TEHNIKA I INFORMATIKA U OBRAZOVANJU
3. Internacionalna Konferencija, Tehnički fakultet Čačak, 7–9. maj 2010.
TECHNICS AND INFORMATICS IN EDUCATION
3rd International Conference, Technical Faculty Čačak, 7–9th May 2010.

UDK: 37:004.738.5 Pregledni stručni rad

ZAŠTITA PODATAKA NA INTERNETU PRIMENOM DIGITALNOG SERTIFIKATA

Danijela Jovanović [1], Branko Marković [2]

***Rezime**: U ovom radu opisani su principi i protokoli kako da se informacije prenošene preko Interneta zaštite korišćenjem digitalnog sertifikata. Razvoj računarskih mreža, a posebno nastanak i razvoj Interneta proširio je mogućnosti za prenos podataka. Ali oni su često i meta hakera. Zbog toga su razvijene različite tehnike kako da se informacije zaštite. Ovde se objašnjava jedan od najsavremenijih metoda ove zaštite.*

***Ključne reči:** Internet, zaštita podataka, enkripcija, javni ključ, tajni ključ, digitalni sertifikat.*

DATA PROTECTION OVER THE INTERNET USING A DIGITAL CERTIFICATE

***Summary**: This paper explains the principles and protocols how to protect information over the Internet by using a digital certificate. Development of networks, especially with beginnig and development of the Internet, gives new abilities for data transfer. The information is often goal of hackers. Therefore different techniques are developed in order to protect data. Here is given one of up-to-date method how to protect data.*

***Key words:** Internet, data protection, encryption, public key, security key, digital certificate.*

1. UVOD

U početku, sa nastankom računarskih mreža one su bile privatne i količina informacija koja se razmenjivala bila je skromna. Ali sa razvojem Interneta i njegovih servisa broj korisnika, a samim tim i broj različitih transakcija rastao je geometrijskom progresijom. Tako da danas, kada milioni ljudi koriste mreže za bankarske transakcije, za kupovanje ili za popunjavanje poreskih prijava, bezbednost na mreži počinje da predstavlja veliki problem. Većinu bezbednosnih problema namerno izazivaju određene osobe koje na taj način žele da ostvare neku dobit, da privuku pažnju ili da nekome naude. Internet je otvorena javna mreža dostupna svima tako da postoji mogućnost da neko neovlašćeno prati vašu komunikaciju i to kasnije zloupotrebi.

[1] Danijela Jovanović, VŠTSS, Svetog Save 65, Čačak, E-mail: jovanovic.danijela1@gmail.com
[2] Branko Marković, VŠTSS, Svetog Save 65, Čačak, E-mail: branko333@nadlanu.com

Zbog toga se u cilju ozbiljne primene Interneta u savremenom poslovanju mora pronaći mehanizam koji će obezbediti:
1. Zaštitu tajnosti informacija (sprečavanje otkrivanja njihovog sadržaja)
2. Integritet informacija (sprečavanje neovlašćene izmene informacija)
3. Autentičnost informacija (definisanje i provera identiteta pošiljaoca)

Kriptografija kao nauka koja se bavi metodama očuvanja tajnosti informacija pruža rešenje za ove probleme. Digitalni sertifikat predstavlja jedan od najpouzdanijih načina zaštite.

2. VRSTE ZAŠTITE

U visokom obrazovanju studenti se upoznaju sa predmetom Internet tehnologije. Susreću se sa informacijama koje se obrađuju, prenose i čuvaju u elektronskoj formi. U velikim komunikacionim i kompjuterskim mrežama, kao što je Internet, informacije mogu biti izložene različitim oblicima zloupotrebe. Da bi se to sprečilo, studenti treba da se upoznaju sa principima zaštite prenošenih podataka.

Bezbednosni problemi se mogu svrstati u 4 kategorije: **tajnost, proveru identiteta, nemogućnost poricanja i kontrolu integriteta.**
Tajnost zvana i poverljivost, vodi računa o tome da informacije ne dospeju u ruke neovlašćenih osoba. To je prva stvar na koju se pomisli kada se pomene bezbednost na mreži. Proverom identiteta treba da se utvrdi sa kim se razgovara, pre nego što se otkriju poverljive informacije ili preduzme poslovni poduhvat. Nemogućnost poricanja se svodi na potpisivanje. Integritet podrazumeva da informacija nije promenjena na putu do odredišta.

Izraz **kriptografija** potiče iz grčkog jezika i znači «tajno pisanje». Kriptografske tehnike obezbeđuju sredstva koja osiguravaju tajnost i integritet, kao i druga srodna svojstva vezana za očuvanje sigurnosti informacija. Predstavlja način kojim se razumljivi tekst prevodi u nerazumljivi, šifrovani tekst. **Kriptovanje** se svodi na upotrebu matematičkih algoritama za pretvaranja razumljivog elektronskog materijala pomoću nekog ključa u nerazumljiv materijal.

Važi: **C=E(P,KE)**, gde je **P** razumljivi tekst, **KE** ključ kriptovanja, **E** funkcija kriptovanja, a **C** dobijeni kriptovani tekst.
Dekriptovnje je obrnuti proces, dobijanje razumljivog iz kriptovanog teksta
Važi: **P=D(C,KD)**, gde je **KD** ključ za dekriptovanje, **D** funkcija dekriptovanja.
Pod pojmom ključa podrazumeva se kratak tekstualni niz kojim se bira jedan od više mogućih načina šifrovanja i može se menjati kad god je to potrebno.

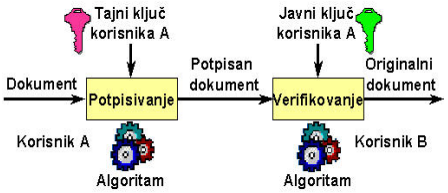
2.1 Sistemi šifrovanja

Metod šifrovanja **tajnim ključem** (simetrično šifrovanje) podrazumeva šifarski sistem kod koga je ključ za šifrovanje identičan ključu za dešifrovanje. Što znači da i pošiljalac i primalac poruke koriste isti tajni ključ.

Kod metoda šifrovanja **javnim ključem** (asimetrično šifrovanje) svaki učesnik u komunikaciji koristi dva ključa. Jedan ključ je javni i može se slobodno distribuirati, dok je drugi tajni i dostupan je samo njegovom vlasniku. Iako su različiti, ključevi su međusobno povezani određenim transformacijama. Poznavanje jednog ključa i algoritma transformacije ne omogućava dobijanje drugog ključa. Najbitnije je da se tajni ključ u celom postupku komunikacije nigde ne šalje jer ne postoji potreba da bilo ko sem njegovog vlasnika bude upoznat sa njim.

2.2 Digitalni potpis

Pošto se u elektronskoj komunikaciji javila potreba za prenošenjem poruka, morala se pronaći tehnika koja će biti digitalni pandan svojeručnog potpisa, a to je digitalni potpis. Digitalni potpis je matematički algoritam koji osigurava da je data informacija potekla od datog entiteta. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da obezbedi garantovanje identiteta pošiljaoca poruke.



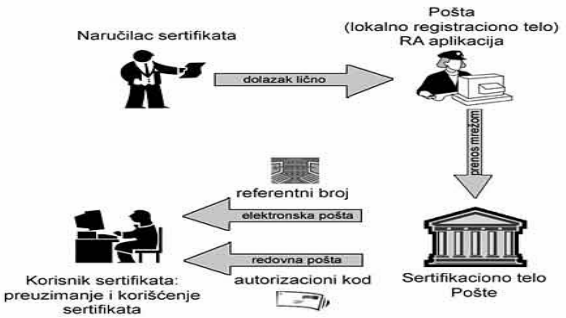
Slika 1:*Tehnologija digitalnog potpisa*

Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljalac primenom odredjenih kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (npr. 512 ili 1024 bita) koji u potpunosti oslikava sadržaj poruke. To praktično znači da svaka promena u sadržaju poruke dovodi do promene potpisa. Ovako dobijen zapis on dalje šifruje svojim tajnim ključem i tako formira digitalni potpis koje se šalje zajedno sa porukom.

I pored velike sigurnosti koje pruža ovaj metod zaštite, i dalje postoji mogućnost prevare. Neko je mogao poslati svoj javni ključ tvrdeći da je nekog drugog lica, a zatim slati poruke za koje se misli da je neko drugi pošiljalac. Rešenje ovog problema pruža upotreba digitalnih sertifikata. To je elektronski dokument, koji identifikuje računar, osobu, preduzeće ili sertifikatora.

3. DIGITALNI SERTIFIKAT U SLUŽBI ZAŠTITE

Ako se koristi sistem šifrovanja javnim ključem i želi nekome poslati poruka, mora se prvo dobiti njegov javni ključ. Za to se koristi **digitalni sertifikat** (često se naziva i digitalnom ličnom kartom). Kompanija koje imaju ulogu da provere i utvrde nečiji identitet i nakon toga mu izda digitalni sertifikat je **CA (Certificate Authority)**.



Slika2. *Princip izdavanja sertifikata*

Digitalni sertifikat izdat od strane CA mora da sadrži ime ili identifikaciju vlasnika sertifikata, njegov javni ključ, period valjanosti sertifikata i digitalni potpis izdavača sertifikata. Svi ovi podaci formiraju sertifikat koji se na kraju šifruje koristeći tajni ključ CA. Ako korisnik ima poverenja u CA i ima CA javni ključ, može biti siguran u ispravnost sertifikata.

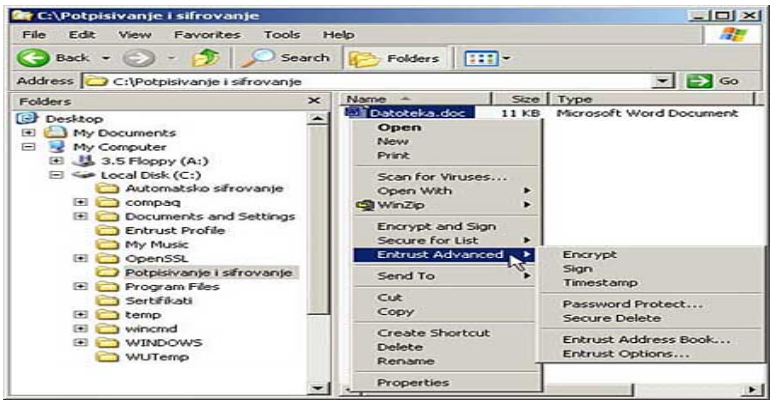
U ovom trenutku, **PTT Srbija** tj. **Sertifikaciono telo Pošte** (http://www.cepp.co.yu/ca) je prvo i jedino javno sertifikaciono telo u Republici Srbiji. Delatnost javnih sertifikacionih tela u Srbiji je uređena Zakonom o elektronskom potpisu ("Službeni glasnik Republike Srbije", br. 135/2004) i podzakonskim aktima ("Sl. glasnik RS", br. 48/2005, 82/2005, 116/2005). U Srbiji postoje interna sertifikaciona tela u nekim kompanijama, i to najčešće u bankama.

Sertifikaciono telo Pošte izdaje sledeće četiri kategorije digitalnih sertifikata:

1. Web sertifikat
2. SID Enterprise sertifikat (Single application ID),
3. MID Enterprise sertifikat (Multiple Application ID),
4. SER sertifikate 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, Excel, PowerPoint 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. Postoji kompatibilnost sa Microsoft CryptoAPI. Korisnička aplikacija **Entrust Entelligence** se isporučuje uz svaki SID i MID Enterprise sertifikat i ona omogućava (Slika 3) preuzimanje i obnavljanje SID i MID Enterprise sertifikata, pregled sadržaja sertifikata i eksportovanje sertifikata u datoteke različitih formata. Takođe i šifrovanje/dešifrovanje datoteka i potpisivanje/verifikovanje potpisanih datoteka.



Slika 3**:Opcije korisničke aplikacije **Entrust Entelligence

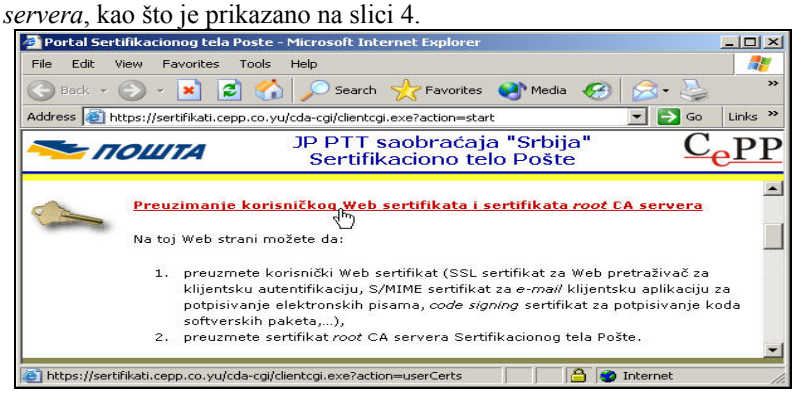
Razlika između SID(Single application ID) i MID(Multiple application ID) Enterprise sertifikata je što SID Enterprise sertifikat poseduje licencu za korišćenje sertifikata sa samo

jednom aplikacijom ili aplikacionim dodatkom (plug-in), a MID Enterprise sertifikat poseduje licencu za korišćenje sertifikata sa neograničenim brojem aplikacija.

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.

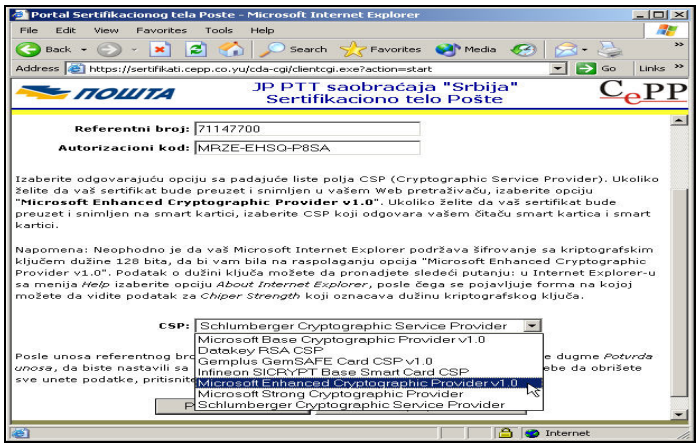
4. PRIMER PRIMENE DIGITALNOG SERTIFIKATA

Pre preuzimanja Web sertifikata, korisnik mora da poseduje **referentni broj** (Reference number) i **autorizacioni kod** (Authorization code) koje je dobio od Sertifikacionog tela Pošte i mora da ima na računaru instalisan **Microsoft Internet Explorer 5.0 ili noviji** .
Preuzimanje Web sertifikata se vrši posredstvom Portala za preuzimanje i pretraživanje sertifikata Sertifikacionog tela Pošte, koji se nalazi na adresi: https://sertifikati.cepp.co.yu/cda-cgi/clientcgi.exe?action=start
Posle toga, pristupa se Portalu za preuzimanje i pretraživanje sertifikata Sertifikacionog tela Pošte, gde je potrebno izabrati opciju *Preuzimanje korisničkog Web sertifikata i sertifikata root CA servera*, kao što je prikazano na slici 4.



Slika 4: *Portal za preuzimanje i pretraživanje sertifikata Sertifikacionog tela Pošte*

Zatim će se pojaviti Web strana na kojoj je potrebno izabrati opciju *Preuzimanje korisničkog Web sertifikata*. Potom se pristupa Web strani za preuzimanje korisničkog Web sertifikata (slika 5). Na ovoj strani potrebno je uneti referentni broj i autorizacioni kod u odgovarajuća polja. Osim toga, neophodno je sa padajuće liste polja CSP (Cryptographic Service Provider) izabrati opciju "**Microsoft Enhanced Cryptographic Provider v1.0**", ukoliko se Web sertifikat snima (importuje) u skladište sertifikata Microsoft Internet Explorer-a (Microsoft CryptoAPI store).



Slika 5: *Web strana za preuzimanje korisničkog Web sertifikata*

Neophodno je da Microsoft Internet Explorer podržava šifrovanje sa kriptografskim ključem dužine 128 bita, da bi postojala CSP opcija ***"Microsoft Enhanced Cryptographic Provider v1.0"***.

Nije preporučljivo da se sa padajuće liste polja CSP (Cryptographic Service Provider) izabere opcija "**Microsoft Base Cryptographic Provider v1.0**", umesto opcije "**Microsoft Enhanced Cryptographic Provider v1.0**", zbog sledeća dva razloga:

1. Dužina RSA kriptografskih ključeva u slučaju Microsoft Enhanced CSP je 1024 bita, a u slučaju Microsoft Base CSP je 512 bita. To znači, da ukoliko se izabere opcija "**Microsoft Enhanced Cryptographic Provider v1.0**", kao što je prikazano na slici 4., na računaru korisnika će se izgenerisati par RSA kriptografskih ključeva (javni i tajni) dužine 1024 bita, a u preuzetom Web sertifikatu će se nalaziti javni RSA kriptografski ključ dužine 1024 bita. Ukoliko se izabere opcija "**Microsoft Base Cryptographic Provider v1.0**", na računaru korisnika će se izgenerisati par RSA kriptografskih ključeva (javni i tajni) dužine 512 bita, a u preuzetom Web sertifikatu će se nalaziti javni RSA kriptografski ključ dužine 512 bita.
2. Rok važnosti preuzetog Web sertifikata u slučaju Microsoft Enhanced CSP je 5 godina, a u slučaju Microsoft Base CSP je 1 godina.

Postoji mogućnost da se Web sertifikat snimi (importuje) na smart karticu (na primer: Datakey Intelligence Model 330 PKI Smart Card) ili USB token (na primer: Rainbow iKey 2032) izborom odgovarajuće opcije sa padajuće liste polja CSP. Na primer, u slučaju snimanja (importovanja) Web sertifikata na Datakey smart karticu ili Rainbow USB token, neophodno je sa padajuće liste polja CSP (Cryptographic Service Provider) izabrati opciju "Datakey RSA CSP".

Posle izabrane opcije "**Microsoft Enhanced Cryptographic Provider v1.0**", potrebno je na istom prozoru pritisnuti dugme *Potvrda unosa.* Zatim se pojavljuje forma sa obaveštenjem(«Do you want to request a certificate now?»). Potrebno je pritisnuti dugme *Yes*.

Zatim se pojavljuje forma koja je prikazana na slici 6. Korisniku se pruža mogućnost da pritiskom na dugme *Set Security Level...* izabere željeni nivo zaštite tajnog (privatnog) kriptografskog ključa: *High* ili *Medium*.

Ukoliko korisnik izabere *High* nivo zaštite tajnog (privatnog) kriptografskog ključa, mora da zapamti *password* koji će se kasnije uneti, i koji je neophodan da bi mogao da koristi

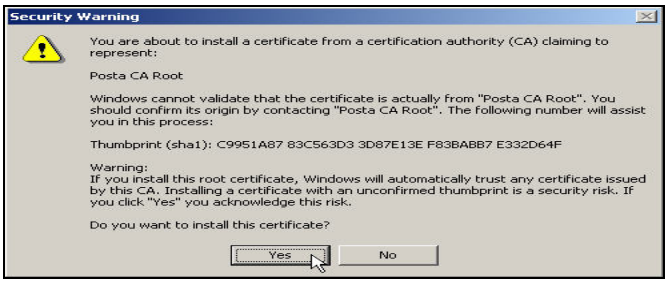
pomenuti ključ, jer će pre svakog korišćenja ključa morati da unese *password* ključa. To znači, da ukoliko korisnik zaboravi *password* neće moći da koristi tajni (privatni) kriptografski ključ, a preuzeti Web sertifikat biće neupotrebljiv.
Ukoliko korisnik izabere *Medium* nivo zaštite tajnog (privatnog) kriptografskog ključa, od korisnika se neće tražiti da unese *password* prilikom korišćenja pomenutog ključa.
S obzirom na to da je poželjno koristiti *High* nivo zaštite tajnog (privatnog) kriptografskog ključa, za nastavak je potrebno pritisnuti dugme *Set Security Level...* na formi sa slike 6 i izabrati opciju *High*.

Slika 6: *Generisanje tajnog (privatnog) kriptografskog ključa i izbor nivoa zaštite ključa*

Posle izbora opcije *High* potrebno je pritisnuti dugme *Next* za nastavak. Zatim se pojavljuje forma za unos *password*-a (slika 7). U polja *Password:* i *Confirm:* potrebno je uneti željeni *password*, kao što je prikazano na slici 7. Za nastavak je potrebno pritisnuti dugme *Finish*.

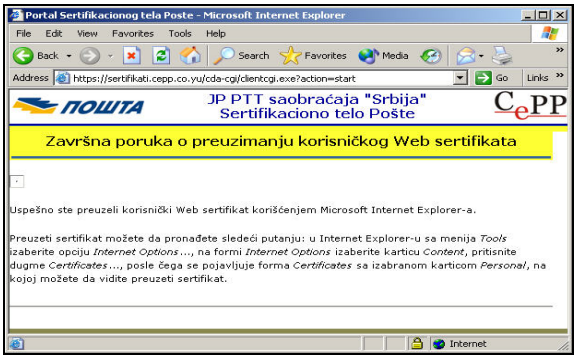
Slika 7: *Izbor password-a tajnog (privatnog) kriptografskog ključa*

Posle toga, pojaviće se nova forma na kojoj je potrebno pritisnuti dugme *OK*.
Ukoliko se pojavi sledeća poruka sa greškom: "**Internal error: (-2628) Undefined Entrust/Authority Error**", to znači da je istekao rok važnosti autorizacionog koda. U tom slučaju, nemoguće je nastaviti sa procesom preuzimanja Web sertifikata sa postojećim autorizacionim kodom. Preuzimanje Web sertifikata može da se uradi isključivo sa novim autorizacionim kodom, koji može da se dobije od Sertifikacionog tela Pošte.
Otvara se nova forma sa obaveštenjem. Potrebno je pritisnuti dugme *Yes*. Zatim se pojavljuje forma sa podacima o sertifikatu *root* CA servera Sertifikacionog tela Pošte ("Posta CA Root") koja je prikazana na slici 8. Potrebno je pritisnuti dugme *Yes*.



Slika 8: *Forma sa podacima o sertifikatu root CA servera Sertifikacionog tela Pošte*

Zatim se pojavljuje nova forma sa obaveštenjem. Potrebno je pritisnuti dugme *Yes*.
Na kraju, posle uspešnog preuzimanja korisničkog Web sertifikata, pojavljuje se poruka koja je prikazana na slici 9.



Slika 9: *Poruka o uspešnom preuzimanju korisničkog Web sertifikata*

5. ZAKLJUČAK

Može se zaključiti da je digitalni sertifikat elektronski dokument kojim se potvrđuje veza između podataka i potpisa, to jest njihova verodostojnost, a sam dokument sa digitalnim potpisom ne može da se menja. Oblasti primene ovako potpisanih dokumenata su različite: od e-poslovanja, e-trgovine i e-bankarstva, do e-uprave, e-zdravstva itd.
U ovom radu pokazano je postupno kako da se primeni digitalni sertifikat i kako da se instalira tj. preuzme od sertifikacionog tela (PTT Srbija tj. Sertifikaciono telo Pošte). Implementacija je objašnjena u Windows okruženju korišćenjem Microsoft Internet Explorer-a 5.0. Da bi se u većoj meri ova zaštita primenila potrebno je da se implementiraju odgovarajući zakoni kao i da se razvije odgovarajuća infrastruktura i obrazuju kadrovi.

6. LITERATURA

[1] Mrež@, časopis o digitalnim komunikacijama i naprednim operativnim sustavima, siječan-veljača, br.1-2, godina 2001.
[2] Čerić, Varga, Birolla (ed.), Poslovno računalstvo, ZNAK, Zagreb, 1996.
[3] Grundler, D., Primijenjeno računalstvo, Graphis, Zagreb, 2000.
[4] Pošta, 2010.: http://www.cepp.co.rs 29. 03. 2010.