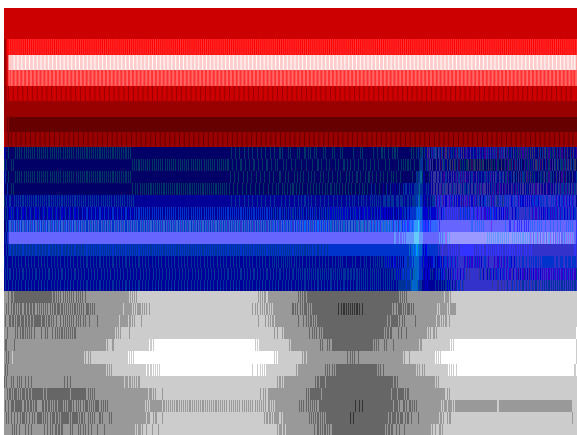
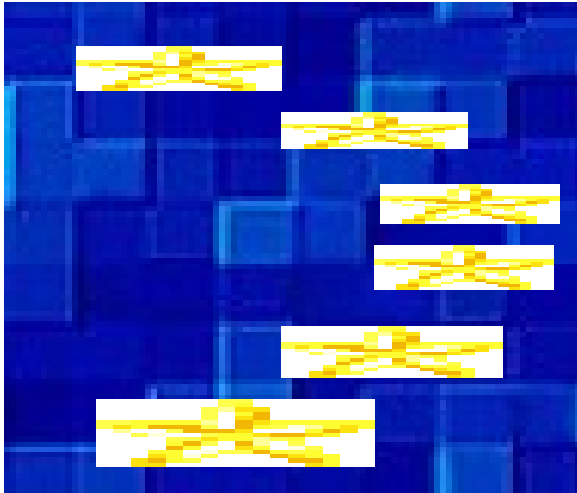




# Elektronski potpis

Prezenter:  
Nebojsa Detki

# Pravni aspekti e-potpisa



- [Direktiva EU 1999/93/EC o elektronskim potpisima](#) (usvojena 13. decembra 1999, a formalno stupila na snagu 19. januara.2000.godine) predstavlja pravno utemeljenje elektronskog potpisa i na osnovu nje su doneti Zakoni o elektronskom potpisu u svim zemljama EU, kao i u većini ostalih zemalja Evrope.
- [Zakon o elektronskom potpisu u Srbiji](#), u potpunosti usklađen sa EU Direktivom 1999/93/EC, izglasan je u Narodnoj skupštini Republike Srbije dana 14. decembra 2004. Publikovan u Službenom glasniku Republike Srbije br. 135 od 21. decembra 2004. godine; ([Pravilnici, Uputstva...](#))



# Definicija



- **Tri osnovne vrste elektronskih potpisa:**
- **Skenirani rucni potpis** (nema pravnu snagu);
- **Digitalni potpis**
- **Biometrijski potpis**
- **Digitalni (elektronski potpis)** predstavlja tehnologiju čijom se primenom u sistemima elektronskog poslovanja omogućava provera autentičnosti potpisnika, date poruke ili dokumenta;
- **Tehnologija** koja zamenjuje svojerucni potpis i pecat za dokumenta u elektronskoj formi;
- To je **niz znakova,** dobijen primenom **asimetricne kriptografije;**
- Otklanja se glavna prepreka za komunikaciju bez papira;
- Ključna pretpostavka za razvoj e-uprave;

# Gde se koristi ?

- elektronsko poslovanje (e-Business)
  - elektronska trgovina (e-Commerce)
  - elektronsko bankarstvo (e-Banking)
  - elektronska uprava (e-Government)
  - elektronsko zdravstvo (e-Healthcare)
  - platni sistemi na bazi čip kartica (EMV) itd
- zaštićene web transakcije
  - zaštićene e-mail poruke;
  - zaštićen FTP servis;
  - formiranje VPN (IPSec) mreža;
  - bezbedno upravljanje dokumentacijom;
  - bezbena plaćanja putem Interneta itd.

# Procedura:

## ZA DOBIJANJE:

- **Gradjani** mogu da predaju zahteve za izdavanje sertifikata na salterima posta;
- Uz licnu kartu, popunjava se obrazac;
- **Pravna lica** i izvod iz privrednog registra;
- Nekoliko dana nakon toga dobija obavestjenje da je njegov **elektronski sertifikat** gotov, i dolazi u postu da ga preuzme;
- **PIN kod** za sertifikat mu stize nakon toga na kucnu adresu;
- Procedura traje oko 10 dana;

## ZA KORISCENJE:

- Slicna koriscenju bankomata;
- Umesto platne kartice, potpisnik poseduje **karticu za potpisivanje**;
- Potreban mu je **citac kartice** i **softver za potpisivanje**;
- Kartica ide u citac i od softvera se zahteva potpisivanje odredjenog dokumenta;
- Unosi se **PIN kod**;
- Tako formiran potpis je posebna datoteka i dostavlja se zajedno sa dokumentom;
- **Verifikacija KOD PRIJEMA** opet na bazi softvera;
- Verifikacija je uspesna, sto znaci da je potpis autentican, dokument nije menjan i ne moze se negirati;

# Prikaz postupka:

PRE:



POSLE:

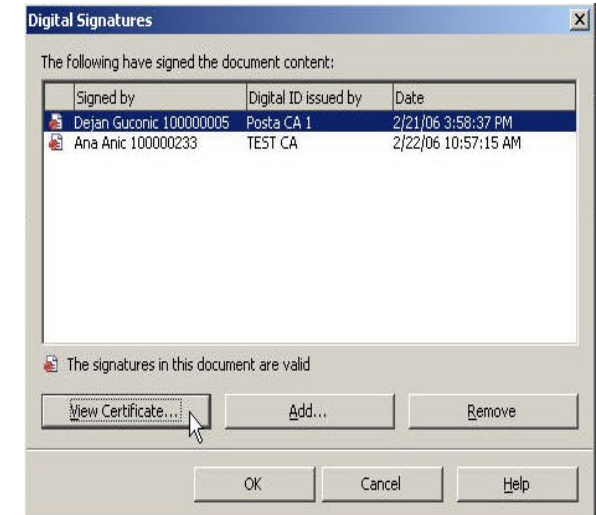
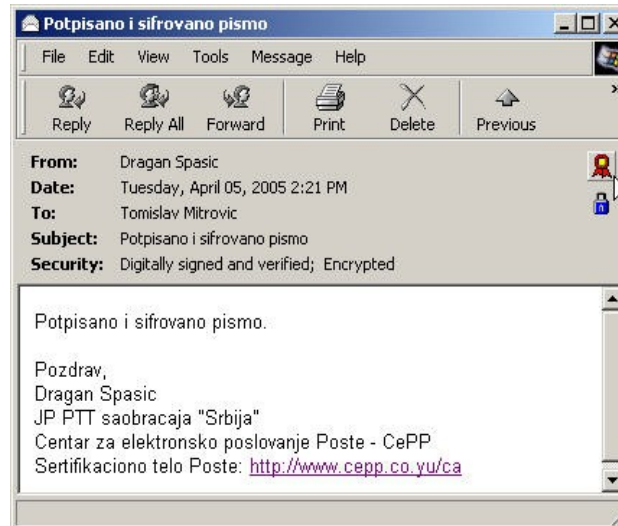
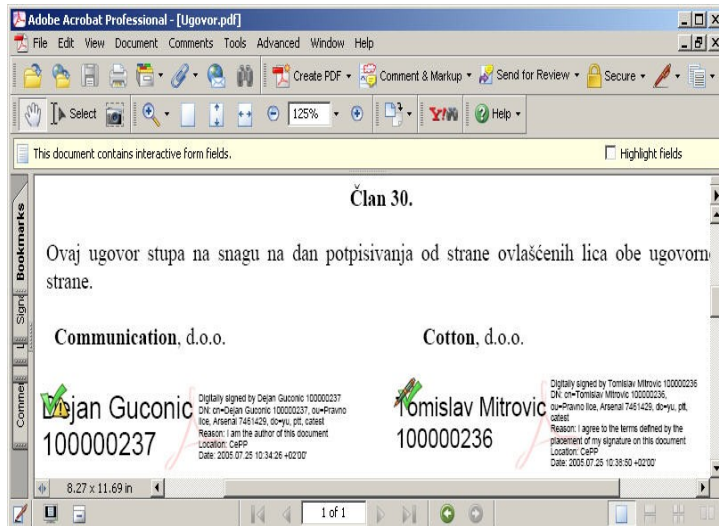
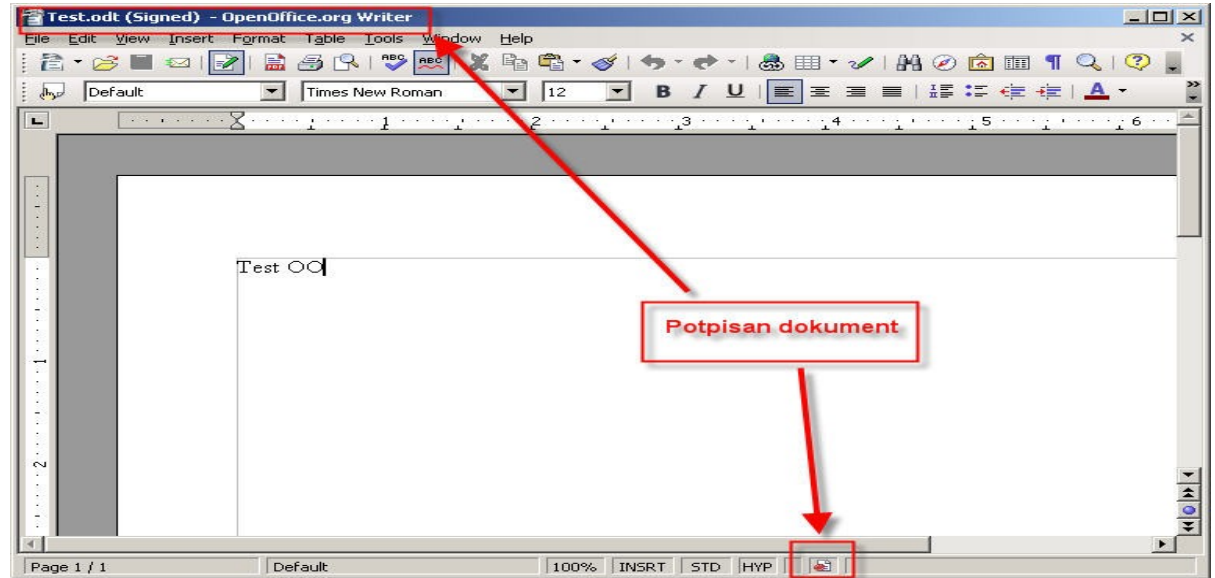
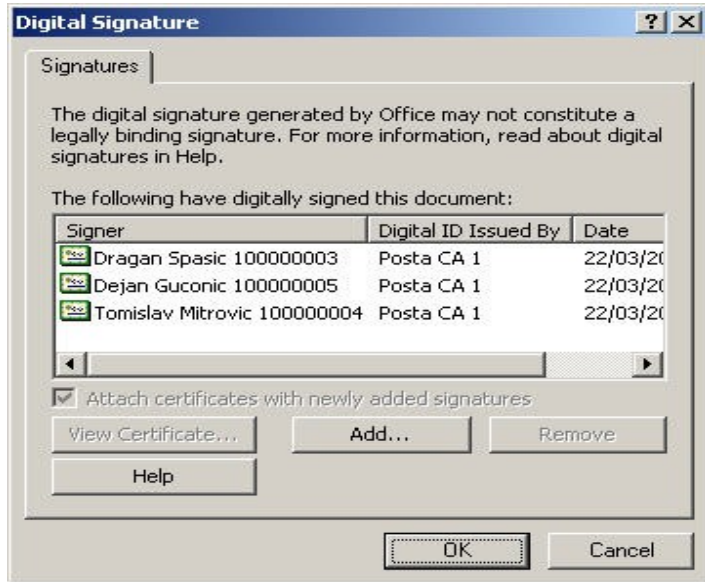
- **Autentifikacija:** Utvrđuje se identitet potpisnika.
- **Integritet:** Proverava se da li je sadržaj dokumenta ili transakcije promenjen posle potpisivanja.
- **Neporecivost:** Onemogućava se poricanje izvršenog potpisivanja.
- **Tajnost:** Garantuje se da sadržaj dokumenta može da sazna jedino korisnik kome je dokument namenjen;

# Digitalni identitet i mediji:

- Digitalni identitet korisnika čine:
- tajni (privatni) kriptografski ključ (private key) korisnika,
- javni kriptografski ključ (public key) korisnika (ime korisnika), ime sertifikacionog tela (CA servera npr. Posta) i digitalni sertifikat (koji sadrži javni kriptografski ključ korisnika).
- Digitalne sertifikate korisnicima izdaju sertifikaciona tela (Certification Authority – CA).
- Sertifikaciona tela poseduju PKI infrastrukturu (Public Key Infrastructure – PKI).



# Izgled nakon potpisivanja u pojedinim programima:



**Hvala na paznji !**

  
13.02.2009.god.  
Beograd, Dubrovacka 35

**Korisceni materijali:**

- delovi Zakona o e-potpisu;
- prezentacija, Prof.dr. Predrag Dimitrijevic, fakultet za drzavne i evropske studije;
- prezentacija, CEPP Mr.Dragan Spasic dipl.inz. Okt. 2007.
- "Blic" Jasna Matic – ministarka za telekomunikacije i info.drustvo jan.2009.
- materijal sa sajta PKS;