https://doi.org/ 10.7251/EMC2201100B
UDK: 004.738.52:658.8]:004.455.1
Datum prijema rada: 1. april 2022.
Submission Date: April 1, 2022
Datum prihvatanja rada: 30. maj 2022.
Acceptance Date: May 30, 2022
Časopis za ekonomiju i tržišne komunikacije
Economy and Market Communication Review
Godina/Vol. **XII** • Br./No. **I**
str./pp. 100-110

PREGLEDNI NAUČNI RAD / OVERVIEW SCIENTIFIC PAPER

DIGITALNI POTPIS I MOGUĆNOSTI NJEGOVE PRIMJENE U POSLOVNOM SISTEMU BOSNE I HERCEGOVINE

Živanka Miladinović Bogavac | Vanredni profesor; Poslovni i pravni fakultet, Univerzitet MB Beograd, Srbija; zivankamiladinovic@gmail.com; ORCID ID: 0000-0003-0477-8277

Sfyrakis Evangelos | Profesor grčkog jezika; Poslovni i pravni fakultet, Univerzitet MB Beograd, Srbija; vagsfy@yahoo.gr; ORCID ID:0000-0002-1097-9545

Adel Bajramović | Student doktorskih studija; Ekonomski fakultet Sveučilišta u Rijeci, Hrvatska; cinkarna.kvarc@gmail.com; ORCID ID: 0000-0001-8514-251

Sažetak: *Digitalni potpis u poslovnom sistemu Bosne i Hercegovine je nešto što još uvijek nije našlo svoju primjenu. Zakonom o carinskoj politici Bosne i Hercegovine, ovaj način potpisivanja jedino se primjenjuje kod špeditera, jer svoje dokumente u postupku elektrosnkog prevoza roba ovjeravaju na novi način i šalju u sistem Uprave elektronskim putem. U drugim sferama poslovnog svjeta, ovaj potpis se koristi isključivo kao prelazno rješenje. Ovaj rad pored ispitivanja zakonske mogućnosti primjene iste, te koristi koje bi poslovni sistem imao od implementacije iste, urađena je i analiza koja pokazuje koji je uticaj digitalnog potpisa na poslovni sistem jedne države, te u kojoj mjeri on olakšava poslovanje. Cilj je analizirati stepen primjene digitalnog potpisa na bh tržištu. Pored toga, analizirat će se najviše korišteni algoritmi u kriptosistemu digitalnog potpisivanja sa fokusom na način rada i sigurnost. Također kroz rad ćemo se osvrnuti na principe na kojima je zasnovano digitalno potpisivanje kao i metode pomoću kojh određujemo autentičnost pošiljaoca. Dalje, definisat ćemo područja primjene digitalnog potpisa. Cilj ovog rada je dokazati da digitalni potpis u Bosni i Hercegovini bi u velikoj mjeri olakšao način poslovanja, te pojednostavio procedure u poslovnom sistemu, te na taj način podigao konkurentnost privrede u odnosu na trenutno stanje. Prema navedenom, nameće se i hipoteza ovog rada, a to je da digitalni potpis, pored digiralnog pečata i digitalnog komuniciranja, ima najveći uticaj na efikasnost i brzinu poslovanja između kompanija koje posluju na području Bosne i Hercegovine. Hipoteza je ispitana primjenom multiplog regresionog modela, koju je istražio i obradio autor.*

Ključne riječi: *digitalni potpis, zakonski okvir, model, poslovni sistem, analiza kompanija.*

JEL klasifikacija: *K20, K22, K29*

UVOD

Digitalni potpis se koristi u cilju zaštite poruka od neželjenih izmjena u transportu kroz put komunikacije i kako bi potvrdili da je poruka zaista primljena od osobe koja to i tvrdi. U infrastrukturi digitalnog potpisivanja upotrijebljeni su princip kriptografije s javnim ključem i digitalni certifikat. Informatičko poslovanje je veoma važan i nezamjenjiv način komunikacije u današnje doba. Bez napredne zaštite i osiguranja, i pored svih prednosti koje donosi, može biti izvor brojnih rizika. "Zato digitalni potpis predstavlja sigurnost i povjerenje na širokom spektru djelatnosti i usluga, a najviše se koriste u područjima potpisivanja dokumenata, slijepog potpisa, potpisa u internetskim aplikacijama i kao zaštita multimedijalnih sadržaja" (Škorić, 2018).

Za BiH kažemo prije svega da je zemlja u razvoju i kao takva digitalni potpis kao aspekt je veoma značajan. On prije svega osigurava integritet poruke, dakle utvrđuje da li se poruka promijenila dok je došla do njenog primaoca. U Bosni i Hercegovini zastupljenost digitalnih potpisa je dosta neistražena pojava. Kada korisnik potpiše poruku privatnim ključem, on je ne može poreći, budući da samo on zna šifru za privatni ključ. Iz tog razloga veoma je bitno istaknuti značaj privatnog ključa i sve što je vezano za njega neophodno je držati u tajnosti. Preporučuje se čuvanje privatnog ključa na smart kartici kao i na računaru. Međutim, u slučaju čuvanja na računaru, korisnik onda samo može potpisati dokumente na tom računaru. Postoji još jedna vrsta digitalnog potpisa, tzv. slijepi potpis. Kod te vrste potpisa je skriven sadržaj poruke od potpisnika prije potpisivanja.Digitalni potpisi se koriste najviše u slučajevima kada potpisnik i autor nisu iste osobe. Primjer takvih situacija su digitalizirani kriptografski sistemi za glasanje i sigurni elektronski platežni sistemi. Još jedno područje primjene slijepih potpisa dolazi iz potrebe sprječavanja potpisnika da poveže potpisanu skrivenu poruku s kasnije otkrivenom porukom.

Analiza rada zasnovana je na multiplom regresionom modelu koji mjeri uticaj netavinih varijabli na zavisnu. Ovaj model daje najbolja moguća predviđanja vrijednost zavisne varijable na temelju vrijednosti neovisne varijable, ako su ispunjene sve pretpostavke. Na osnovu veličine regresijskih koeficijenata, zaključujemo koliki je relativni utjecaj od važnost svake nezavisne varijable je ako ovi koeficijenti se pretvaraju u beta koeficijente β. Dobijaju se koeficijenti kada su sve vrijednosti varijable standardizirane. „Preduslov za korištenje regresije analiza je postojanje linearne ovisnosti između varijabli. To je neophodno budući da analiza počinje s izračun koeficijenta jednostavne korelacije (bivarijantne korelacije) za sve parove varijabli, i svi ti proračuni zahtijevaju linearni odnos između parova varijabli." (Šupuković, Jakupović, & Obhođaš, 2019) Zahvaljujući internetu, fizička i pravna lica iz različitih dijelova svijeta mogu razmijeniti informacije za samo nekoliko sekundi. Stoga, najveći dio komunikacije se i odvija upravo putem interneta. Moramo posebno naglasiti autentičnost kao vrlo bitan dio komunikacije – važno nam je da znamo da je primljena informacija zaista i upućena od lica od kojeg je i očekivana. U prošlosti je to regulisano voštanim pečatom na koverti u srednjem vijeku, u novijoj historiji vlastoručnim potpisom.Danas se autentičnost elektronskog dokumenta utvrđuje putem digitalnog potpisa. Ukoliko poznajemo identitet autora, dokument ćemo smatrati autentičnim. Vjerodostojnost potpisanog dokumenta provjerava se enkripcijom. Enkripcija je postupak putem kojeg se prije slanja podaci kodiraju na način da ih samo primatelj može dekodirati i razumjeti. Digitalnim potpisom se, pored autentičnosti, osigurava i integritet i neporeci-

vost. Kada govorimo o integritetu, govorimo o sigurnosti podataka u smislu da nije došlo do promjene ili uništenja prilikom prenosa od pošiljatelja do primatelja.

Neporecivost znači činjenicu da pošiljatelj informacije ne može poreći svoje sudjelovanje u procesu komunikacije, budući da jeidno on ima uvid u privatni ključ pomoću kojeg je potpisana predmetna poruka. Nekoliko kriptografskih ključeva, privatni i javni, stvaraju se funkcijom digitalnog potpisa. Potpisana poruka sažeta je hash1 algoritnom. Privatni kriptografski ključ je u cijelosti tajan, dok je javni ključ dostupan svima. Iz korisnikovog privatnog ključa i sažete poruke stvara se digitalni potpis koje se šalje u sklopu potpisane poruke, ili se objavljuje.

Digitalni potpis je ključ sigurnosti i povjerenja u savremenom internet poslovanju. Digitalni potpis omogućava brže i jednostavnije potpisivanje, uštedu kada je riječ o poštanskim troškovima, jednostavnije sklapanje ugovora, elektronsko slanje dokumenata, zahtjeva i slično. Uprkos tehnološkom napretku, mnogi preduzetnici i danas preferiraju ličnu komunikaciju, ne edukuju se ili se malo edukuju, nisu povjerljivi prema tehnologiji digitalnog potpisa, a također, prisutni su povećani troškovi implementacije (baza podataka, certifikati, programska podrška). Uprkos tome, očekuje se da će u budućnosti digitalni potis biti preovladavajući način za utvrđivanje da li su dokumenti autentični. Vremenom se digitalni potpisi sve više približavaju ručnim potpisima. Smatra se da će se u skorijoj budućnosti ručni potpisi u potpunosti prestati koristiti. Također, očekuje se da će povećanom upotrebom digitalnih potpisa doći i do povećanja pokušaja zloupotrebe istih i cyber napada. Iz tog razloga je bitno raditi na razvijanju mehanizama i algoritama kako bi se isti sprječavali.

METODOLOGIJA RADA

U istraživačkom radu, gdje su preuzeta sekundarna istraživanja korišteni su podaci, te za statističku obrade podataka sljedeće metode: opisna ili deskriptivna statistika, regresija i korelacija. „Deskriptivna statistika korištena u ovome rada ogleda se u prikazu podataka tabelarno i grafički, bez dublje analize. Na temelju serijala iz prethodnih godina, metoda trenda predvidja da li je moguće trendove prognozirati u budućem razdoblje“ (Newbold, Carslon, William, & Thorne, 2010). Korišteni podaci prikupljeni su na području Bosne i Hercegovine, te ciljna skupina i veličina uzorka pokazuje da se radi o reprezentativnom uzorku. „Jedan od preduvjeta za korištenje regresijske analize su postojanje linearne ovisnosti između varijabli. To je neophodno budući da analiza počinje računanjem određivanje jednostavnih koeficijenata korelacije (bivarijantno korelacije) za sve analizirane varijable, i svi izračuni zahtjevaju da su odnosi između varijabli linearni i statistički značajni“. (Šupuković, Jakupović, & Obhođaš, 2019)

Primarni podaci mogu dati rezultate na osnovu kojih će se utvrditi koje motivacijske tehnike najbolje utiču na kvalitetu digitalnog potpisa, te koliko isti utiče na uspiješnost I efikasnots kompanije. “U korelaciji sa problemom, predmetom i objektom istraživanja, te postavljenom radnom i pomoćnim hipotezama postavlja se svrha istraživanja, a to je pokazati pomoću statističkih metoda da je digitalin potpis u odnosu na digitalin pečat i ostale digitalna pomagala u smislu podizanja efikasnosti poslovanja, najvažniji, ta da ima najveći uticaj na podizanje efikasnosti kompanije” (Danović, Obhodjas, & Jakupović, 2020).

DIGITALIZACIJA POTPISA I NJEGOVA ZAKONSKA OSNOVA

Zakon o elektronskom potpisu je usvojila Parlamentarna skupština BiH i Dom naroda 2006. godine. Ovaj Zakon uređuju osnove formiranja i upotrebe elektronskog potpisa i pružanja usluga u vezi s elektronskim potpisom i ovjeravanjem poslovnih subjekata. "Također, ovaj Zakon podrazumjeva da se u pravnom i poslovnom prometu mogu koristiti elektronski potpisi formirani postupcima različitih nivoa sigurnosti i zasnovani na potvrdama različitih klasa. Pravno djelovanje elektronskog potpisa i njegova upotreba kao dokaznog sredstva ne može se isključiti zbog činjenice da je elektronski potpis dostupan jedino u elektronskoj formi ili zbog toga što nije zasnovan na kvalificiranoj potvrdi, ili kvalificiranoj potvrdi akreditiranog ovjerioca, ili zbog toga što nije formiran upotrebom tehničkih sredstava i postupaka iz člana 14. ovog Zakona." (Ministarstvo pravde FBiH, 2021)

Prema Zakonmu o elektronskom potpisu, da bi potvrda bila kvalificirana mora sadržavati sljedeće podatke:

- oznaku ili dokaz koji potvrđuje da se radi kvalificiranoj potvrdi,
- ime ili firmu, kao i sjedište,
- ime - pseudonim potpisnika
- dodatne podatke o potpisniku
- podatke za provjeru potpisa, a koji pri tome odgovaraju podacima kako bi se formirao potpis koji je I pod kontrolom potpisnika,
- podatke o početku i prestanku važenja potvrde,
- jedinstvenu oznaku potvrde,
- ograničenja upotrebe potpisa, ako postoji,
- ograničenja u pogledu vrijednosti transakcija

Kvalificirana potvrda mora biti potpisana elektronskim potpisom ovjerioca. Prema Zakonu o digitalnom potpisu (Ministarstvo pravde FBiH, 2021) Ovjerilac koji izdaje kvalificirane potvrde dužan je da:

- pokaže pouzdanost i sigurnost kod korištenja elektronskog potpisa i ovjere;
- pomaže kod pružanja neodložive usluge opoziva i vodi registar potvrda na brz i siguran način;
- za kvalificirane potvrde, kao i za registar potvrda i pružanje usluga opoziva, koristiti podatak o vremenu koji je nesumnjivo kvalitetan (npr. siguran vremenski pečat) i osigurati za sve slučajeve da se datum i vrijeme izdavanja ili opoziva potvrde mogu tačno utvrditi,
- provjerava identitet i druga pravna obilježja kod lica koja podnesu zahtjev za izdavanje potvrde;
- zapošljavati pouzdana lica, koja za pružanje usluga imaju potrebna specijalistička znanja, iskustvo i stručne kvalifikacije i naročito upravljačke sposobnosti i poznavanje tehnologije elektronskog potpisa i odgovarajućih sigurnosnih postupaka, i primjenjuju administrativne i upravljačke postupke i propise, u skladu s važećim pravilima struke,
- imati finansijsku sposobnost za obavljanje djelatnosti u skladu s ovim zakonom i na osnovu njega donesenim podzakonskim propisima, i za pokriće eventualnih zahtjeva za naknadu štete,
- evidentirati sve okolnosti i činjenice značajne za kvalificirane potvrde, tokom vremena njihove primjene, tako da se ovjeravanje može dokazati, na-

ročito u sudskom postupku, te čuvati ove podatke trajno i u elektronskom obliku,
- poduzima neophodne mjere i spriječava kopiranje ili čuvanje podataka ovjeriocu i trećim licima.

Osoba, u ovom slučaju ovjerilac, koja pruža usluge vezane za elektronski potpis, kao i za izdavanje, formiranje i čuvanje potvrda, dužna je da koristi sistem koji je pouzdan i tehnički zaštićen od izmjena. Također, taj sistem mora pružati i tehničku i kriptografsku sigurnost. Pored toga, mora preduzeti neophodne mjere da osigura tajnost podataka za formiranje potpisa. Za generiranje i čuvanje podataka za formiranje potpisa i za formiranje i čuvanje kvalificiranih potvrda ovjerilac je dužan koristiti tehnička sredstva i postupke.

Pored toga, bitno je naglasiti i važnost elektronskih nabavki. Ovim zakonima je unaprijeđeno trenutno stanje u Federaciji Bosne i Hercegovine na način da je uvedena mogućnost korištenja elektronskog pečata i potpisa, u cilju unaprjeđenja pravnog prometa i poboljšanja koja prate najviše tehnološke i tehničke standarde. Usvajanje ovih zakona je i dio ispunjavanja Reformske agende, i znatno doprinose kreiranju sigurnijeg i povoljnijeg poslovnog i društvenog okruženja u Federaciji Bosne i Hercegovine, u Bosni i Hercegovini, na domaćem tržištu, kada su upitanju ne samo domaći, nego i strani investitori. Time je napravljen veliki korak kada su u pitanju tehnološki napredak, komunikacija i obavljanje poslovih aktivnosti. Javna uprava je postala mnogo ekonomičnija i efikasnija za građane. Ovi zakoni su i važan, tj. Ključni korak ka implementaciji Programa uvođenja jednošalterskog sistema i elektronske registracije privrednih subjekata u Federaciji BiH, što predstavlja jedan od prioritetnih zadataka Vlade Federacije Bosne i Hercegovine. Na kraju, usvajanjem ovih zakona, građanima Federacije Bosne i Hercegovine i Bosne i Hercegovine su omogućena najviša komunikacijska i tehnološka dostignuća koja će im olakšati život u velikoj mjeri, a državu Bosnu i Hercegovinu približiti Evropskoj uniji.

TEMELJNI PRINCIPI I ALGORITMI DIGITALNOG POTPISIVANJA

"Internet je najrasprostranjenija računarska mreža koja omogućuje pojedincima iz svih dijelova svijeta međusobnu komunikaciju, razmjenu informacija i dokumenata. Tipična situacija je kada osoba A putem interneta želi kupiti nešto od osobe B. Međutim u takvom vidu komunikacije, uz klasične, pojavljuju se i neki sasvim novi problemi. Tako treba biti siguran da poruku koju je osoba A poslala osobi B ne može pročitati niko drugi, te da ta poruka nije promijenjena. Također, problem je da osoba B može biti u potpunosti sigurna da joj je upravo osoba A poslala primljenu poruku i da osoba A ne može poreći da je upravo osoba B poslala tu poruku. U rješavanju ovih problema pomaže nam digitalni potpis." (Liđan & Ibrahimpašić, 2010)

Danas je komunikacija elektronskim putem zastupljena u gotovo cijelom svijetu. U velikoj mjeri je klasična pošta na papiru zamijenjena elektronskom poštom. Elektronska pošta je danas izuzetno značajna, poslovnim partnerima je nezamjenjiv način komunikacije. Ključan faktor uspjeha e-trgovine je digitalni potpis. Digitalni potpis je osnovni uslov da e-trgovina ne bude nepouzdana i nesigurna. Iako današnja tehnologija kakvu znamo ne pruža stoprocentnu sigurnost, ona ipak omogućava dovoljnu razinu zaštite koja se uporediva, i možda čak i bolja od papirnate komunikacije.

Internet ima mnogobrojne prednost za poslovanje. Pristup informacijama, elek-

tronsko plaćanje, predaja i preuzimanje obrazaca i drugih dokumenata, razmjena računa i informacija, elektronsko potpisivanje dokumenata su samo neke od njih. Međutim, pored mnogobrojnih prednosti, internet i internet poslovanje nose i velike rizike, stoga je potrebno voditi računa o naprednoj elektroničkoj zaštiti i platformama povjerenja. Da bi elektronski dokument bio prihvatljiv, mora biti tehnički ispravan, nepromjenljivog sadržaja, te izvor, odnosno stvaraoc dokumenta moraju biti vjerodostojni. Sve to je obuhvaćenom elektronskim potpisom kao instrumentom kojim je moguće osigurati zaštitu integriteta sadržaja i vjerodostojnost izvora. Sistem digitalnog potpisivanja možemo podijeliti na 3 algoritma:

- Algoritam za generisanje javnog i privatnog ključa - rezultati su privatni i odgovarajući javni ključ;
- Algoritam za izradu potpisa - generiše se digitalni potpis na osnovu sažetka (digesta) poruke i privatnog ključa;
- Algoritam za provjeru potpisa – koristeći poruku i javni ključ, potvrđuje ili opovrgava autentičnost poruke.

Tri najčešća i najpouzdanija algoritma koji se koriste za digitalno potpisivanje su: (Vranješ, 2017)

1. DSA *(Digital Signature Algorithm)*
2. ECDSA *(Elliptic Curve Digital Signature Algorithm)*
3. RSA (*Rivest – Shamir – Adleman)*

DSA (Digital Signature Algorithm) i generisanje ključeva i parametara

Digital Signature Algorithm (DSA) je algoritam koji se najviše koristi u vladinim i nevladinim organizacijama, odobren od strane DSS (eng. *Digital Signature Standard*) - standarda savezne vlade SAD-a i koristi se isključivo za digitalno potpisivanje.

Generisanje ključeva je jedan proces koji se sastoji od 6 faza:

a. Odabrati odobrenu kriptografsku hash funkciju H. U originalnom DSS-u, preporuka je bila koristiti SHA-1, ali u trenutnom DSS-u je preporučena upotreba SHA-2. Rezultat hash funkcije se može skratiti na veličinu para ključeva.
b. Odabrati dužine ključeva L i N. Dužine ključeva su prvi simptomi kriptografske snage ključeva. Prvi DSS je uslovljavao da L bude broj između 512 i 1024, te da bude djeljiv sa 64.
c. Odabrati prosti broj q dužine N bita.
d. Odabrati prosti broj p dužine L bita tako da vrijedi $p=q*z+1$ za neki cijeli broj z, L mora biti između 512 i 1024 i djeljiva sa 64.
e. Odabrati proizvoljno broj h takav da vrijedi $1 < h < (p - 1)$
f. Izračunati broj g takav da vrijedi $g = h^z \bmod p$. Ako se pokaže da je $g = 1$, treba odabrati drugačiju vrijednost h. Ipak, većina uzoraka će polučiti upotrebljiv broj g, a najčešće se za vrijednost h uzima broj 2.

ECDSA (Elliptic Curve Digital Signature Algorithm)

„Iz ranije objašnjenog DSA algoritma je nastao ECDSA algiritam. Kao ANSI standard prihvaćen je 1999. godine, a kao IEEE i NIST standard, prihvaćen je godinu kasnije“ (Johanson, Menzes, & Vanstone, 2001). Za razliku od prethodnika na čijim je temeljima nastao, ECDSA se ne oslanja na problem faktorizacije velikih brojeva,

već na eliptičke krive što snagu njegovih ključeva čini mnogo većom. Svaka se vrsta enkripcije zasniva na složenosti rješavanja određenog problema i upravo su te složenosti iskorištavali autori dosad napravljenih enkripcijskih algoritama kako bi razvili što sigurnije i neprobojnije algoritme.

„Do pojave primjene eliptičkih krivih u kriptografiji, većina algoritama se zasnivala na složenosti problema faktorizacije velikih brojeva. Primjenu eliptičkih krivih u kriptografiji su prvi uveli Koblitz i Miller 1985. godine iskoristivši činjenicu da je u grupi eliptičkih krivih matematička operacija potenciranja puno lakša od matematičke operacije logaritmiranja“ (Dujella & Maretić, 2007). Da bi primjena eliptičkih krivih bila jasna, u dijelu rada koji slijedi su objašnjenje postavke i matematičke operacije nad grupom eliptičkih krivih koje su potrebne za primjenu spomenutih krivih u kriptografiji.

RSA (Rivest – Shamir – Adleman) algoritam

„RSA algoritam je jedan od prvih praktičnih kriptografskih algoritama koji koristi ideju javnog ključa (Wikipedija, 2022). Asimetrija algoritma se ogleda u praktičnoj nemogućnosti faktorizacije produkta dva velika prosta broja. Algoritam je nazvan po prvim slovima prezimena njegovih tvoraca, Rona Rivesta, Adija Shamira i Leonarda Adlemana koji su algoritam prvi puta predstavili 1978. godine. „Korisnik RSA algoritma kreira i objavljuje javni ključ koji se bazira na dva velika prosta broja zajedno s pomoćnom vrijednošću“ (Wezika, 2007). Pritom je važno naglasiti da odabrani prosti brojevi moraju ostati tajni. Svako može šifrirati poruku pomoću javnog ključa, ali samo osoba koja zna o kojim se prostim brojevima radi je može i dešifrirati.

„Do danas se algoritam pokazao prilično sigurnim iako mnoge stvari, koje se u algoritmu podrazumijevaju, nisu dokazane“ (The World Bank, 2018). Na primjer, nije dokazano da je moduo aritmetika najbolji izbor za proračun velikih prostih brojeva. Također, nije dokazano da je osnovni postulat ovog algoritma, složenost proračuna prostih brojeva, toliko složen problem kao što se čini. „Postoji mogućnost da će napredak u teoriji brojeva donijeti nova otkrića. Algoritam koji koristi RSA za digitalno potpisivanje se sastoji od 5 koraka“ (Wikipedija, 2022).

ANALIZA UTICAJA DIGITALNOG POTPISA NA EFIKASNOST POSLOVANJA

U narednom dijelu rada primjenom odgovarajućihg statističkih metoda i alata izvršit će se analiza varijabli koje analiziraju efikasnost kompanije. Naime, izmjerit će se utiacaj određenih varijabli, koje se mogu okarakterisati kao nezavisne, na efikasnost kompanije, primjenom višestrukog regresionog modela. „Bitno je istaknuti da korištenje digitalnog potpisa omogućava kvalitativni skok u razvoju mnogih aplikacija jer omogućava brže i jednostavnije poslovanje, lakše sklapanje ugovora. Koncepcija digitalnog potpisa zasigurno će otvoriti vrata novim uslugama i oblicima poslovanja” (Zovkić & Vrbanec, 2012).

Ovaj uzorak obuhvata 235 kompanija u Bosni i Hercegovini, a podaci su prikupljeni uz pomoć anketnog upitnika. Pored ispitanih varijabli, anektni upitnik je sadržavao još neke interesantne teme koje se tiču efikasnosti poslovanja, a koje su predmet nekog drugog istraživanja. Fokus ove analize je uticaj digitalnog potpis, digitalnog pečata i digitalnog komuniciranja na efikasnost poslovanja. “Promjene jedne pojave

uvijek su uzrokovane djelovanjem više fakora, odnosno postoji visok stepen slaganja varijacija između više pojava. Ukoliko jednu pojavu možemo identifikovati kao zavisno promjenjivu, a ostale pojave kao nezavisno promjenjive, tada možemo odrediti model regresije, koji izražava prosječnu vezu između zavisno promjenjive i nezavisno promjenjivih" (Ophodjas, Jerković, & Iličić, 2015). Postojanje linearne zavisnosti između varijabli je jedna od pretpostavku za upotrebu regresione analize.

„Analiza počinje tako što se prvo izračuna koeficjent proste korelacije - bivarijantnih korelacija, za sve parove varijabli, a sva ova izračunavanja zahtevaju linearan odnos između parova varijabli" (Newbold, Carslon, William, & Thorne, 2010).

Tabela 1: Korelacija modela

Correlations					
		EP	**DP**	**DPČ**	**DK**
Pearson Correlation	EP	1.000	.734	.629	.427
	DP	.734	1.000	.636	.401
	DPČ	.629	.336	1.000	.399
	DK	.427	.401	.399	1.000
Sig. (1-tailed)	EP	.	.003	.020	.031
	DP	.003	.	.040	.034
	DPČ	.020	.040	.	.040
	DK	.031	.034	.040	.

Izvor: Obrada autora u statističkom paketu SPSS 20

Prema Pearsonovom koeficijentu korleacije, može se zaključiti da između zavisne i nezavisnih varijabli postoji visok stepen povezanosti, koje se nalaze u pozitivnom linearnom odnosu. Naime, najveća povezanost je između efikasnosti poslovanja i digitalnogf potpisa, gdje koeficijent korelacije iznosi 0,734, zatim digitaln og pečata, pa tek onda digitalnog komuniciranja. Važno je spomenuti da su sva tri koeficijenta izuzetno visoka, te da iznose između 0,427 do 0,734.

„Ovaj model daje najbolje moguće predviđanje vrijednosti zavisne promijenjive na osnovu vrijednosti nezavisnih promijenjivih, ako su sve pretpostavke ispunjene. Na osnovu veličine regresionih koeficijenata možemo zaključiti koliki je relativni uticaj ili važnost svake nezavisne promjenjive, ako se ti koeficijenti konvertuju u beta koeficijente β. Ovi koeficijenti se dobiju kada se sve vrijednosti promenljivih standardizuju" (Šupuković, Jakupović, & Obhođaš, 2019).

Tabela 2: Koeficijenti modela

Nezavisne varijable	**Beta**	**t**	**Singifikantnost**
Digitalni potpis - DP	0,771	4,940	0,029 (p < 0,05)
Digitalni pečat - DPČ	0,689	4,092	0,047 (p > 0,05)
Digitalno komunicijranje - DK	0,414	3,132	0,045 (p > 0,05)
Zavisna varijabla: Efikasnost poslovanja - EP			

Izvor: Obrada autora u statističkom paketu SPSS 20

Prema rezultatima analize, koje mjere uticaj nezavisnih varijabli na zavisnu, može s ezaključiti da sve tri nezavisne varijable imaju uticaj na zavisnu. Naime, digitalno komuniciranje, digitalni pečat i digitalni potpis utiču na efikasnost poslovanja, jer je p vrijednost u sva tri slučaja manja od 0,05. Pored toga, može se zaključiti da najveći uticaj na efikasnost poslovanja ima digitalni potpis, sa beta koeficiejntom od 0,771, zatim digitalni pečat, pa tek na kraju digitalno komuniciranje.

Tabela 3: Heteroskedastičnost

Test	LM	Sig.
B – P test	47,916	0,000

Izvor: Obrada autora u statističkom paketu SPSS 20

Ukoliko je sig.vrijednost manja od 0,05 tada Test Breusch - Pagan test nije prisutan. Ovom analizom smo dobili rezultat od $p = 0,000 < 0,05$ što znači da je testirani model normalno distribuiran te da se analizirani koeficijenti koji su predstavljeni u prethodnoj tabeli mogu uzeti kao tačni.

ZAKLJUČNO RAZMATRANJE

Zakon o elektronskom potpisu u Federaciji Bosne i Hercegovine i Zakon o elektronskom dokumentu stvorili su podlogu za primjenu najboljih i najviših tehnoloških, tehničkih, komunikacijskih i informacionih dostignuća u evropskim i svjetskim pravnim sistemima. Ovim zakonima stvara se elektronsko poslovno okruženje u kojem je omogućen promet elektonskih dokumenata u pravosuđu, državnoj upravi, privredi i ostalim oblastima, te su stvoreni uslovi za razvoj racionaline i efikasnije državne uprave, konkurentnije privrede, te se putem uspostavljanja e-servisa ostvaruje uspješna komunikacija među poslovnim partnerima, državnom upravom i građanima. Na ovaj način smanjeni su troškovi poslovanja, povećane uštede, stvorena dodatna vrijednost, smanjena siva ekonomija i korupcija.

Ukoliko dođe do usvajanja zakona, to će odmah značajno olakšati poslovnim subjektima, građanima, itd. Vrlo važan aspekt elektronskog poslovanja jeste mogućnost izdavanja i dostavljanja elektronskih faktura, uzevši u obzir da većina pravnih lica ima mogućnosti da elektronski ispostavlja fakture putem vlastitih informacionih sistema ili infrastrukture za elektronsko bankarstvo.

Predstavljeno je i IT rješenje po kojima bi potpis i pečat digitalnog potpisnika bio maksimlano zaštičen. Međutim, danas kriptosistemi zasnovani na eliptičkim krivim daju istu sigurnost kao i RSA algoritam uz desetak puta kraću dužinu ključeva i da će u budućnosti taj odnos dodatno rasti u korist algoritama s eliptičkim krivim, što je pojašnjeno u gornjem dijelu rada. Dokazano je da u poređenju sa DSA algoritmom, RSA je brži u šifriranju i verifikaciji potpisa, dok je DSA brži u generisanju ključeva i dešifriranju. Algoritmi su podjednako jaki, ali u slučaju digitalnog potpisivanja, ipak se mala prednost pri izboru daje DSA algoritmu, što je jedan od zaključaka. Pokazalo se da u Bosni i Hercegovini generalno postoji percepcija da je upotreba digitalnih potpisa i njegova korisnost na globalnom nivou ipak, primjenom adekvatnih metoda i tehnika, moguće poboljšati i unaprijediti i na taj način povećati broj korisnika digitalnog potpisa.

Posebno ovome ide u prilog provedeno istraživanje i urađeni model. Naime, autor je na uzorku od 235 kompanija istražio i analizirao primjenom višestrukog regresijskog modela uticaj digitalnog potpisa, digitalnog pečata i digitalne komunikacije na efikasnost poslovanja. Rezultati su pokazali da sve tri varijable imaju uticaj na efikasnost poslovanja u određenoj mjeri. Prema rezuzltatima, ipak, se može zaključiti da digitalni potpis, pa zatim i digitalni pečat imaju veoma visok uticaj na efikasnost poslovanja.

Prema navedenom, može se zaključiti da je postavljena hipoteza u ovom radu, koja glasi: „*Digitalni potpis, pored digiralnog pečata i digitalnog komuniciranja, ima najveći uticaj na efikasnost i brzinu poslovanja između kompanija koje posluju na području Bosne i Hercegovine"* (Yan, 2002)*,* u potpunosti ispitana i dokazana kroz navedeni model. Prema rezultatima analize, upravo je dokazano da najveći beta koeficijent je upravo kod varijable koja analizira uticaj digitalnog potpisa na efikasnost poslovanje, prema tome, rezultati modela su se poklopili sa postavljenom hipotezom. Ispunjen je i cilj rada, a koji treba da analizira stepen primjene digitalnog potpisa na bh tržištu, koji je trenutno veoma skroman, kao i najčešće algoritme koji se koriste u kriptosistemu digitalnog potpisivanja, što je i urađeno, i analizirano u radu i zaključku ovog rada.

LITERATURA

Danović, L., Obhodjas, I., & Jakupović, E. (2020). Istraživanje uticaja motivacionih tehnika na kvalitet usluga u financijskom sektoru pomoću statističkih metoda. *Tranzicija*, pp. 1 - 12.

Dujella, A., & Maretić, M. (2007). *Kriptografija.* Zagreb: Element.

Johanson, D., Menzes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algoritam. *ECDSA*, (pp. 22 - 36).

Liđan, E., & Ibrahimpašić, B. (2010). *Digitalni potpis.* Osijek: Osječki matemati.

Ministarstvo pravde FBiH. (2021). *Zakon o elektronskom potpisu.* Sarajevo: Ministarstvo pravde.

Newbold, P., Carslon, William, & Thorne, N. (2010). *Statistika za poslovanje i ekonomiju.* Zagreb: Mate.

Ophodjas, I., Jerković, D., & Iličić, L. (2015). Primjena regresione analize u prognoziranju potražnje u mliječnoj industriji u BiH. *Tranzicija - časopis za ekonomiju*, pp. 79 - 89.

Škorić, I. (2018). *Digitalni potpis.* Rijeka: Sveučilište u Rijeci.

Šupuković, V., Jakupović, S., & Obhođaš, I. (2019). Modeliranje procesa upravljanja u funkciji dugoročnog ispunjavanja ciljeva u hrvatskim poduzećima. *Notitia - časopis za ekonomske, poslovne i drustvene teme*, str. 21-29.

The World Bank. (2018). *Publish.*

Vranješ, A. (2017). *Algoritam za kreiranje digitalnog potpisa.* Osijek: Sveučilište Osijek.

Wezika, D. (2007). *Measurement of National Intellectual Capital.* Instead: IRISS Working Paper Series .

Wikipedija. (2022). *Kriptosistem.* Wikipedija.

Yan, S. (2002). *Number theory for Computiing, .* Berlin: Springerr - Verlag.

Zovkić, M., & Vrbanec, T. (2012). *Digitalni potpis.* Zagreb: Sveučilište u Zagrebu.

DIGITAL SIGNATURE AND POSSIBILITIES OF ITS APPLICATION IN THE BUSINESS SYSTEM OF BOSNIA AND HERZEGOVINA

Živanka Miladinović Bogavac
Associate Professor; Faculty of Business and Law, University MB Belgrade, Serbia; zivankamiladinovic@gmail.com;
(ORCID ID: 0000-0003-0477-8277)

Sfyrakis Evangelos
Greek language teacher; Faculty of Business and Law, University MB Belgrade, Serbia; vagsfy@yahoo.gr;
(ORCID ID:0000-0002-1097-9545)

Adel Bajramović
PhD student; Faculty of Economics, University of Rijeka, Croatia; cinkarna.kvarc@gmail.com; (ORCID ID: 0000-0001-8514-2515)

Summary: *Digital signature in the business system of Bosnia and Herzegovina is something that has not yet found its application. According to the Law on Customs Policy of Bosnia and Herzegovina, this method of signing is only applied to freight forwarders, because they certify their documents in the procedure of electronic transport of goods in a new way and send them to the Administration system electronically. In other spheres of the business world, this signature is used exclusively as a transitional solution. This paper, in addition to examining the legal possibility of its application, and the benefits that the business system would have from its implementation, also made an analysis that shows the impact of digital signatures on the business system of a country, and to what extent it facilitates business. The aim is to analyze the degree of application of digital signatures in the BiH market. In addition, the most widely used algorithms in the digital signature cryptosystem with a focus on mode and security will be analyzed. Also through the paper we will look at the principles on which digital signing is based as well as the methods by which we determine the authenticity of the sender. Next, we will define the areas of application of the digital signature. The aim of this paper is to prove that a digital signature in Bosnia and Herzegovina would greatly facilitate the way of doing business, and simplify procedures in the business system, and thus raise the competitiveness of the economy compared to the current situation. According to the above, the hypothesis of this paper is that digital signature, in addition to digital printing and digital communication, has the greatest impact on the efficiency and speed of business between companies operating in Bosnia and Herzegovina. The hypothesis was tested using a multiple regression model, which was investigated and processed by the author. The author investigated and analyzed the impact of digital signature, digital printing and digital communication on business efficiency in a sample of 235 companies using a multiple regression model. The results showed that all three variables have an impact on business efficiency to a certain extent. According to the results, however, it can be concluded that the digital signature and then the digital stamp have a very high impact on business efficiency.It has been shown that in Bosnia and Herzegovina there is a general perception that the use of digital signatures and its usefulness at the global level, however, by applying adequate methods and techniques, can be improved and improved and thus increase the number of digital signature users.*

Keywords: *digital signature, legal framework, model, business system, company analysis.*

JEL classification: *K20, K22, K29*