ᐯᑎᑐᑌᐯᒪᐃᐩᐯ ᒪᓗᓂᐱᐩᓗᒪᑎᑌᐯ

ᒧᔅᓂᐱᒪᐩᐯᒧᑎ

ᑐᓗᒪᔅ ᐺᓗᓂᓗᒪ

Otvoreno računarstvo

Sigurnost

- Uvod - osnovni pojmovi
- Napadi i metode zaštite
- Primjena i primjeri

Mario Žagar

Predgovor

- Želite li vjerovati da su Vaši podaci 100% sigurni, nedostupni drugima, nepromjenljivi, ...

...NEMOJTE NIKADA, NIGDJE, NIZAŠTO, ...
KORISTITI RAČUNALO, Internet,...!

- Ako gornji postotak (100%) zamijenimo s nekim drugim postotkom (10%,...50%,..., 99%, ...99,9%...),

- možemo nastaviti!

Vaš sveučilišni profesor računarstva
Mario Žagar

Uvod

Uvod - Sigurnost (*Security*)

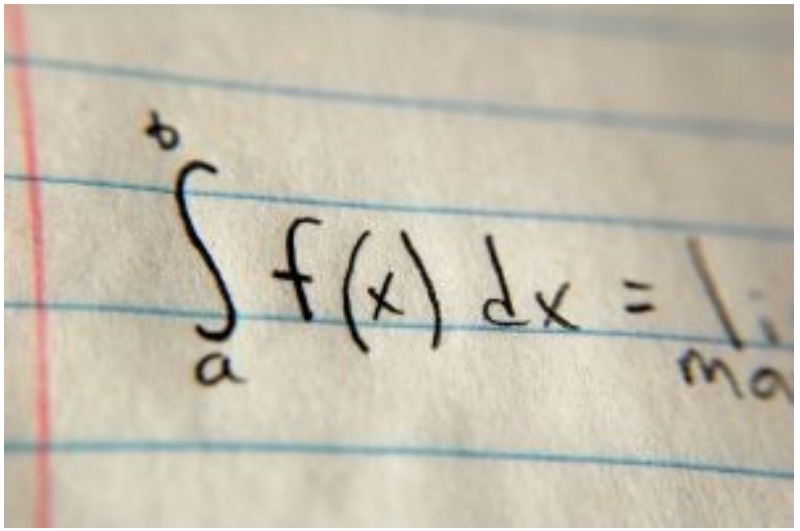
- Široko dostupne računalne mreže
  - Javne informacije
  - Privatne informacije
    - Kako ih odvojiti i zaštititi?
    - Sve više i više različitih podataka na Mreži
      - Sintagma: "Ako nešto nije na Internetu - NE POSTOJI!"
    - Kako kontrolirati dostupnost/nedostupnost,....?
- Sigurnosni zahtjevi - ciljevi:
  - Povjerljivost, tajnost (*confidentiality, secrecy*)
  - Cjelovitost, očuvanost (*integrity*)
  - Izvornost, ovjera (*authenticity*)
  - Neporicljivost (*nonrepudiation*)
  - Dostupnost (*availability*)
  - Kontrola pristupa (*access control*)

Ciljevi

- Povjerljivost, tajnost (*confidentiality, secrecy*)
  - Očuvanje tajnosti poruke
  - Treba biti razumljiva samo pošiljatelju i namjeravanom primatelju

Ciljevi

- Cjelovitost, očuvanost (*integrity*)
  - Sadržaj poruke ne smije se mijenjati prilikom prijenosa
    - Zbog grješaka u prijenosu
    - Namjernom promjenom – napadom
  - Svaku promjenu poruke treba moći primijetiti



Ciljevi

- Izvornost, ovjera (*authenticity*)
  - Sposobnost određivanja izvornosti (autentičnosti, ovjere) partnera u komunikaciji
  - Mogućnost otkrivanja promjene sugovornika

Ciljevi

- Neporicljivost (*nonrepudiation*)
  - Nemogućnost poricanja slanja poslane poruke
  - Za svaku poslanu poruku moguće utvrditi autora

Ciljevi

- Dostupnost (*availability*)
  - Osiguranje dostupnosti usluge aktivnim sprječavanjem napada

Ciljevi

- Kontrola pristupa (*access control*)
  - Sposobnost dodjele ili zabrane prava pristupa i korištenja resursa na pouzdan način

Osnovni pojmovi

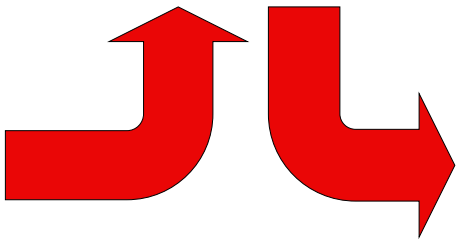
- Kriptologija (*Cryptology*)
  - Kriptografija (*Cryptography*) – umijeće čuvanja tajnih informacija
    - Nešto kao *iu9o5gfmxcv[grs*
    - Umjetnost pretvaranja razumljivog u nerazumljivo svima osim nekolicini
    - Nešto što malo ljudi potpuno razumije, ali svi možemo koristiti.
  - Kriptoanaliza (*Cryptanalysis*) – umijeće otkrivanja (tuđih) tajnih informacija
- Izvorni tekst (*clear-text*, *plain-text*)
- Šifrirani, kriptirani tekst (*cypher-text*, *cipher-text*)
- Šifriranje, kriptiranje, dešifriranje, dekriptiranje (*encryption/decryption*)

Osnovni pojmovi

- Ključ (*key*)
  - Informacija koja se koristi u postupku kriptiranja i/ili dekriptiranja i jednoznačno određuje postupak kriptiranja i/ili dekriptiranja
- Šifra (*cypher, cipher*)
  - Par algoritama koji se koriste za pretvorbu iz izvornog u kriptirani oblik i natrag
  - Katkad može imati značenje ključa
- Kôd (*code*)
  - Zamjena jedinice izvornog teksta kodnom riječi
  - Bilo koja metoda skrivanja izvornog značenja

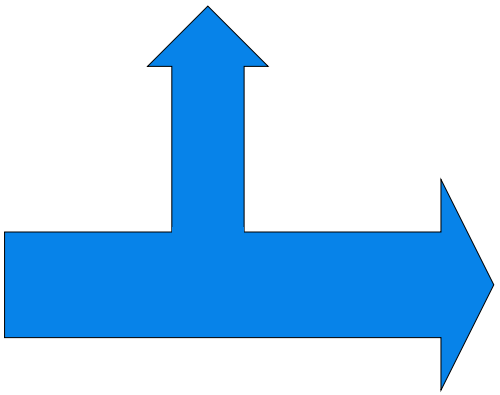
Aktivni napadi

- Lažno predstavljanje
  - Korisnika – *impersonation*
  - Usluge – *phishing*
- Ubacivanje u komunikaciju (*man in the middle*)
- Uskraćivanje usluge (*denial of service*, DOS/DDOS)
- Napad lažnim porukama
  - Ponavljanjem poruka (*replay attack*)
  - Zamjenom poruka (*substitution attack*)



Pasivni napadi

- Prisluškivanje (*eavesdropping*, *tapping*)
- Pogađanje ključeva ili lozinki
  - Grubom silom (*brute force*)
  - Napad rječnikom (*dictionary attack*)
  - Odabranim porukama (*chosen cipher-/plain-text*)
  - Kriptoanaliza, statističke metode



Metode zaštite

- Zaštita na više razina
  - Sustav
    - Arhitektura mreže (demilitarizirane zone, DMZ)
    - Vatrozid (*firewall*)
    - Antivirusna zaštita
    - Sigurnosni alati
  - Komunikacijski kanal
    - Secure Sockets Layer (SSL)
    - IPSEC
    - Kriptiranje komunikacije (sklopovsko)
  - Poruke
    - Digitalni potpis
    - Digitalna omotnica

Primjer: telnet

- Protokol telnet ne koristi zaštitu prilikom prijenosa osjetljivih informacija
  - Korisničko ime

```
login: mario

TELNET:  ----- TELNET: -----
TELNET:
TELNET:  "mario"
TELNET:
 0:0800 200e 1a39 0060 9795 628d 0800 4500 ..  ..9.`..b...E.
16:0029 1e00 4000 8006 13fe a135 4364 a135 .)..@.....5Cd.5
32:4302 0404 0017 0023 17fa 3ac5 4bf6 5018 C......#..:.K.P.
48:21cf b537 0000 6d61 7269 6f              !..7..mario
...
```

Primjer: telnet

- Protokol telnet ne koristi zaštitu prilikom prijenosa osjetljivih informacija
  - Lozinka

```
Password: xxxxx

TELNET:  ----- TELNET: -----
TELNET:
TELNET:  "123456"
TELNET:
 0:0800 200e 1a39 0060 9795 628d 0800 4500 .. ..9.`..b...E.
16:0029 2b00 4000 8006 06fe a135 4364 a135 .)+.@.....5Cd.5
32:4302 0404 0017 0023 1801 3ac5 4c07 5018 C......#..:.L.P.
48:21be b530 0000 3132 3334 3536           !..0..123456
...
```

Algoritmi

- Tajni algoritmi
  - Neprikladni za ozbiljnu primjenu
- Javni algoritmi
  - Sažetak (*digest*, *hash*)
    - Digitalni otisak prsta (*fingerprinting*)
  - S ključem
    - Tajni ključ (*secret key*) – simetrični algoritmi
      - Šifriranje blokova (*block cipher*)
      - Šifriranje toka (*stream cipher*)
    - Javni ključ (*public key*) – asimetrični algoritmi
  - Steganografija
    - Digitalni vodeni žig (*watermarking*)

Svojstva algoritama

- Sažetak (*digest*, *hash*)
  - Cjelovitost
  - (Izvornost)
- Šifriranje (*cipher, cypher*) s ključem
  - Povjerljivost
  - (Cjelovitost)
  - (Izvornost)
- Steganografija
  - Povjerljivost

Algoritmi sažetaka (*hash*)

- Prevode sadržaj poruke u jedinstveni sažetak
- Funkcija generiranja sažetka
  - Jednosmjerna (gubitak informacija)
  - Prevodi izvorni tekst u sažetak fiksne duljine
    - Različiti izvorni tekstovi mogu imati iste sažetke
  - Nije moguće odrediti koje dvije poruke imaju isti sažetak
  - Generirani sažetak treba sličiti slučajno generiranim podacima
    - Minimalna promjena ulaza – velika promjena izlaza
- Sažetak poruke odgovara digitalnom otisku prsta poruke
- Algoritmi: MD5, SHA-1, SHA-3 (dolazi)

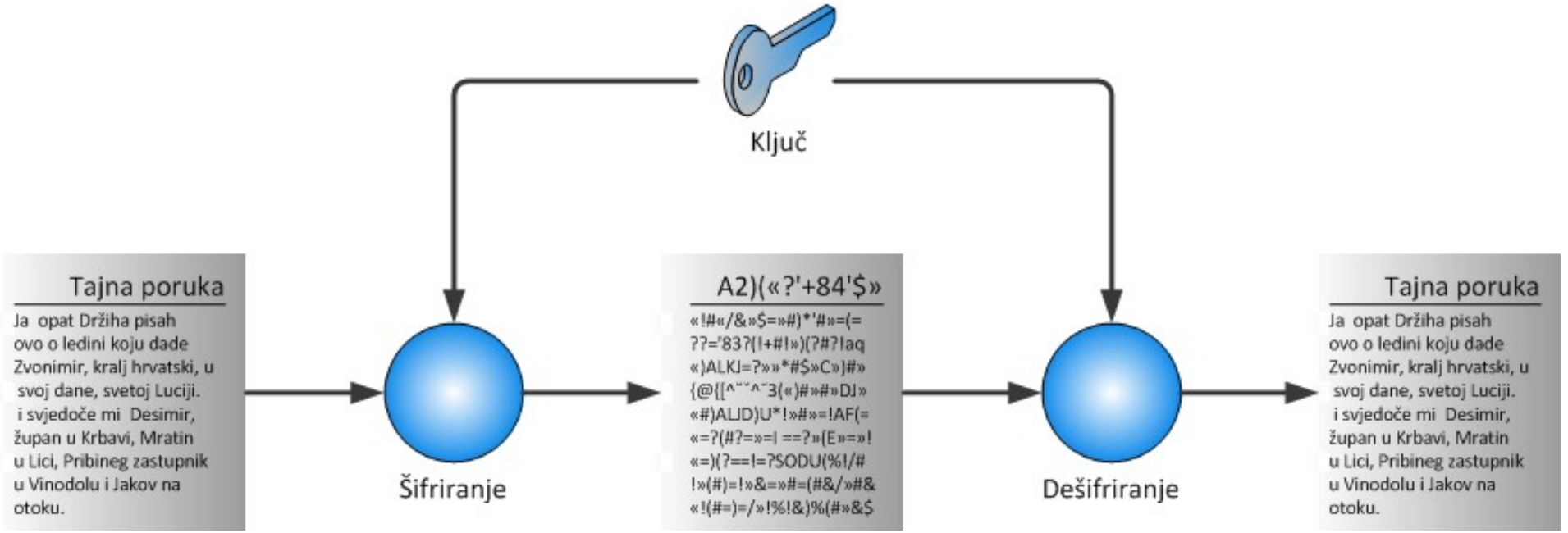
Algoritmi s tajnim ključem

- Isti ključ za kriptiranje i dekriptiranje - simetrični
  - Tajni ključ, dijeljeni ključ
- Sigurnost ovisi o:
  - Ključu (duljini ključa)
  - Mehanizmu dogovora ključa među sugovornicima
- Osnovne grupe
  - Blokovske šifre - najčešće
    - Ulaz u funkciju – blok podataka stalne duljine
  - Šifre tôka
    - Ulaz u funkciju – bit po bit iz tôka podataka koji se šifrira
- Gradivni blokovi
  - S (supstitucijske) i P (permutacijske) kutije
  - Sklopovske implementacije – brzina!

Simetrični algoritmi

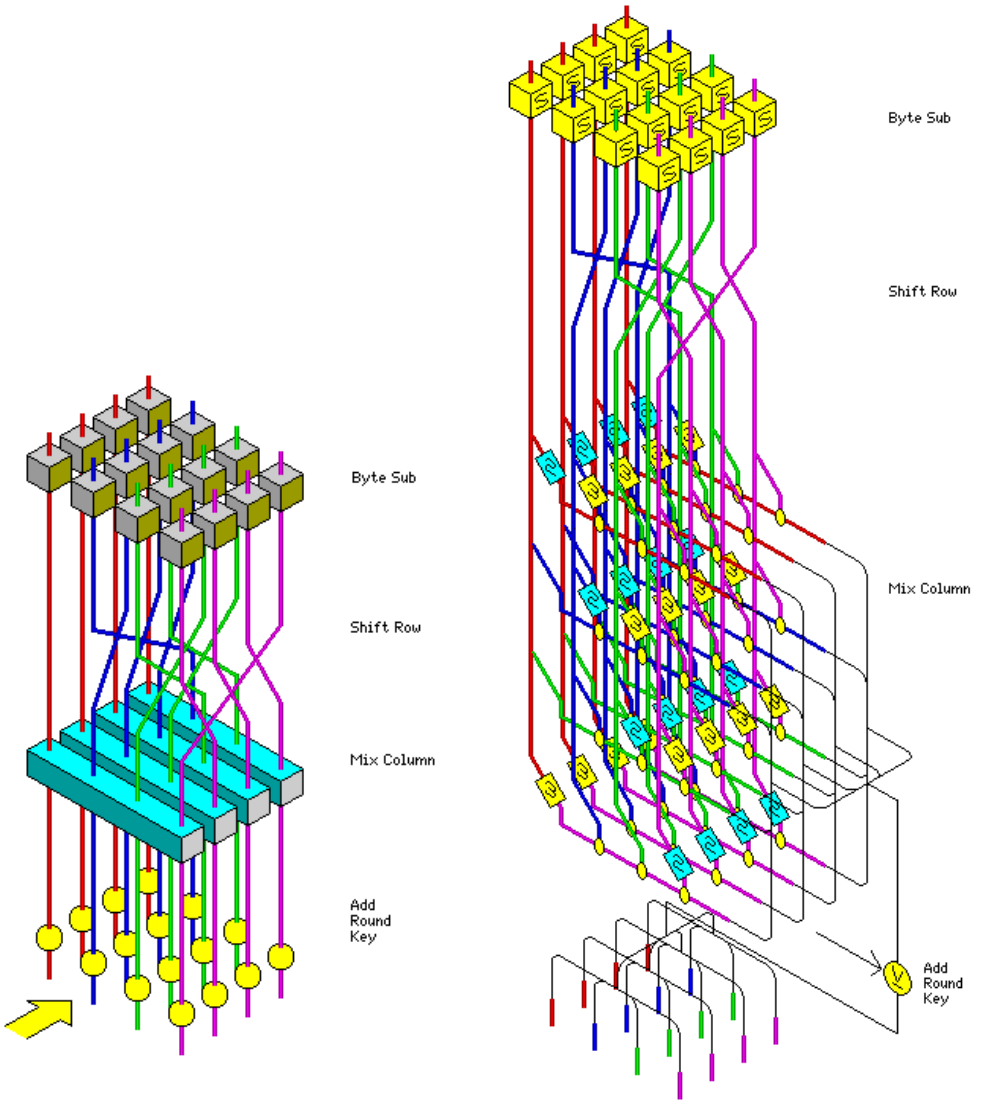
- Tajni (dijeljeni) ključ
  - Početni problem sigurnog prenošenja poruke (veća količina podataka) prevodimo u problem sigurnog prenošenja ključa (mala količina podataka)
- Dogovor o ključu
  - Dogovor dviju strana o zajedničkom (dijeljenom) ključu putem nesigurnog kanala

Simetrični algoritmi



Simetrični algoritmi

- AES (Rijndael)
- Serpent
- Twofish
- Blowfish
- IDEA
- 3DES
- DES



Ilustracija AES/Rijndael algoritma, John Savard

Primjer: probijanje ključa (DES) sirovom snagom

Napadač	Proračun	Alat	Vrijeme i troškovi za svaki ključ		Duljina ključa koja jamči sigurnost	
			40 bitova	56 bitova	1996.	2015.
Haker vulgaris	Mali $400	PC FPGA	1 tjedan 5 sati $0.08	Nepraktično 38 godina $5000	45 50	59 64
Malo poduzeće	$10.000	FPGA	12 min $0.08	556 dana $5.000	55	69
Korporacijski odjel	$300.000	FPGA ASIC	24 sec $0.08 0.18 s $0.001	19 dana $5000 3 sata $38	60	74
Velika kompanija	$10.000.000	FPGA ASIC	0.7 s $0.08 0.005 s $0.001	13 sati $5.000 6 min $38	70	84
Obavještajna agencija	$300.000.000	ASIC	0.0002s $0.001	12 s $38	75	89

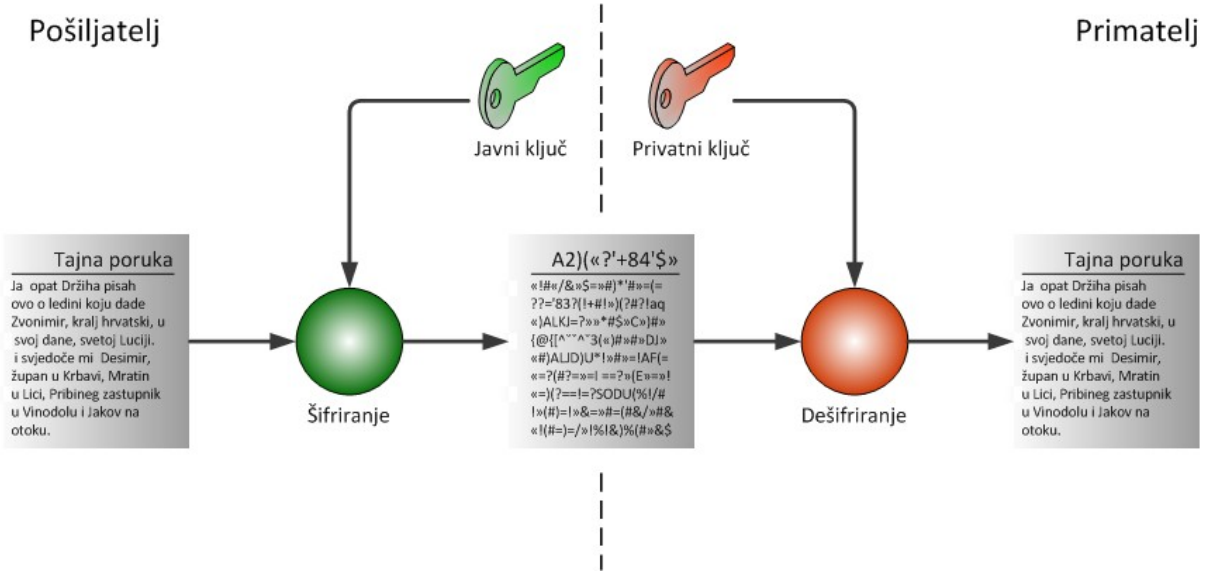
Algoritmi s javnim ključem

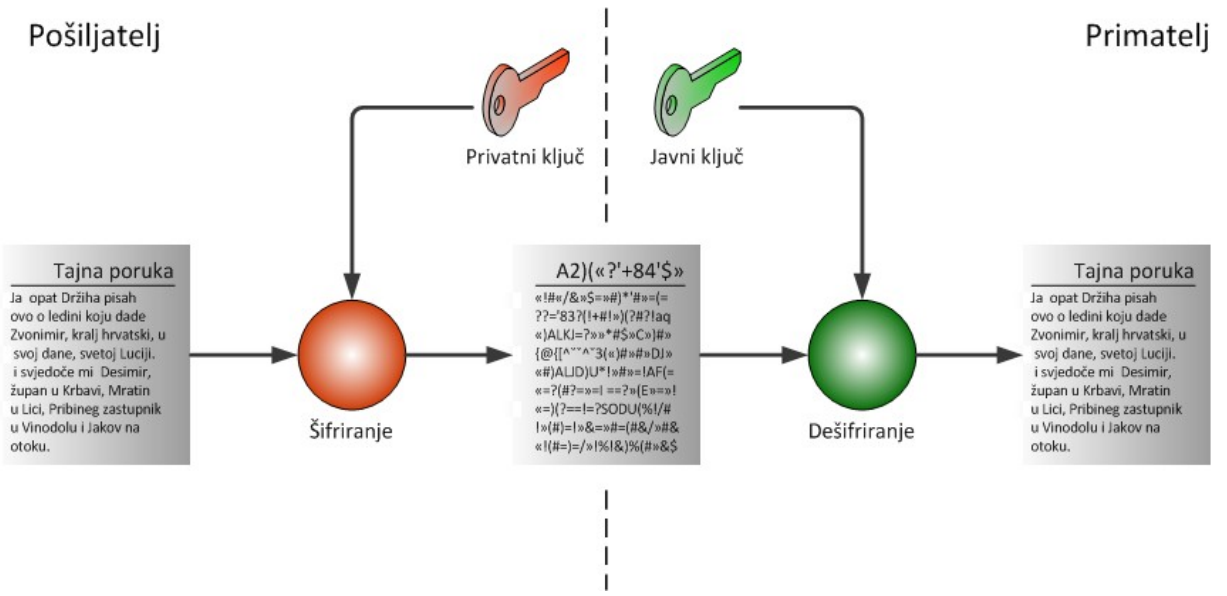
- Različiti ključevi za šifriranje i dešifriranje
  - Asimetrični
  - Tajni ključ – šifriranje / dešifriranje
  - Javni ključ – šifriranje / dešifriranje
- Temeljeni na NP-teškim matematičkim problemima
  - Nema poznatog algoritma polinomne (P) složenosti za poznate NP-teške probleme i vjeruje se da takvi algoritmi ne postoje
- Sigurnost ovisi o:
  - Odabranom problemu
  - Ključu (duljini ključa)
  - Zaštiti tajnog ključa

Asimetrični algoritmi

- Kako izgraditi algoritam?
  - Uzeti težak problem (NP-težak) s posebnim slučajem koji se može riješiti u P (polinomne složenosti)
  - Šifriranje – pretvoriti poruku u poseban slučaj problema, zatim javnim ključem pretvoriti jednostavan problem u težak
  - Dešifriranje – korištenjem privatnog ključa pretvoriti težak problem u jednostavan i riješiti ga
- Primjeri problema
  - Faktorizacija brojeva (RSA, Rabin)
  - Diskretni logaritmi (Diffie-Hellman, DSS, El-Gamal)
  - Eliptičke krivulje (LUC, XTR)

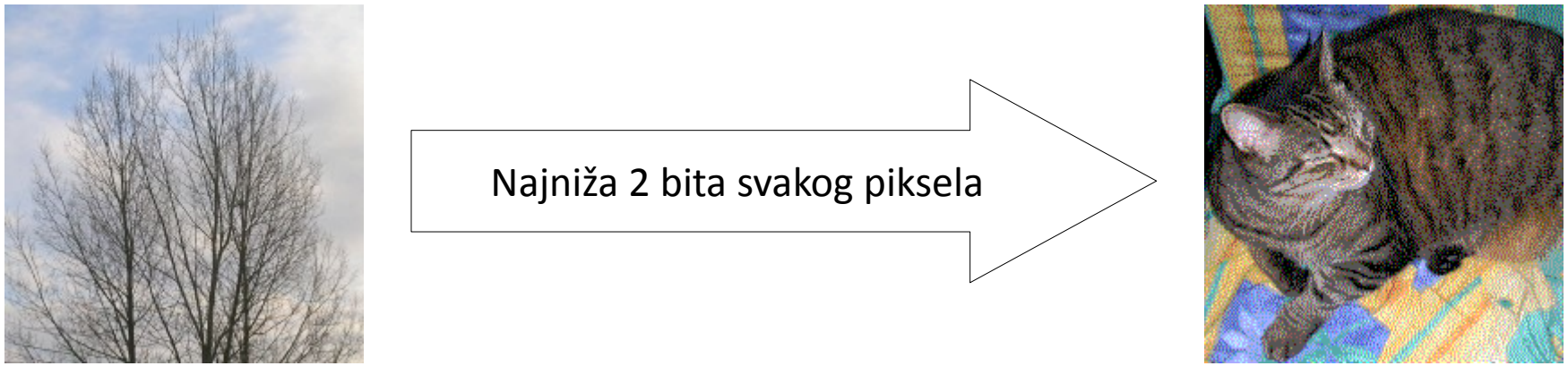
Asimetrični algoritmi (svojstvo)





Steganografija

- Skrivanje poruke
  - Nitko osim pošiljatelja i primatelja nije svjestan postojanja poruke
- Primjer
  - Skrivanje tajne slike u niže bitove kamuflažne slike



Izvor: Wikipedia: Steganography

- Primjena: *vodeni žig* u multimedijalnim sadržajima (©, DRM)

Usporedba algoritama

- Simetrični algoritmi

  Prednosti

  - Velika raznolikost algoritama
  - Brzina
    - Manja računska složenost
    - *Jednostavna* sklopovska implementacija

  Mane

  - Distribucija ključeva
    - Razgovor N sugovornika zahtijeva n·(n-1)/2 ključeva
    - Problem razmjene ključa

Usporedba algoritama

- Asimetrični algoritmi

  Mane

  - Sporost
    - Velika računska složenost
    - Složena implementacija

  Prednosti

  - Distribucija ključeva
    - Javni ključ se može slobodno dijeliti

- Idealni algoritam imao bi dobra svojstva obje grupe
  - Brzinu simetričnih
  - Rukovanje ključevima asimetričnih

Primjena algoritama

- Šifriranje podataka (npr. na disku)
  - Cjelovitost
  - Tajnost
- Digitalni potpis
  - Ovjera izvornosti
  - Cjelovitost
  - Neporicljivost
- Digitalna omotnica
  - Ovjera izvornosti
  - Cjelovitost
  - Neporicljivost
  - Tajnost

Ključevi

- Što sve može biti ključ?
- Vrste ključeva
  - Kratki (pamtljivi)
    - Alfanumerički
      - Lozinke
      - TAN (transakcijski broj, varijanta ključa za jednokratnu uporabu)
      - Token – sklopovska izvedba TAN-a
  - Dugi
    - Sažetak
    - Certifikat
      - Pametna kartica
  - Biometrijski
    - Otisak prsta
    - Uzorak šarenice
    - Slika lica

Važnost ključa

- Sigurnost ovisi o kvaliteti ključa
  - Idealan ključ – slučajni broj velike duljine
- Ključevi za simetrične kriptosustave
  - (Pseudo)slučajni brojevi
  - Bitna kvaliteta generatora slučajnih brojeva
    - Predvidivost generatora = predvidivost ključa
- Ključevi za asimetrične sustave
  - Posebna svojstva
    - Npr. umnožak dva velika prosta broja (RSA)
  - Potrebna veća duljina ključa za istu razinu sigurnosti

Pohrana ključeva

- Tajni ključ (simetrični i asimetrični algoritmi)
  - Sigurnosni standardi zahtijevaju pohranu unutar uređaja
    - Pametne kartice (ključ, certifikat)
    - Kripto-uređaji (ključ, certifikat)
  - Ključ ne može (ne smije) napustiti uređaj
    - Pokušaj otvaranja uređaja rezultira uništenjem ključa

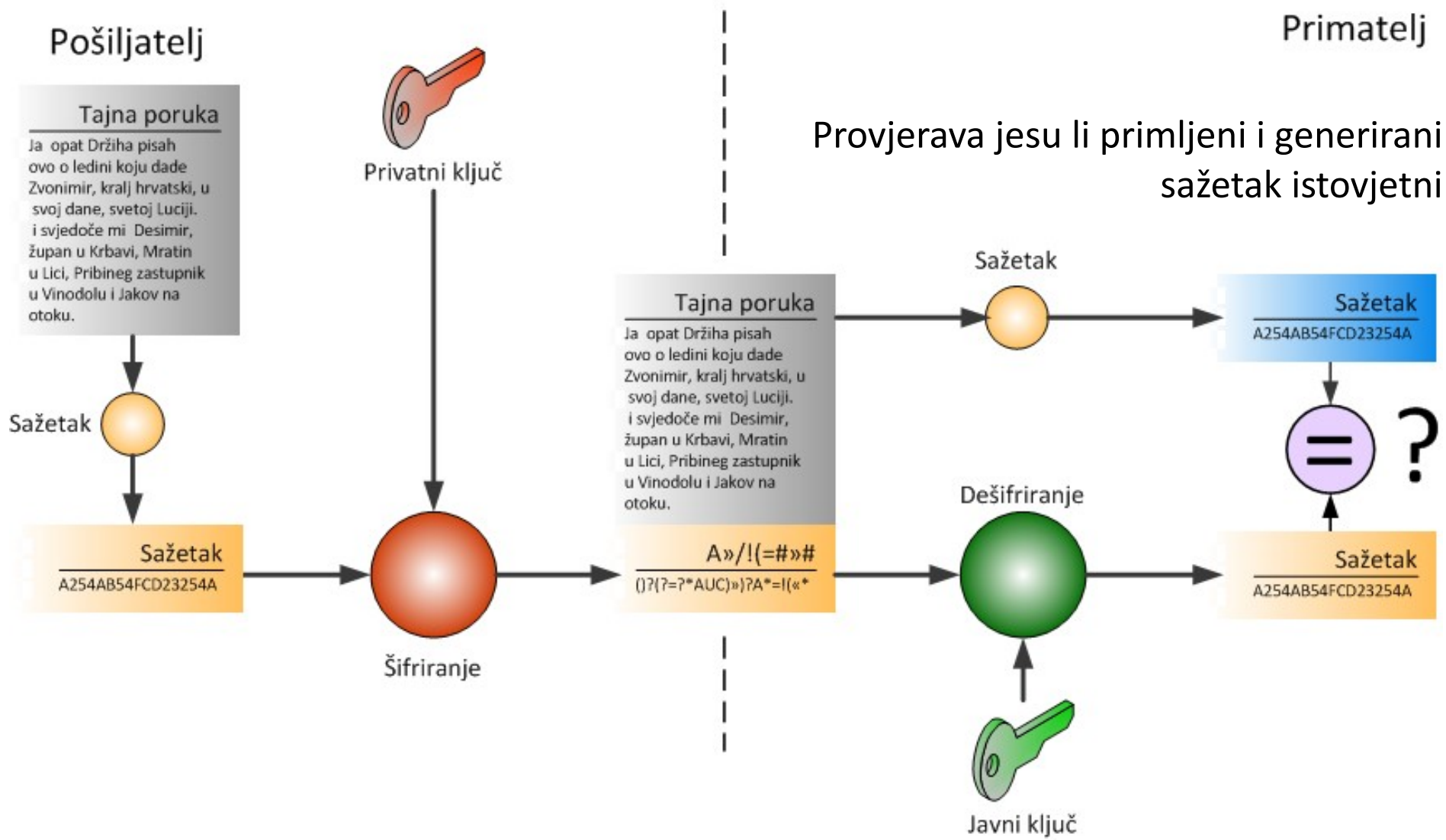
- Slično je i s biometrijskim ključevima :)

Digitalni potpis

- Generiramo sažetak poruke S
- Sažetak šifriramo ključem Pk (Privatni ključ)
  - Ključ (Pk) ostaje u našem posjedu
- Dodajemo šifrirani sažetak na poruku

- Sugovornik ključem Jk (Javni ključ) dešifrira sažetak S
  - Ovjera (autentičnost)
  - Neporicljivost
- Sugovornik generira sažetak primljene poruke S'
  - Ako je S = S', primljena poruka je istovjetna originalu
  - Očuvanost (integritet)

Digitalni potpis

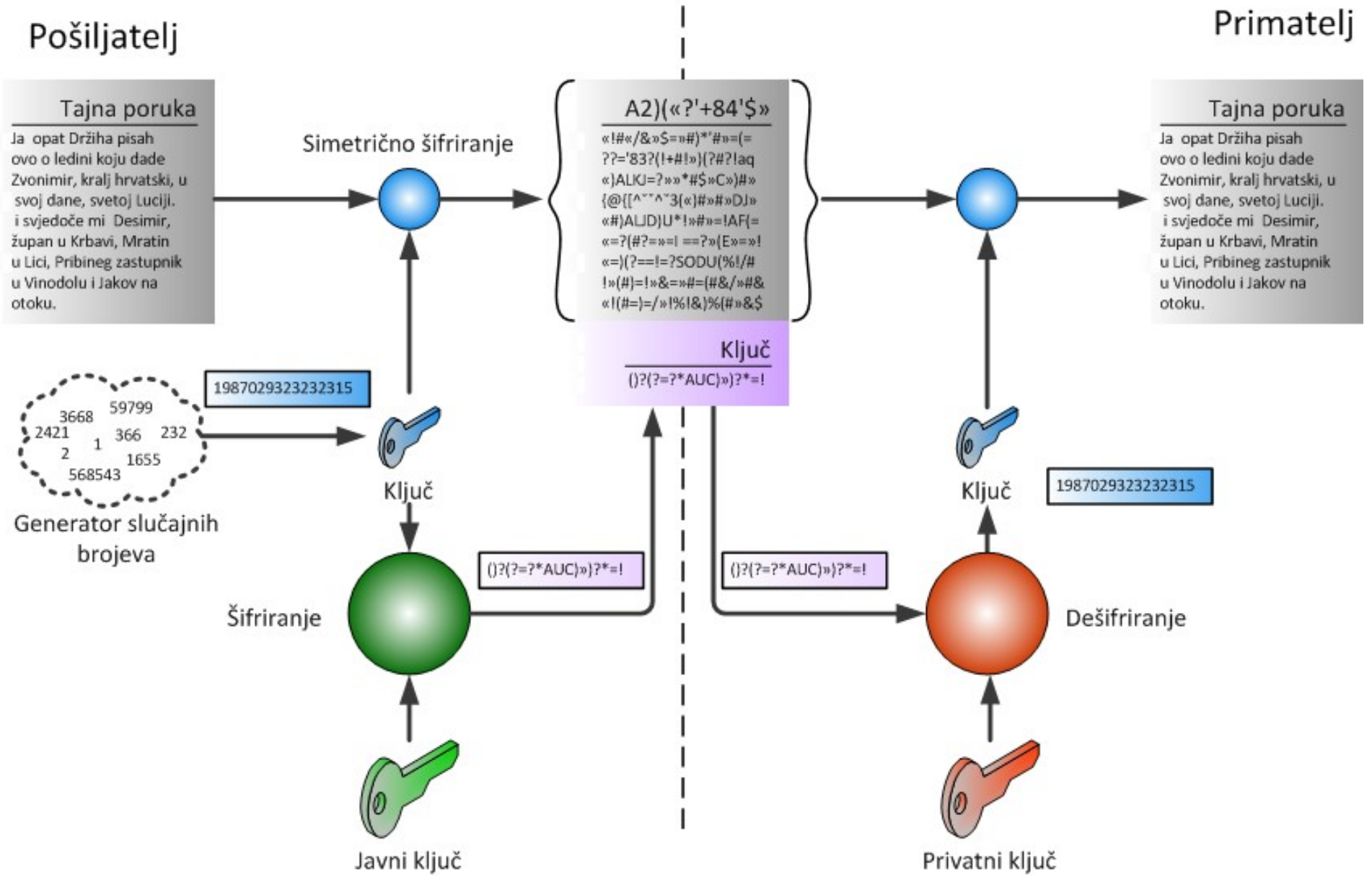


Provjerava jesu li primljeni i generirani sažetak istovjetni

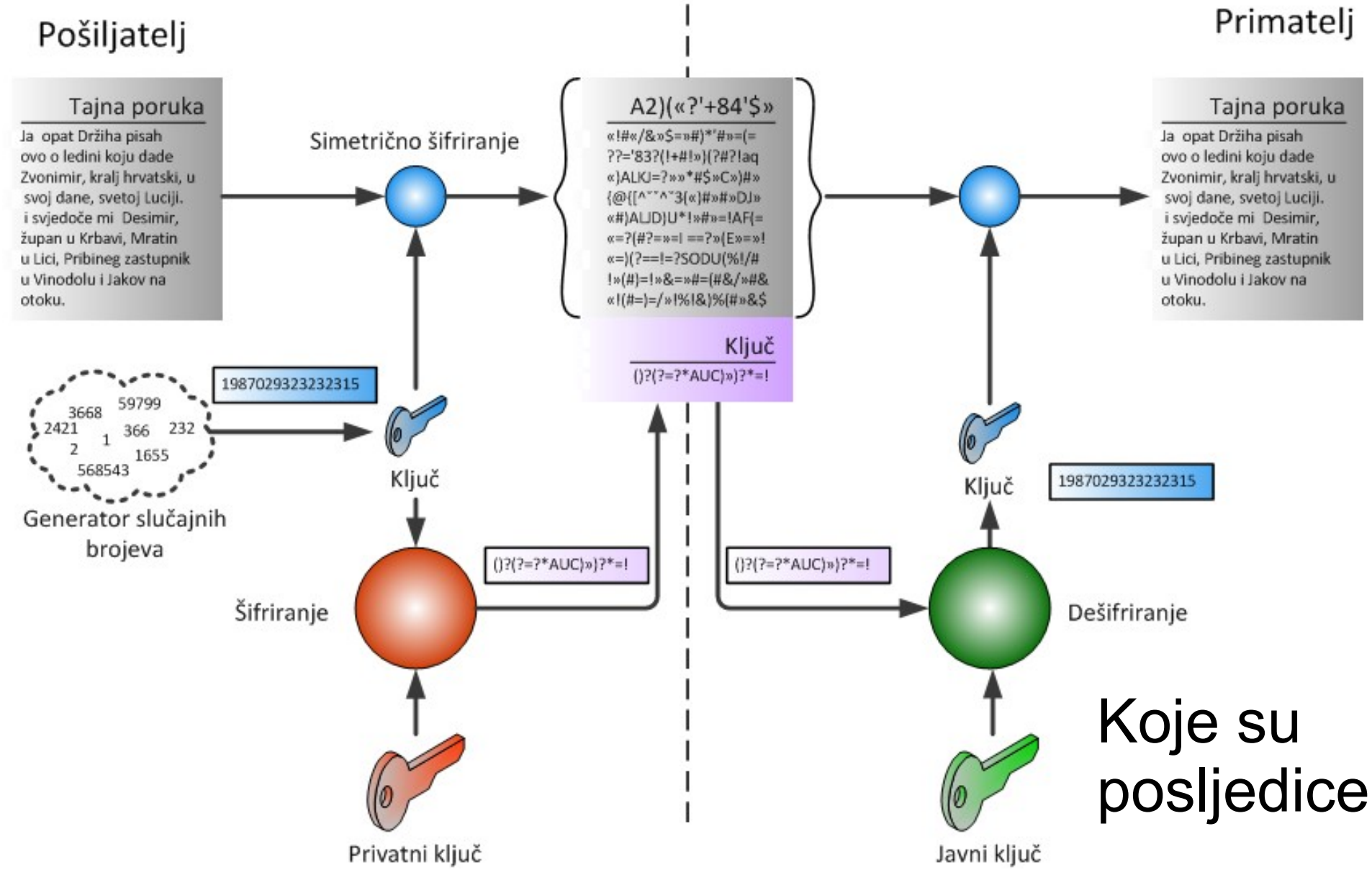
Digitalna omotnica

- Poruku šifriramo simetričnim algoritmom ključem K
  - Ključ K je generiran slučajno
  - Brzina
- Ključ K šifriramo asimetričnim algoritmom
  - Javnim ključem Jk (Pk je kod vlasnika ključa)
  - Nema problema distribucije ključeva
- Sugovornik ključem Pk dešifrira ključ K
- Ključem K dešifrira poruku
  - Tajnost

Digitalna omotnica



Pitanje: Je li ovo ispravno???



Koje su posljedice?

Zakonodavstvo

- Zakon o elektroničkom potpisu, 2002.
  - Osigurava zakonsku istovjetnost naprednog elektroničkog potpisa sa ručnim potpisom, odnosno potpisom i pečatom
  - Razrađuje zakonske podakte za definiranje uloge države u procesu
  - Definira tko može postati CA (Certificate Authority)
    - Vrlo strogi kriteriji, među strožima u svijetu

Zakonodavstvo

- Zakon o elektroničkom potpisu, 2002.
- Elektronički potpis
  - *Skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta*

- Našom terminologijom
  - Ovjera (identifikacija potpisnika)
  - Očuvanost (vjerodostojnost)

Zakonodavstvo

- Napredan elektronički potpis
  - *Elektronički potpis koji pouzdano jamči identitet potpisnika i koji*
    - je povezan isključivo s potpisnikom
    - nedvojbeno identificira potpisnika
    - nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika
    - sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka
  - Neporicljivost (povezan isključivo s potpisnikom)
  - Ovjera (identificira potpisnika)
  - Očuvanost (vjerodostojnost)

Kako to izvesti?

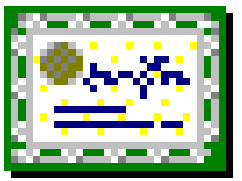
- Potpis dijeljenim (simetričnim) ključem
  - Potreba za središnjim autoritetom koji ovjerava naš potpis simetričnim ključem
  - Komunikacija sa središnjim autoritetom zaštićena je simetričnom kriptografijom
  - Autoritet označava vrijeme primitka poruka
    - Zaštita od napada ponavljanjem poruka
  - Problem:
    - Ključevi za komunikaciju sa središnjim autoritetom
      - Moraju biti tajni
      - Velika količina tajnih informacija koja se čuva u središnjem autoritetu i kod svakog sugovornika
    - Središnji autoritet može čitati sve poruke
    - Središnji autoritet ovjerava svaku poruku

Kako to izvesti?

- Potpis javnim (asimetričnim) ključem
  - Poruku potpisujemo našim tajnim ključem
  - Sugovornik provjerava potpis našim javnim ključem
    - Nužno da su operacije šifriranja (potpisa) i dešifriranja (provjere) međusobno inverzne
  - Nema potrebe za središnjim autoritetom koji ovjerava svaku poruku
  - Problem:
    - Kako vjerovati da je javni ključ sugovornika baš njegov?
    - Središnji autoritet jamči ispravnost ključa
    - Potvrda o valjanosti ključa = certifikat

Certifikati

- Zakon: *potvrda u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe*
- Certifikat
  - Potvrda o vezi između identiteta i javnog ključa
  - Javan
    - Norma za certifikate ITU X.509 v3
  - Sadrži
    - Identifikaciju izdavatelja i subjekta
    - Oznaku algoritma potpisa i javni ključ
    - Razdoblje važenja
    - Potpis



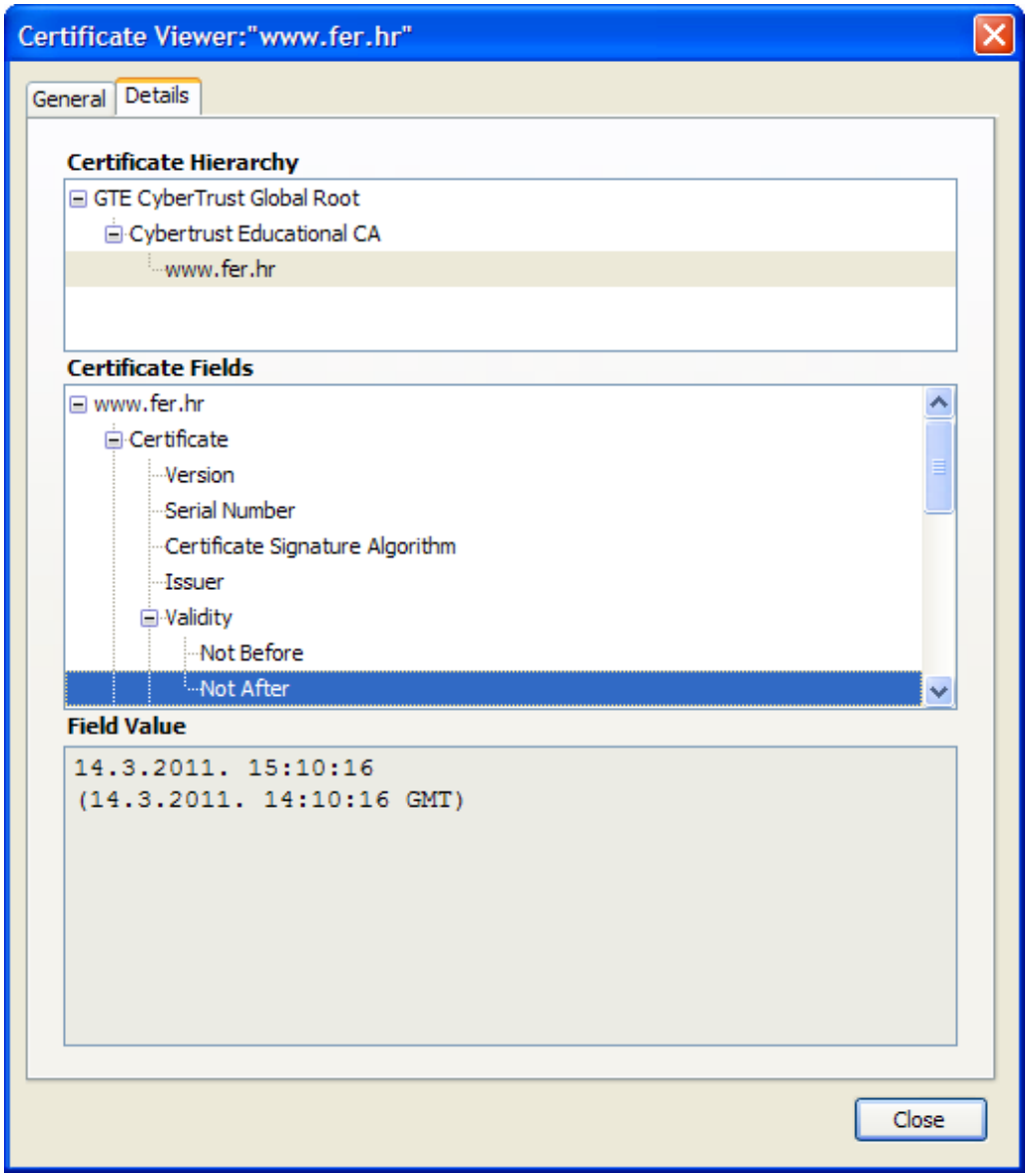
Izdavatelj certifikata

- Davatelj usluga certificiranja
  - pravna ili fizička osobu koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima
- CA – *Certificate Authority*
  - Izdaje certifikate
  - Moguće ostvarenje hijerarhije CA
    - Lanac povjerenja, staza certificiranja
      - Stablo certifikata od korijenskog CA do našeg certifikata
    - Ne postoji jedinstvena hijerarhija
      - Internet – niz CA
        - GTE CyberTrust Global Root
          - CyberTrust Educational CA
            - ahyco.fer.hr

C=HR/S=Zagreb/L=Zagreb/O=FER/OU=ZPR/CN=ahyco.fer.hr

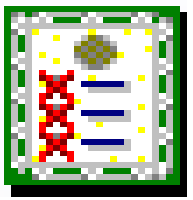
Primjer

- Certifikat www.fer.hr
  - CN = www.fer.hr
  - OU = www.fer.hr
  - O = Fakultet elektrotehnike i racunarstva
  - L = Zagreb
  - C = HR



Povlačenje certifikata

- Certifikat potvrđuje vezu između javnog ključa i osobe
  - Javni ključ nećemo izgubiti, ne može biti ukraden
  - Što ako izgubimo privatni ključ ili je ukraden?
- Certifikat sadrži razdoblje valjanosti
  - Što kad to razdoblje istekne?
- CA održava mehanizme provjere valjanosti certifikata
  - Provjera potpisa
  - Održavanje popisa povučenih certifikata (CRL)



Zakonodavstvo

- Potpisnik
  - *koji izgubi ili mu je otuđeno sredstvo za izradu elektroničkog potpisa te u slučajevima kada mu je onemogućen pristup podacima za izradu elektroničkog potpisa, dužan je o tome odmah obavijestiti davatelja usluga certificiranja*

- Davatelj usluga certificiranja
  - *koji je zaprimio obavijest ... provodi uvid u postupak opoziva izdatog certifikata i dalje postupa po utvrđenim pravilima opozivanja izdatih certifikata*

Popis povučenih certifikata

- CRL – Certificate Revocation List
- Popis povučenih certifikata
  - Ne uključuje certifikate kojima je automatski istekla valjanost
- Provjera valjanosti certifikata
  - Provjera digitalnih potpisa certifikata
  - Provjera razdoblja valjanosti certifikata
  - Provjera popisa povučenih certifikata
    - Adresa CRL upisana u certifikat
    - Certifikat može biti označen kao *non-critical*
      - Ako pristup popisu (CRL) nije moguć, smatramo da je sigurnost dovoljna
        - Npr. nedostupna mrežna veza, ...

Značaj CA

- CA
  - Ovjerava certifikate
  - Održava popise povučenih certifikata

- Kompromitirani CA unosi veliku štetu
  - Cijela hijerarhija od tog CA na niže postaje nevažeća
  - Sigurna komunikacija s članovima hijerarhije nije moguća
    - Uskraćivanje usluge - DOS

Norme

- Public Key Cryptography Standards (PKCS)
  - RSA Security definirao niz normi
    - PKCS #1 – *RSA Cryptography Standard*
    - PKCS #3 – *Diffie-Hellman Key Agreement Standard*
    - PKCS #7 – *Cryptographic Message Syntax Standard*
    - PKCS #8 – *Private-Key Information Syntax Standard*
    - PKCS #10 – *Certification Request Standard*
    - PKCS #11 – *Cryptographic Token Interface (programsko sučelje)*
    - PKCS #12 – *Personal Information Exchange Syntax Standard*
- X.509
  - ITU-T - norme za ostvarenje PKI
  - Oblik certifikata

Norme

- FIPS – Federal Information Processing Standards
  - Između ostalog – DES i AES
- W3C
  - Struktura XML-a s digitalnim potpisom
  - XML DSig, XML AdES
- Problem
  - XML istog značenja može biti zapisan na više načina
    - Razmaci u oznakama elemenata
    - Redoslijed atributa, elemenata, ...

```
<SignatureValue>C7di9  ....  ligw+o=</SignatureValue>
<X509SubjectName>Ivo Ivić #BrojCertifikata</X509SubjectName>
<X509Certificate>
    MIIEazCCA  .... iG9w0BA
</X509Certificate>
```

Primjeri

- Zaštita lozinki
- Jedinstvena autentikacija na različitim sjedištima
- Kreditne kartice
- Elektronički potpis

Primjer: Zaštita lozinki

- Čuvanje lozinki u operacijskom sustavu ili aplikacijama?
  - Pohranom lozinki u izvornom obliku odgovornost za sigurnost lozinke prelazi na aplikaciju
  - Uspjeli napad na aplikaciju – lozinke svih korisnika

- Rješenje
  - Pohrana šifriranog oblika lozinke
  - Je li nam potrebna mogućnost povrata u izvorni oblik?
    - Ne, samo želimo znati je li unesena lozinka istovjetna pohranjenoj
    - Treba nam samo sažetak lozinke

Lozinke

- Realizacija
  - Sažeci generirani varijacijom DES-a (Unix, Windows)
  - MD5 sažeci lozinki (Linux, Unix, PHP)
  - SHA sažeci lozinki (Unix, Linux, PHP)
  - Sažeci generirani varijacijom Blowfisha

- Primjer (PHP)

```
<?php
      $lozinka = crypt('tajna');

      if (crypt($ulaz, $lozinka) == $lozinka) {
         echo "Dobrodošli!";
      }
?>
```

Primjer: Generiranje SHA-1

- Java i .Net sadrže implementacije algoritama
- Primjer (Java):

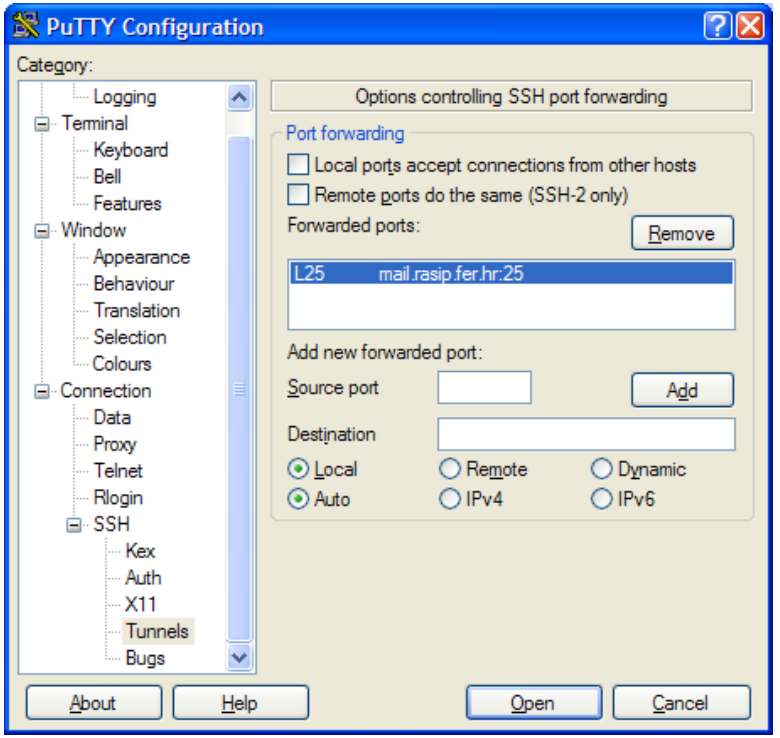
```
String plaintext = new String("Napad u zoru!");

java.security.MessageDigest md = null;

md = MessageDigest.getInstance("SHA1");
md.update(plaintext.getBytes("UTF-8"));

byte sha1[] = md.digest();
```

- Izostavljeno je rukovanje iznimkama

Primjer: Zaštita komunikacije

- Secure Socket Layer (SSL)
- HTTPS – SSL umjesto TCP-a kao transportni protokol

- Možemo iskoristiti i za vlastite potrebe
  - Klijent SSH – npr. PuTTY
    - Stvaranje tunela kroz SSL
    - Sigurni kanal povezuje port na lokalnom i port na udaljenom računalu



Primjer: Jedinstvena autentikacija

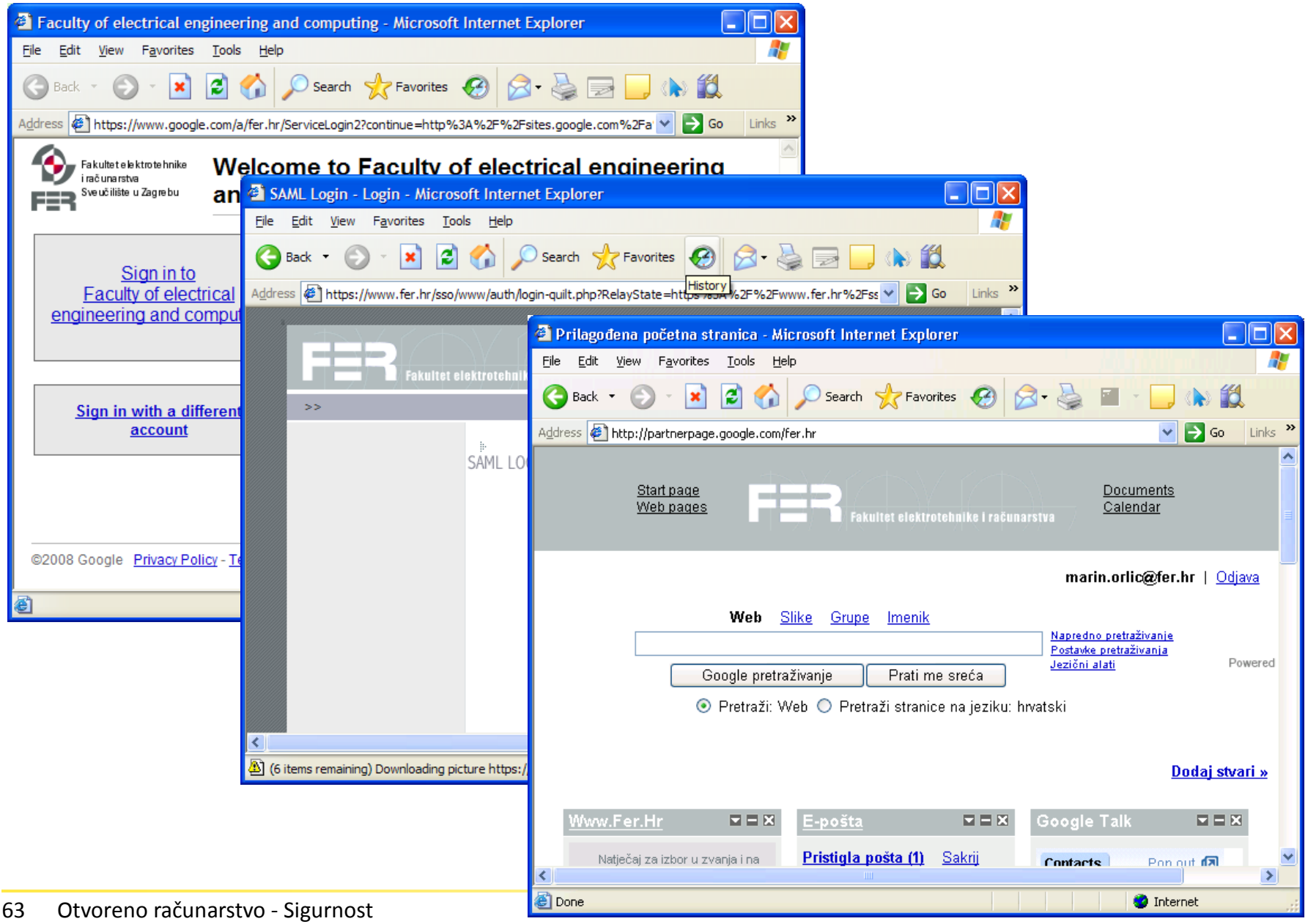
- Jedinstvena prijava (*Single Sign-On*)
  - Olakšava rad korisniku
    - Pamti samo jednu lozinku – može biti kvalitetnija
  - Uspostavlja mrežu povjerenja između pružatelja usluga

- Sugovornici
  - IdP – *Identity Provider* – provjerava identitet korisnika
  - SP – *Service Provider* – pruža uslugu korisniku
  - Preglednik (podržava *kolačiće*)
    - Sučelje prema korisniku
    - Komunicira sa poslužiteljima

Jedinstvena autentikacija

- Preglednik pristupa SP-u
  - Google Apps
- SP provjerava koji je IdP za tog korisnika
  - FER CMS
- SP preusmjerava (HTTP Location) prijavu na IdP
  - Kao parametar šalje vlastiti URL
- IdP provjerava identitet korisnika
  - Prijavljuje korisnika ako nije prijavljen
- IdP preusmjerava (HTTP Location) korisnika na SP
  - Adresu za preusmjeravanje je dobio od SP

Jedinstvena autentikacija



Jedinstvena autentikacija

- Iza svega leži SAML
  - Security Assertion Markup Language (SAML)
  - Zasnovan na XML-u
  - Protokol provjere autentikacije između IdP i SP
  - Struktura poruka
    - Digitalno potpisani XML
- Kritika
  - Presložen za jednostavnije primjene
  - Identitet pod kontrolom *Identity Provider*-a, ne korisnika

Primjer: Zaštita e-pošte

- OpenPGP (RFC 4880)
  - PGP, GnuPG (GPG), ...
- Digitalni potpis, digitalna omotnica
- Problem
  - Nema središnjeg autoriteta, korisnik ima kontrolu
  - Kako vjerovati da javni ključ zaista pripada osobi?

```
-----BEGIN PGP SIGNED MESSAGE-----

Pozdrav posjetiteljima zainteresiranim
za kriptografsku zastitu podataka :-)

-----BEGIN PGP SIGNATURE-----
Version: 2.6.3i

iQB1AwUBMn81FeLAsiJAX7ttAQHYsQMAnT216JJG569K49w7mZa0S40aMtUzRSwm
dh9ijMpJR0dOEneUMF6G722oCcJli81V9pLIo12Lon5cElZRP5emx+n9DckRAU0w
q++v1cGYsIJUa7/LUEtHLMyvXEp2JkRL
=dtfP
-----END PGP SIGNATURE-----
```

Primjer: Plaćanje karticama

- EMV – Europay, MasterCard, Visa
  - Fizička i električka izvedba čipa na kreditnim karticama
  - Podaci i sučelje za rad s čipom
  - Koriste se algoritmi sažetaka, simetrični i asimetrični
    - SHA-1, DES, RSA
- SET – Secure Electronic Transaction
  - Sigurno plaćanje kreditnim karticama na webu
  - Unos broja kreditne kartice
- 3-D Secure
  - Evolucija SET-a
  - Uvodi treću domenu sigurnosti (3-D)

Plaćanje karticama

- SET – sudionici
  - Acquirer – stjecatelj – banka koja naplaćuje trošak kartice za račun trgovca
  - Merchant – trgovac – fizička ili web-trgovina
  - Banka stjecatelj provjerava karticu postojećim kanalom
- 3-D Secure – sigurnosne domene
  - Acquirer – stjecatelj – banka koja naplaćuje trošak kartice za račun trgovca
  - Interoperability – podrška kartične kuće
    - Imenički poslužitelj koji provjerava je li kartica važeća i koja banka ju je izdala
    - Prosljeđuje zahtjev za kupnju izdavatelju
  - Issuer – izdavatelj – banka koja je izdala karticu

Plaćanje karticama

- Dodatna sigurnost
  - Kartična kuća omogućava korisniku kartice da registrira karticu i pridijeli joj lozinku za plaćanje putem weba
  - Stroži zahtjevi na implementaciju protokola
    - Prebacivanje dijela odgovornosti na banku izdavatelja
- Kritika
  - Prilikom postupka plaćanja karticom, korisniku se prikazuju prozori s različitih web sjedišta
    - Može zbuniti korisnika
      - Sumnja na lažno predstavljanje poslužitelja – *phishing*
- *Primjeri implementacije*
  - *Ouroboros Payment Gateway, T-Com PayWay*

Primjer: Potpis dokumenata

- Kratki pregled stanja u Hrvatskoj
- Zakon o elektroničkom potpisu
  - Istovjetnost naprednog elektroničkog potpisa i ručnog potpisa
- Zašto?
  - Ubrzanje birokratskih procedura
    - Smanjivanje papirologije
    - Revizija administrativnih procesa
  - Efikasnije poslovanje
    - Smanjenje troškova papira, transporta, vremena
    - Obavljen isti posao u kraće vrijeme

Trenutno stanje (sredina 2008.)

- Jedini certificirani CA – Financijska Agencija (FINA)
  - Registar Digitalnih Certifikata (RDC)
- Postoje nekvalificirani CA
  - Za potrebe poslovanja preko interneta
  - Banke svaka za sebe osnovale interni CA
  - Nisu ovjerovljeni od države
    - Nemaju ispunjene sve zakonom propisane uvjete
- Nije uspostavljena hijerarhija CA
  - Jedini *pravi* CA – FINA-in CA
- Većina pravnih i fizičkih osoba nije educirana
  - Ne zna se za postojanje ni za vjerodostojnost digitalnog potpisa

Trenutno stanje (sredina 2008.)

- Počeo razvoj usluga zasnovanih na digitalnom potpisu
  - Uglavnom u segmentu B2G (Business to Government)
- FINA-in CA prihvaćen kao jedini autoritet za izdavanje i provjeru digitalnog potpisa
  - Uglavnom među poslovnim subjektima gdje FINA ionako ima autoritet
  - Izdaje autentikacijske i potpisne certifikate
    - Potpisni osigurava neporicljivost
  - Certifikati namijenjeni osobama, poslovnim subjektima i tijelima državne uprave

Ponuđene usluge

- FINA (Financijska Agencija)
  - Predaja periodičkih statističkih izvještaja
  - Izdavanje potvrda o bonitetu poslovnih subjekata
  - NKS (Nacionalni Klirinški Sustav)
    - Sve transakcije između banaka digitalno potpisane
  - Elektroničko plaćanje
  - eRegos (registar osiguranika drugog stupa mirovinskog osiguranja)

- Banke
  - Internet bankarstvo za poslovne subjekte

Usluga FINA-e

Ponuđene usluge – državna uprava

- PU MFIN (Porezna Uprava Ministarstva financija)

  ePorezna:

  - Uvid u PKK (poreznu knjigovodstvenu karticu)
  - Predaja obrazaca za PDV, prijave poreza na dobit, izvještaja o isplaćenim plaćama
- HZZO (Hrvatski Zavod za Zdravstveno Osiguranje)

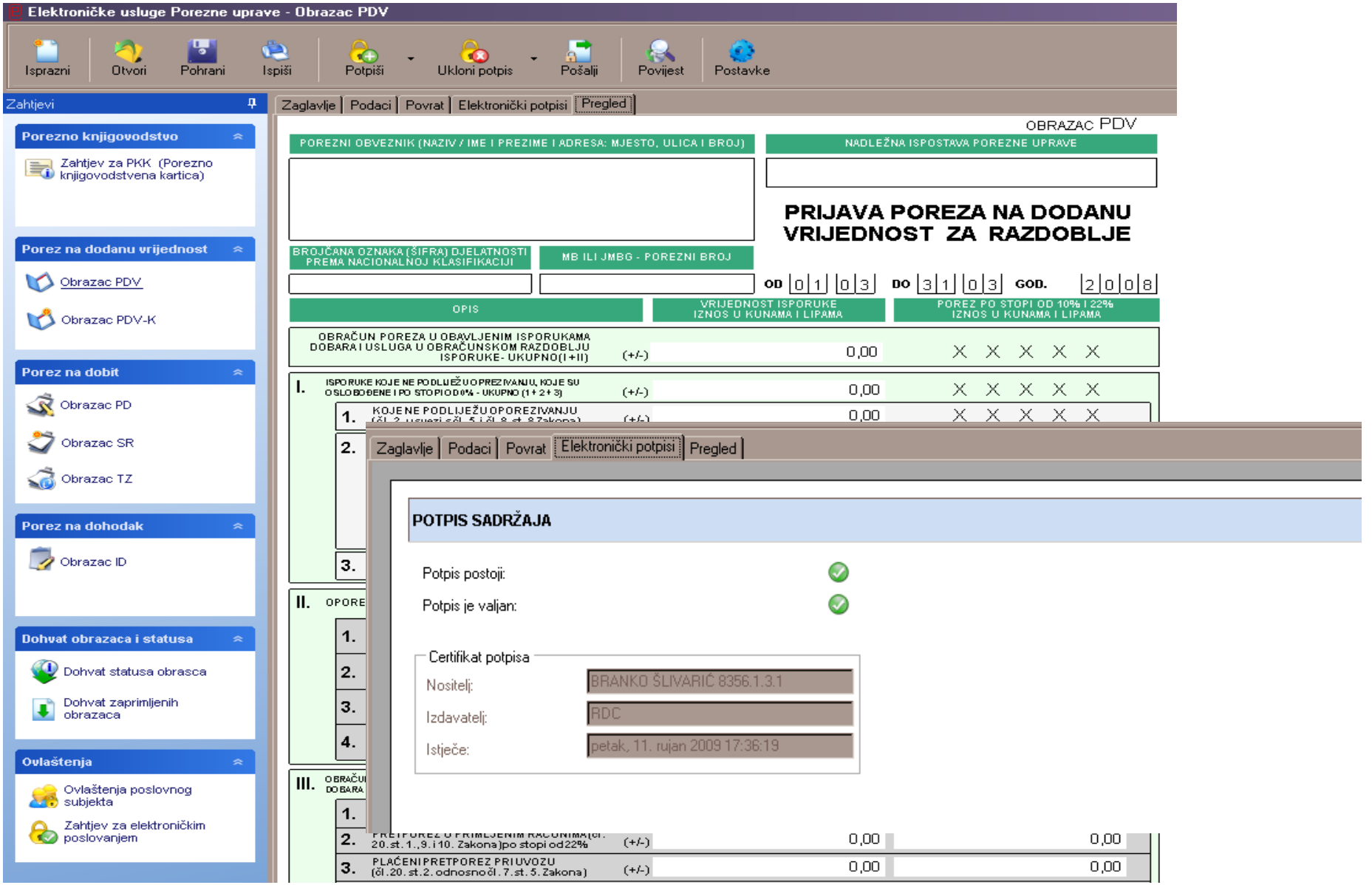
  eZdravstveno:

  - Prijava i odjava radnika na zdravstveno osiguranje
  - Promjena podataka o zdravstvenom osiguranju radnika
- HZMO (Hrvatski Zavod za Mirovinsko Osiguranje)

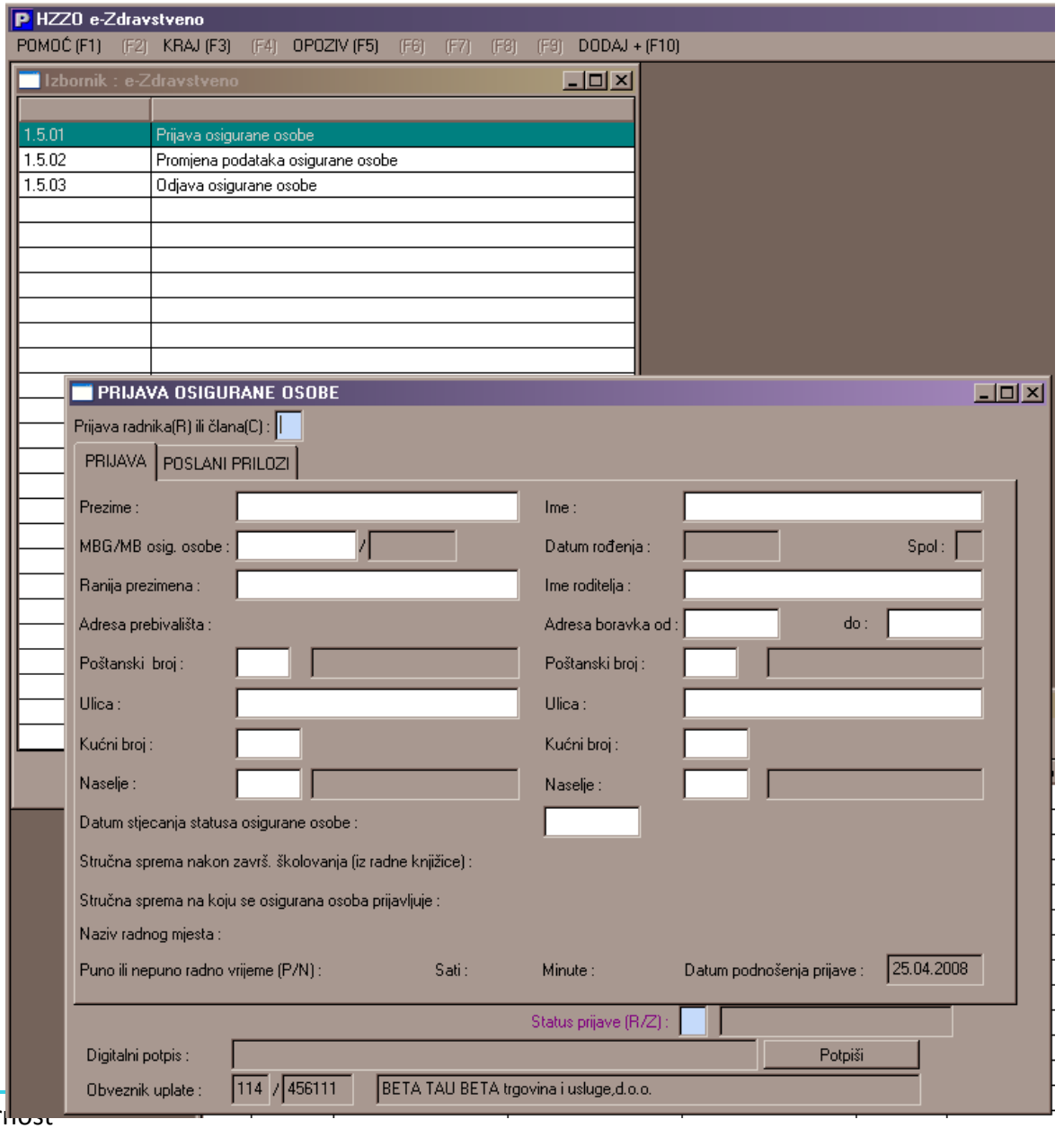
  eMirovinsko:

  - Prijava i odjava radnika na mirovinsko osiguranje
  - Promjena podataka o mirovinskom osiguranju radnika

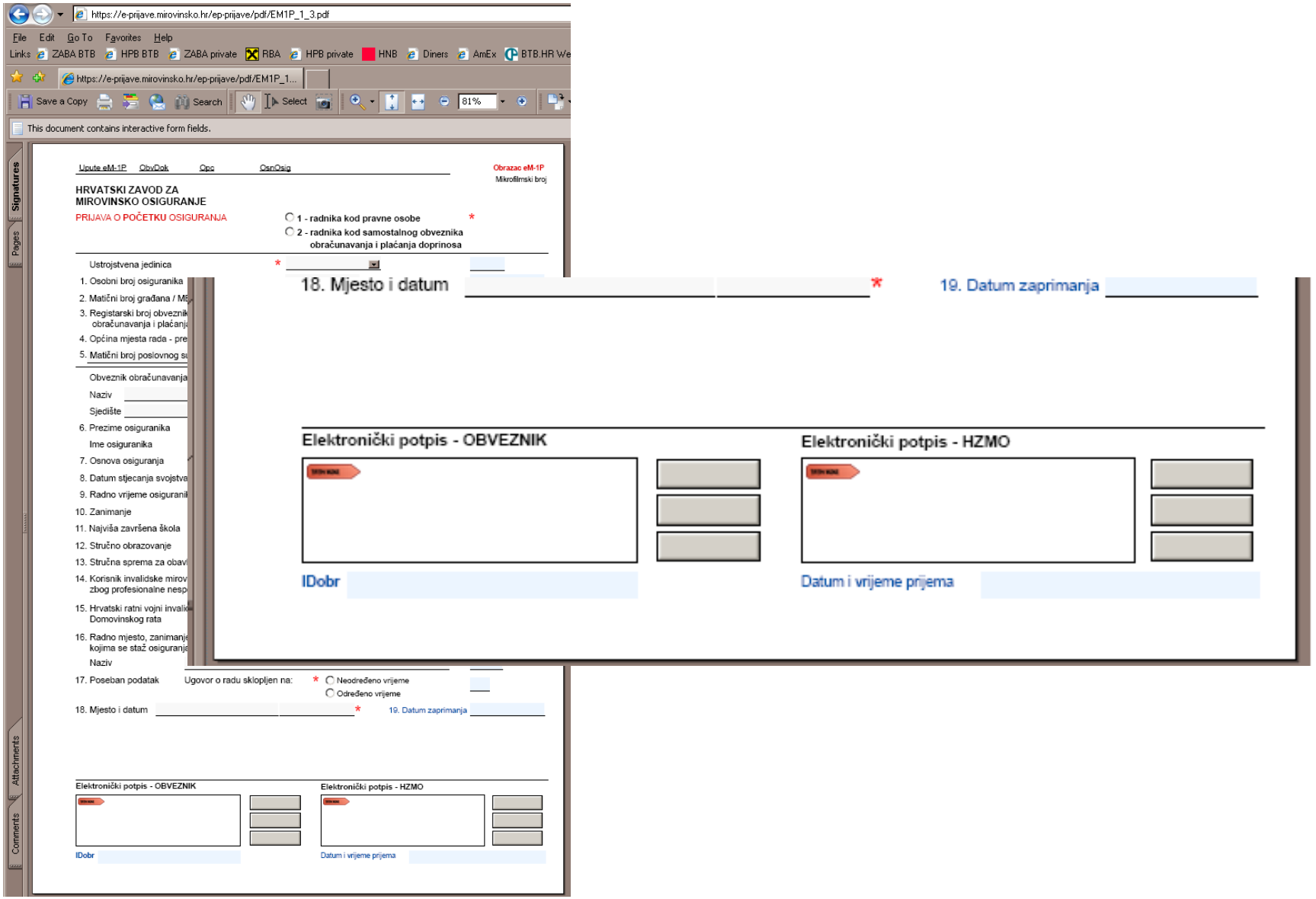
ePorezna


Elektroničke usluge Porezne uprave - Obrazac PDV
Isprazni
Otvori
Pohrani
Ispiši
Potpiši
Ukloni potpis
Pošalji
Povijest
Postavke
Zahtjevi
Porezno knjigovodstvo
Zahtjev za PKK (Porezno knjigovodstvena kartica)
Porez na dodanu vrijednost
Obrazac PDV
Obrazac PDV-K
Porez na dobit
Obrazac PD
Obrazac SR
Obrazac TZ
Porez na dohodak
Obrazac ID
Dohvat obrazaca i statusa
Dohvat statusa obrasca
Dohvat zaprimljenih obrazaca
Ovlaštenja
Ovlaštenja poslovnog subjekta
Zahtjev za elektroničkim poslovanjem
Zaglavlje
Podaci
Povrat
Elektronički potpisi
Pregled
OBRAZAC PDV
POREZNI OBVEZNIK (NAZIV / IME I PREZIME I ADRESA: MJESTO, ULICA I BROJ)
NADLEŽNA ISPOSTAVA POREZNE UPRAVE
PRIJAVA POREZA NA DODANU VRIJEDNOST ZA RAZDOBLJE
BROJČANA OZNAKA (ŠIFRA) DJELATNOSTI PREMA NACIONALNOJ KLASIFIKACIJI
MB ILI JMBG - POREZNI BROJ
OD 0 1 0 3 DO 3 1 0 3 GOD. 2 0 0 8
OPIS
VRIJEDNOST ISPORUKE IZNOS U KUNAMA I LIPAMA
POREZ PO STOPI OD 10% I 22% IZNOS U KUNAMA I LIPAMA
OBRAČUN POREZA U OBAVLJENIM ISPORUKAMA DOBARA I USLUGA U OBRAČUNSKOM RAZDOBLJU ISPORUKE- UKUPNO(I+II)
0,00
I.
1.
2.
3.
II.
III.
POTPIS SADRŽAJA
Potpis postoji:
Potpis je valjan:
Certifikat potpisa
Nositelj:
BRANKO ŠLIVARIĆ 8356.1.3.1
Izdavatelj:
RDC
Istječe:
petak, 11. rujan 2009 17:36:19
PLAĆENI PRETPOREZ PRI UVOZU (čl.20.st.2.odnosno čl.7.st.5.Zakona)

eZdravstveno



eMirovinsko



Cijena?

- Fizičke osobe
  - Registracija 20,00 kn jednokratno
  - Godišnja pretplata za pametnu karticu s jednim certifikatom – osobni certifikat 139,00 kn godišnje
- Što se dobije?
  - Digitalno potpisivanje dokumenata (ugovora, računa, ponuda, dopisa, itd.)
  - Razmjena podataka između pravnih subjekata sa osiguranjem vjerodostojnosti i neporicljivosti podataka

Mogućnosti

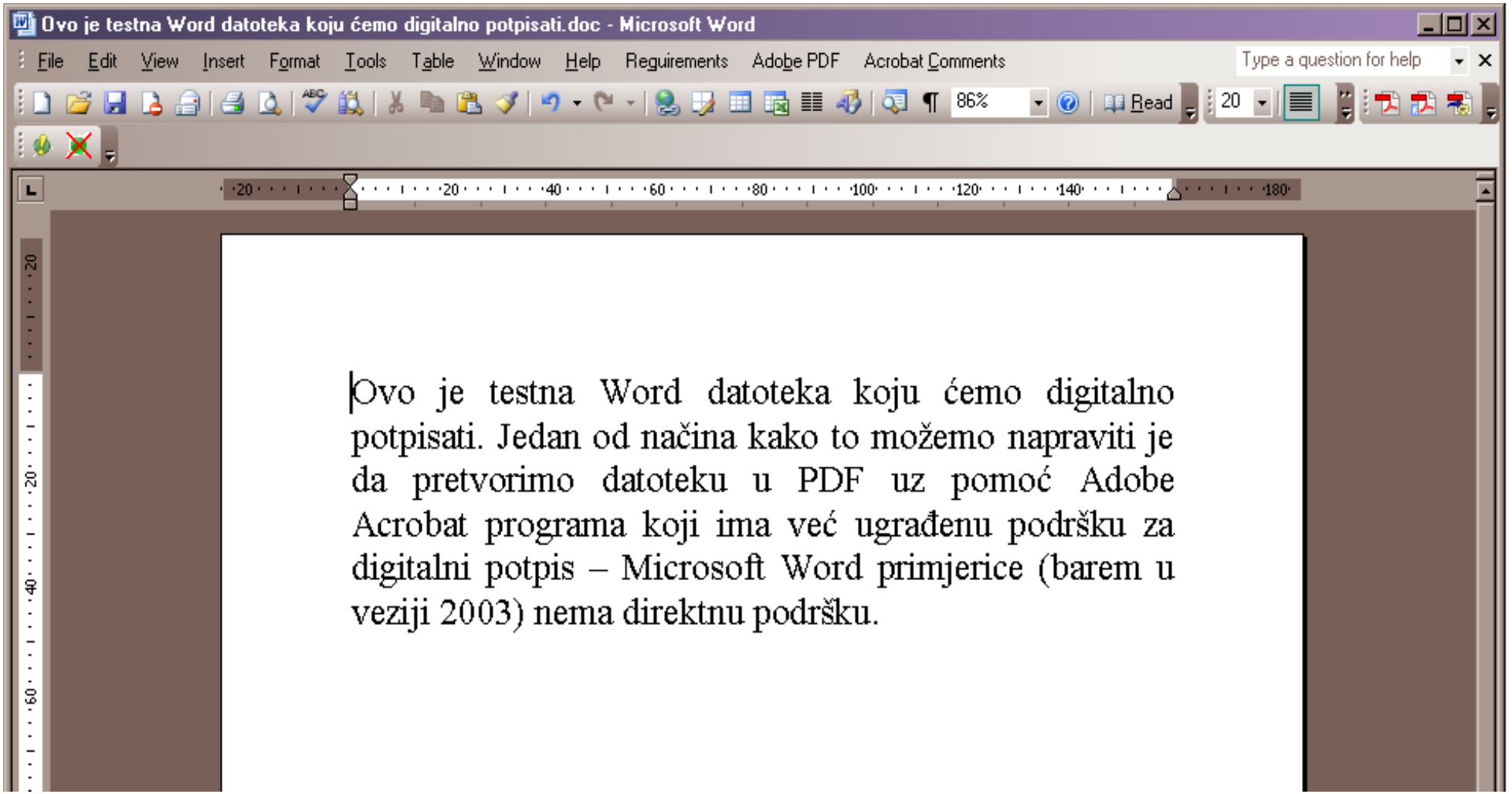
- Digitalno potpisivanje bilo kakvih dokumenata (ugovora, računa, ponuda, dopisa itd.)
- Razmjena digitalnih podataka između pravnih subjekata (firmi) sa osiguranjem vjerodostojnosti i neporicljivosti podataka

- Budućnost?
  - Svaka fizička osoba ima svoj digitalni potpis pohranjen u osobnoj iskaznici (kao što na iskaznici ima klasični ručni potpis)

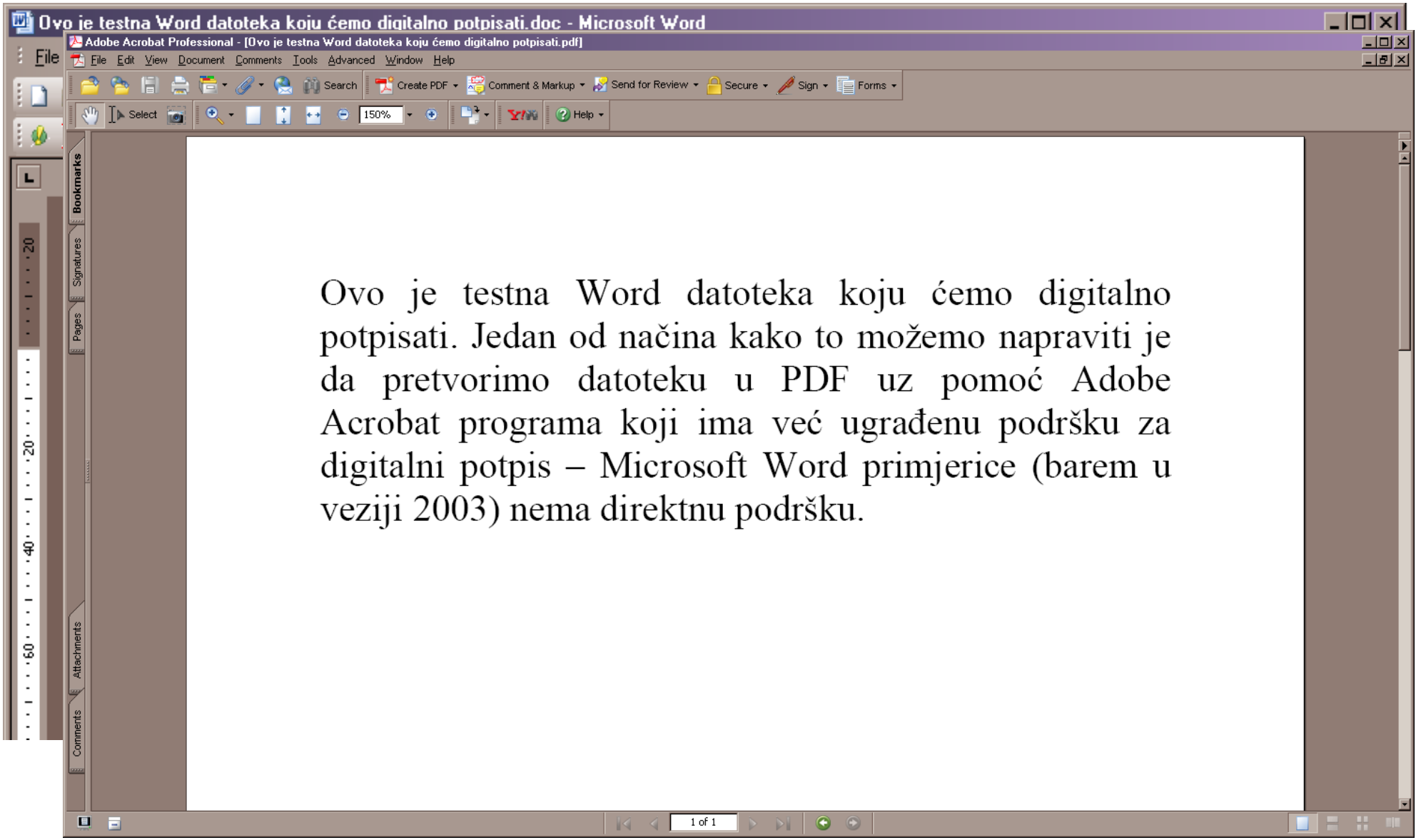
Problemi

- Fizičke i pravne osobe su nepovjerljive
  - Firma XY šalje digitalno potpisani račun za usluge – računovodstvo traži papirnatu veziju
- Tijela državne uprave nedovoljno organizirana za prihvat, obradu, arhiviranje digitalnih dokumenata čak kad i priznaju digitalni potpis
- Država treba financirati izgradnju digitalne infrastrukture
  - Definirati pravila koja bi zakonski poticala uporabu digitalnih dokumenata
  - Organizirati državne sustave za upravljanje i razmjenu digitalnih dokumenata
    - Document Management System (DMS)

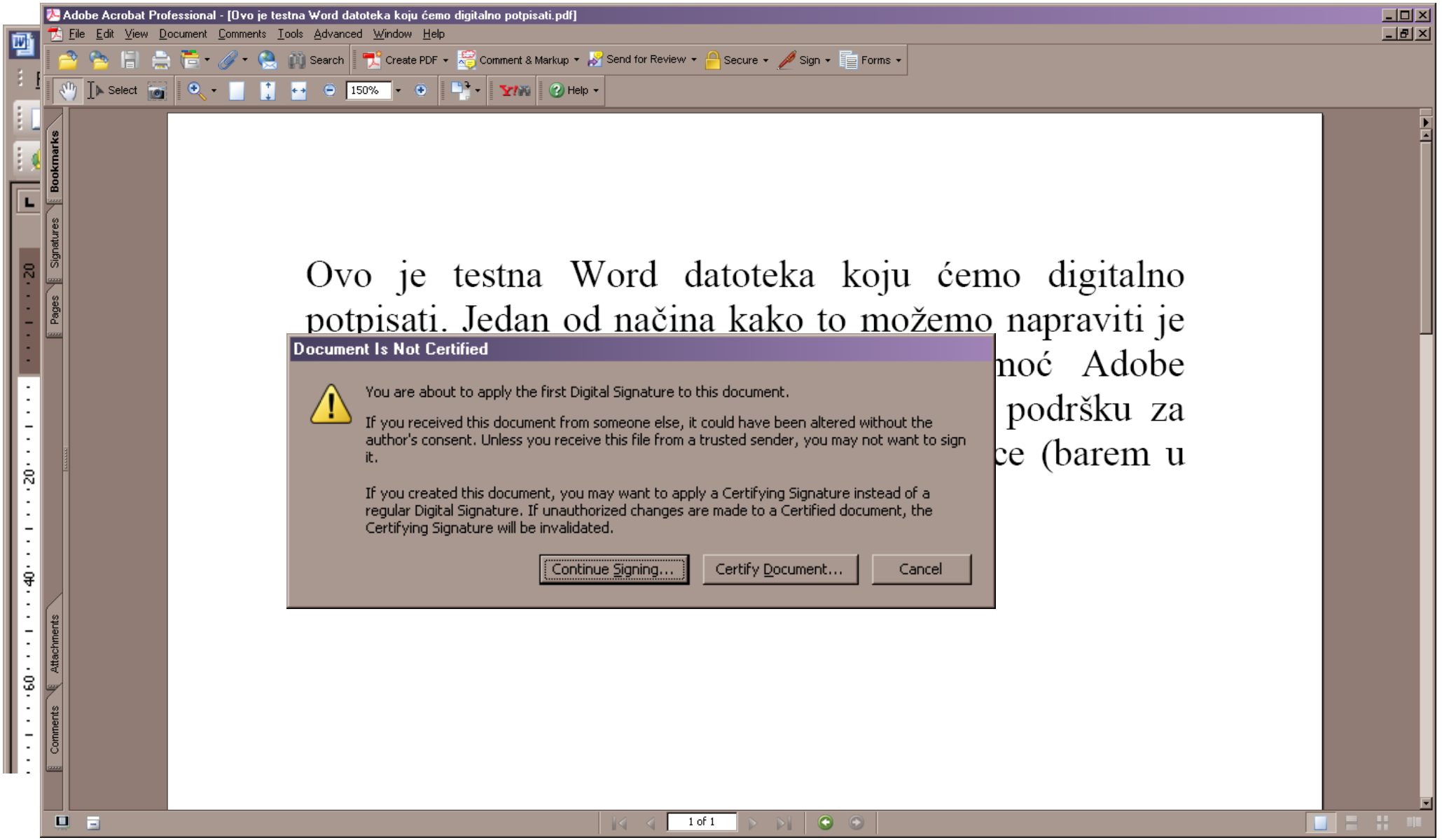
Kako (is)koristiti?



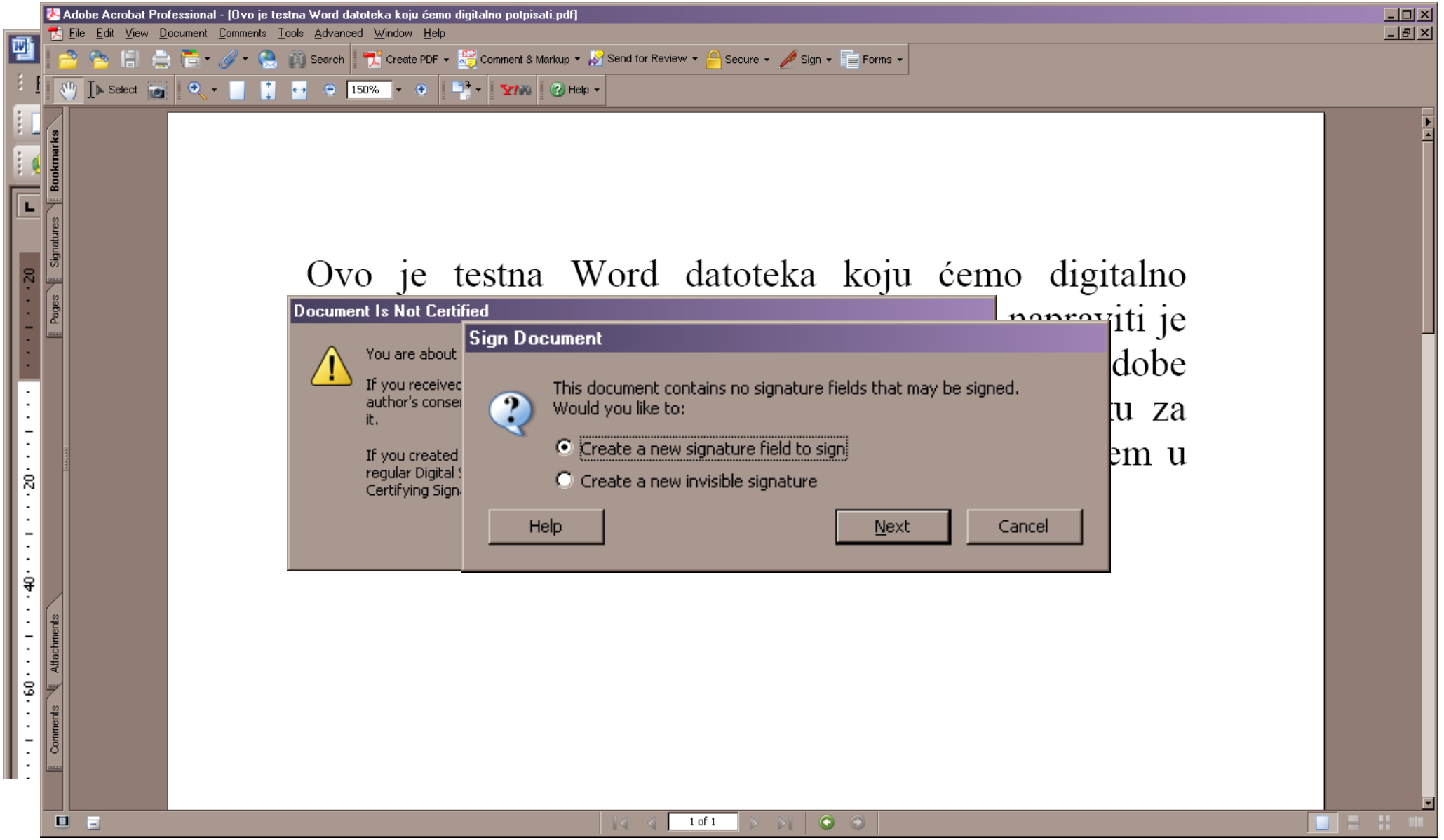
Kako (is)koristiti?



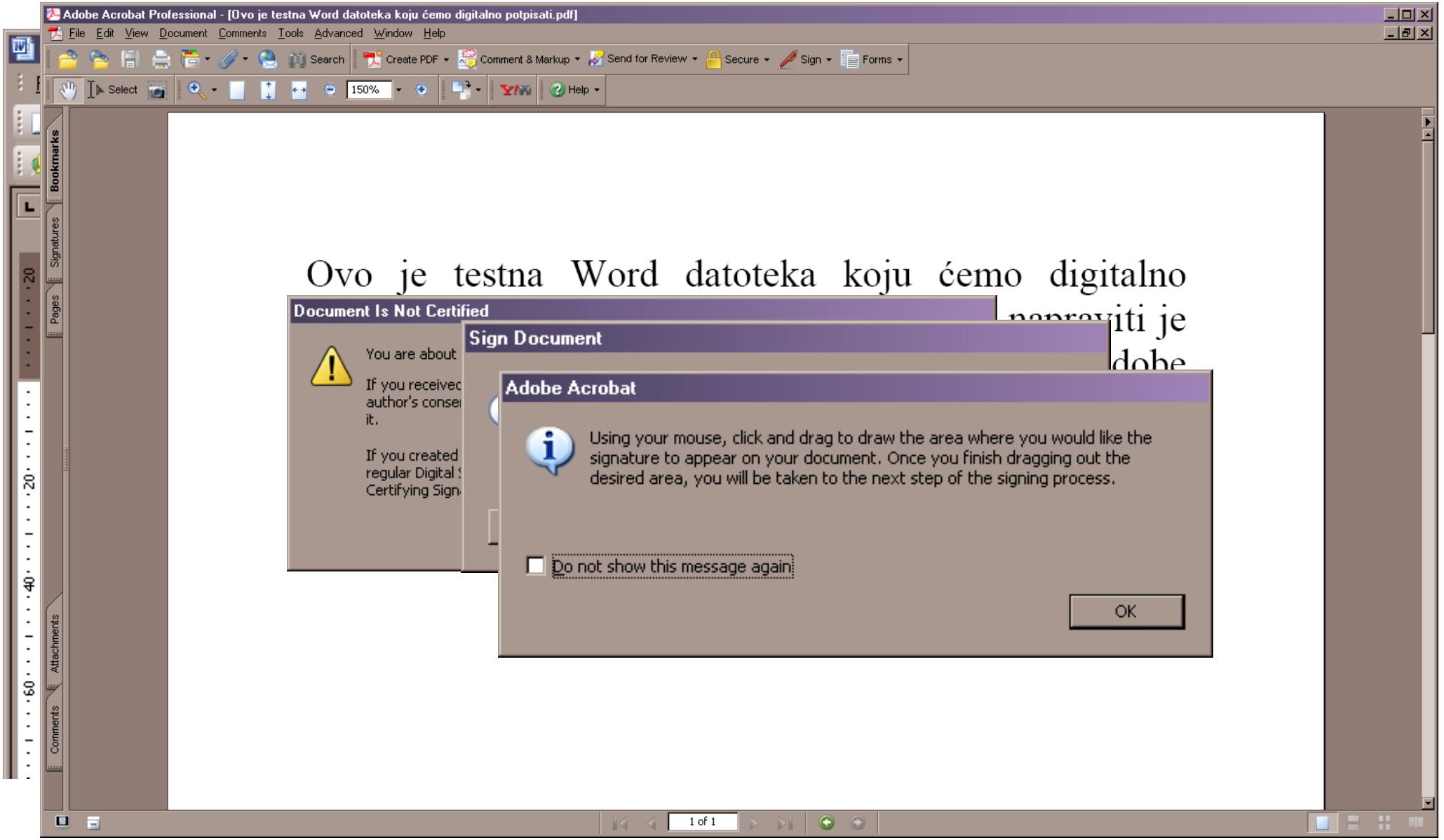
Kako (is)koristiti?



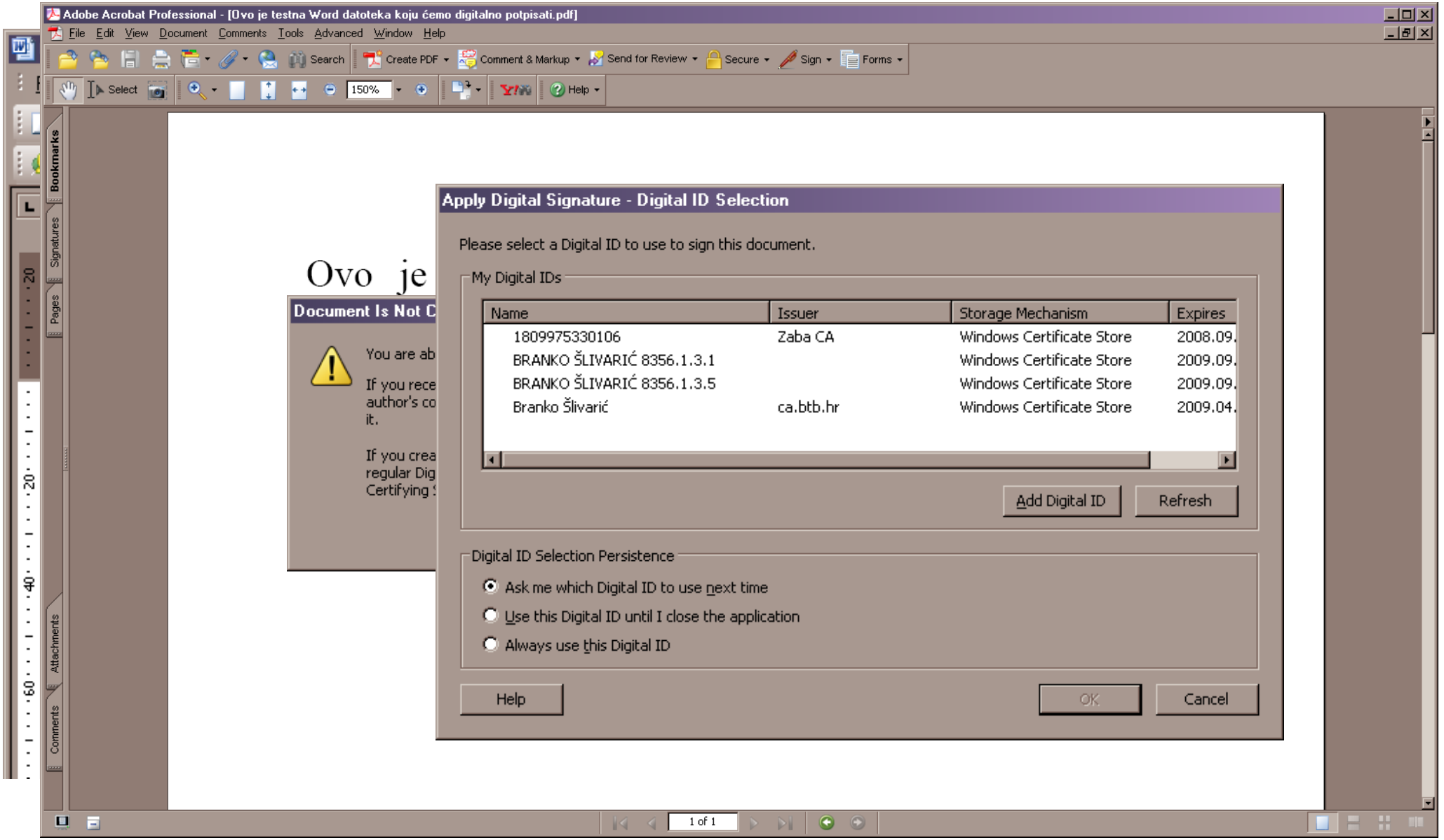
Kako (is)koristiti?



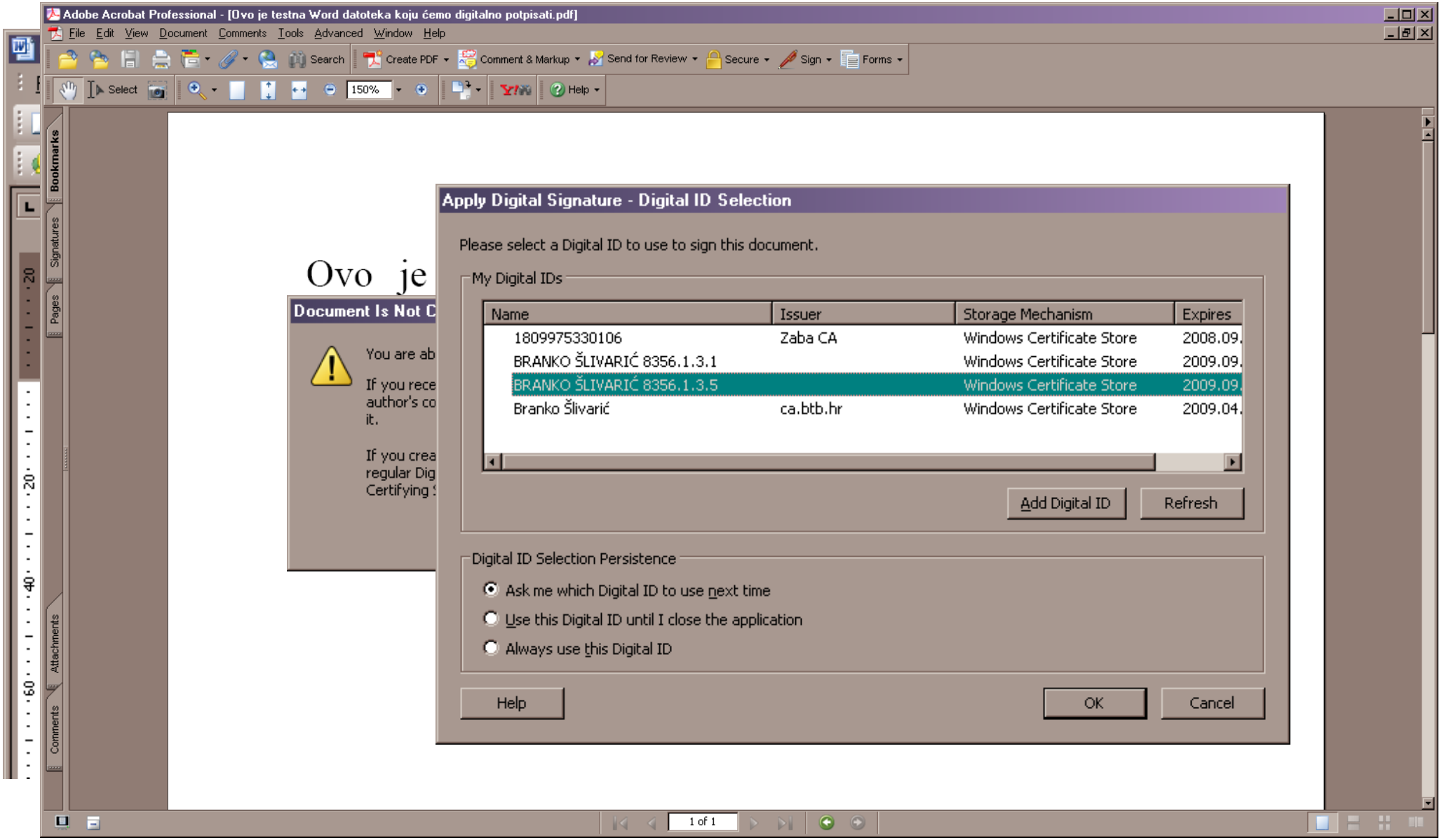
Kako (is)koristiti?



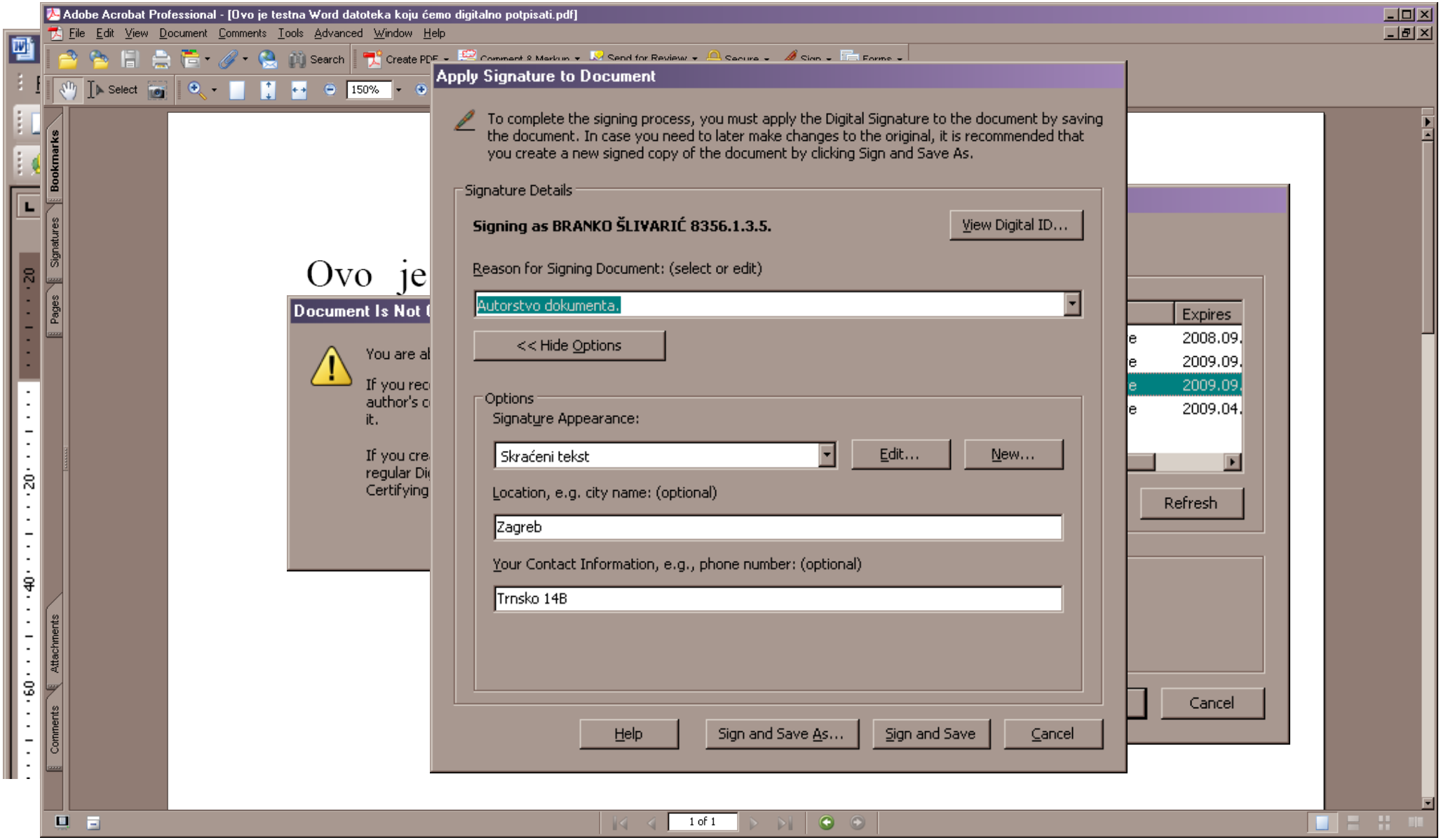
Kako (is)koristiti?



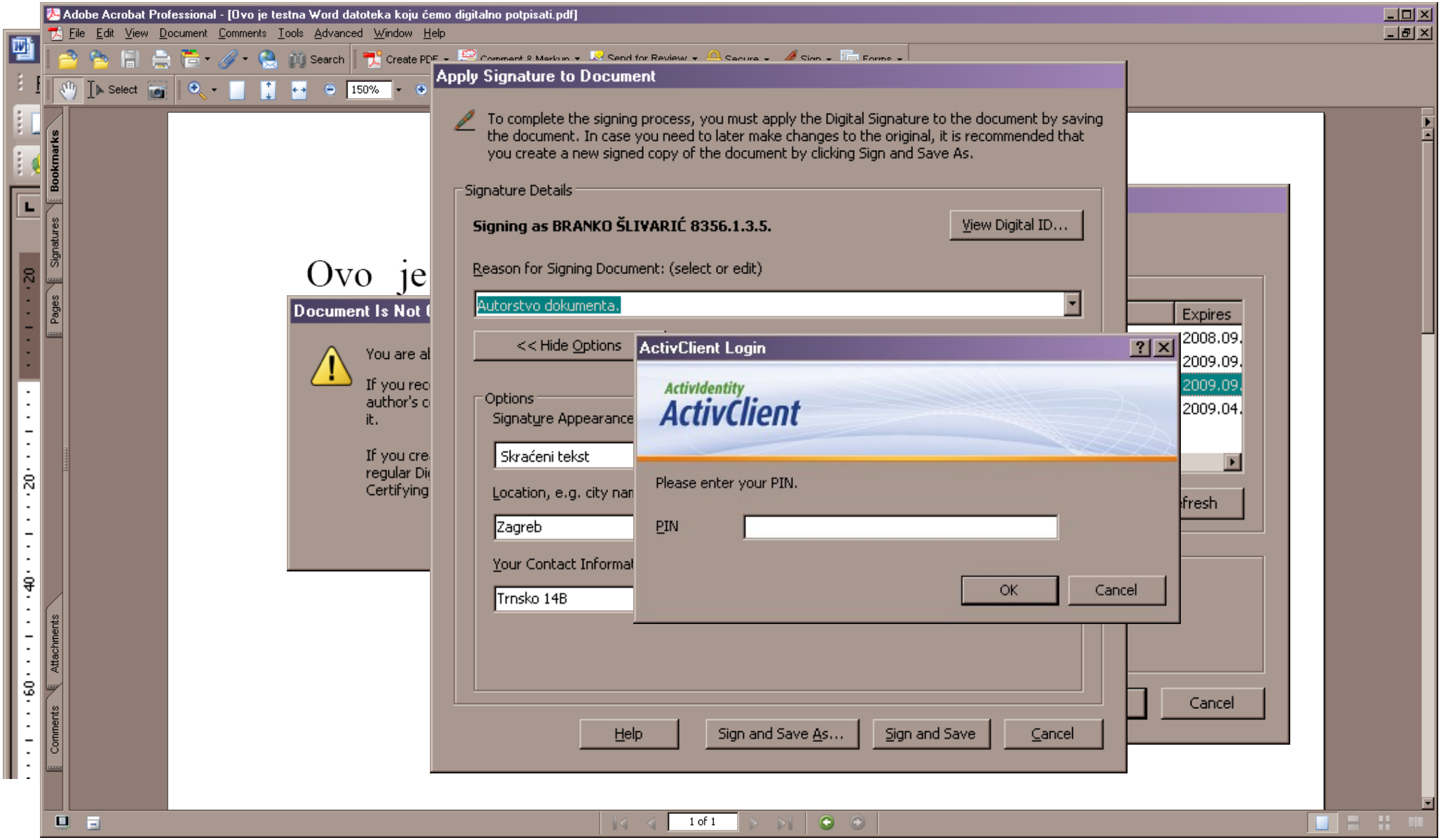
Kako (is)koristiti?



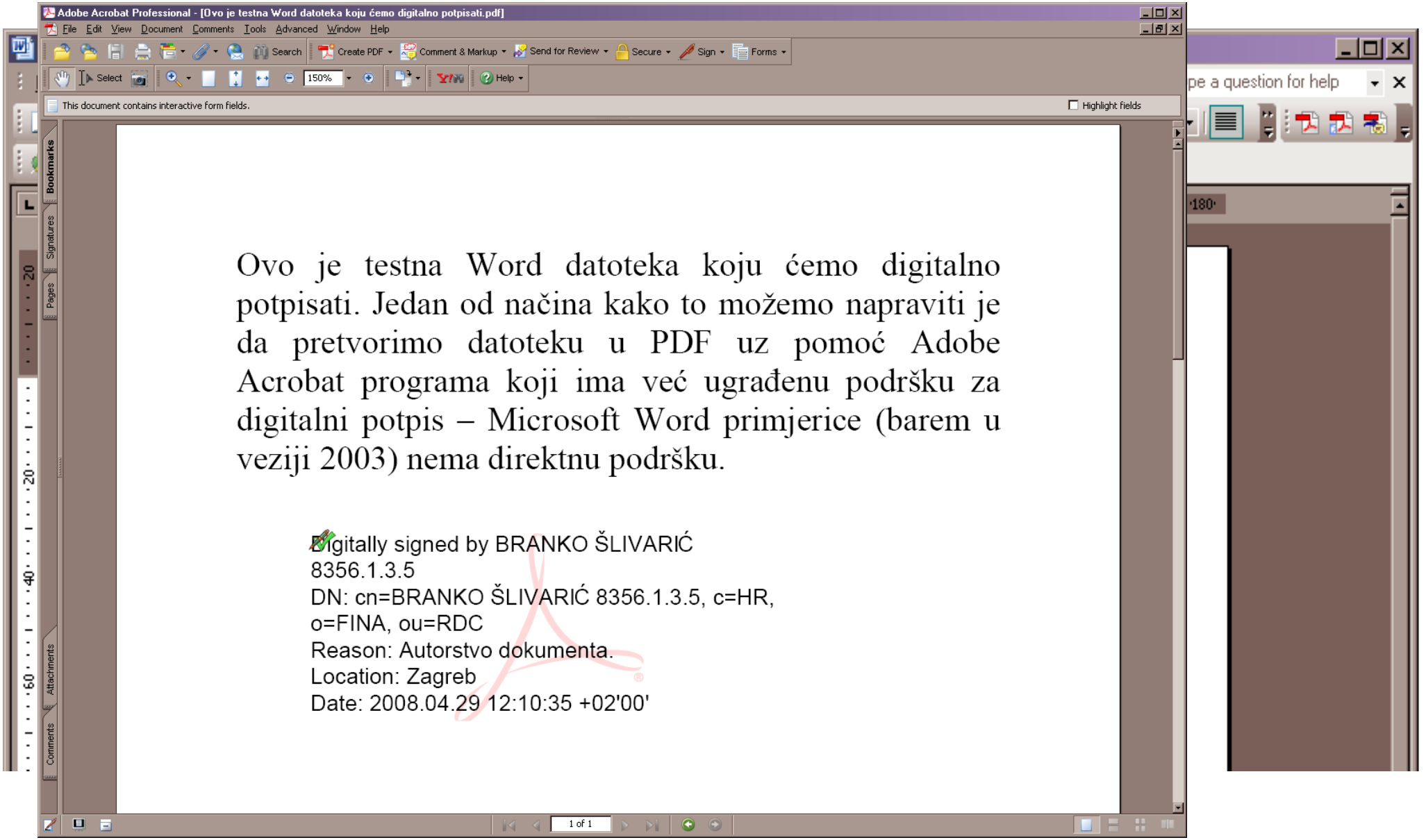
Kako (is)koristiti?



Kako (is)koristiti?



Kako (is)koristiti?



I za kraj...

- Primjer
  - Izgradili smo portal predmeta Otvoreno računarstvo
  - Zahtijevamo sigurni pristup (HTTPS)
  - Pazimo da ne čuvamo osjetljive informacije u nesigurnom obliku (lozinke, JMBG korisnika, ...)
  - Provjeravamo digitalne potpise pri predaji vježbe

- Stranici pregleda bodova prenosimo JMBAG studenta kao parametar (GET)
  - JMBAG koristimo za pristup bazi podataka

  http://otvoreno.rasip.fer.hr/pregled.php?jmbag=0036...

I za kraj...

- U kôdu – SQL

```
SELECT * FROM student
        WHERE jmbag = \'$_REQUEST['jmbag']\';
```

- Što će se desiti ako netko pozove

```
...pregled.php?jmbag=1';%20delete%20from
   %20student;select%20*%20from%20bodovi%20where
   %20ime%20like%20'%25
```

I za kraj...

- Izvršit će se SQL

```
SELECT * FROM student WHERE jmbag='1';
        delete from student; select * from bodovi where ime
    like '%'
```

- Ovo je napad umetanjem SQL-a (*SQL injection*)
  - Ne provjeravamo podatke koji dolaze od korisnika mrežom
- Kad se štitimo od *velikih* prijetnji ne smijemo zaboraviti na male!

Pitanja

- Zahvaljujemo Branku Šlivariću za pregled stanja u Hrvatskoj i primjer digitalnog potpisivanja dokumenta