.
  2. Bezbednost INFORMACIONOG SISTEMA označava zaštitu informacija UNUTAR RAČUNARA, odnosno, računarskog sistema i obuhvata:
     - Bezbednost OPERATIVNOG SISTEMA;
     - Bezbednost APLIKATIVNOG SOFTVERA za manipulaciju podacima.
- Smanjenje rizika u e-trgovini je **KOMPLEKSAN PROCES** koji uključuje:
  - STANDARDE i zakonsku REGULATIVU,
  - Organizacionu POLITIKU,
  - Nove TEHNOLOGIJE.

Tehnološke mere bezbednosti (1)

- Bezbedna e-trgovina zahteva **SKUP ZAKONA**, **PROCEDURA**, **BEZBEDNOSNIH POLITIKA** i **TEHNOLOŠKIH** MERA.
- **SKUP PRAVILA** kojim se reguliše bezbednost u jednoj organizaciji naziva se **POLITIKA BEZBEDNOSTI**.
- BEZBEDNOSNA POLITIKA se u praksi realizuje putem BEZBEDONOSNIH SERVISA.
- U **TEHNOLOŠKE MERE** bezbednosti spadaju:
  - POVERLJIVOST;
  - INTEGRITET PODATAKA;
  - AUTENTIFIKACIJA;
  - NEPORECIVOST.
- Da bi se **TEHNOLOŠKE MERE** uspešno aplikovale u praksi, neophodna je upotreba **KRIPTOLOŠKIH TEHNOLOGIJA** u koje spadaju **DIGITALNI POTPIS** i **SISTEMI ŠIFRIRANJA** sa **JAVNIM** i **TAJNIM** ključem.

Tehnološke mere bezbednosti (2)

- **POVERLJIVOST** (tajnost) je **TEHNOLOŠKA MERA BEZBEDNOSTI** koja osigurava DOSTUPNOST INFORMACIJAMA samo **AUTORIZOVANIM KORISNICIMA**.
- **POVERLJIVOST** se može realizovati na razne načine počev od **FIZIČKE ZAŠTITE** do **MATEMATIČKIH ALGORITAMA** koji čine podatke nerazumljivim.
- **NEAUTORIZOVANI PRISTUP** ili presretanje podataka tokom komunikacijskog procesa sprečava se **ŠIFROVANJEM PODATAKA**.
- Pored **ŠIFROVANJA** za realizaciji poverljivosti koriste se tehnologije **DIGITALNOG POTPISA**, odnosno, **INFRASTRUKTURA JAVNOG KLJUČA PKI** (engl. *Public Key Infrastrukture*).
- **INTEGRITET PODATAKA** se odnosi na osiguravanje **IZVORNOSTI PODATAKA**, odnosno **SPREČAVANJE PROMENE PODATAKA** primenom **DIGITALNOG POTPISA** (promene podataka se odnose na ubacivanje, brisanje i zamenu).

Identitet – verodostojnost korisnika

- **AUTENTIFIKACIJA** (verodostojnost) treba da obezbedi pouzdano utvrđivanje **IDENTITETA KORISNIKA**.
- U cilju **UTVRĐIVANJA IDENTITETA** korisnika u upotrebi su sledeće tehnologije:
  1. Korisnički ID i statička lozinka;
  2. Token i/ili biometrijske tehnologije;

     Tokeni su dizajnirani da generišu nasumične brojeve koji mogu da evidentiraju korisnika na korporativnoj mreži sa bilo kojeg mesta bezbedno i bez mogućnosti da neovlašćni korisnik dobije pristup.
  3. Simetrična/asimetrična KRIPTOGRAFIJA i DIGITALNI SERTIFIKATI;
  4. Pametne (engl. *smart*) kartice.

Izgled tolkena

- **NEPORECIVOST** je tehnološka mera bezbednosti koja **SPREČAVA PORICANJE** prethodno obavljenih akcija.
- **NEPORECIVOST** obezbeđuje da su pošiljalac i primalac zaista **ENTITETI** koji su poslali, odnosno, primili poruku.

Šifrovanje

- Pod **ŠIFROVANJEM** se podrazumeva proces **MATEMATIČKE TRANSFORMACIJE** izvorne poruke u ŠIFROVANU (novu) poruku.
- Ovako transformisana (šifrovana) poruka se šalje NA **ODREDIŠTE** putem **KOMUNIKACIONOG KANALA**.
- Primalac poruke **NE MOŽE DEŠIFROVATI** primljenu poruku, osim ako ne poseduje ovlašćeni **KRIPTOGRAFSKI KLJUČ** za dešifrovanje.
- **KRIPTOGRAFSKI KLJUČ** predstavlja **KOD** koji se uobičajeno sastoji od velikog broja slova, simbola i brojeva.
- U osnovi postoje **DVE** metode šifrovanja:
  1. **ŠIFROVANJE SIMETRIČNIM** (prostim) **KLJUČEM** (ovi ključevi mogu biti sekvencijalni i blokovski).
  2. **ŠIFROVANJE ASIMETRIČNIM** (duplim) **KLJUČEM**.

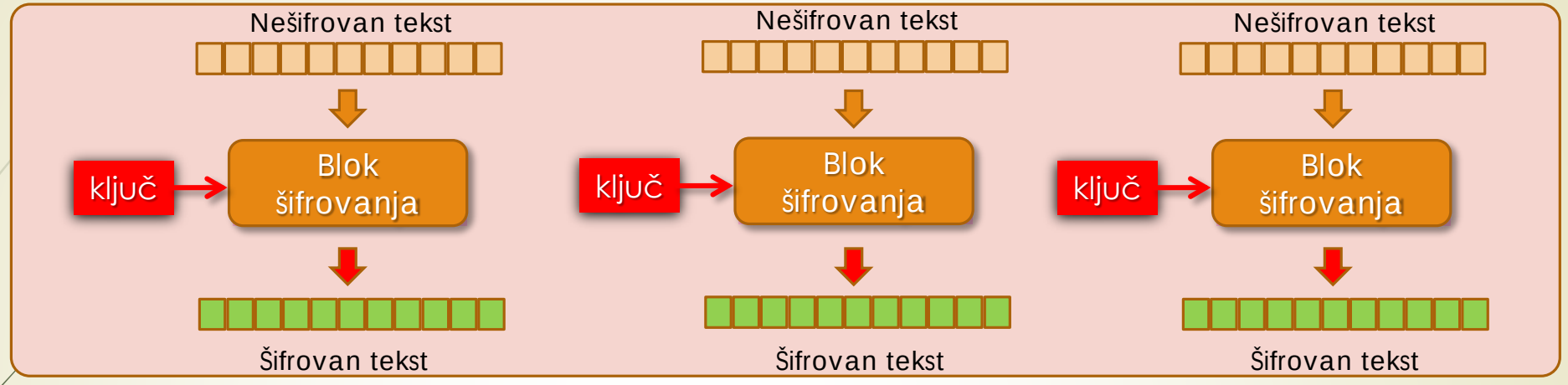
Blokovski algoritmi šifrovanja (1)

- **BLOKOVSKI ALGORITAM ŠIFROVANJA** podrazumeva šifrovanje originalne poruke PO GRUPAMA (blokovima) koje se sastoje od najmanje dva ili više elemenata.
- Specifičnosti **BLOK ŠIFARA** su sledeće:
  - Način šifrovanja svakog elementa zavisi od šifrovanja susednih blokova;
  - Svaki blok simbola se šifruje na isti način;
  - Jedake poruke daju jednake šifrate;
  - Omogućava se dešifrovanje delova poruka.
- SVAKA **BLOK ŠIFRA** se sastoji od **ČETRI ELEMENTA**:
  - Inicijalne transformacije;
  - Jedne kriptografski slabe funkcije (ponovljene *r* puta);
  - Finalne transformacije;
  - Ekspanizije ključa.

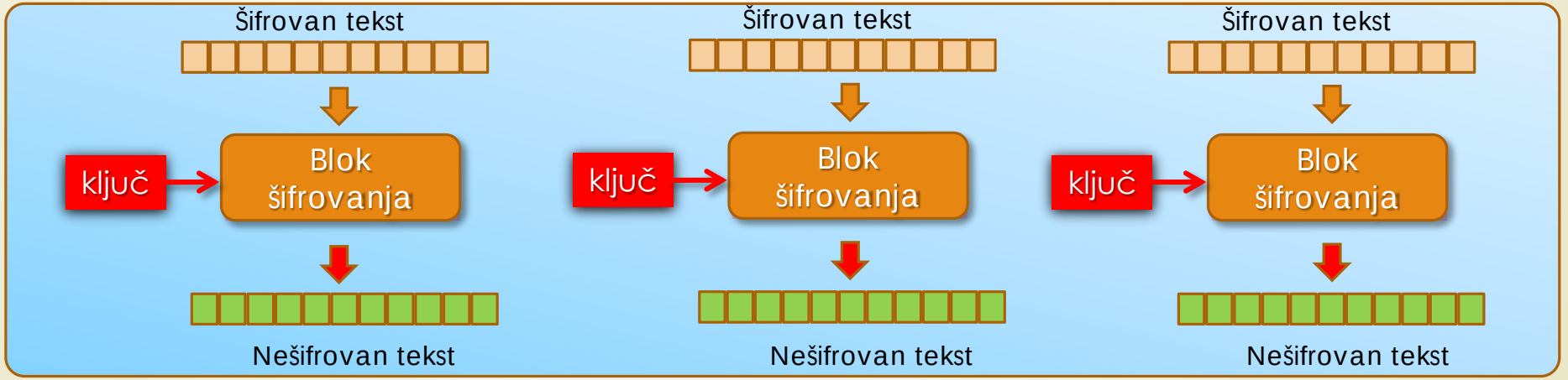
Blokovski algoritmi šifrovanja (2)

- Najpoznatiji **BLOKOVSKI ALGORITMI** šifrovanja su:
  - **DES** (engl. *Data Encryption Standard*) – kod koga je ključ dužine 56 bitova, a blok podataka je dužine 64 bita.
  - **Triple DES**, DESX, GDES, RDES – ključ je FIKSNE DUŽINE 168 bitova.
  - **RIVEST**: RC2, RC4, RC5, RC6 – PROMENLJIVA DUŽINA ključa do 2048 bitova.
  - **IDEA** – osnovni algoritam za **PGP** (engl. *Pretty Good Privacy*) (uslužni program za kriptovanje) – ključ je dužine 128 bitova.
  - **BLOWFISH** – PROMENLJIVA DUŽINA ključa do 448 bitova.
  - **AES** (engl. *Advanced Encryption Standard*) - radi sa blokovima od po 128 bitova i koristi ključeve dužine 128, 192 i 256 bitova.

Blokovski algoritmi šifrovanja

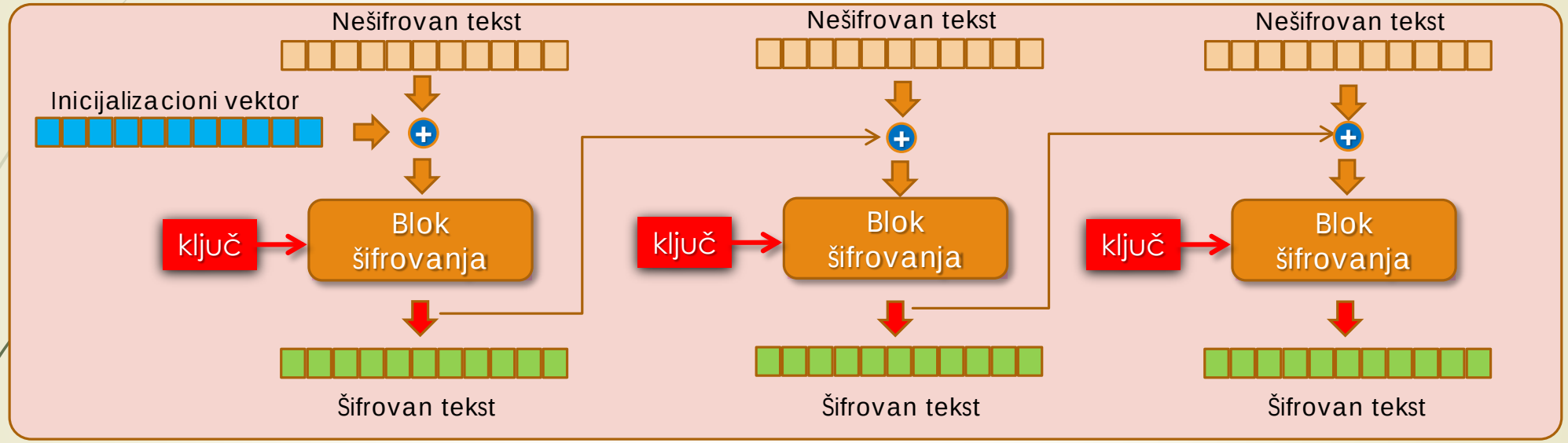


Blokovski algoritmi **ŠIFROVANJA** - svaki blok se **NEZAVISNO ŠIFRUJE**



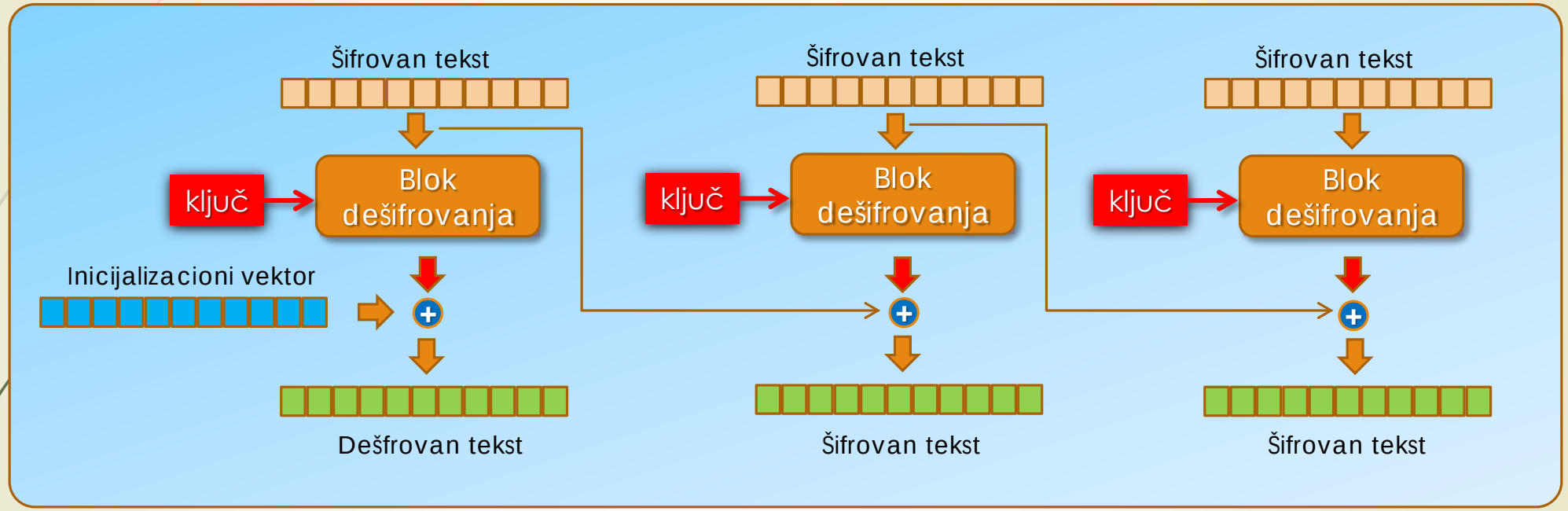
Blokovski algoritmi **DEŠIFROVANJA** - svaki blok se **NEZAVISNO DEŠIFRUJE**

Blokovski algoritmi šifrovanja CBC



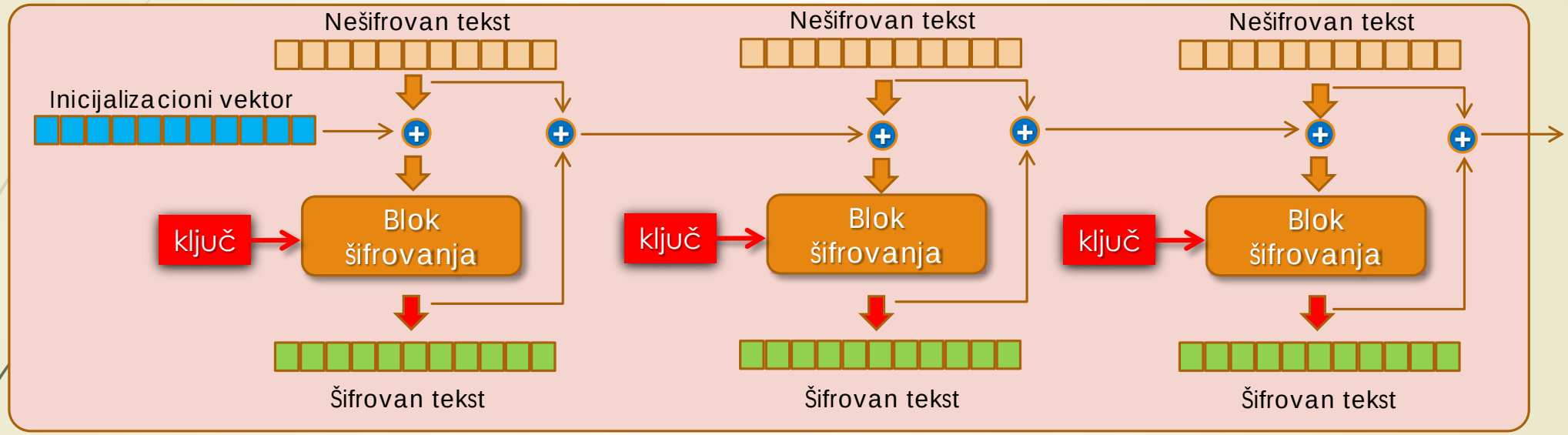
Blokovski **CBC** (engl. ***C**ipher **B**lock **C**haining*) algoritmi **ŠIFROVANJA**

Blokovski algoritmi dešifrovanja CBC



Blokovski **CBC** (engl. ***C**ipher **B**lock **C**haining*) algoritmi **DEŠIFROVANJA**

Blokovski algoritmi šifrovanja - PCBC

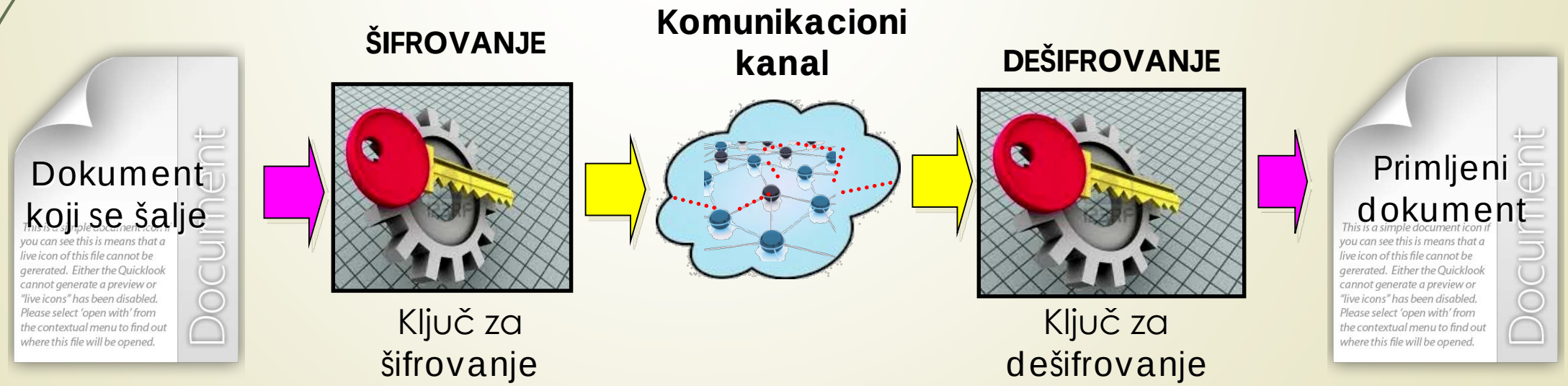


Blokovski PCBC (engl. Propagating Cipher Block Chaining) algoritmi **ŠIFROVANJA**

- **BLOKOVSKI ALGORITAM DEŠIFROVANJA - PCBC** se na sličan način prikazan prethodno može kreirati.

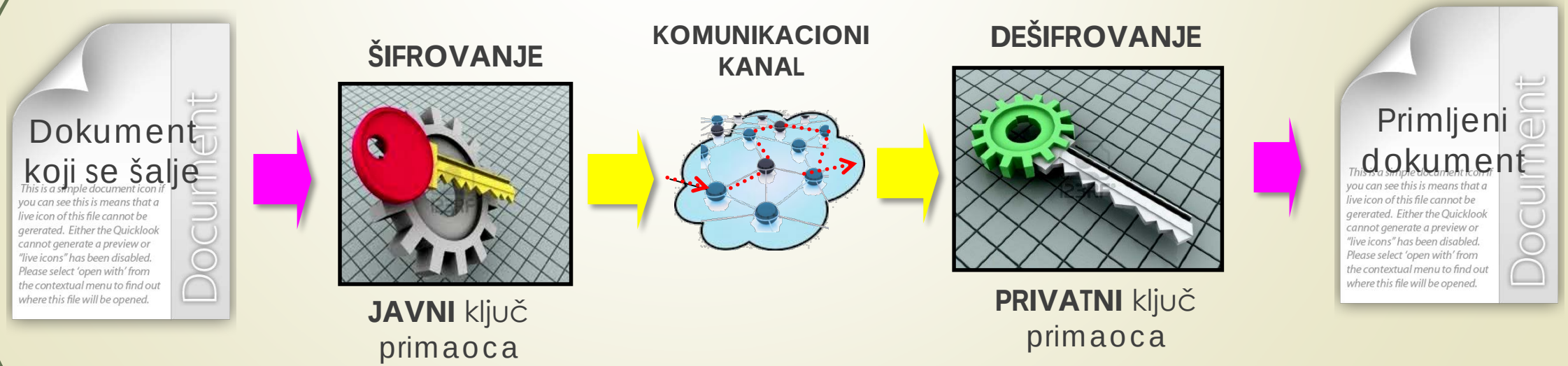
Simetrično šifrovanje

- **SIMETRIČNO ŠIFROVANJE** je šifrovanje tajnim ključem, pri čemu je ključ za šifrovanje **IDENTIČAN** ključu za dešifrovanje.
  - Ovaj način šifrovanja je STVARAO PROBLEME u praksi jer se mogao nelegalno koristiti za čitanje svih poruka ili čak krađu novca.
  - SIMETRIČNO ŠIFRIROVANJE **NIJE DOVOLJNO BEZBEDNO** i koristi se samo kao komponenta u sistemu javnog ključa PKI-a (engl. *Public Key Infrastructure*).



Asimetrično šifrovanje (1)

- **ASIMETRIČNO ŠIFROVANJE** je šifrovanje **JAVNIM KLJUČEM**.
- Svaki učesnik u komunikaciji koristi **DVA** KLJUČA.
- Jedan ključ se naziva JAVNIM (engl. *public*) – i on je svima dostupan i uobičajeno se koristi se za **ŠIFROVANJE**, dok se drugi ključ naziva TAJNIM i koristi se za **DEŠIFROVANJE** primljene poruke koja je šifrirana javnim ključem.
- TAJNI KLJUČ je dostupan samo vlasniku.
- Poznavanjem jednog ključa **NE MOŽE** se odrediti drugi ključ.

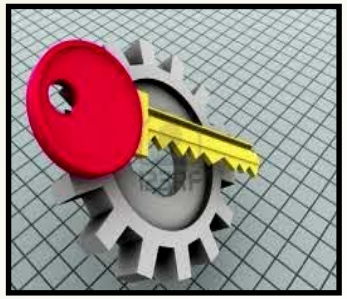


Izvod poruke i digitalni potpis

- **IZVOD** (SAŽETAK) **PORUKE** (engl. *Message Digest*, *Hash*) je **ZNAKOVNI NIZ FIKSNE DUŽINE** koji se dobija matematičkom transformacijom od ULAZNOG DOKUMENTA **PROMENLJIVE VELIČINE**.
- **IZVOD PORUKE** služi za **PROVERU CELOVITOSTI PORUKE**, a primenjene matematičke transformacije za njeno određivanje su **JEDNOSMERNE**.
- **JEDAN SMER** matematičkih transformacija obezbeđuje da se sa datim izvodom poruke, **NE MOŽE** kreirati originalna poruka.
- Postoji više algoritama za izračunavanje izvoda poruke:
  - SHA – stndard vlade U.S.;
  - MD2, MD4 i MD5.
- Proces generisanja **DIGITALNOG POTPISA** sastoji se od **DVA KORAKA**:
  - GENERISANJE IZVODA PORUKE (engl. *hash*) na osnovu dokumenta koji se potpisuje,
  - KRIPTOVANJE IZVODA PORUKE privatnim ključem potpisnika.

Šifrovanje i digitalni potpis

ŠIFROVANJE (opciono)

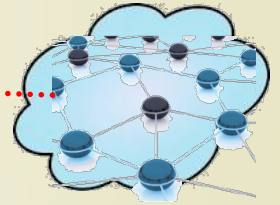


JAVNI ključ primaoca

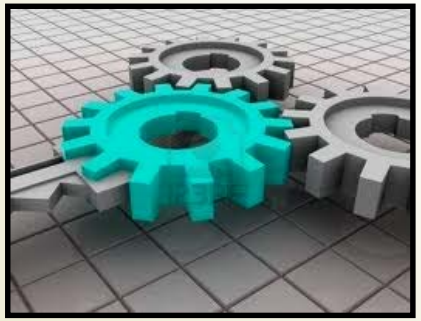
Dokument koji se šalje

+

Slanje na liniju

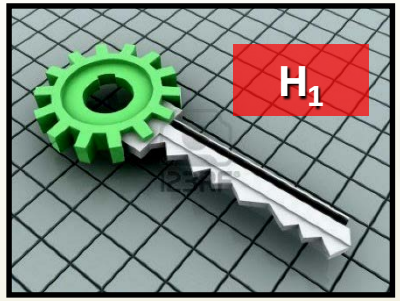


HASH algoritam

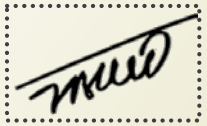


H_1

ŠIFROVANJE



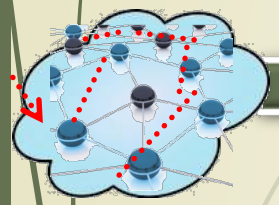
+

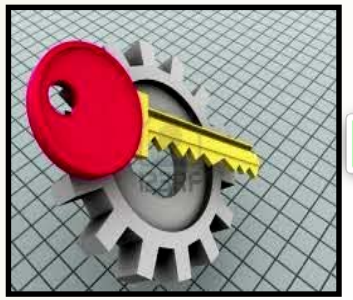


Šifrovani sažetak

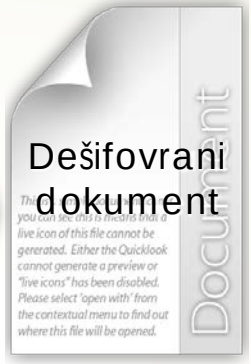
PRIVATNI ključ pošiljaoca

Dešifrovanje i autentifikacija

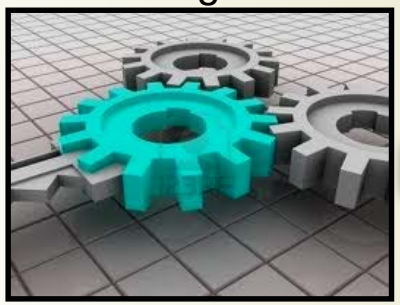




Dešifrovanje dokumenta
(**Privatni** ključ primaoca)



Hash algoritam

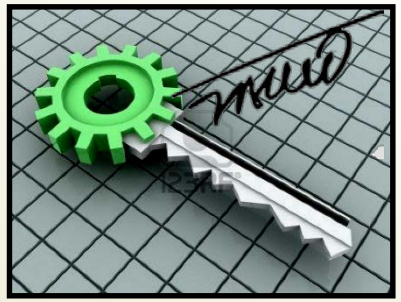


Izračunati
sažetak

H_2

1

Dešifrovanje dig. potpisa



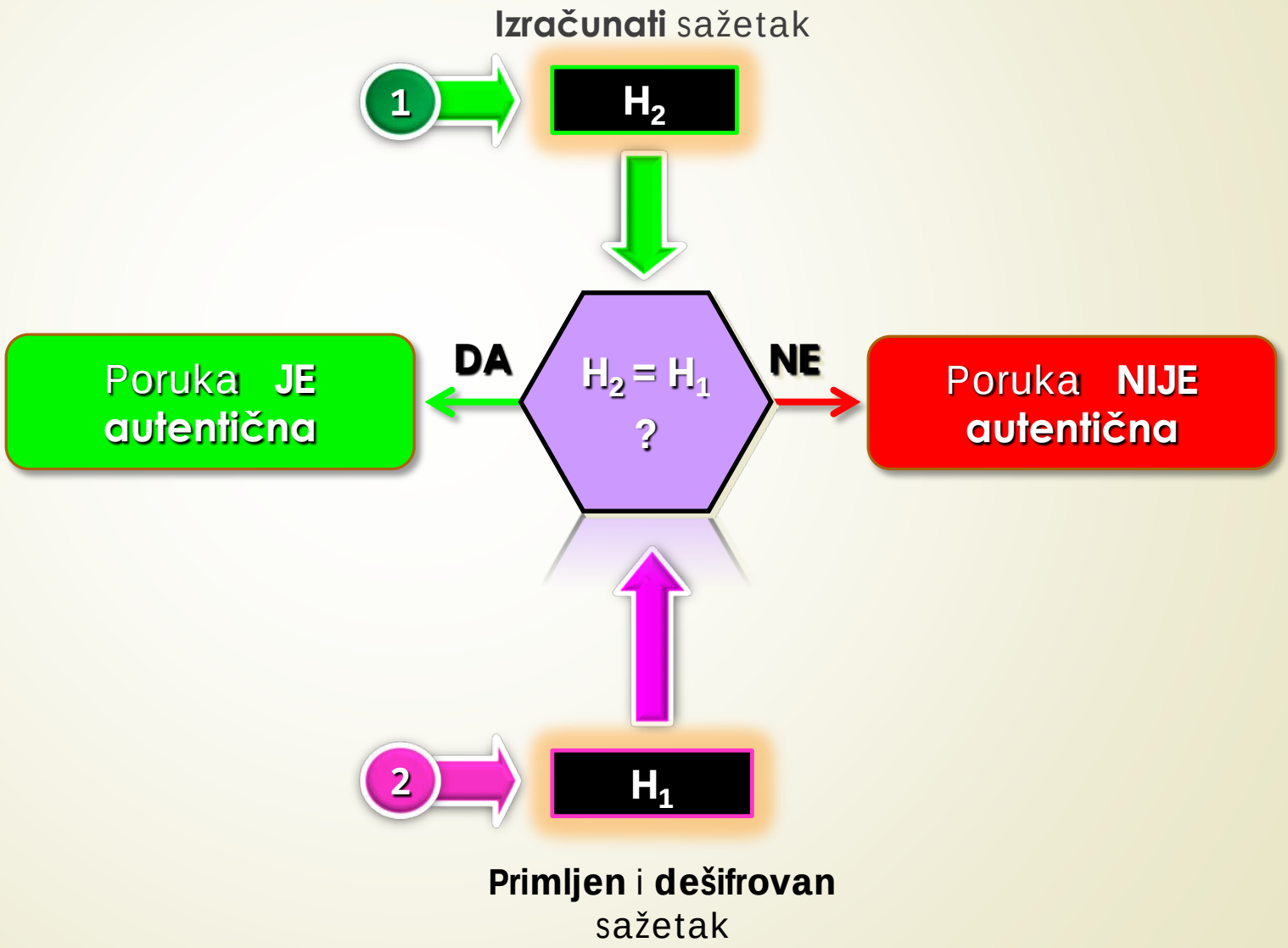
(**Javni** ključ pošiljaoca)

Primljen i **dešifrovan**
sažetak

H_1

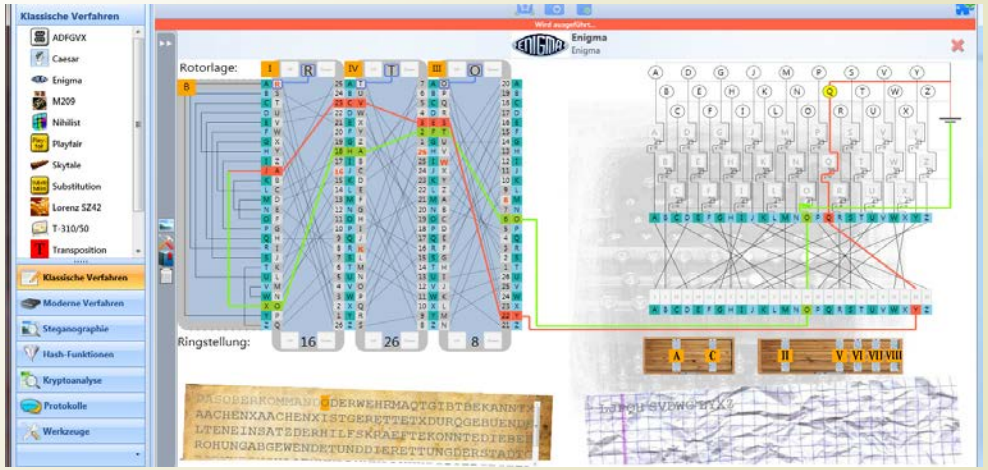
2

Verifikacija digitalnog potpisa (1)



Verifikacija digitalnog potpisa (2)

- Proces **VERIFIKACIJE** se odvija u sledećim koracima:
  - Digitalni potpis se dekriptuje pomoću javnog ključa pošiljaoca što kao rezultat daje **HASH** funkciju $\mathbf{H_1}$.
  - Na poslatim podacima primaoc primenjuje istu hash funkciju koju je primenio pošiljalac i izračunava sada hash funkciju $\mathbf{H_2}$.
  - Ukoliko je $\mathbf{H_1 = H_2}$ to znači da je pošiljalac stvarni potpisnik podataka ili dokumenta, kao i da podaci ili dokument nisu izmenjeni tokom procesa komunikacije.
- Dobar **alat** za učenje kriptografije se može naći na URL-u: http://www.cryptool.org/en/cryptool2-en.



Verifikacija digitalnog potpisa (2)

- Pametne kartice SC (engl. *Smart Cards*) se koriste za **ZAŠTITU** i **ČUVANJE** kriptografskih ključeva.
- Pored postojećeg **SERTIFIKATA** i **TAJNOG KLJUČA**, sam digitalni potpis se generiše unutar čipa i nije dostupan aplikacijama izvan čipa.
- Posebno predavanje će biti posvećeno tehnologiji izrade, i korišćenja pametnih kartica.

MIKROKONTROLER je **ugrađen** na SC karticu.

Eksterno su dostupni su samo kontakti za **serijsku** komunikaciju sa mikrokontrolerom.

Infrastruktura javnog ključa PKI

- Pouzdano utvrđivanje **VLASNIKA JAVNOG KRIPTOGRAFSKOG KLJUČA** je OSNOVA BEZBEDNOSTI **PKI**-a (engl. ***P**ublic **K**ey **I**nfrastructure*).
- **PRAĆENJE IZRADE**, **IZDAVANJA** i **ČUVANJA** kriptografskih ključeva je osnova bezbednosti sistema javnog ključa **PKI**.
- Uverenje **VLASNIKU** javnog kriptografskog ključa se izdaje od strane poverljivog **TREĆEG LICA**.
- **TRI** osnovne **SOFTVERSKE KOMPONENTE** bezbednosti PKI-a su:
  - AUTORITET ZA IZDAVANJE SERTIFIKATA **CA** (engl. *Certificate Authority*);
  - AUTORITET ZA REGISTRACIJU SERTIFIKATA **RA** (engl. *Registration Authority*)
    - REPOZITORIJUM OPOZVANIH SERTIFIKATA **CR** (engl. *Certificate Repository*)
  - AUTORITET ZA VALIDACIJU - VERIFIKACIJU SERTIFIKATA **AV** (engl. *Validation Authority*).

Autoritet za izdavanje sertifikata CA

- **CA** (engl. *Certificate Authority*) je **CENTRALNA KOMPONENTA** PKI-a sa funkcijama **IZDAVANJA** i **ADMINISTRIRANJA** sertifikata.
- **CA** se može realizovati kao **IN-HOUSE** rešenje ili kao **THIRD-PARTY** rešenje korišćenjem CA-OUTSOURCING SERVISA.
- **CA** je odgovoran za **PROIZVODNJU** sertifikata i njihovu **VALJANOST**.
- **CA** izdaje **UVERENJE** vlasniku sertifikata koje može da potvrdi uzrast, pol i druge lične pojedinosti.
- Mogu postojati **VIŠE NIVOA** (hijerarhija) uverenja.
- Uverenja imaju važnost samo **DO NAZNAČENOG DATUMA**.
- Najveći izdavač uverenja je VeriSign, a kod nas je POŠTA CA.

Autoritet za registraciju sertifikata RA

- **RA** (engl. *Registration Authority*) je komponenta PKI-a koja osigurava proces **REGISTRACIJE KORISNIKA**, prihvata i obrađuje zahteve za izdavanjem sertifikata.
- Koncept **RA** se implementira **ŠTO BLIŽE KORISNIKU**, jer je **IDENTIFIKACIJA KORISNIKA** prilikom registracije ključni korak u izdavanju sertifikata.
- Proces registracije predstavlja **PRVU** i **NAJVAŽNIJU KARIKU** u realizaciji neporecivosti.

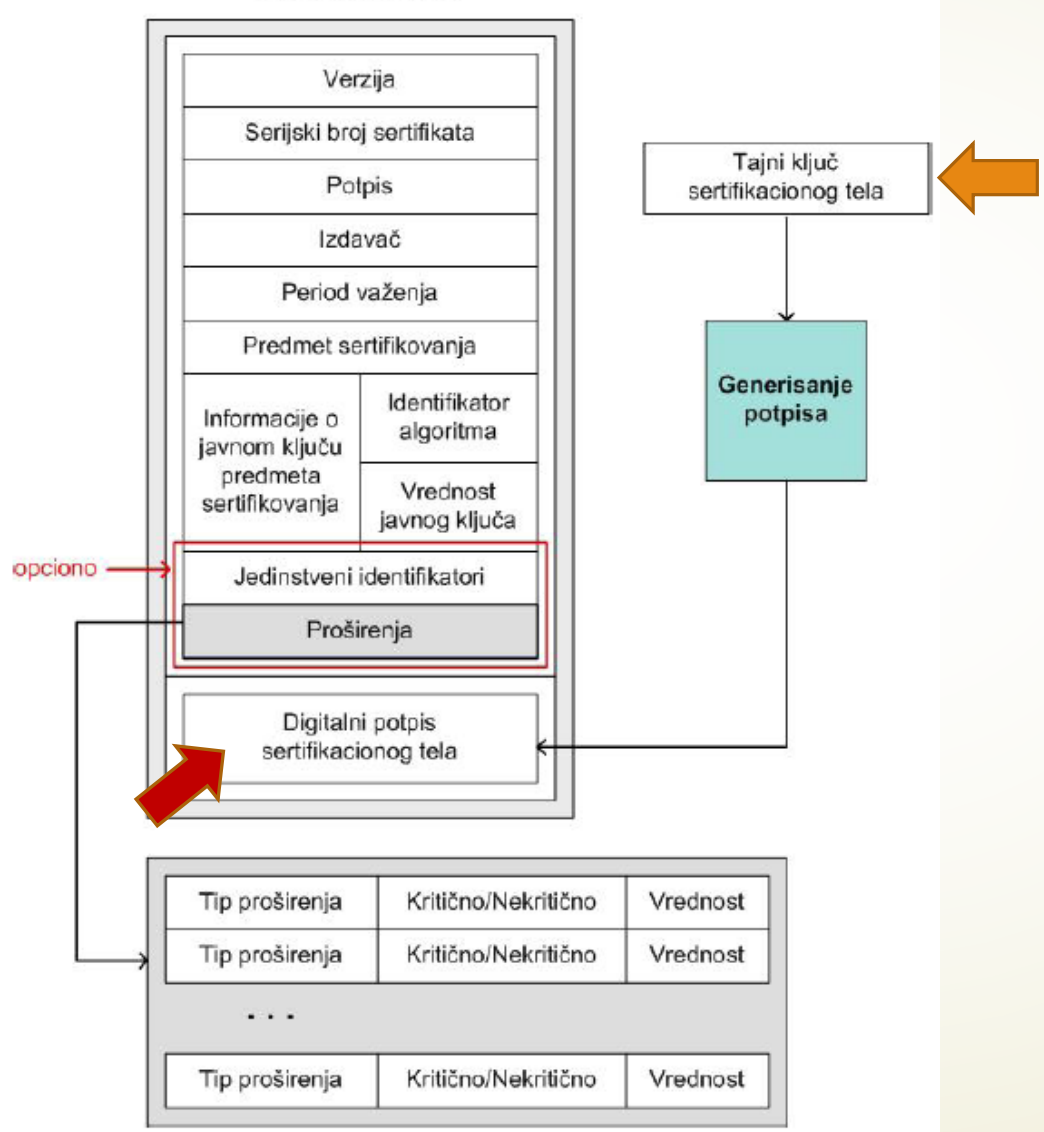
Repozitorijum opozvanih sertifikata CR

- U **CR**-u (engl. *Certificate Repository*) se kreiraju **JAVNI KLJUČEVI** i **SERTIFIKATI** korisnika, kao i **REVOKACIJSKE** (opozvane) **CLR** (engl. *Certificate Revocation List*) LISTE.
- U slučaju da dođe do kompromitovanja ključeva ili promene osnovnih ličnih podataka, **SERTIFIKAT** se **MORA OPOZVATI**.
- OPOZVANI SERTIFIKATI se objavljuju **U LISTAMA OPOZVANIH SERTIFIKATA** CLR .
- **PROVERA VALJANOSTI** sertifikata se može obaviti **UVIDOM U LISTU OPOZVANIH SERTIFIKATA** CLR ili se mogu koristiti protokoli koji daju odziv u realnom vremenu.
- Sadržina i format digitalnog sertifikata je određena standardom **ITU-T X.509** verzija 3.
- Podaci u digitalnom sertifikatu se mogu dopuniti kroz standardna i privatna proširenja.

Autoritet za validaciju sertifikata VA

- **VA** (engl. *Validation Authority*) je **PKI AUTORITET ZA VALIDACIJU** koji pruža uslugu PROVERE VALJANOSTI DIGITALNOG SERTIFIKATA po mehanizmima opisanim u **X.509** i RFC 5280.
- Prikazivanje **LISTE OPOZVANIH SERTIFIKATA** (CRL) je glavni način obavljanja ovog posla, a sama CRL lista se preuzima putem **HTTP** ili **LDAP** protokola.
- Iako **VA** entitet može odgovarati na mrežni zahtev za CRL-om, on **NE MOŽE** oduzeti sertifikat.
- **VA** omogućava **DINAMIČKU VALIDACIJU** sertifikata izdatih od autentičnog sertifikacionog autoriteta.
- Sam **CA** je **MREŽNO NEDOSTUPAN** ali se sertifikati koje je **CA** izdao mogu uvek verifikovati putem **VA** i **HTTP** ili **LDAP** protokola.

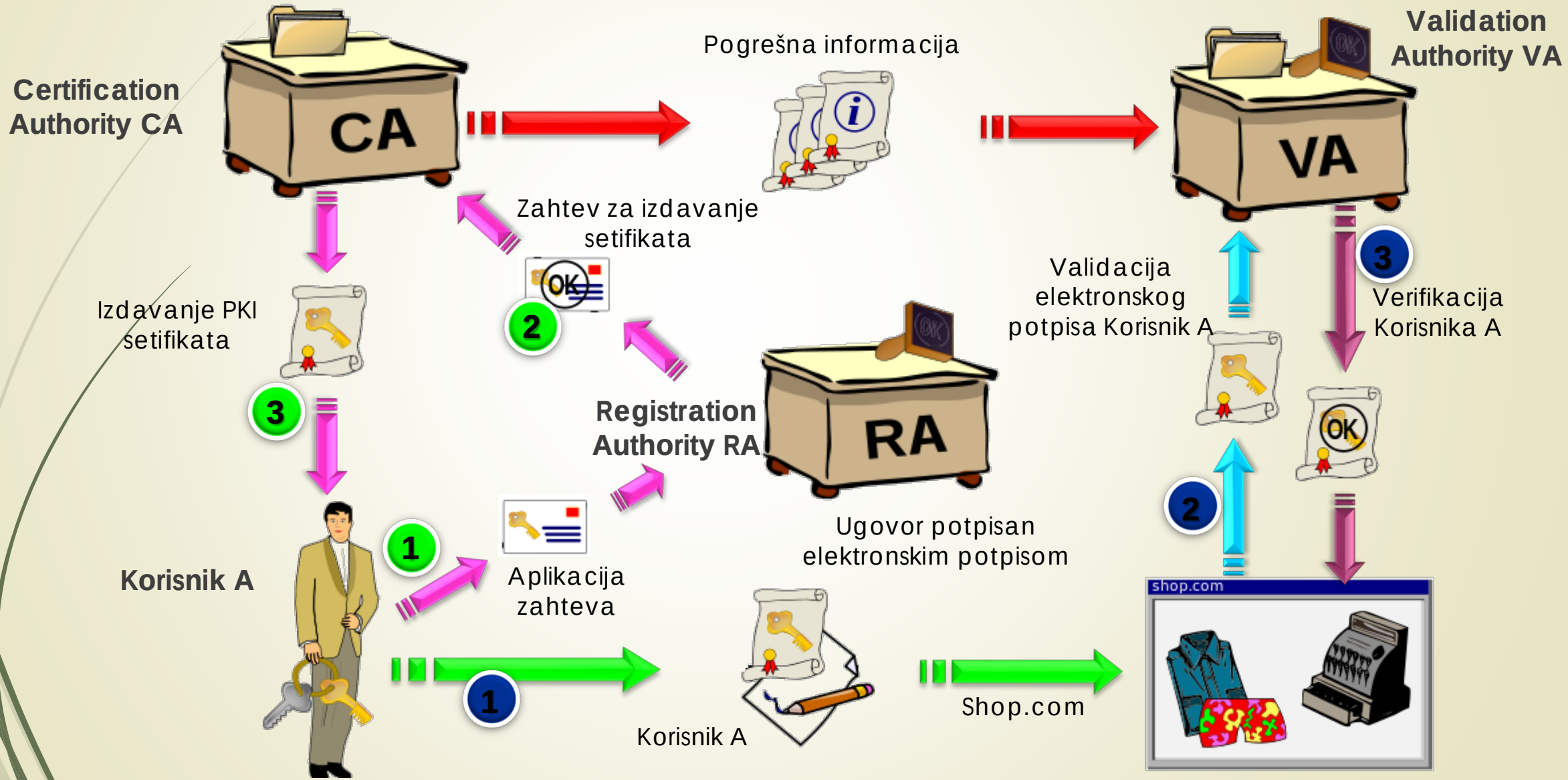
Struktura i primer digitalnog sertifikata




```
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 38 (0x26)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: O=Grid, OU=GlobusTest,
      OU=simpleCA-coit-grid02.uncc.edu, CN=Globus Simple CA
      Validity
      Not Before: Jan 23 18:12:36 2007 GMT
      Not After : Jan 23 18:12:36 2008 GMT
      Subject: O=Grid, OU=GlobusTest,
      OU=simpleCA-coit-grid02.uncc.edu, OU=uncc.edu, CN=Barry Wilkinson
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit):
               00:d7:a9:cc:42:0f:0d:b4:75:4d:e7:0c:aa:25:11:
               db:b9:fb:e9:e7:e5:76:73:e3:99:3f:07:90:18:41:
               b9:93:5f:16:bc:e0:17:dc:7a:c3:f9:57:ed:b4:4d:
               76:ac:58:91:2d:46:24:5c:ed:06:16:e6:58:11:a2:
               18:19:62:7a:84:d1:09:3b:7f:42:91:c[illegible]38:aa:1c:
               4f:93:15:5a:ba:76:8e:6e:a3:4c:5[illegible]42:c8:2a:
               9c:52:b7:29:20:eb:c1:bb:b2:6f[illegible]3:35:a1:e0:
               98:69:6c:2a:1a:d1:e8:6c:68:b8[illegible]16:19:33:22:
               eb:31:7c:18:fa:dc:5b:93:d[illegible]
            Exponent: 65537 (0x10001)
            X509v3 extensions:
               Netscape Cert Type:
               SSL Client, SSL Server, S/MIME, Object Signing
   Signature Algorithm: md5WithRSAEncryption
      8c:f0:b6:df:81:41:bf:cf:34[illegible]3:47:96:38:4d:0e:ac:0e:10:
      f7:e6:b2:21:c0:c0:47:95[illegible]9f:3f:48:42:6c:e9:9a:8e:78:20:
      ce:e9:7a:8f:e8:b3:e4[illegible]87:20:c9:74:6a:dd:dc:c5:b0:a7:
      72:29:59:82:93:0d:[illegible]35:e4:01:2f:68:77:d1:65:14:dd:28:
      e3:1d:97:db:d1:95:[illegible]3f:89:da:d5:fb:e0:a5:c9:bc:b2:59:
      f7:8d:a1:89:4e:0[illegible]f:d2:a8:53:f9:9f:2e:6f:e4:4d:c2:f8:
      4e:b0:16:69:[illegible]36:2c:03:e8:08:3c:2a:ac:29:eb:69:26:
      97:c1
-----BEGIN CERTIFICATE-----
MIICazCCAdSgAwIBAgIBJjANBgkqhkiG9w0BAQQFADBnMQ0wCwYDVQQKEwRHcmlk
MRMwEQYDVQQLEwpHbG9idXNUZXN0MSYwJAYDVQQLEx1zaW1wbGVDQS1jb2l0LWdy
aWQwMi51bmNjLmVkdTEZMBcGA1UEAxMQR2xvYnVzIFNpbXBsZSBDQTAeFw0wNzAx
MjMxODEyMzZaFw0wODAxMjMxODEyMzZaMHkxDTALBgNVBAoTBEdyaWQxEzARBgNV
BAsTCkdsb2J1c1Rlc3QxJjAkBgNVBAsTHXNpbXBsZUNBLWNvaXQtZ3JpZDAyLnVu
Y2MuZWR1MREwDwYDVQQLEwh1bmNjLmVkdTEYMBYGA1UEAxMPQmFycnkgV2lsa2lu
c29uMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDXqcxCDw20dU3nDKolEdu5
++nn5XZz45k/B5AYQbmTXxa84BfcesP5V+20TXasWJEtRiRc7QYW5lgRohgZYnqE
0Qk7f0KR4DiqHE+TFVq6do5uo0xehULIKpxStykg68G7sm+30zWh4JhpbCoa0ehs
aLh7FhkzIusxfBj63FuT2wIDAQABoxUwEzARBglghkgBhvhCAQEEBAMCBPAwDQYJ
KoZIhvcNAQEEBQADgYEAjPC234FBv880w0eWOE0OrA4Q9+ayIcDAR5WfP0hCbOma
jnggzul6j+iz5KOHIMl0at3cxbCncilZgpMNfzXkAS9od9FlFN0o4x2X29GFHz+J
2tX74KXJvLJZ942hiU4EX9KoU/mfLm/kTcL4TrAWaUhaNiwD6Ag8Kqwp62kml8E=
-----END CERTIFICATE-----
```

primer sertifikata

Proces sertifikacije i autentifikacije



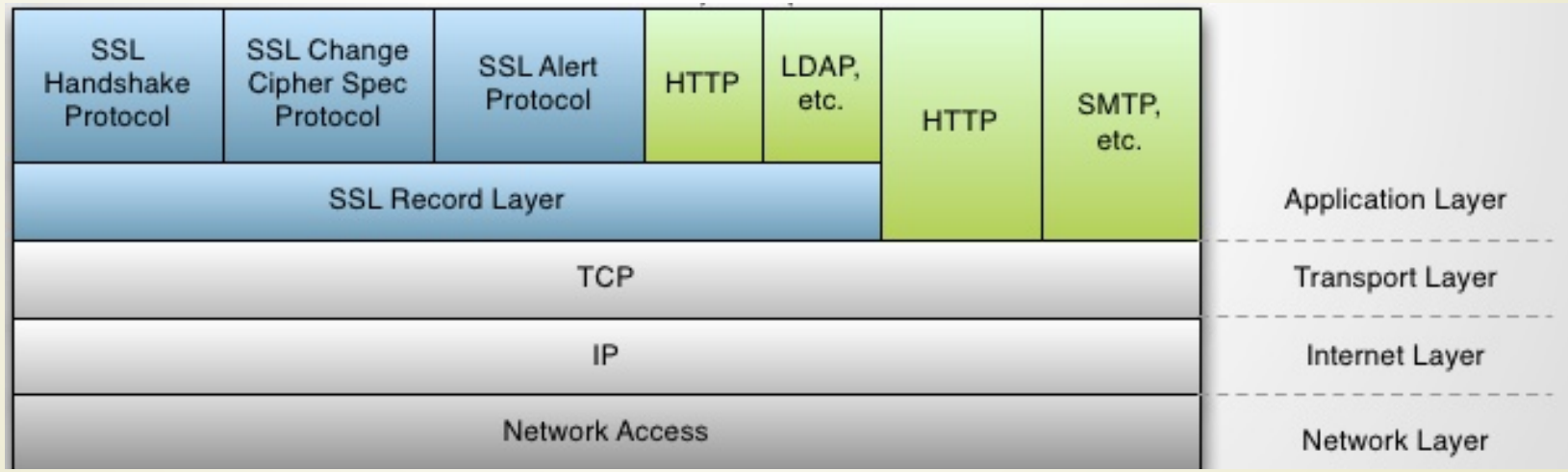
Bezbednost na komunikacionim kanalima

- Pored zaštite podataka INFRASTRUKTUROM PKI–a, Internet pruža mogućnost korišćenja **ŽAŠTIĆENIH KOMUNIKACIJA** (https ptotokol).
- Zaštita je **TRANSPARENTNA** i **NE ZAHTEVA** angažovanje aplikacije - realizovana je na transportnom ISO/OSI sloju.
- Zaštita je smeštena između **APLIAKTIVNOG** i **TRASPORTNOG** sloja u ISO/OSI steku.
- Zaštita podataka se koristi kao **USLUGA** iz steka protokola.
- Dva osnovna protokola kojima se realizuje ovaj vid zaštite su:
  - **SSL** (TSL) (engl. *Secure Socket Layer*)
  - **SET** (engl. Secure *Electronic Transaction*)

SSL protokol (1)

- Upotreba **SSL PROTOKOLA** je garancija sigurnog i pouzdanog prenosa podataka između dve strane u komunikaciji jer su podaci **KRIPTOVANI** i procesiraju se **SERTIFIKATIMA**.
- **SSL** je razvijen od strane Netscape Comm.Corp.
- Za kriptovanje podataka SSL najčešće koristi **DVE** dužine ključeva: 40-bitni i 128 bitni ključ zavisno od željene zaštite i Web browsera koji se koristi.

Lokacija SSL protokla u TCP/IP steku



SSL protokol (2)

- Transakcija korišćenjem **SSL** protokola uključuje sledeće aktivnosti:
  1. Server šalje svoj DIGITALNI SERTIFIKAT klijentu.
  2. Klijent PROVERAVA da li je sertifikat izdat od strane CA, i ako ustanovi da nije, pruža korisniku mogućnost da odabere da li će nastaviti transakciju ili će je prekinuti.
  3. Klijent i server RAZMENJUJU JAVNE KLJUČEVE.
  4. Klijent generiše TAJNI KLJUČ koji se koristi samo u započetoj transakciji.
  5. Klijent ŠIFRUJE GENERISANI TAJNI KLJUČ, korišćenjem serverovog javnog ključa i ŠALJE ga serveru.
  6. U daljem toku transakcije server i klijent koriste ISTI TAJNI KLJUČ metodom simetričnog kriptovanja.

SSL i zaštićena Web stranica

KLIJENT

1	Klijent pristupa stranici koja radi sa SSL-om	→
2	←	Server odgovara svojim javnik ključem
3	Klijent svoj tajni ključ šifruje serverovi javnim ključem	→
4	←	Server potvrđuje prijem tajnog ključa šifrovanjem odgovora
5	Klijent potvrđuje tajni ključ i potpisuje se	→
6	Razmena poruka simetričnim šifrovanjem	↔

SERVER

Vežbe i SSL/TLS protokoli

- Secure Sockets Layer **SSL** i Transport Layer Security **TLS** su OS (engl. ***O****pen Source*) rešenja za protokole koji podržavaju bezbednu komunikaciju.
- Ovi kriptografski protokoli šifruju CELOKUPNU KOMUNIKACIJU IZNAD Trasnportnog ISO/OSI sloja.
- Već je pokazano da SSL i TLS koriste **ASIMETRIČNO ŠIFRIRANJE** za razmenu ključeva, **SIMETRIČNO ŠIFRIRANJE** za očuvanje privatnosti i HEŠ FUNKCIJE za očuvanje integriteta poruke.
- Na vežbama će se obraditi ovi protokoli u okviru OS paketa OpenSSL.
- Biće generisan PAR PKI KLJUČEVA i odgovarajući SERTIFIKAT.

SET protokol

- **SET** (engl. *Secure Electronic Transaction*) je **BEZBEDONOSNI PROTOKOL** razvijen od strane **VISA** i **MasterCard** organizacija koji obezbeđuje:
- **POVERLJIVOST** jer koristi **JAVNI KLJUČ** da KRIPTUJE BROJ PLATNE KARTICE tako da jedino PROCESORSKI CENTAR može da je dekriptuje.
- Za obezbeđenje **INTEGRITETA PODATAKA**, koristi se **DIGITALNI POTPIS** kako bi se sprečila oštećenja ili prevare korisnika .
- **AUTORIZACIJA KUPCA**: korisnik dobija DIGITALNI SERTIFIKAT od banke koja je izdala karticu sa podacima o IDENTITETU korisnika i njegov JAVNI KLJUČ. Sertifikat je digitalno potpisano ODOBRENJE BANKE da je korisnik legitiman. Ako je potpis na digitalnom sertifikatu odgovarajući javnom ključu banke TRGOVAC JE SIGURAN da je kupac legitiman.
- **AUTENTIFIKACIJA TRGOVCA**: Web čitač obrađuje poruku sa SERVEROVOG SERTIFIKATA i istovremeno DEKRIPTUJE PORUKU javnim ključem CA. Ako su poruke iste onda je trgovac legitiman.