*XXVII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – **PosTel 2009**, Beograd, 15. i 16. decembar 2009.*

ELEKTRONSKA POŠTANSKA MARKA SVETSKOG POŠTANSKOG SAVEZA

Dragan Spasić
Javno preduzeće PTT saobraćaja "Srbija"

Sadržaj: *Svetski poštanski savez (UPU) je razvio aplikacioni dodatak EPCM (Electronic Postal Certification Mark) za Microsoft Word 2007 koji može da uspostavi konekciju sa bilo kojim EPCM serverom koji je izgrađen u skladu sa UPU standardom S43 "Secure Electronic Postal Services Interface Specification" i da od EPCM servera primi elektronsku poštansku marku i stavi je na Microsoft Word 2007 dokument. Elektronska poštanska marka na elektronskom dokumentu obezbeđuje garanciju integriteta elektronskog dokumenta, podatke o korisniku koji je elektronski potpisao dokument, neporecivost potpisivanja, i datum i vreme vremenskog žigosanja elektronskog dokumenta.*

Ključne reči: *Svetski poštanski savez, Elektronska poštanska marka, elektronski potpis, vremenski žig.*

1. Uvod

Svetski poštanski savez (Universal Postal Union - UPU, www.upu.int) je na kongresu koji je održan 1994. godine u Seulu, doneo odluku o formiranju tela čiji je naziv Telematik kooperativa (Telematics Cooperative - TC). Dve godine kasnije, 1996. godine, Poštansko operativno veće (Postal Operations Council - POC) Svetskog poštanskog saveza je formiralo Telematik kooperativu. Razlog formiranja Telematik kooperative je pružanje pomoći poštanskim operatorima u primeni i korišćenju savremenih informacionih i komunikacionih tehnologija u cilju unapređenja poslovnih procesa. Osim toga, zadatak Telematik kooperative je saradnja sa poštanskim operatorima na razvoju novih elektronskih proizvoda i usluga (servisa), koji bi se ponudili korisnicima.

Bilo koji poštanski operator, javni ili privatni, čija je država članica Svetskog poštanskog saveza, može da postane član Telematik kooperative. Članstvo je dobrovoljno, s tim što je neophodno plaćati godišnju članarinu, koja zavisi od članskog razreda. Od januara 2009. godine Telematik kooperativa ima 128 država članica. Javno

preduzeće PTT saobraćaja "Srbija" (Pošta Srbije) je član Telematik kooperative od 2002. godine.

Organizaciona struktura Telematik kooperative prikazana je na slici 1. Hijerarhijski najviši organi Telematik kooperative su Generalna skupština (General Assembly - GA) i Upravljačko telo (Cooperative Management Board - CMB). Operativno telo Telematik kooperative je Centar za poštansku tehnologiju (Postal Technology Centre - PTC, www.ptc.upu.int). Zadatak Centra je da sprovodi projekte i aktivnosti koje odobri Generalna skupština i Upravljačko telo.

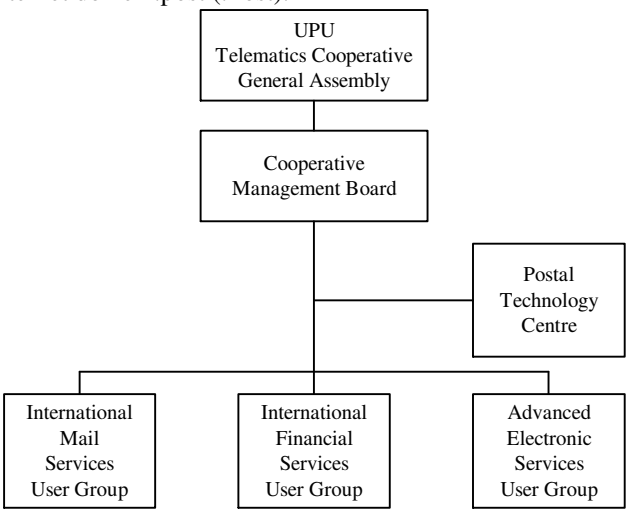
Postoje tri (3) radne grupe u okviru Telematik kooperative (slika 1.):

1. Grupa za međunarodne poštanske servise (The International Mail Services (IMS) User Group). Zadatak IMS grupe je definisanje strategije i poslovnih procesa sistema za elektronsko praćenje pošiljaka (EMS, pisama i paketa) u međunarodnom poštanskom saobraćaju, koji obuhvataju poštanske tehnološke procese, opertivno upravljanje i slanje EDI (Electronic Data Interchange) poruka. Dva najvažnija sistema koja je po zahtevima IMS grupe razvio Centar za poštansku tehnologiju (PTC) su: IPS (International Postal System) i IPS Light (International Postal System Light).
2. Grupa za međunarodne finansijske servise (The International Financial Services (IFS) User Group). Zadatak IFS grupe je definisanje strategije i poslovnih procesa sistema za međunarodni elektronski transfer novca, koji obuhvataju finansijske tehnološke procese, opertivno upravljanje i slanje EDI (Electronic Data Interchange) poruka. Tri najvažnija sistema koja je po zahtevima IFS grupe razvio Centar za poštansku tehnologiju (PTC) su: IFS (International Financial System), IFS Light (International Financial System Light) i STEFI (Secured Transfer of Electronic Financial Information).
3. Grupa za napredne elektronske servise (The Advanced Electronic Services (AES) User Group). U okviru AES grupe postoje sledeće podgrupe:
   - **3.1. Grupa za UPU standard S43 "Secure Electronic Postal Services (SEPS) Interface Specification" [1] koji definiše interfejs za Elektronsku poštansku marku (Electronic Postal Certification Mark - EPCM) i druge S43 elektronske servise, kao što je Registrovano elektronsko pismo (Postal Registered Electronic Mail - PReM).**
   - 3.2. Grupa za globalnu hibridnu poštu (Global Hybrid Mail).
   - 3.3. Grupa za RFID (Radio Frequency Identification).
   - 3.4. Grupa za Internet domen .post najvišeg nivoa (.post Top Level Domain - TLD).
   - 3.5. Grupa za bazu znanja o studijama slučaja (Case Study Knowledge Base).

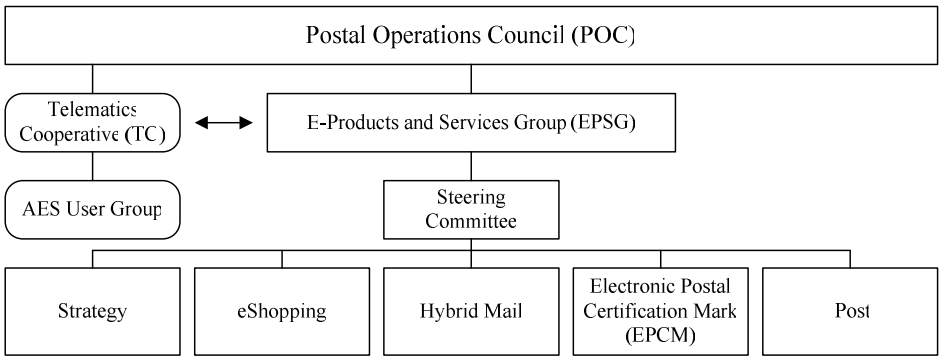
Osim AES grupe Telematik kooperative, poslovima kreiranja i implementacije novih elektronskih proizvoda i usluga (servisa) bavi se i EPSG grupa (E-Products and Services Group) Poštanskog operativnog veća (POC). EPSG grupa je formirana posle kongresa Svetskog poštanskog saveza koji je održan 2004. godine u Bukureštu. U okviru EPSG grupe postoje sledeće podgrupe (slika 2.):

1. Grupa za strategiju (Strategy).
2. Grupa za e-Trgovinu (eShopping).
3. Grupa za hibridnu poštu (Hybrid Mail).

4. **Grupa za elektronsku poštansku marku (Electronic Postal Certification Mark - EPCM).**
5. Grupa za Internet domen .post (.Post).



Slika 1. Organizaciona struktura Telematik kooperative



Slika 2. Organizaciona struktura EPSG grupe

2. Infrastruktura sistema Elektronske poštanske marke

Elektronska poštanska marka (Electronic Postal Certification Mark - EPCM) Svetskog poštanskog saveza je elektronski servis koji omogućava:

- elektronsko potpisivanje dokumenata (electronic signing a desktop document),
- elektronsko vremensko žigosanje dokumenata (date and time postmarking (stamping) a desktop document) i
- verifikovanje elektronski potpisanih i vremenski žigosanih dokumenata (verifying a signed and postmarked (timestamped) document).

EPCM infrastrukturu čine (slika 3.):

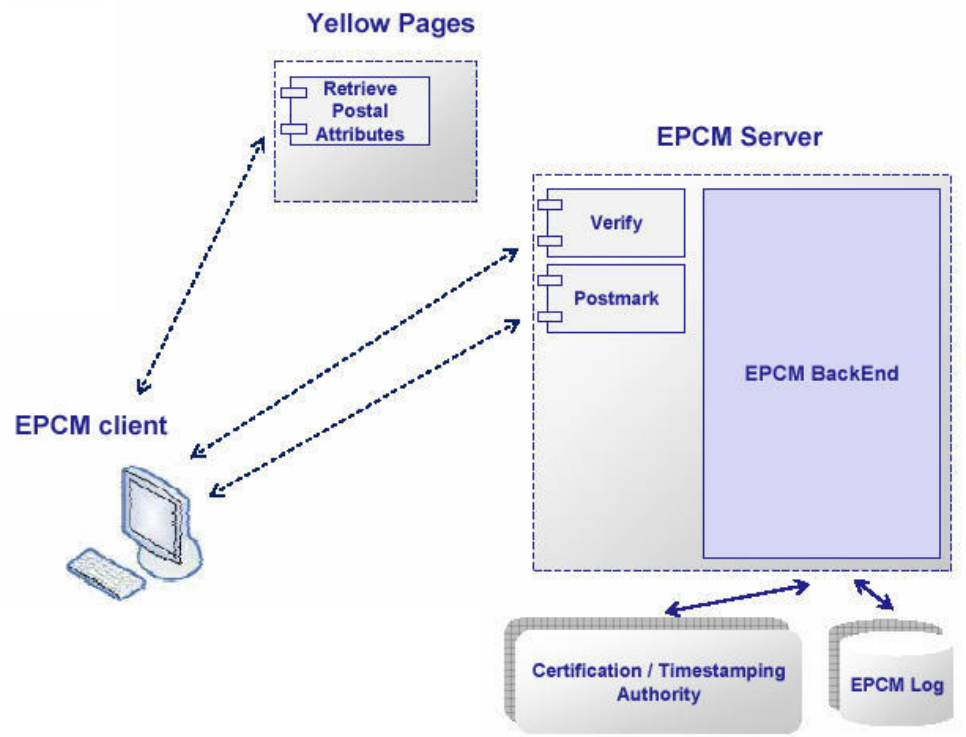
1. EPCM server, koji prihvata zahteve EPCM klijenata za vremenskim žigosanjem i izdaje vremenski žigosanu potvrdu (PostMarkedReceipt). Osim toga, EPCM server sprovodi verifikovanje elektronskog potpisa u vremenski žigosanoj potvrdi (PostMarkedReceipt). EPCM server je integrisan sa serverom za vremensko žigosanje (Timestamping server) i registrom sprovedenih EPCM transakcija (EPCM Log).
2. Yellow Pages server, koji predstavlja registar svih raspoloživih EPCM servera, sa podacima (atributima) o EPCM serverima, kao što su: jedinstveno ime (distinguished name), URL adresa, elektronski sertifikat, podržani formati elektronskog potpisa i drugi podaci. Yellow Pages server se nalazi u nadležnosti Centara za poštansku tehnologiju (Postal Technology Centre - PTC) Telematik kooperative Svetskog poštanskog saveza.
3. EPCM klijent, koji je aplikacioni dodatak (plug-in) za Microsoft Word 2007 (slika 4.).
4. Sertifikaciono telo (Certification Authority - CA), koje izdaje elektronske sertifikate korisnicima aplikacionog dodatka EPCM za Microsoft Word 2007. Elektronskim sertifikatima korisnici vrše elektronsko potpisivanje Word 2007 dokumenata.

Standard Svetskog poštanskog saveza koji definiše tehničku specifikaciju EPCM servera ima oznaku **S43**, a njegov naziv je "**Secure Electronic Postal Services (SEPS) Interface Specification**" (prethodni naziv je bio "Electronic PostMark (EPM) Interface Specification"). Poslednja verzija standarda **S43** je **S43-3** [1] koja je odobrena 23.4.2007. godine. Standard **S43** je tesno povezan sa sledeća dva standarda Svetskog poštanskog saveza:

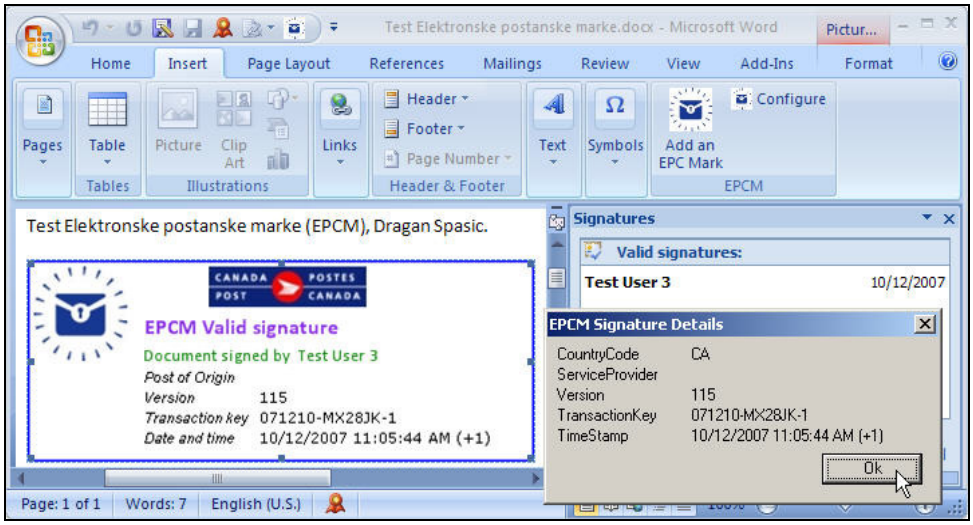
- UPU standard **S33**: "Interoperability Framework for Postal Public Key Infrastructures" [2].
- UPU standard **S39**: "Trusted Time Stamp" [3].

Tehnička specifikacija Yellow Pages servera data je u dokumentu "EPCM - Yellow Pages, Functional and technical specifications" [4], čija poslednja verzija od 19.5.2008.

Tehnička specifikacija EPCM klijenta, tj. aplikacionog dodatka (plug-in) EPCM za Microsoft Word 2007, data je u dokumentu "DPM in the Office 12 Signature Services Framework, Technical analysis and specifications" [5]. DPM je skraćenica od reči "Digital PostMark", što je bio prethodni naziv za Elektonsku poštansku marku (EPCM). Komercijalni naziv za paket aplikacija za kancelarijsko poslovanje Microsoft Office 12, je Microsoft Office 2007, a u okviru njega postoji Microsoft Word 2007.



Slika 3. EPCM infrastruktura sa istaknutim funkcionalnostima "Verify", "Postmark" i "Retrieve Postal Attributes"

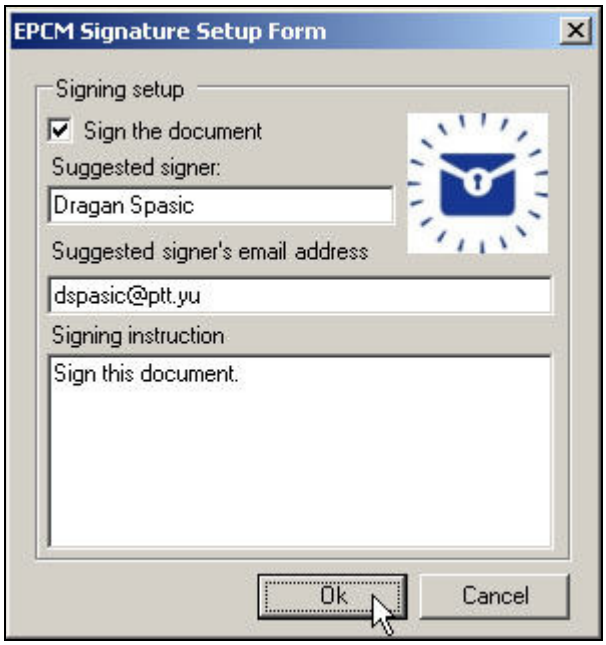


Slika 4. Elektronski potpisan i vremenski žigosan Microsoft Word 2007 dokument korišćenjem aplikacionog dodatka EPCM (EPC Mark)

3. Elektronsko potpisivanje i vremensko žigosanje dokumenta

Postupak elektronskog potpisivanja i vremenskog žigosanja Microsoft Word 2007 dokumenta je sledeći:

1. Otvoriti aplikaciju Microsoft Word 2007, napisati željeni tekst i snimiti dokument.
2. U okviru menija Insert na EPCM površini pritisnuti dugme "Add an EPC Mark" (slika 4.).
3. Na formi "EPCM Signature Setup Form" čekirati opciju "Sign the document", uneti podatke potpisnika i pritisnuti dugme "OK" (slika 5.), posle čega se u dokumentu kreira EPCM grafički okvir za potpis.
4. Uraditi dvostruki klik na EPCM grafički okvir za potpis.
5. Na formi "Add an EPCM" izabrati elektronski sertifikat potpisnika i pritisnuti dugme "OK" (slika 6.).
6. Uneti lozinku tajnog kriptografskog ključa potpisnika.
7. Na formi "Signature applied" pritisnuti dugme "OK", čime se završava postupak elektronskog potpisivanja i vremenskog žigosanja. Tada EPCM grafički okvir ima izgled kao na slici 7.



Slika 5. Forma "EPCM Signature Setup Form" sa podacima o potpisniku

Slika 6. Forma "Add an EPCM" sa izabranim sertifikatom potpisnika

Slika 7. EPCM grafički okvir posle elektronskog potpisivanja i vremenskog žigosanja

Na EPCM grafičkom okviru (slika 7.) prikazani su sledeći podaci:

1. EPCM logo i logo Pošte čiji je EPCM server izdao vremenski žigosanu potvrdu (PostMarkedReceipt).

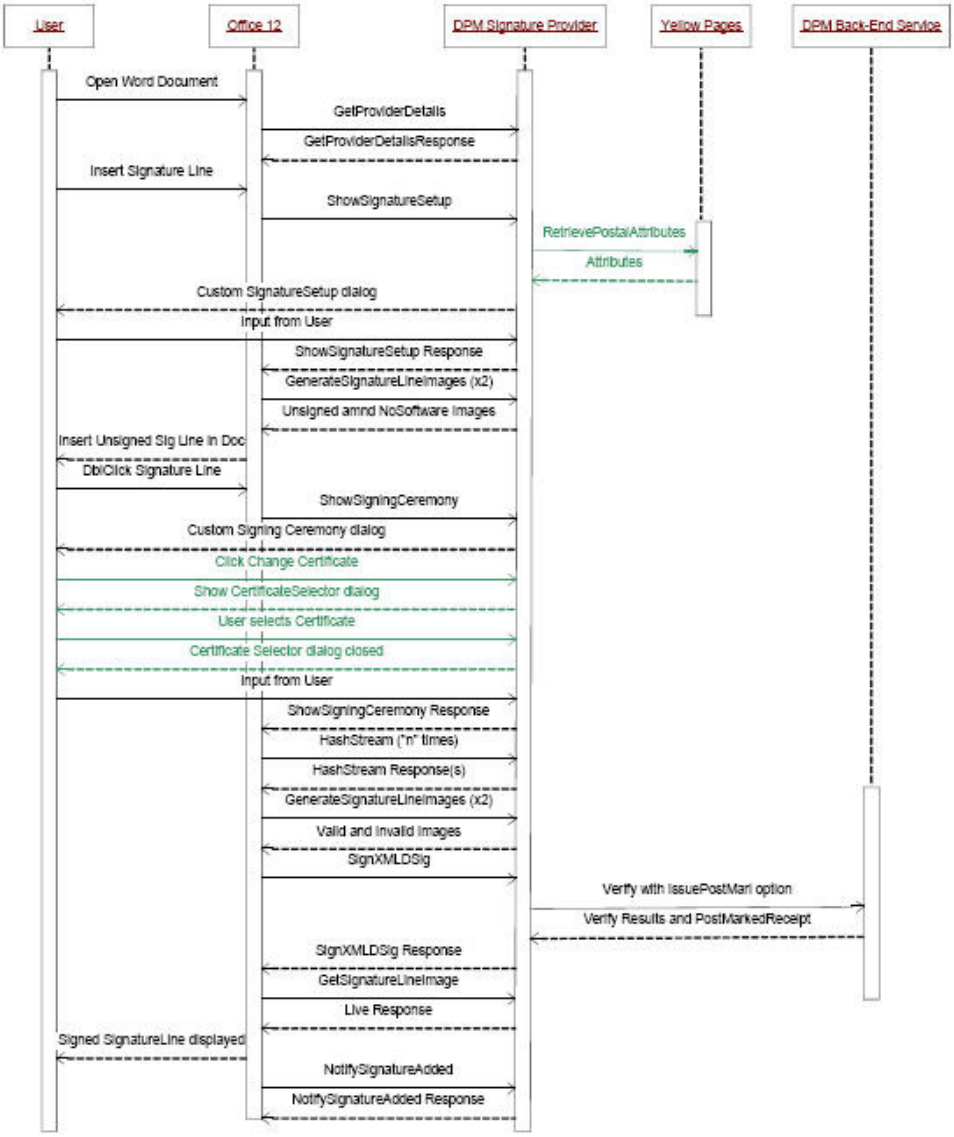
2. Poruka o statusu elektronskog potpisivanja i vremenskog žigosanja (na primer: "**EPCM Valid signature**").
3. Ime i prezime korisnika koji je elektronski potpisao dokument. Ukoliko dokument nije elektronski potpisan od strane korisnika već je samo vremenski žigosan, tada postoji poruka "Document only with EPCM".
4. Naziv Pošte čiji je EPCM server izdao vremenski žigosanu potvrdu.
5. Verzija EPCM servera.
6. Transakcioni ključ dobijen od EPCM servera.
7. Datum i vreme vremenskog žigosanja.

Celokupni tok komunikacije prilikom elektronskog potpisivanja i vremenskog žigosanja Microsoft Word 2007 dokumenta, između korisnika (potpisnika), Microsoft Word 2007 (Office 12), aplikacionog dodatka EPCM (DPM Signature Provider), Yellow Pages servera i EPCM servera, prikazan je na slici 8.

4. Verifikovanje elektronski potpisanog i vremenski žigosanog dokumenta (*on-line* i *off-line*)

Verifikovanje elektronski potpisanog i vremenski žigosanog Microsoft Word 2007 dokumenta, kada postoji konekcija ka EPCM serveru (*on-line* verifikacija) i kada ne postoji konekcija ka EPCM serveru (*off-line* verifikacija), sprovodi se automatski kada se otvori dokument. Ukoliko postoji konekcija ka EPCM serveru, aplikacioni dodatak EPCM iz dokumenta izdvaja vremenski žigosanu potvrdu (PostMarkedReceipt) i šalje je ka EPCM serveru, koji proverava da li je elektronski potpis vremenski žigosane potvrde (PostMarkedReceiptSignature) ispravan. Ukoliko je elektronski potpis ispravan, u dokumentu se na EPCM grafičkom okviru dobija poruka "**EPCM Valid signature**" (slika 7.), a ako elektronski potpis nije ispravan (na primer: narušen je integritet dokumenta), dobija se poruka "**EPCM Not valid signature!**" (slika 9.).

Ukoliko ne postoji konekcija ka EPCM serveru, moguće je da se izvrši *off-line* verifikovanje elektronski potpisanog i vremenski žigosanog dokumenta, a to sprovodi aplikacioni dodatak EPCM. Ako keš aplikacionog dodatka EPCM sadrži sertifikat EPCM servera koji je izdao vremenski žigosanu potvrdu (PostMarkedReceipt) i ako je keš u okviru roka važnosti u trenutku verifikovanja potpisa, a elektronski potpis je ispravan, u dokumentu se na EPCM grafičkom okviru dobija poruka "**EPCM Valid signature (offline - certificate)**". U svim ostalim slučajevima, ako je elektronski potpis ispravan, na EPCM grafičkom okviru se dobija poruka "**EPCM Valid signature (offline only crypt)**". Ako elektronski potpis nije ispravan (na primer: narušen je integritet dokumenta), dobija se poruka "**EPCM Not valid signature!**" (slika 9.). U slučaju da korisnik ne želi da sprovede *off-line* verifikovanje, dobija se poruka "**Error contacting EPCM Server**" (slika 10.).



Slika 8. Dijagram toka elektronskog potpisivanja i vremenskog žigosanja dokumenta [5]

Slika 9. EPCM grafički okvir kada elektronski potpis nije ispravan

Slika 10. EPCM grafički okvir kada ne postoji konekcija ka EPCM serveru i korisnik ne želi da sprovede off-line verifikovanje

Literatura

[1] "Secure electronic postal services (SEPS) interface specification", S43-3, UPU status 1, version approved 23 April 2007.
[2] "Interoperability Framework for Postal Public Key Infrastructures", S33, UPU.
[3] "Trusted Time Stamp", S39, UPU.
[4] "EPCM - Yellow Pages, Functional and technical specifications", UPU, version approved 19 May 2008.
[5] "DPM in the Office 12 Signature Services Framework, Technical analysis and specifications", Prepared by Poste Italiane SpA, Version 1.0.

Abstract: *The Universal Postal Union (UPU) has developed EPCM (Electronic Postal Certification Mark) plug-in software for Microsoft Word 2007 that can connect to any EPCM server that is compliant to the UPU Standard S43 "Secured Electronic Postal Services Interface Specification" and receive a postal electronic certification mark on a Microsoft Word 2007 document. This postal electronic certification mark on electronic document provides the guarantee of the integrity of electronic document, data of signer, non-repudiation, and date and time postmarking (stamping) of electronic document.*

Key words: *Universal Postal Union, Electronic Postal Certification Mark, electronic signature, time stamp.*

THE ELECTRONIC POSTAL CERTIFICATION MARK OF THE UNIVERSAL POSTAL UNION

Dragan Spasić