

# **ELEKTRONSKO POTPISIVANJE KORIŠĆENJEM DIGITALNIH CERTIFIKATA CERTIFIKACIONOG TELA POŠTE**

*Mr Dragan Spasić dipl. inž, Javno preduzeće PTT saobraćaja "Srbija", Beograd,  
[dspasic@ptt.yu](mailto:dspasic@ptt.yu)*

**Apstrakt:** *U radu je objašnjeno elektronsko potpisivanje Microsoft Office dokumenata i elektronskih pisama korišćenjem digitalnih sertifikata Certifikacionog tela Pošte.*

**Ključne reči:** *Certifikaciono telo - CA, digitalni sertifikati, Zakon o elektronskom potpisu.*

## **DIGITALLY SIGNING USING DIGITAL CERTIFICATES OF THE POST SERBIA CERTIFICATION AUTHORITY**

**Abstract:** *This paper describes digitally signing Microsoft Office documents and e-mails using digital certificates of the Post Serbia Certification Authority.*

**Key words:** *Certification Authority - CA, digital certificates, Electronic Signature Act.*

## 1. UVOD

Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je izgradilo sertifikaciono telo (Certification Authority - CA) za izdavanje digitalnih (elektronskih) sertifikata, poznato pod nazivom Sertifikaciono telo Pošte [1, 2]. Sertifikaciono telo Pošte je izgrađeno u skladu sa Zakonom o elektronskom potpisu [3] i podzakonskim aktima [4, 5, 6, 7].

Digitalni sertifikati Sertifikacionog tela Pošte su standardni X.509 verzija 3 sertifikati koji mogu da se koriste za autentifikaciju (predstavljanje) Web korisnika i Web servera, šifrovanje/dešifrovanje i digitalno potpisivanje/verifikovanje potpisanih dokumenata, elektronskih pisama i transakcija, u okviru aplikacija koje podržavaju rad sa digitalnim sertifikatima.

Od 16.11.2004. godine Sertifikaciono telo Pošte izdaje (prodaje) digitalne sertifikate zainteresovanim korisnicima izvan PTT-a, i fizičkim i pravnim licima.

U ovom trenutku (kraj oktobra 2006.), PTT tj. Sertifikaciono telo Pošte je prvo i jedino **javno** sertifikaciono telo u Republici Srbiji.

Primarni cilj PTT-a kao sertifikacionog tela je da se registruje za izdavanje KVALIFIKOVANIH digitalnih sertifikata u Republici Srbiji. Nadležan organ za registrovanje sertifikacionih tela u Republici Srbiji je Ministarstvo za nauku i zaštitu životne sredine, u okviru koga postoji Sektor za informaciono društvo.

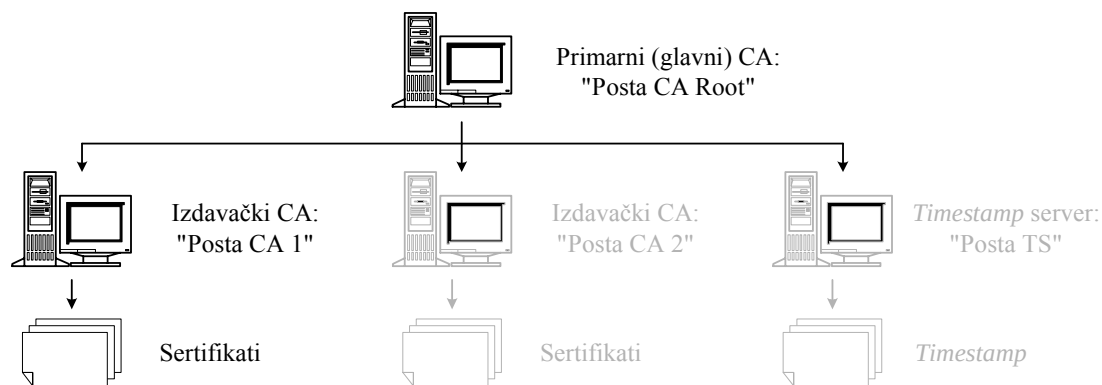
Implementacija Zakona o elektronskom potpisu je nekoliko puta odlagana (1.9.2005, 1.1.2006, 1.7.2006.). Konačno, implementacija je počela **1.7.2006.** PTT je **18.7.2006.** dostavio Ministarstvu nauke i zaštite životne sredine: "Zahtev za upis u registar sertifikacionih tela za izdavanje KVALIFIKOVANIH elektronskih sertifikata u Republici Srbiji", "Prijavu za upis u evidenciju sertifikacionih tela" i prateću dokumentaciju.

Prema Zakonu o elektronskom potpisu, član 20, stav 2, Ministarstvo je dužno da u roku od **30 dana** od dana podnošenja urednog Zahteva, donese rešenje o upisu sertifikacionog tela u Registar sertifikacionog tela. S obzirom na to da je navedeni zakonski rok odavno prošao, PTT očekuje da Sertifikaciono telo Pošte u najskorije vreme bude registrovano od strane Ministarstva, za izdavanje KVALIFIKOVANIH digitalnih sertifikata.

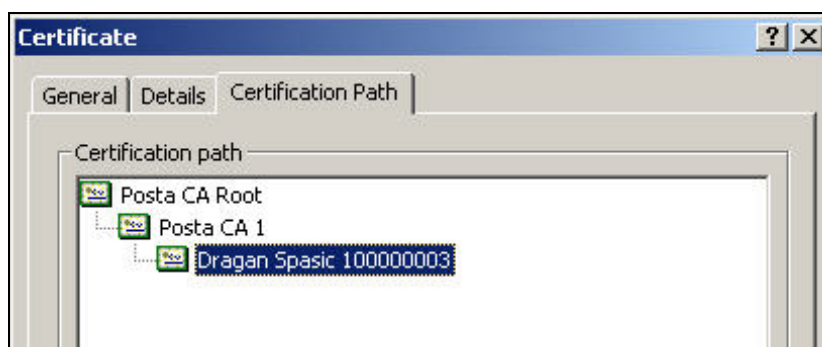
## 2. HIJERARHIJSKA ORGANIZACIJA CA SERVERA SERTIFIKACIONOG TELA POŠTE

Sertifikaciono telo Pošte koristi u svojoj infrastrukturi za izdavanje X.509 verzija 3 digitalnih (elektronskih) sertifikata, hijerarhiju više CA (Certification Authority) servera koji se nalaze u relaciji nadređeni-podređeni CA serveri. Infrastrukturu Sertifikacionog tela Pošte u ovom trenutku čine dva CA servera (slika 1. i 2.) [2]:

- **"Posta CA Root"** server, kao primarno (glavno ili centralno) tj. **ROOT** sertifikaciono telo.
- **"Posta CA 1"** izdavački server, kao podređeno sertifikaciono telo.  
Planirano je da se naknadno instališe (slika 1.):
- Dodatni izdavački CA server **"Posta CA 2"**.
- *Timestamp* server **"Posta TS"**.



Slika 1. Hijerarhijska organizacija CA servera Sertifikacionog tela Pošte



Slika 2. Sertifikaciona putanja sertifikata Sertifikacionog tela Pošte

### 3. ELEKTRONSKO POTPISIVANJE MICROSOFT OFFICE DOKUMENATA

Korisnici za elektronsko potpisivanje elektronskih dokumenata mogu da koriste Microsoft Office aplikacije: Word, Excel ili PowerPoint [8].

Preduslovi za elektronsko potpisivanje elektronskih Microsoft Office dokumenata su sledeći:

1. Korisnik koji vrši elektronsko potpisivanje tj. potpisnik mora da ima lični (personalni) elektronski sertifikat Sertifikacionog tela Pošte.
2. Na računaru potpisnika mora da bude podešen tačan datum, vreme i vremenska (časovna) zona (GMT+01:00).
3. Na računaru potpisnika mora da bude instalisana aplikacija Microsoft Office (Word, Excel i PowerPoint) 2002 SP3, 2003 ili novija. Preporučljivo je da se koristi poslednja verzija aplikacije i poslednji SP.
4. Računar potpisnika mora da ima pristup Internet serverima Sertifikacionog tela Pošte na kojima se nalaze registri opozvanih sertifikata (Certificate Revocation List - CRL) [9].

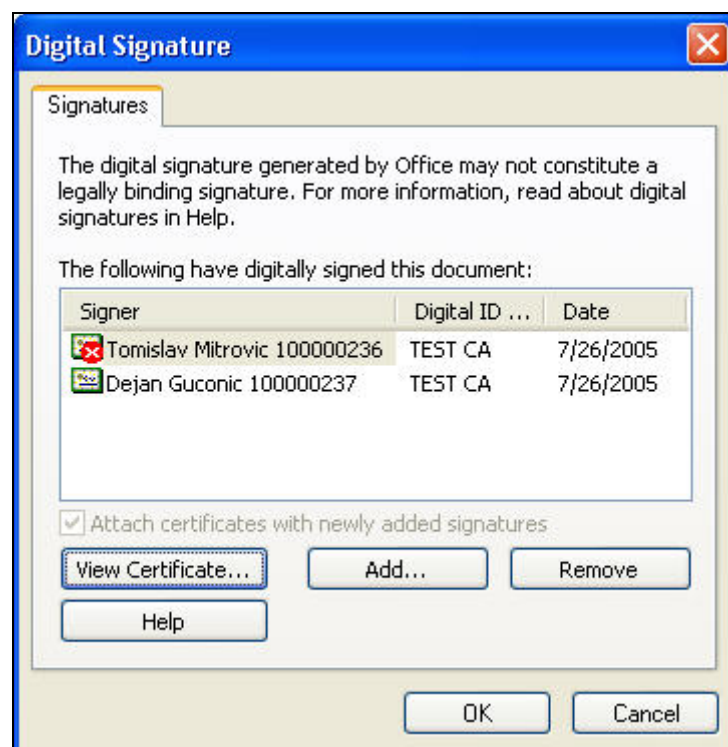
Preduslovi za verifikovanje tj. proveru elektronskog potpisa potpisanih elektronskih dokumenata su sledeći:

1. Na računaru korisnika koji vrši verifikovanje mora da bude instalisan sertifikat *root* CA servera Sertifikacionog tela Pošte ("**Posta CA Root**"). Korisnik koji vrši verifiko-

vanje **ne** mora da ima lični (personalni) elektronski sertifikat Sertifikacionog tela Pošte.

2. Na računaru korisnika koji vrši verifikovanje mora da bude podešen tačan datum, vreme i vremenska (časovna) zona (GMT+01:00).
3. Na računaru korisnika koji vrši verifikovanje mora da bude instalisana aplikacija Microsoft Office (Word, Excel i PowerPoint) 2002 SP3, 2003 ili novija. Preporučljivo je da se koristi poslednja verzija aplikacije i poslednji SP.
4. Računar korisnika koji vrši verifikovanje mora da ima pristup Internet serverima Sertifikacionog tela Pošte na kojima se nalaze registri opozvanih sertifikata (Certificate Revocation List - CRL) [9].

Prilikom verifikovanja elektronskog potpisa, sprovodi se postupak verifikovanja elektronskog sertifikata potpisnika koji je potpisao elektronski dokument. Kao rezultat sprovedenog verifikovanja, dobija se uspešna ili neuspešna verifikacija elektronskog potpisa. Ukoliko je verifikacija elektronskog potpisa uspešna, korisnik koji vrši verifikovanje mora da se pouzda u identitet potpisnika i integritet elektronskog dokumenta, a potpisnik mora da odgovara za sadržaj elektronskog dokumenta u trenutku elektronskog potpisivanja. Ukoliko je verifikacija elektronskog potpisa neuspešna (što će u aplikaciji biti vidljivo označeno karakterističnom oznakom neispravnog elektronskog sertifikata, kao što je prikazano na slici 3.), korisnik koji vrši verifikovanje ne sme da se pouzda u identitet potpisnika i integritet elektronskog dokumenta, a potpisnik ne treba da odgovara za sadržaj elektronskog dokumenta. Najvažniji razlog zbog koga verifikacija elektronskog potpisa nije uspešna je kada je elektronski sertifikat kojim je izvršeno elektronsko potpisivanje opozvan (This certificate has been revoked by its certification authority.). Opozvan elektronski sertifikat je obeležen crvenom oznakom (slika 3.) [10].



Slika 3. Microsoft Word/Excel/PowerPoint verifikovanje elektronskog potpisa potpisanog elektronskog dokumenta: simbolički prikazi dva sertifikata dva potpisnika koji su potpisali isti Microsoft Office dokument, od kojih je jedan sertifikat ispravan (Dejan Guconić), a drugi neispravan tj. opozvan (Tomislav Mitrović)

## 4. ELEKTRONSKO POTPISIVANJE ELEKTRONSKIH PISAMA

Korisnici za elektronsko potpisivanje elektronskih pisama mogu da koriste Microsoft aplikacije: Outlook [11] ili Outlook Express [12].

Preduslovi za elektronsko potpisivanje elektronskih pisama su sledeći:

1. Korisnik koji vrši elektronsko potpisivanje tj. potpisnik mora da ima lični (personalni) elektronski sertifikat Sertifikacionog tela Pošte. U elektronskom sertifikatu potpisnika mora da bude upisana tačna adresa elektronske pošte potpisnika (polje *Subject Alternative Name* sertifikata: RFC822 Name=username@domain).
2. Na računaru potpisnika mora da bude podešen tačan datum, vreme i vremenska (časovna) zona (GMT+01:00).
3. Na računaru potpisnika mora da bude instalisana aplikacija Microsoft Outlook 2000 SP3, 2002 SP3, 2003 ili novija, ili aplikacija Microsoft Outlook Express 5, 6 ili novija. Preporučljivo je da se koristi poslednja verzija aplikacije i poslednji SP.
4. Računar potpisnika mora da ima pristup Internet serverima Sertifikacionog tela Pošte na kojima se nalaze registri opozvanih sertifikata (Certificate Revocation List - CRL) [9].
5. Na računaru potpisnika mora da bude podešeno proveravanje opozvanosti sertifikata tj. pretraživanje registra opozvanih sertifikata [10].

Preduslovi za verifikovanje tj. proveru elektronskog potpisa potpisanih elektronskih pisama su sledeći:

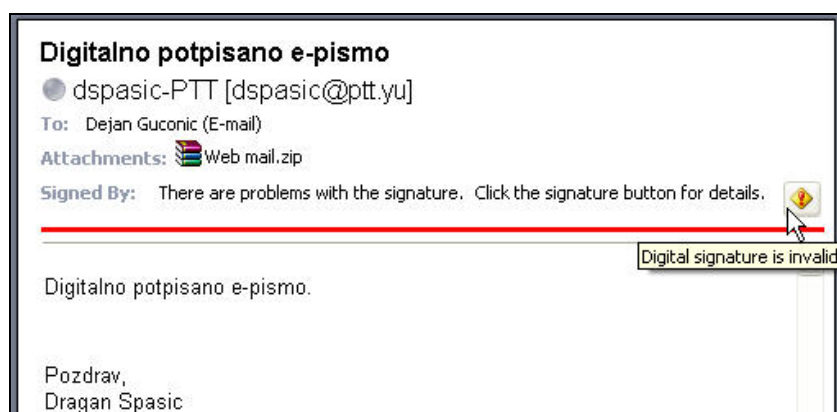
1. Na računaru korisnika koji vrši verifikovanje mora da bude instalisan sertifikat *root CA* servera Sertifikacionog tela Pošte ("**Posta CA Root**"). Korisnik koji vrši verifikovanje **ne** mora da ima lični (personalni) elektronski sertifikat Sertifikacionog tela Pošte.
2. Na računaru korisnika koji vrši verifikovanje mora da bude podešen tačan datum, vreme i vremenska (časovna) zona (GMT+01:00).
3. Na računaru korisnika koji vrši verifikovanje mora da bude instalisana aplikacija Microsoft Outlook 2000 SP3, 2002 SP3, 2003 ili novija, ili aplikacija Microsoft Outlook Express 5, 6 ili novija. Preporučljivo je da se koristi poslednja verzija aplikacije i poslednji SP.
4. Računar korisnika koji vrši verifikovanje mora da ima pristup Internet serverima Sertifikacionog tela Pošte na kojima se nalaze registri opozvanih sertifikata (Certificate Revocation List - CRL) [9].
5. Na računaru korisnika koji vrši verifikovanje mora da bude podešeno proveravanje opozvanosti sertifikata tj. pretraživanje registra opozvanih sertifikata [10].

Prilikom verifikovanja elektronskog potpisa, sprovodi se postupak verifikovanja elektronskog sertifikata potpisnika koji je potpisao elektronsko pismo. Kao rezultat sprovedenog verifikovanja, dobija se uspešna ili neuspešna verifikacija elektronskog potpisa. Ukoliko je verifikacija elektronskog potpisa uspešna, korisnik koji vrši verifikovanje mora da se pouzda u identitet potpisnika i integritet elektronskog pisma, a potpisnik mora da odgovara za sadržaj elektronskog pisma u trenutku elektronskog potpisivanja. Ukoliko je verifikacija elektronskog potpisa neuspešna (što će u aplikaciji biti vidljivo označeno, kao što je prikazano na slici 4. i 7.), korisnik koji vrši verifikovanje ne sme da se pouzda u identitet potpisnika i integritet elektronskog pisma, a potpisnik ne treba da odgovara za sadržaj elektronskog pisma. Najvažniji razlozi zbog kojih verifikacija elektronskog potpisa nije uspešna su sledeći:

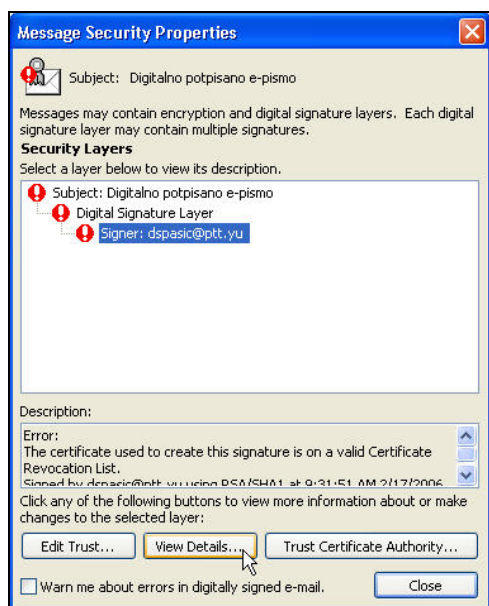
- Elektronski sertifikat kojim je izvršeno elektronsko potpisivanje je opozvan (The certificate used to create this signature is on a valid Certificate Revocation List; slika 5; The digital ID has been revoked; slika 7.).

- Nemoguće je pristupiti registru opozvanih sertifikata i proveriti da li je elektronski sertifikat potpisnika opozvan (The Certificate Revocation List needed to verify the signing certificate is either unavailable or it has expired.).
- Sadržaj elektronskog pisma je izmenjen posle potpisivanja, tj. narušen je integritet elektronskog pisma (The message contents may have been altered; slika 6.).
- Adresa elektronske pošte potpisnika i adresa elektronske pošte koja je upisana u elektronskom sertifikatu potpisnika se razlikuju (The digital ID's e-mail address does not match sender's.).

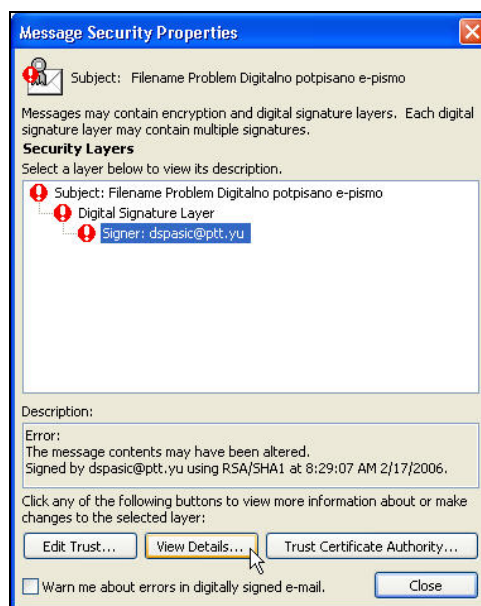
Jedini razlog zbog koga verifikacija elektronskog potpisa elektronskog pisma nije uspešna, a korisnik koji vrši verifikovanje bi trebao da se pouzda u identitet potpisnika i integritet elektronskog pisma, a potpisnik mora da odgovara za sadržaj elektronskog pisma u trenutku elektronskog potpisivanja, je kada je elektronskom sertifikatu kojim je izvršeno elektronsko potpisivanje istekao rok važnosti (The certificate used to create this signature is no longer valid.).



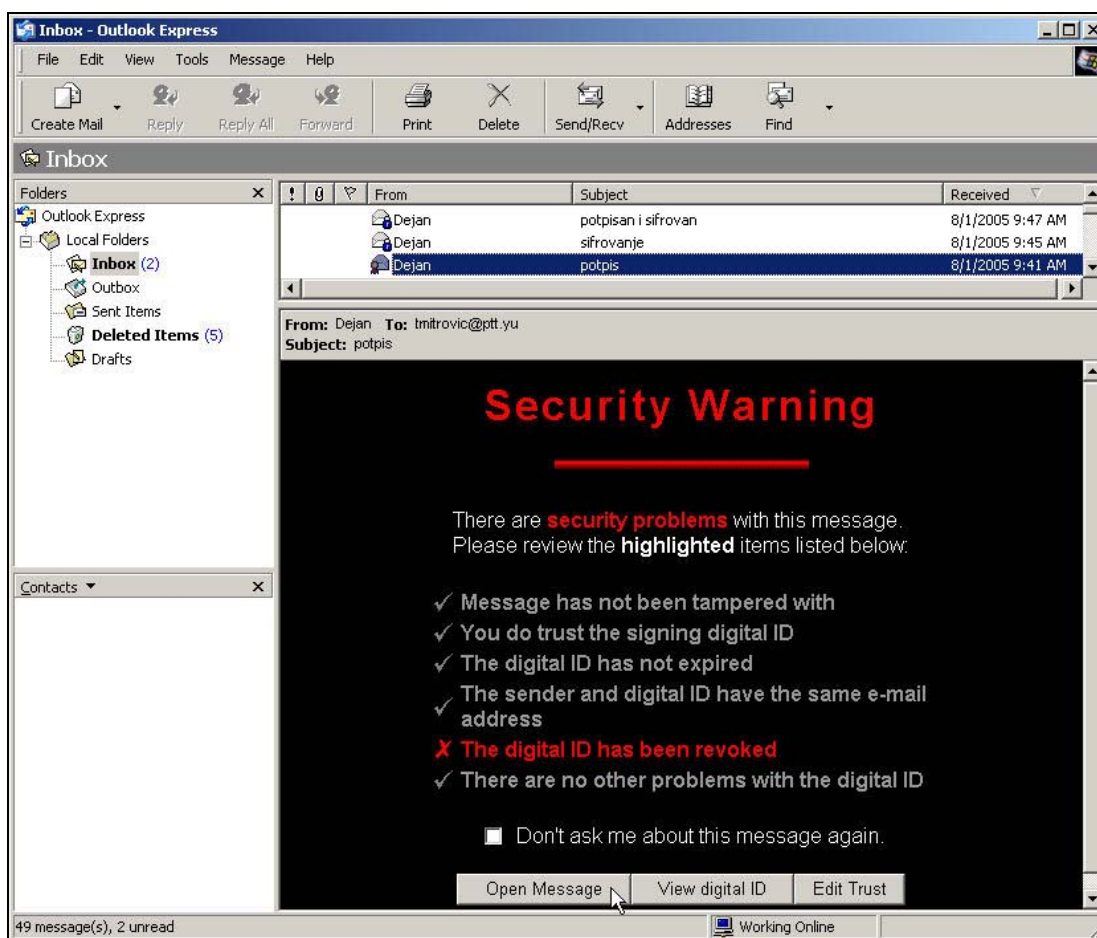
Slika 4. Microsoft Outlook verifikovanje elektronskog potpisa potpisanog elektronskog pisma: neuspešna verifikacija je vidljivo predstavljena crvenom oznakom tj. crvenom linijom



Slika 5. Microsoft Outlook verifikovanje elektronskog potpisa: elektronski sertifikat kojim je izvršeno potpisivanje je opozvan



Slika 6. Microsoft Outlook verifikovanje elektronskog potpisa: sadržaj elektronskog pisma je izmenjen



Slika 7. Microsoft Outlook Express verifikovanje elektronskog potpisa potpisnog elektronskog pisma: neuspešna verifikacija (Security Warning) i razlog neuspešnosti verifikacije (prema slici: sertifikat je opozvan)

## 5. ZAKLJUČAK

Uvođenjem elektronskom poslovanja (e-business) ili poslovanja posredstvom Interneta, omogućeno je brže, efikasnije i ekonomičnije poslovanje, u odnosu na poslovanje bez korišćenja Interneta. Pri tome, uspeh elektronskog poslovanja (e-business) zavisi od zaštite Internet komunikacija. Naime, Internet pruža velike mogućnosti u oblasti elektronskog poslovanja, ali sa druge strane donosi problem zaštite identiteta korisnika, podataka i mrežnih resursa. Među problemima koji se javljaju ističu se sledeći:

- lažiranje identiteta na Internetu,
- neovlašćena prijava i pristup resursima na Internetu,
- neovlašćeno otkrivanje sadržaja poruka koje se razmenjuju Internetom - problem tajnosti podataka,
- neovlašćeno modifikovanje poruka - problem integriteta podataka,
- poricanje ili nepriznavanje sprovedenih aktivnosti,...

Navedeni problemi mogu se rešiti primenom elektronskog potpisivanja i šifrovanjem elektronskih dokumenata, elektronskih pisama i transakcija. Za potrebe elek-

tronskog potpisivanja i šifrovanja dokumenata, elektronskih pisama i transakcija, mogu da se koriste digitalni (elektronski) sertifikati koje izdaje **Javno preduzeće PTT saobraćaja "Srbija" - Sertifikaciono telo Pošte**.

Sertifikaciono telo Pošte izdaje sledeće četiri (4) kategorije digitalnih sertifikata [1, 2]:

1. **WEB sertifikat**,
2. **SID Enterprise sertifikat** (Single application ID),
3. **MID Enterprise sertifikat** (Multiple application ID),
4. **SER sertifikat za Web server**.

**WEB sertifikati** su standardni X.509 verzija 3 sertifikati koji mogu da se koriste u okviru Microsoft aplikacija (Internet Explorer, Outlook, Outlook Express, Word 2002/2003, Excel 2002/2003, PowerPoint 2002/2003 i drugih) i aplikacija drugih proizvođača, za autentifikaciju, šifrovanje / dešifrovanje i potpisivanje / verifikovanje potpisanih datoteka, elektronskih pisama i transakcija.

**SID i MID Enterprise sertifikati** su standardni X.509 verzija 3 sertifikati koji su prilagođeni Entrust aplikacijama, a mogu da ih koriste i "Entrust-Ready" aplikacije. S obzirom na to da postoji kompatibilnost sa Microsoft CryptoAPI, omogućeno je korišćenje SID i MID Enterprise sertifikata u okviru Microsoft aplikacija (Internet Explorer, Outlook, Outlook Express, Word 2002/2003, Excel 2002/2003, PowerPoint 2002/2003 i drugih) i aplikacija drugih proizvođača.

Korisnička aplikacija **Entrust Intelligence** se isporučuje uz svaki SID i MID Enterprise sertifikat i ona omogućava:

- Preuzimanje i obnavljanje SID i MID Enterprise sertifikata, pregled sadržaja sertifikata i eksportovanje sertifikata u datoteke različitih formata.
- Šifrovanje / dešifrovanje datoteka i potpisivanje / verifikovanje potpisanih datoteka.

Razlika između SID i MID Enterprise sertifikata je sledeća: SID (Single application ID) Enterprise sertifikat poseduje licencu za korišćenje sertifikata sa samo jednom aplikacijom ili aplikacionim dodatkom (*plug-in*), dok MID (Multiple application ID) Enterprise sertifikat poseduje licencu za korišćenje sertifikata sa neograničenim brojem aplikacija ili aplikacionih dodataka (*plug-in*).

**SER sertifikati za Web servere** su standardni X.509 verzija 3 sertifikati koji se koriste za konfigurisanje SSL (Secure Sockets Layer) i/ili TLS (Transport Layer Security) protokola na Web serverima. Namena SSL i TLS protokola je uspostavljanje zaštićenog komunikacionog kanala između Web servera i Web klijenata.

## 6. LITERATURA

1. Web strana Sertifikacionog tela Pošte: <http://www.cepp.co.yu/ca>.
2. "Pravilnik o elektronskim sertifikatima Javnog preduzeća PTT saobraćaja "Srbija"", "Službeni PTT glasnik", broj 341, 8.10.2004. godine (<http://www.cepp.co.yu/ca>).
3. "Zakon o elektronskom potpisu", "Službeni glasnik Republike Srbije", broj 135/2004.
4. "Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa", "Sl. glasnik RS", br. 48/2005.
5. "Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata", "Sl. glasnik RS", br. 48/2005.
6. "Pravilnik o registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji", "Sl. glasnik RS", br. 48/2005.
7. "Pravilnik o evidenciji sertifikacionih tela", "Sl. glasnik RS", br. 48/2005.
8. "Potpisivanje Microsoft Office datoteka korišćenjem Microsoft Office aplikacija i Web sertifikata", ver. 1.1, Korisničko uputstvo, Sertifikaciono telo Pošte, 2006 (<http://www.cepp.co.yu/ca/dokumentacija>).

9. D. Spasić, "Registri opozvanih sertifikata Sertifikacionog tela Pošte", XII festival informatičkih dostignuća "Infofest 2005", Zbornik radova, str. 57-64, Republički sekretarijat za razvoj Republike Crne Gore i kompanija Biznis Link, Budva, septembar-oktobar 2005.
10. D. Spasić, "Provera opozvanosti sertifikata u okviru različitih aplikacija", VI međunarodni simpozijum o elektronskoj trgovini i elektronskom poslovanju "E-trgovina 2006", Zbornik radova (medijum je CD-ROM), Agencija "E-trgovina", Palić, april 2006.
11. "Potpisivanje i šifrovanje elektronskih pisama korišćenjem Microsoft Outlook-a i Web sertifikata", ver. 1.0, Korisničko uputstvo, Sertifikaciono telo Pošte, 2004.
12. "Potpisivanje i šifrovanje elektronskih pisama korišćenjem Microsoft Outlook Express-a i Web sertifikata", ver. 1.0, Korisničko uputstvo, Sertifikaciono telo Pošte, 2003.