*XXV Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2007**, Beograd, 11. i 12. decembar 2007.*

STATUS IMPLEMENTACIJE ZAKONA O ELEKTRONSKOM POTPISU U REPUBLICI SRBIJI

Dragan Spasić
Javno preduzeće PTT saobraćaja "Srbija"

Sadržaj: *U radu je objašnjen status implementacije Zakona o elektronskom potpisu u Republici Srbiji. Takođe, u radu su navedene preporuke za implementaciju javnih elektronskih Internet servisa (e-Uprava), u oblasti Zakona o elektronskom potpisu i elektronskog (digitalnog) identiteta Internet korisnika.*

Ključne reči: *Zakon o elektronskom potpisu, Sertifikaciono telo - CA, elektronski (digitalni) sertifikati.*

1. Uvod

Pravni okvir za implementaciju Zakona o elektronskom potpisu u Republici Srbiji čine sledeći pravni akti:

- Zakon o elektronskom potpisu, "Službeni glasnik Republike Srbije", broj 135, 21.12.2004. godine.
- 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, 82/2005 i 116/2005).
- Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata ("Sl. glasnik RS", br. 48/2005, 82/2005 i 116/2005).
- Pravilnik o registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji ("Sl. glasnik RS", br. 48/2005, 82/2005 i 116/2005).
- Pravilnik o evidenciji sertifikacionih tela ("Sl. glasnik RS", br. 48/2005, 82/2005 i 116/2005).

Implementacija Zakona o elektronskom potpisu je nekoliko puta odlagana (1.9.2005., 1.1.2006., 1.7.2006.). Implementacija Zakona je formalno počela **1.7.2006**., ali praktično još uvek nije, jer nije registrovano, niti evidentirano ni jedno sertifikaciono telo (Certification Authority - CA) u Republici Srbiji. **Prvi korak u implementaciji**

Zakona o elektronskom potpisu predstavlja registrovanje i evidentiranje postojećih sertifikacionih tela. Posle formiranja nove Vlade Republike Srbije, implementacija Zakona o elektronskom potpisu data je u nadležnost novoformiranom Ministarstvu za telekomunikacije i informatičko društvo (http://www.mtid.sr.gov.yu).

Sa početkom implementacije Zakona o elektronskom potpisu omogućiće se puna primena postojećih zakona koji podržavaju mogućnost elektronskog potpisa (Zakon o poštanskim uslugama i Zakon o računovodstvu i reviziji), kao i zakona čija se izrada i usvajanje očekuje u najskorije vreme (Zakon o e-Trgovini, e-Upravi i e-Arhivama).

2. Javna sertifikaciona tela u Republici Srbiji

U ovom trenutku (novembar 2007.), Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je prvo i jedino **javno** sertifikaciono telo u Republici Srbiji.

Javno preduzeće PTT saobraćaja "Srbija" je izgradilo javno sertifikaciono telo za izdavanje **kvalifikovanih** elektronskih sertifikata [1, 2], u skladu sa Evropskom direktivom o elektronskom potpisu [3], srpskim Zakonom o elektronskom potpisu ("Sl. glasnik RS", br. 135/2004) i podzakonskim aktima ("Sl. glasnik RS", br. 48/2005, 82/2005 i 116/2005). Sertifikaciono telo Javnog preduzeća PTT saobraćaja "Srbija" (Sertifikaciono telo Pošte) se sastoji od centralnog ROOT CA servera ("**Posta CA Root**") i izdavačkog CA servera ("**Posta CA 1**"), kao što je prikazano na slici 1. Usluge Sertifikacionog tela Pošte su namenjene svim učesnicima elektronskog poslovanja u Republici Srbiji, bilo da su u pitanju fizička ili pravna lica (državna uprava, lokalna samouprava, javne službe, preduzeća, organizacije, institucije,...).

Dana **18.7.2006. godine**, Javno preduzeće PTT saobraćaja "Srbija" je dostavilo bivšem 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 dokumentacija. Prema Zakonu o elektronskom potpisu, član 20., stav 2., pomenuto Ministarstvo je bilo dužno da u roku od **30 dana** od dana podnošenja urednog Zahteva, donese rešenje o upisu sertifikacionog tela u Registar sertifikacionog tela, što **nije** urađeno. Sada je implementacija Zakona o elektronskom potpisu u nadležnosti Ministarstva za telekomunikacije i informatičko društvo.

Sertifikaciono telo Pošte koristi u svojoj infrastrukturi za izdavanje X.509 verzija 3 elektronskih (digitalnih) sertifikata hijerarhiju više CA 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.):

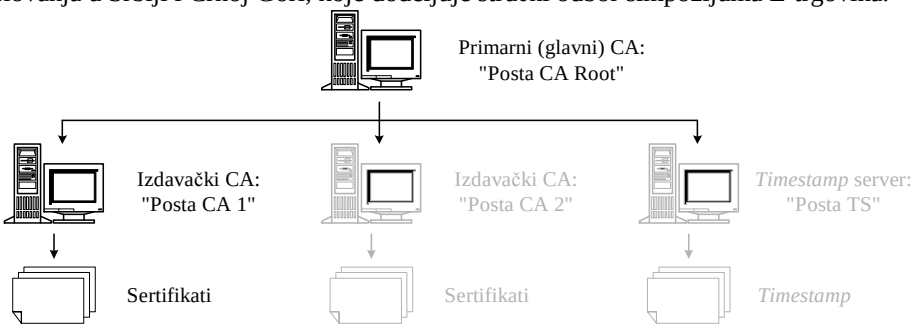
- "**Posta CA Root**" server, kao centralno (glavno) sertifikaciono telo.
- "**Posta CA 1**" izdavački server, kao podređeno sertifikaciono telo.

Planirano je da se naknadno instališe (slika 1.):

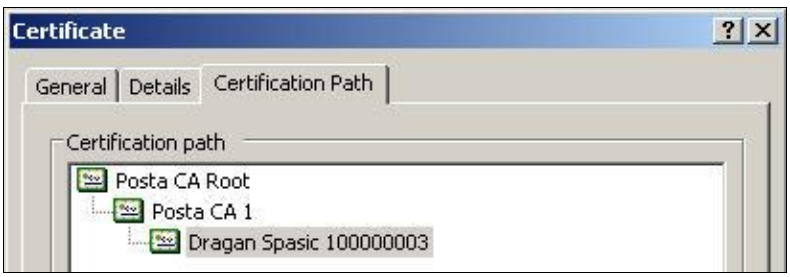
- Dodatni izdavački CA server "**Posta CA 2**".
- Timestamp server "**Posta TS**".

Za realizovan projekat Sertifikacionog tela Pošte, PTT je dobio prestižnu godišnju nagradu Diskobolos 2004, koju dodeljuje Jedinstveni informatički savez Srbije i

Crne Gore (JISA), i priznanje E-trgovina Award 2005 za doprinos razvoju elektronskog poslovanja u Srbiji i Crnoj Gori, koje dodeljuje stručni odbor simpozijuma E-trgovina.



Slika 1. *Hijerarhijska organizacija CA servera Sertifikacionog tela Pošte [2]*



Slika 2. *Sertifikaciona putanja sertifikata Sertifikacionog tela Pošte [2]*

Realno je očekivati da u Republici Srbiji postoji još nekoliko institucija i preduzeća koja bi bila javna sertifikaciona tela za izdavanje elektronskih sertifikata, s tim što broj sertifikacionih tela za izdavanje kvalifikovanih elektronski sertifikata verovatno neće biti veći od četiri (4).

3. Javna *Time Stamping* tela u Republici Srbiji

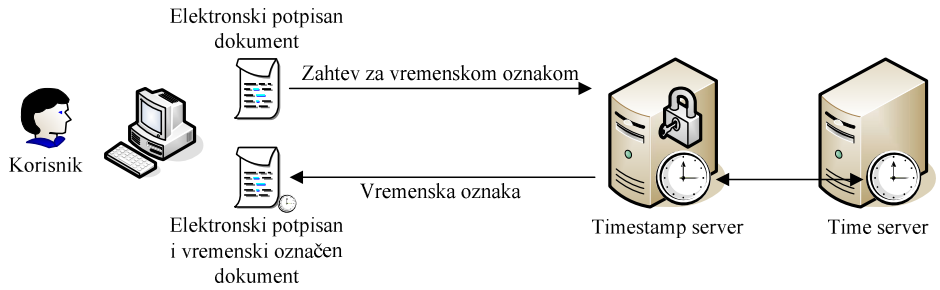
U ovom trenutku (novembar 2007.), u Republici Srbiji ne postoji ni jedno javno *Time Stamping* telo (Time Stamping Authority - TSA). Javno preduzeće PTT saobraćaja "Srbija" ima u planu da postane javno *Time Stamping* telo, instalisanjem Timestamp servera, kao što je prikazano na slici 1. *Time Stamping* telo je neophodno za realizaciju projekta **Elektronske poštanske marke** (Electronic Postal Certification Mark - EPCM).

Operacija vremenskog označavanja (pečatiranja) datoteka i transakcija (date and time stamping) je tesno povezana sa elektronskim potpisivanjem datoteka i transakcija, i predstavlja dodatnu vrednost elektronskom potpisu. Naime, vremenskim označavanjem koje pruža *Time Stamping* telo dobija se tačno vreme sprovedenog elektronskog potpisivanja (signing time). Osim toga, primenom vremenskog označavanja omogućena je uspešna verifikacija (provera) valjanog elektronskog potpisa i posle isteka roka važnosti

elektronskog sertifikata kojim je elektronski potpis kreiran, i posle opoziva elektronskog sertifikata.

Postupak vremenskog označavanja (pečatiranja) elektronski potpisanog dokumenta prikazan je na slici 3. Korisnik najpre izvrši elektronsko potpisivanje dokumenta korišćenjem odgovarajuće aplikacije, a zatim se prema Timestamp serveru pošalje zahtev za vremenskom oznakom. Timestamp server generiše vremensku oznaku, koja se pridruži elektronski potpisanom dokumentu.

Da bi Timestamp server mogao precizno da vrši vremensko označavanje, potrebno je da bude vremenski sinhronizovan sa nekim Time serverom, tj. serverom tačnog vremena, kao što je prikazano na slici 3.



Slika 3. *Postupak vremenskog označavanja (pečatiranja) elektronski potpisanog dokumenta*

4. Primeri aplikacija koje omogućavaju elektronsko potpisivanje i vremensko označavanje

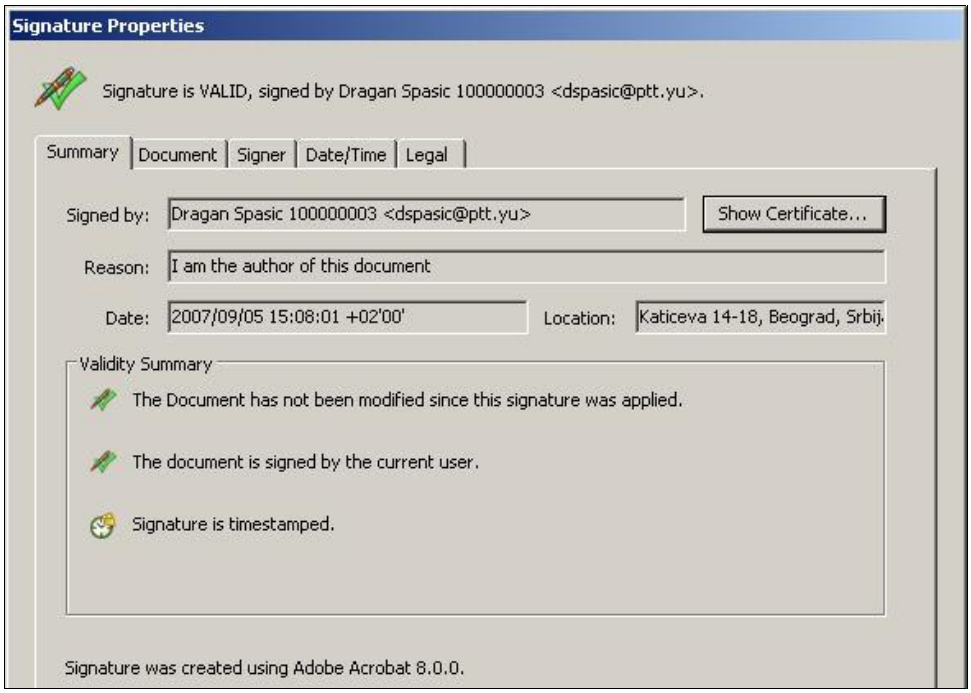
Adobe Acrobat 7.x i 8.x predstavljaju dobre primere aplikacija koje omogućavaju digitalno potpisivanje i vremensko označavanje (pečatiranje) elektronskih PDF dokumenata. Preduslov za digitalno potpisivanje i vremensko označavanje je da korisnik pored pomenutih aplikacija poseduje elektronski (digitalni) sertifikat, ima pristup CRL (Certificate Revocation List) i/ili OCSP (Online Certificate Status Protocol) serverima sertifikacionog tela, i ima pristup Timestamp serveru koji je RFC 3161 kompatibilan (na primer: http://adobe-timestamp.geotrust.com/tsa). Pre elektronskog potpisivanja, izuzetno je korisno da se u okviru Adobe Acrobat 7.x i 8.x podesi da se prilikom potpisivanja u okviru potpisanog PDF dokumenta ugradi CRL i/ili OSCP *response* prilikom potpisivanja (Include signature's revocation status when signing).

Verifikovanje digitalno potpisanog i vremenski označenog PDF dokumenta moguće je uraditi ne samo sa Adobe Acrobat 7.x i 8.x, već i sa Adobe Reader-om 7.x i 8.x, kao što je prikazano na slici 4. i 5. Verifikovanje je moguće uraditi u tri različita vrenenska trenutka:

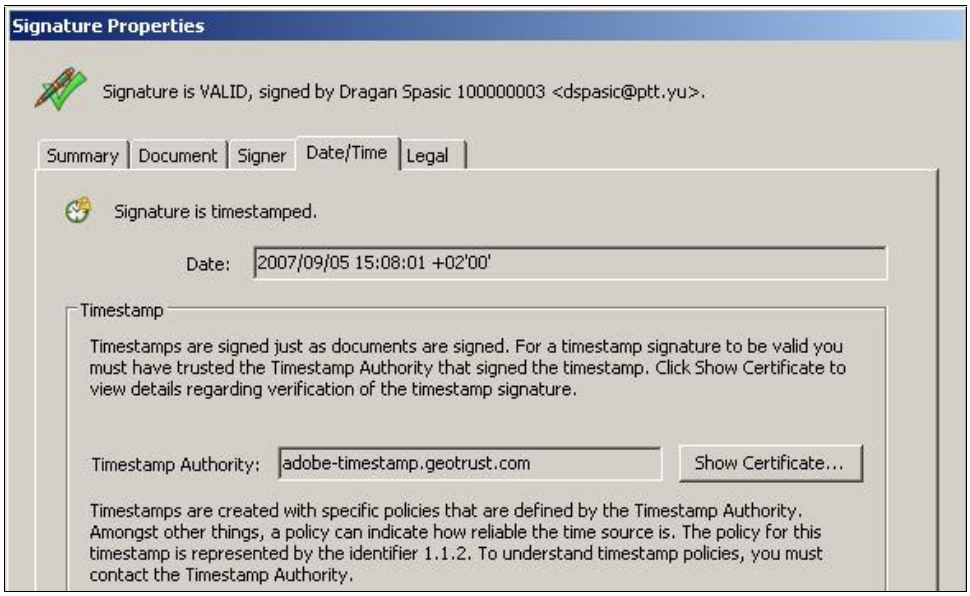
1. Trenutak u realnom vremenu (The current time).
2. Trenutak kada je potpisani PDF dokument vremenski označen (Secure time (e.g. timestamp) embedded in the signature if available, current time otherwise), što je po *default*-u podešeno.

3. Trenutak kada je elektronski potpis kreiran (The time at which the signature was created).

Adobe Acrobat i Reader rezultati verifikovanja potpisa posle isteka roka važnosti sertifikata i posle opoziva sertifikata, navedeni su u tabeli 1. i 2., respektivno.



Slika 4. *Adobe Acrobat i Reader verifikovanje elektronskog potpisa, kartica Summary*



Slika 5. *Adobe Acrobat i Reader verifikovanje elektronskog potpisa, kartica Date/Time*

Tabela 1. *Adobe Acrobat i Reader verifikovanje elektronskog potpisa posle isteka roka važnosti sertifikata*

Karakteristike potpisanog PDF dokumenta	Trenutak verifikovanja potpisa		
	1. Trenutak u realnom vremenu	2. Trenutak vremenskog označavanja	3. Trenutak kreiranja potpisa
Potpisan PDF dokument, bez ugrađenog CRL, sa vremenskom oznakom (Timestamp)	**Nepoznat status potpisa (Unknown):** Sertifikatu potpisnika je istekao rok važnosti.	**Nepoznat status potpisa (Unknown):** Sertifikatu potpisnika je istekao rok važnosti.	**Nepoznat status potpisa (Unknown):** Nemoguće je proveriti da li je sertifikat potpisnika u trenutku kreiranja potpisa bio opozvan.
Potpisan PDF dokument, bez ugrađenog CRL, bez vremenske oznake (Timestamp)	**Nepoznat status potpisa (Unknown):** Sertifikatu potpisnika je istekao rok važnosti.	**Nepoznat status potpisa (Unknown):** Sertifikatu potpisnika je istekao rok važnosti.	**Nepoznat status potpisa (Unknown):** Nemoguće je proveriti da li je sertifikat potpisnika u trenutku kreiranja potpisa bio opozvan.
Potpisan PDF dokument, sa ugrađenim CRL, sa vremenskom oznakom	**Nepoznat status potpisa (Unknown):** Sertifikatu potpisnika je	**Ispravan potpis (Valid)**	**Ispravan potpis (Valid)**

(Timestamp)	istekao rok važnosti.		
Potpisan PDF dokument, sa ugrađenim CRL, bez vremenske oznake (Timestamp)	**Nepoznat status potpisa (Unknown):** Sertifikatu potpisnika je istekao rok važnosti.	**Nepoznat status potpisa (Unknown):** Sertifikatu potpisnika je istekao rok važnosti.	**Ispravan potpis (Valid)**

Tabela 2. *Adobe Acrobat i Reader verifikovanje elektronskog potpisa posle opoziva sertifikata*

Karakteristike potpisanog PDF dokumenta	Trenutak verifikovanja potpisa		
	1. Trenutak u realnom vremenu	2. Trenutak vremenskog označavanja	3. Trenutak kreiranja potpisa
Potpisan PDF dokument, bez ugrađenog CRL, sa vremenskom oznakom (Timestamp)	**Neispravan potpis (Invalid):** Sertifikat potpisnika je opozvan.	**Neispravan potpis (Invalid):** Sertifikat potpisnika je opozvan.	**Nepoznat status potpisa (Unknown):** Nemoguće je proveriti da li je sertifikat potpisnika u trenutku kreiranja potpisa bio opozvan.
Potpisan PDF dokument, bez ugrađenog CRL, bez vremenske oznake (Timestamp)	**Neispravan potpis (Invalid):** Sertifikat potpisnika je opozvan.	**Neispravan potpis (Invalid):** Sertifikat potpisnika je opozvan.	**Nepoznat status potpisa (Unknown):** Nemoguće je proveriti da li je sertifikat potpisnika u trenutku kreiranja potpisa bio opozvan.
Potpisan PDF dokument, sa ugrađenim CRL, sa vremenskom oznakom (Timestamp)	**Neispravan potpis (Invalid):** Sertifikat potpisnika je opozvan.	**Ispravan potpis (Valid)**	**Ispravan potpis (Valid)**
Potpisan PDF dokument, sa ugrađenim CRL, bez vremenske oznake (Timestamp)	**Neispravan potpis (Invalid):** Sertifikat potpisnika je opozvan.	**Neispravan potpis (Invalid):** Sertifikat potpisnika je opozvan.	**Ispravan potpis (Valid)**

5. Poštanska sertifikaciona i registraciona tela

U velikom broju država, a pre svega Evropskih, poštanski operatori su vodeća ili među vodećim sertifikaciona tela. Najpoznatija poštanska sertifikaciona i registraciona tela su (slika 6.) [4]:

1. Post.Trust (http://www.post.trust.ie), Pošta Irske (http://www.anpost.ie).
2. Postecom (http://www.postecom.it), Pošta Italije (http://www.poste.it).
3. Signtrust (http://www.signtrust.de), Pošta Nemačke (http://www.deutschepost.de).
4. Certinomis (http://www.certinomis.com), Pošta Francuske (http://www.laposte.fr).
5. Certipost (http://www.certipost.be), Pošta Belgije (http://www.post.be).
6. Multicert (http://www.multicert.pt), Pošta Portugalije (http://www.ctt.pt).
7. Buypass (http://www.buypass.no), Pošta Norveške (http://www.posten.no).
8. Post Signum (http://www.postsignum.cz), Pošta Češke (http://www.cpost.cz).
9. E-paraksts (http://www.e-me.lv), Pošta Letonije (http://www.pasts.lv).
10. Certifikatska agencija Pošte Slovenije (http://postarca.posta.si), Pošta Slovenije (http://www.posta.si).
11. KeyPOST (http://www.auspost.com.au/keypost), Pošta Australije (http://www.auspost.com.au).
12. Hongkong Post e-Cert (http://www.hongkongpost.gov.hk), Pošta Honkonga (http://www.hongkongpost.com).

Među navedenim poznatim poštanskim sertifikacionim telima, u prezentaciji "The Information Society - an inspiration and an aspiration for the Posts" [4] je navedeno i sertifikaciono telo Javnog preduzeća PTT saobraćaja "Srbija", Centra za elektronsko poslovanje Pošte - **CePP** (slika 6.), koje se naziva **Sertifikaciono telo Pošte Srbije** (Post Serbia Certification Authority).

Slika 6. *Poštanska sertifikaciona i registraciona tela [4]*

6. Zaključak: Digitalni identitet građana Republike Srbije kao preduslov za uvođenje javnih elektronskih Internet servisa

Prema EU direktivi o elektronskom potpisu [3], **elektronskom potpisu** se **ne** može osporiti zakonsko dejstvo u zakonskim postupcima samo zato što je u elektronskoj formi, ili zato što nije kreiran kvalifikovanim sertifikatom izdatim od akreditovanog sertifikacionog tela ili zato što nije kreiran sa sredstvom za kreiranje sigurnog elektronskog potpisa (Secure Signature Creation Device - SSCD) kao što je PKI smart kartica ili PKI USB smart token (član 5., tačka 2. EU direktive).

U Francuskoj i Nemačkoj postoji veliki broj elektronskih Internet servisa koji se nude građanima, a koji se izvršavaju korišćenjem elektronskih sertifikata, i **postoji nekoliko desetina sertifikacionih tela** [5, 6, 7]. Na Web strani koju održava francusko Ministarstvo ekonomije, finansija i industrije (http://www.telecom.gouv.fr), postoji spisak sertifikacionih tela koja izdaju elektronske sertifikate zainteresovanim građanima. Spisak nemačkih sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate dat je na Web strani koju održava nemačka Federalna agencija za električnu energiju, gas, telekomunikacije, poštu i železnicu (http://www.nrca-ds.de). U Nemačkoj postoji čak 28 registrovanih sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata.

Francuska i Nemačka su vodeće države u svetu u oblasti tehnologije smart kartica. Francuske i nemačke kompanije Gemalto (Francuska, 42,2% svetskog tržišta), Giesecke & Devrient (Nemačka, 12,1%), Oberthur Card Systems (Francuska, 9,5%) i Sagem Orga (Nemačka i Francuska, 8,7%) su imale udeo od **72,5%** na svetskom tržištu smart kartica tokom 2005. godine [8]. I pored toga, od građana u Francuskoj se **ne** zahteva da njihov digitalni identitet, tj. elektronski sertifikat i tajni (privatni) kriptografski ključ bude uskladišten isključivo na smart kartici, već im je omogućeno da uskladište **digitalni identitet** na **hard disk** računara, što građani najčešće i čine [9]:

> *Francuska Vlada snažno podržava elektronsku upravu, tako da postoji 300 servisa kojima građani mogu da pristupe sa mišom u ruci. Više od 3 miliona građana je popunilo poreske prijave Internetom prošle godine, uglavnom korišćenjem digitalnog identiteta sa hard diska računara.*

Jedan od preduslova za uvođenje javnih elektronskih Internet servisa u Republici Srbiji (tu se pre svega misli na servise e-Uprave tj. e-Government-a), je da se građanima tj. korisnicima tih servisa dodele digitalni identiteti (Digital ID), odnosno digitalni ili elektronski sertifikati. Pri tome, korisnicima javnih elektronskih Internet servisa treba dati mogućnost da **samostalno izaberu od kog će sertifikacionog tela (Certification Authority) da nabave tj. kupe i koriste elektronske sertifikate**. Korisnici se ne bi smeli uslovljavati da koriste elektronske sertifikate samo jednog sertifikacionog tela, jer bi to predstavljalo uvođenje monopola u oblasti sertifikacionih tela i izdavanja elektronskih sertifikata.

Osim toga, korisnicima javnih elektronskih Internet servisa u Republici Srbiji treba dati mogućnost da **samostalno izaberu uređaj na kome će biti uskladišten njihov digitalni identitet**, tj. elektronski sertifikat i tajni (privatni) kriptografski ključ (hard disk računara, PKI smart kartica, PKI USB smart token, PKI SIM kartica,...). Korisnici se ne bi smeli uslovljavati da kao uređaj za skladištenje sertifikata koriste isključivo PKI smart kartice i PKI USB smart tokene. Korisnicima treba omogućiti da mogu da elektronski sertifikat i tajni (privatni) kriptografski ključ uskladište na hard disk računara, bez obzira što se viši nivo zaštite tajnog (privatnog) kriptografskog ključa postiže ako je on

uskladišten na smart kartici ili USB smart tokenu. Korisnicima je znatno jeftinije i jednostavnije ukoliko im je elektronski sertifikat i tajni (privatni) kriptografski ključ uskladišten na hard disku računara, u poređenju sa slučajem da je sertifikat i tajni ključ uskladišten na smart kartici ili USB smart tokenu. Naime, kupovina smart kartice i čitača smart kartica ili USB smart tokena predstavlja dodatno novčano ulaganje korisnika, u odnosu na kupovinu sertifikata. Pri tome, korisnik mora da bude napredni korisnik tj. administrator računara, jer je neophodno da na računaru instališe drajver za čitač smart kartica ili USB smart token i klijentski softver (middleware) za rad sa smart karticom ili USB smart tokenom, što je za prosečnog korisnika računara izuzetno komplikovano, pa i neizvodljivo.

Za uvođenje javnih elektronskih Internet servisa (e-Uprave,...) **nije** neophodno postojanje **elektronskih ličnih karata sa čipom**, koje bi sadržale u čipu elektronski sertifikat i tajni (privatni) kriptografski ključ korisnika kome je takva lična karta izdata. Dovoljno je da u državi postoji barem jedno **javno** sertifikaciono telo koje izdaje elektronske sertifikate, s tim što je poželjno da postoje barem dva **javna** sertifikaciona tela, kako bi korisnici mogli da izaberu od kog će sertifikacionog tela da nabave tj. kupe i koriste elektronske sertifikate.

Javno preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je izgradilo **javno** sertifikaciono telo za izdavanje elektronskih (digitalnih) sertifikata, poznato pod nazivom **Sertifikaciono telo Pošte** [1, 2]. Elektronski sertifikati Sertifikacionog tela Pošte su namenjeni svim učesnicima elektronskog poslovanja u Republici Srbiji, i pravnim i fizičkim licima.

Literatura

[1] Web strana Sertifikacionog tela Pošte: http://www.cepp.co.yu/ca.

[2] D. Spasić, "Izdavanje digitalnih sertifikata Sertifikacionog tela Pošte", XXIV simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju "PosTel 2006", Zbornik radova, str. 225-232, Saobraćajni fakultet, Beograd, decembar 2006.

[3] "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures", Official Journal of the European Communities, L 13/12, 19.1.2000.

[4] P. Donohoe - E-Business Programme Manager, Universal Postal Union, International Bureau, Operations and Technology Directorate, "The Information Society - an inspiration and an aspiration for the Posts", Post Expo 2006, Amsterdam, Netherlands.

[5] D. Spasić, "Prikaz postojanja digitalnog identiteta u nekim evropskim državama", VII međunarodni simpozijum o elektronskoj trgovini i elektronskom poslovanju "E-trgovina 2007", Zbornik radova (medijum je CD-ROM), Agencija "E-trgovina", Palić, april 2007

[6] Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE FRANCE, April 2007 (http://www.epractice.eu/files/media/media1346.pdf).

[7] Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, NATIONAL PROFILE GERMANY, April 2007 (http://www.epractice.eu/files/media/media1343.pdf).
[8] D. Balaban, "Ready To Dominate?", Card Technology, Volume 11, Number 10, pp. 44-57, November 2006.
[9] D. Balaban, "Is Europe Ready For A Standard National ID?", Card Technology, Volume 10, Number 7, pp. 20-23, July / August 2005.
[10] EU: eSignature Profiles of 29 countries (EU-27, Croatia and Turkey): http://www.epractice.eu/document/3757, http://ec.europa.eu/idabc/en/document/6485.

Abstract: *This paper describes Electronic Signature Act implementation status in the Republic of Serbia. Also, recommendations for implementation public electronic Internet services (e-Government), in the field of Electronic Signature Act and digital identity of Internet users, are defined in this paper.*

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

ELECTRONIC SIGNATURE ACT IMPLEMENTATION STATUS IN THE REPUBLIC OF SERBIA

Dragan Spasić