NOVI ZAKON O ELEKTRONSKOM POTPISU U REPUBLICI SRPSKOJ

NEW LOW OF THE DIGITAL SIGNATURE IN REPUBLIC OF SRPSKA

Dr Srđan Damjanović, docent
Fakultet spoljne trgovine Bijeljina

Rezime: Kada se podaci obrađuju, prenose i čuvaju u elektronskoj formi postaju izloženi čitanju, kopiranju i neautorizovanoj promjeni. Kriptografija se bavi metodama očuvanja tajnosti informacija. Primjenom kriptografije realizuju se četiri osnovna bezbjedonosna zahtjeva: tajnost, integritet, autentičnost i neporecivost. Elektronski potpis je nastao kao pandan svojeručnom potpisu na papirnom dokumentu. Svrha elektronskog potpisa je da potvrdi autentičnost sadržaja poruke, kao i da obezbijedi garantovanje identiteta pošiljaoca poruke. Osnovu elektronskog potpisa čini sadržaj same poruke. Zakonodavne vlasti mnogih zemalja, koje teže promovisanju e-trgovine i e-uprave, dale su prioritet donošenju zakona koji stvaraju pravnu osnovu za korišćenje i prihvatanje elektonskog potpisa. U Republici Srpskoj zakon o elektronskom poslovanju i elektronskom potpisu donesen je 2002. godine, ali je ovaj zakon izmijenjen 2008. godine i to samo u dijelu koji se odnosi na elektronski potpis. To je bio jedan dobar preduslov za ulazak stranih banaka na tržište Republike Srpske, kao i za povećanje obima elektronskog poslovanja.

Ključne riječi: elektronski potpis, podatak, zaštita, zakon, elektronsko poslovanje

Abstract: When the information is transferred, analyzed, and stored in electronic data, it could be exposed to misuse, copies, and unauthorized changes. Cryptography, the art of writing or deciphering messages in code by protecting authenticity of the stored information has four main ways of regulation; secrecy, integrity, authenticity and irrefutability. An digital signature is equivalent to a hand made signature. Purpose of a digital signature is to confirm authenticity of the message on the document. The government and law makers in many advanced countries are promoting electronic commerce and electronic governing as a priority, and the easiest and most rapid form of communication. In the Republic of Srpska the law of the electronic business and digital signature was adopted in 2002, but amended in 2008 regarding digital signature. That was the prerequisite for allowing foreign investors and banks to enter our market and develop the electronic business.

Key words: digital signature, data, protection, low, electronic business.

UVOD U KRIPTOGRAFIJU

Julije Cezar nije vjerovao kuririma kada je slao poruke preko njih svojim generalima. Zato je on u porukama svako slovo A zamjenio sa D, svako slovo B sa E,… Samo ona osoba koja je znala pravilo "pomereno za tri" mogla je da razumije sadržaj poruke. Tako je sve počelo…

U modernoj “eri informatike“, kada se podaci obrađuju, prenose i čuvaju u elektronskoj formi, informacije postaju izložene čitanju, kopiranju i neautorizovanoj promjeni. Savremene računarske mreže se, u velikoj mjeri, zasnivaju na Internet tehnologijama. Slabosti koje su uočene u arhitekturi mreža Internet tipa sa aspekta bezbjednosti, su protokoli na kojima se Internet zasniva. Protokoli nisu projektovani da zadovolje zahtjeve za zaštitom informacija koje se preko njih prenose. Rješenje ovog problema donekle pruža kriptologija, nauka koja razmatra različite aspekte obezbjeđivanja tajnosti informacija.

Kriptologija je termin koji potiče od grčkih rijeći kriptos (skriven, tajan) i logos (nauka), i označava naučnu disciplinu koja se bavi sigurnim (tajnim) komunikacijama. Dvije osnovne, tijesno povezane grane kriptologije su: kriptografija i kriptoanaliza. Predmet kriptografije je, prije svega, sinteza postupaka za obezbjeđivanje tajnosti informacija, tzv.kriptozaštitu informacija. Kriptografija, kao nauka, se bavi metodama očuvanja tajnosti informacija. Predmet kriptoanalize je razmatranje metoda kojim se kompromituju ("razbijaju" od strane neovlašćenih korisnika) postupci kripto-zaštite informacije.
Primjenom kriptografije realizuju se četiri osnovna bezbjedonosna zahtjeva:

- **tajnost** – obezbjeđuje da informacioni sadržaj poruke bude dostupan samo ovlašćenim korisnicima,
- **integritet** – obezbjeđuje **otkrivanje** neovlašćene izmjene informacionog sadržaja poruke,
- **autentičnost** – omogućava provjeru identiteta učesnika u komunikaciji,

- **neporecivost** – sprečava mogućnost poricanja realizacije određenih aktivnosti učesnika u komunikaciji (kao što su slanje poruke, transakcija i dr.).

Kroz istoriju kriptografija se razvijala i koristila kao alat u zaštiti informacija, naročito u vojnim, diplomatskim i državnim komunikacijama uopšte. Imala je dugu i fascinantnu istoriju uspona i padova dosežući čak i do odlučujućih uloga u ishodima ratova. Najbolji primer za to je dešifrovanje Nemačke Enigma mašine u Drugom svetskom ratu.

Javni interes za kriptografiju u elektronskoj komunikaciji dramatično je porastao uvođenjem tzv. kriptografije javnih ključeva 1976 godine, tj. asimetičnih algoritama za očuvanje bezbjednosti informacija, čime se dobila mogućnost postizanja tajnosti informacija bez prethodne razmene tajnog ključa putem sigurnog komunikacionog kanala.

Kriptografske tehnike obezbjeđuju sredstva koja osiguravaju tajnost i inegritet, kao i druga srodna svojstva vezana za očuvanje sigurnosti informacija. Vremenom, komercijalne i civilne kriptografske aplikacije su napredovale od aplikacija klasičnih komunikacionih sistema kao što su kablovska telefonija, telegrafija, televizija i bežične komunikacije, do aplikacija vezanih za mobilnu bežičnu telefoniju i različitie servise na integrisanim komunikacionim mrežama (kao što je Internet). Danas su kriptografske aplikacije vezane i za elektronske medicinske datoteke, elektronsku razmenu podataka, elektronsko bankarstvo i trgovinu, uključujući tzv. smart ("pametne") kartice i elektronski novac. To zaista nepregledno područje, odnosno skoro kompletna aktivnost najznačajnijih svijetskih tokova, nužno zahtjeva bezbjednost informacija**.**
Kada se govori o bezbjednosti informacija misli se, između ostalog, na očuvanje tajnosti, tj. povjerljivosti i očuvanje integriteta podataka.

Tajnost podataka je svojstvo da se podaci mogu čitati samo od strane autorizovanih korisnika. Brojni su načini da se obezbjedi tajnost, počev od fizičke zaštite, pa sve do matematičkih algoritama koji sadržaj informacija čine nerazumljivim, šifrovanim. Potrebno je informaciju (poruku) transformisati (jedinstveno) da bi se dobio šifrovani tekst poruke. Da bi se to ostvarilo potrebno je raspolagati sa ključevima, koji upravo svaki za sebe definiše tu jedinstvenu transformaciju skupa poruka u skup šifrata. Ta transformacija mora da bude obostrano jednoznačna, jer je neophodno iz šifrovanog teksta dobiti originalnu poruku.

Integritet podataka je svojstvo koje obezbjeđuje detekciju neautorizovane promjene izvora podataka kao i samih podataka. Novi načini čuvanja, obrade i prenosa informacija donijeli su teškoću koja u klasičnom postupku nije ni približno imala takav značaj. Prekrajanje podataka koji se čuvaju u elektronskoj formi je moguće u takvoj mjeri, da bi se bez alata za očuvanje integriteta podataka bilo kakva ozbiljnija komunikacija mogla pokazati besmislena. Brojni su primeri za to počev od najjednostavnijih poruka (ali nimalo bezazlenih) tipa: Isplatiti osobi **A** $100, gde se može promijeniti i ime i valuta i iznos. Bilo kakva promijena teksta može da ima dalekosežne poslijedice i za pošiljaoca i za primaoca poruke.

ELEKTRONSKI POTPIS

Pošto se u elektronskoj komunikaciji javila potreba za prenošenjem poruka, morala se pronaći tehnika koja će biti digitalni pandan svojeručnog potpisa na papirnom dokumentu. Iz te potrebe je nastao elektronski ili digitalni potpis. Svrha elektronskog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promjenjena na putu od pošiljaoca do primaoca), kao i da obezbijedi garantovanje identiteta pošiljaoca poruke. Osnovu elektronskog potpisa čini sadržaj same poruke.
Elektronski potpis je 51-bitni broj koji se dobija primjenom RSA algoritma na HASH vrednost generisanu iz bloka podataka koji se štiti. Elektronski potpis i elektronski potpisani dokumenat se mogu izraziti formulom:

Elektronski potpis = E [H(m), SA]

Elektronski potpisani dokument = m; E [H(m), SA]
gdje su:

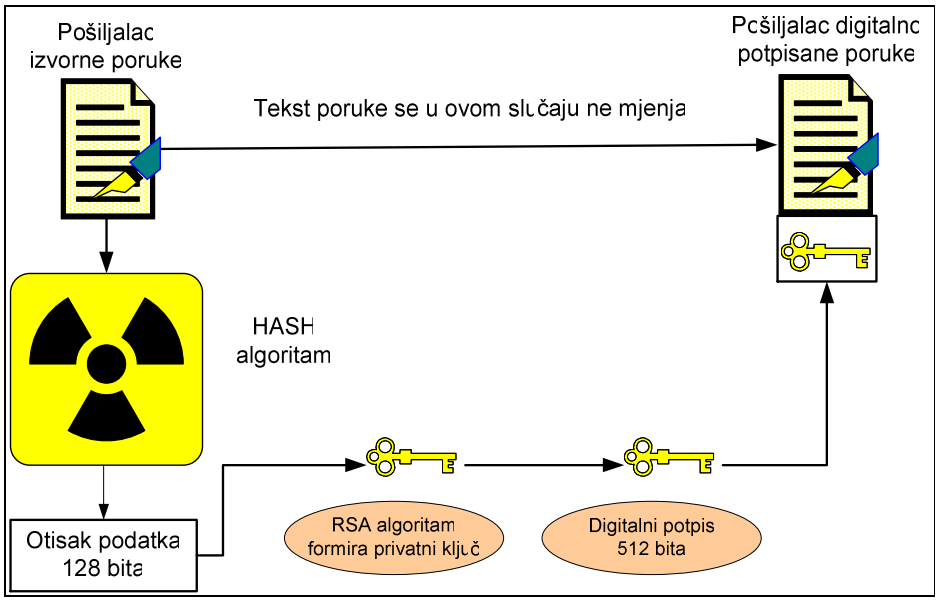
m - elektronski dokument koji se potpisuje,
H(m) - otisak elektronskog dokumenta, a H funkcija sažimanja,
SA – tajni (privatni) ključ potpisnika,

E - funkcija šifrovanja (asimetrično kriptovanje).

Postupak kreiranja elektronskog potpisa (prikazan na slici1.) se sastoji od dvije faze:

- u prvoj fazi se primenom odgovarajuće kriptografske kompresione funkcije (MD5 HASH) određuje otisak poruke,
- u drugoj fazi potpisnik poruke šifruje dobijeni otisak svojim tajnim (privatnim) ključem, primjenom odgovarajućeg asimetričnog algoritma (RSA). Šifrovani otisak poruke predstavlja njen elektronski potpis i pridružuje joj se.

Slika 1. Kreiranje digitalnog potpisa uz primjenu HASH i RSA algoritma



Da bi potpisao dokument, potpisnik mora jasno naznačiti granice dokumenta koji potpisuje. Za označenu poruku (podatak) koji treba sigurno prenijeti, HASH funkcija softvera potpisnika izračunava jedinstveni otisak, pridružen jedino toj poruci. HASH funkcija svaku poruku, svaki tekst (predmet šifrovanja) bez obzira na njegovu veličinu, bukvalno samelje (to joj i sam naziv kaže), kao u mašini, tako da na izlazu dobijemo niz od 128 nula i jedinica. Poznato je da takvih nizova ima 2^{128}, a koliko je to ogroman broj o tome ne treba trošiti riječi. Bitno je istaći da je računski nemoguće naći bilo koji ulaz čija je hash vrijednost unaprijed zadati izlaz, a takođe je računski nemoguće naći dva različita ulaza sa istom hash vrijednošću. Dakle kao što je teško, a možda i nemoguće, naći dva čoveka sa istim otiskom prsta tako bi i falsifikatoru bilo teško da nađe dvije poruke sa istom hash vrednošću. Vjerovatnoća da u poruci neko izmijeni neku stavku, tako da novodobiveni tekst ima istu hash vrednost kao i originalni je $1/2^{128}$=0.00000… , dakle zanemarljivo mala vjerovatnoća. Softver zatim transformiše otisak u elektronski potpis koristeći se potpisnikovim tajnim (privatnim) ključem. Tako nastali elektronski potpis je stoga jedinstven i za poruku i za privatni ključ koji ga je kreirao. Uobičajeno je da se elektronski potpis pridodaje poruci, skladišti i šalje zajedno s njom. Medutim, on se može poslati i kao odvojeni podatak, dokle god zadržava pouzdanu vezu s originalnom porukom. Kako je svaki potpis jedinstveno vezan uz original, besmisleno ga je u potpunosti odvojiti od izvora na osnovu kojeg je nastao.

Postupak verifikacije elektronskog postupka sastoji se od 3 faze:

- U prvoj fazi se iz dobijene poruke izdvaja elektronski potpis i dešifruje javnim ključem pošiljaoca.
- U drugoj fazi primalac kreira otisak informacionog dijela dobijene poruke identičnim postupkom kao na predajnoj strani.
- U trećoj fazi vrši se poređenje, i ako je dobijeni otisak poruke identičan sa dešifrovanim otiskom, verifikacija je uspješna.

Na osnovu iznesenog može se zaključiti da je za funkcionalnost elektronskog potpisa potrebno izvršiti dva procesa, od kojih jedan sprovodi potpisnik, a drugi primalac. Uspješnom provjerom elektronskog potpisa garantuje se:

- Autentičnost, pouzdanost identiteta pošiljaoca je posledica činjenice da je otisak poruke koji je šifrovan tajnim ključem, moguće uspešno dešifrovati samo primjenom odgovarajućeg javnog ključa.
- Integritet, upoređivanjem izračunatog i dešifrovanog otiska poruke utvrđuje se da poruka nije modifikovana.
- Neporecivost, pošiljalac ne može da porekne slanje poruke pošto je potpisana njegovim tajnim ključem.

Važno je napomenuti da elektronski potpisi uopšte ne pružaju zaštitu Tajnosti podataka od neovlašćenog čitanja, jer se svi podaci šalju u svom originalnom (nepromijenjenom) obliku.
Vjerovatnoća otkaza ili problem sigurnosti u sistemima kriptografije koji su dizajnirani i implementirani prema razvijenim industrijskim standardima je beznačajan, i puno je manji od rizika neprimjećenog falsifikata ili izmene dokumenta na papiru.

REGULISANJE ELEKTRONSKOG POTPISA U ZEMLJAMA U RAZVOJU

Mnoge zemlje u razvoju i zemlje u tranziciji žele da učestvuju u globalnoj ekonomiji koja se bazira na informacijama i internetu. Ove zemlje moraju da shvate da pravni okvir i politika vlade mogu da igraju važnu ulogu u sputavanju ili pomaganju razvoja informacionih i komunikacionih tehnologija, kao i razvoju onlajn ekonomije. Ono što očekuje sve ove zemlje je i e-uprava, koja podrazumijeva da građani sa državnim institucijama komuniciraju preko interneta od kuće. Vođenje poslovanja i pružanje usluga e-uprave u globalnom digitalnom okruženju pokreće važna pitanja zakonske validnosti elektronskih dokumenata. Tu se javljaju složena pitanja izgradnje povjerenja i utvrđivanje identiteta.

Zakonodavne vlasti mnogih zemalja, koje teže promovisanju e-trgovine i e-uprave, dale su prioritet donošenju zakona koji stvaraju pravnu osnovu za korišćenje i prihvatanje elektonskog potpisa. Tokom proteklih deset godina oko pedeset zemalja usvojilo je zakone ili uredbe o elektronskim potpisima.

U zemljama koje su nastale raspadom Jugoslavije prvi zakon o elektronskom poslovanju i elektronskom potpisu donesen je 2000 godine u Sloveniji. U Hrvatskoj je zakon o elektronskom poslovanju donesen 2003. godine. U Srbiji je zakon o elektronskom potpisu donesen 2004 godine. U Republici Srpskoj zakon o elektronskom poslovanju i elektronskom potpisu donesen je 2002 godine, ali je ovaj zakon izmijenjen 2008. godine i to samo u dijelu koji se odnosi na elektronski potpis.

Prema nekim zakonima, obavezujući će biti samo oni potpisi koji su napravljeni tehnologijama odobrenim od strane vlade. Na taj način može da se spriječi razvoj e-trgovine, jer se tehnologija u ovoj oblasti neprestano razvija i usavršava. Vladine regulative to mogu teško da prate. To može da dovede do toga da uloga zakona o elektronskom potpisu u praksi ima često manji značaj od onoga koji mu je predviđen. Poenta je u tome da zakonski okviri mogu da ponude samo ograničenu sigurnost i ne mogu automatski stvoriti povjerenje u neku tehnologiju. Vrijednosti elektronskog potpisa i drugih sistema potvrde identiteta u manjoj mjeri se baziraju na zakonskim propisima, a više zavise od mogućnosti same tehnologije koju korisnici praktično primjenjuju u svom elektronskom poslovanju. U ranim fazama razvoja elektronske trgovine u zemljama u razvoju, pretjerano oslanjanje na zakonsku regulativu o elektronskom potpisu odvlači pažnju od mnogo važnijih pitanja. Još gore, postoji mogućnost da određene birokratske regulative nepotrebno blokiraju procese vezane za izdavanje i upotrebu elektronskih potpisa. To može znatno da sputa razvoj elektronske trgovine i dovede do toga da multinacionalne kompanije zaobilaze tu zemlju u svojim investicijama.

Reforme pravnih sistema treba da podrže širenje interneta kao komponente razvoja. Mora se neprestano tragati za telekomunikacionim tehnologijama koje će obezbjediti brz protok elektronskih informacija. Bez novih telekomunikacionih tehnologija elektronska trgovina neće moći da napreduje u zemljama koje su u razvoju, bez obzira na kvalitet zakona o elektronskom potpisu koji donesu. Ovo su pokazala iskustva sa zakonima o elektronskom potpisu u razvijenim zemaljama.

RAZLIKA IZMEĐU NOVOG I STAROG ZAKONA O ELEKTRONSKOM POTPISU

U Republici Srpskoj zakon o elektronskom poslovanju i elektronskom potpisu donesen je 2002 godine ("Službeni glasnik Republike Srpske", broj 36/02). Ovaj zakon doživio je izmjenu 2008 godine ("Službeni glasnik Republike Srpske", broj 59/08) i to samo u dijelu koji se odnosi na elektronski potpis. Dio zakona koji se odnosi na elektronsko poslovanje nije doživio izmjenu. Sada ću navesti razlike između zakona iz 2002 i 2008 godine.

U zakonu iz 2008 godine na drugi način su definisani pojmovi: elektronski potpis, potpisnik, sredstva za izradu elektronskog potpisa, sredstva za verifikaciju elektronskog potpisa, kvalifikovani elektronski certifikat i davalac usluga certifikovanja. Dodate su definicije za elektronski zapis i sredstvo za elektronski potpis. U članu 6. novog zakona navedeni su ugovori koji se ne mogu prihvatiti u elektronskom obliku. Član 9. novog zakona je proširen u odnosu na član 18. starog zakona, koji govori o tome šta moraju osigurati sredstva za izradu kvalifikovanog elektronskog potpisa. Potpuno je iz starog zakona izbrisan član 19. koji govori o tome koje kriterijume moraju da zadovolje sredstva za verifikaciju kvalifikovanog elektronskog potpisa, kao i član 20. koji govori o tome kako se ostvaruje uspješna verifikacija kvalifikovanog elektronskog potpisa.

U stavu 3. člana 11. novog zakona definisano je da najniži nivo obaveznog osiguranja za rizik od odgovornosti za štetu koja nastane obavljanjem usluga elektronske certifikacije utvrđuje ministar pravilnikom, a u starom zakonu je to vršila vlada svojom odlukom.

U članu 14. novog zakona definisano je da ministarstvo nauke i tehnologije vodi evidenciju o certifikacionom tijelu u Republici Srpskoj, a u starom zakonu to je radilo ministarstvo finansija Republike Srpske.

U članu 14. novog zakona definisano je da certifikaciono tijelo mora prijaviti ministarstvu nauke i tehnologije početak obavljanja usluga elektronske certifikacije najmanje 14 dana prije početka rada, a u starom zakonu je ovaj period bio 8 dana.

U stavu 3. član 23. novog zakona dodato je, u odnosu na stari zakon, da potpisnici (lice koje posjeduje sredstvo za izradu elektronskog potpisa) mogu koristiti i usluge certifikacionog tijela u inostranstvu.
Član 24. novog zakona sadrži novi stav 2. koji kaže da certifikaciono tijelo izdaje elektronski certifikat za svakog pojedinačnog potpisnika na osnovu ugovora sa potpisnikom.

Član 27. novog zakona sadrži novi stav 2. koji kaže da je potpisnik obavezan da odmah zatraži opoziv certifikata u svim slučajevima gubitka ili oštećenja sredstva ili podataka za izradu elektronskog potpisa.

Član 34. novog zakona sadrži novi stav 2. koji kaže da ministarstvo, uz prethodnu saglasnost Agencije za informaciono društvo Republike Srpske, pravilnikom uređuje tehnička pravila za osiguranje povezanosti evidencija izdatih i opozvanih certifikata od certifikacionih tijela u Republici Srpskoj.

Član 36. novog zakona sadrži odredbu po kojoj upravni nadzor nad radom certifikacionog tijela vrši ministarstvo, a stručni nadzor vrši Agencija za informaciono društvo Republike Srpske.

U kaznenim odredbama novog zakona povećani su iznosi novčanih kazni za prekršaje koje učine fizička lica i odgovorna lica u radu sa elektronskim potpisom. U članu 40. novog zakona dodati su prekršaji za koje se mogu kazniti certifikaciona tijela

Kada se zakon o elektronskom potpisu sagleda u potpunosti, može se reći da stari zakon nije doživio krupne promjene. Za Republiku Srpsku je pozitivno, što je prvi zakon o elektronskom potpisu usvojila čak prije Srbije. To je bio jedan dobar preduslov za ulazak stranih banaka na tržište Republike Srpske, kao i za povećanje obima e-poslovanja.

ZAKLJUČAK

Zakoni o elektronskom potpisu koji za cilj imaju promovisanje e-trgovine ne bi trebalo da opterećuju e-trgovinu više nego što to čine u svijetu papira. Regulativa zemalja u razvoju i tranziciji iz oblasti e-trgovine ne bi trebalo da bude podređena rješavanju odnosa između partnera koji se ne poznaju. Umjesto toga, ove zemlje bi trebalo da osiguraju mogućnost potpisivanja elektronskih ugovora između već uspostavljenih trgovinskih partnera. Postoje važna pitanja izgradnje povjerenja u okviru e-trgovine, koja ne mogu biti riješena zakonskim putem. Zapravo, oštar regulatorni pristup može da koči, prije nego što promoviše, razvoj e-trgovine. E-trgovini najviše može da pomogne otklanjanje prepreka, a ne stavranje novih. Multinacionalnim kompanijama potreban je sistem elektronskog potpisa na koji mogu da računaju na globalnom nivou. Ako zakon o elektronskom potpisu ne pruža mogućnost slobodnog ugovaranja, onda bi on mogao da naudi učešću zemlje u globalnoj digitalnoj ekonomiji, više nego da ne postoji uopšte.

Razvoj tehnologija i procesa elektronskog potpisivanja biće nastavljen. U tome vodeću ulogu imaju tehnološki najrazvijenije zemlje. Međutim, zemlje u razvoju i tranziciji moraju takođe da se uključe u istraživanja i eksperimente kako tehnološi ne bi još više zaostajale za visokorazvijenim i bogatim zemljama.

LITERATURA:

1. Stankić, R., Krsmanović, B., *Elektronsko poslovanje,* Fakultet spoljne trgovine, Bijeljina, 2007.
2. Turban, E., McLean, J.Wetherbe, *Informaciona tehnologija za manadžment*, Univerzitetski udžbenik, Beograd, 2003.
3. Vidaković, D., *Mala škola kriptografije*
4. Zakon o elektronskom poslovanju i elektronskom potpisu, "Službeni glasnik Republike Srpske", broj 36/02.
5. Zakon o elektronskom potpisu, "Službeni glasnik Republike Srpske", broj 59/08.

Web izvori:
www.e-trgovina.co.rs