Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 659.2:004
DOI: https://doi.org/10.24867/02OO04Cvejic

ELEKTRONSKI POTPIS – ZNAČAJ I PRIMENA

ELECTRONIC SIGNATURE, SIGNIFICANCE AND APPLICATION

Ana Cvejić, *Fakultet tehničkih nauka, Novi Sad*

Oblast: INFORMACIONO – KOMUNIKACIONI SISTEMI

Abstrakt – *Ovaj rad se bavi značajem i primenom elektronskog potpisa u informacionim sistemima, sa posebnim fokusom na primenu i implementaciju elektronskog potpisa. Takođe, prikazani su osnovni koncepti elektronskog poslovanja, dok je u istraživačkom delu rada prikazana implementacija elektronskog potpisa, koji treba da pomogne organizacijama da unaprede svoje poslovanje.*

Ključne reči: *Elektronski potpis, elektronsko poslovanje, veb aplikacija, MSSQL, Angular 5, .NET, Entity Framework Code First*

Abstract *– This paper deals with the importance and application of electronic signatures in information systems, with a special focus on the application and implementation of electronic signatures. Also, the basic concepts of electronic business are presented, while the research part of the paper shows the implementation of electronic signatures, which should help organizations to improve their business.*

Keywords: *Electronic Signature, e-Business, Web application, MSSQL, Angular 5, .NET, Entity Framework Code First*

1. UVOD

Savremena tehnologija i upotreba *Interneta* su u potpunosti promenili način poslovanja i omogućili kreiranje novih i inovativnih modela. U razvoj oblasti savremenih tehnologija spada i elektronska revolucija koja deluje u širokom ekonomskom kontekstu, obuhvatajući interne procese i poslovanje organizacija, kao i tržišno okruženje. Elektronsko poslovanje, poznatije kao *e-Business*, mora biti definisano kao određeni poslovni proces, baziran na automatizovanom informacionom sistemu, što se danas najčešće realizuje uz pomoć naprednih *Web* tehnologija i aplikacija, i sve većem broju raspoloživih mrežnih servisa koji generalno olakšavaju sve procese koji posredno i neposredno opslužuju elektronsko poslovanje i samim tim korisnicima pružaju usluge čime se poslovanje između kompanija dodatno olakšava.

Da bi se upravljalo bilo kojom organizacijom, to sa sobom uključuje donošenje odluka i rešavanje problema, a u tu svrhu su neophodne informacije i znanja.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji je mentor dr Darko Stefanović, vanr. prof.

Informacioni sistem obezbeđuje informacije koje su neophodne za donošenje odluka i rešavanje problema. Samim tim, značaj prenosa određenih informacija sa sobom nosi i probleme, svrsishodno tome inženjeri su osmislili pametne aplikacije za prenos dokumenata, izveštaja, elektronskim putem, koji mogu biti potpisani elektronskim potpisom.

Savremene tehnologije omogućavaju slanje velikog broja informacija u kratkom vremenskom period na velike razdaljine što u stvari omogućava kompanijama da efikasnije obavaljuju svoje svakodnevne zadatke. U dosadašnjem periodu, elektronsko poslovanje doživelo je posebnu ekspanziju u maloprodaji, izdavaštvu i finansijskim uslugama. Prednosti elektronskog poslovanja u odnosu na tradicionalno su značajne. Vezane su za povećanje kvaliteta i za sniženje prodajnih cena, smanjenje vremena izlaska na tržište kao i realizovanje transkacija. Ono što je danas posebno popularno jeste razvoj elektronskih partnerstava, baziran na zajedničkom nastupu pojedinih kompanija na elektronskom tržištu. Sam razvoj elektronskih partnerstava, doprineo je uvođenje i razvoj elektronskog potpisivanja u oblast elektronskog poslovanja, što je omogućilo značajan napredak među kompanijama. Samim tim olakšana je komunikacija, kao i samo poslovanje sa državnom upravom, bankama, institucijama i poslovnim partnerima, sa ciljem da se ostvare uštede u vremenu i troškovima.

2. POJAM I DEFINICIJA ELEKTRONSKOG POTPISA U INFORMACIONIM SISTEMIMA

Kada se govori o elektronskom potpisu u informacionim sistemima, pre svega se misli na tehnologiju čijom se primenom u sistemima elektronskog poslovanja omogućava provera autentičnosti potpisnika, date poruke ili dokumenta. Analogno svojeručnom potpisu u standardnom poslovanju, elektronski potpis se koristi u elektronskom poslovanju koji ima i dodatnu osobinu da štiti integritet i elektronski potpisane poruke, dok svojeručni potpis to nema.

Zakon o elektronskom potpisu definiše isti na različite načine:

- Elektrosnki potpis, jeste skup podataka u elektrosnkom obliku, koji su pridruženi ili logički povezani sa elektronskim dokumentom i služe za identifikaciju potpisnika. [3],
- Kvalifikovani elektronski potpis, jeste elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje

odgovornosti za njihov sadržaj, koji ispunjava uslove utvrđene Zakonom o elektronskom potpisu [3].,

Da bi bio validan, kvalifikovani elektronski potpis mora da zadovolji sledeće uslove, da bude povezan isključivo sa potpisnikom, da nedvosmisleno identifikuje potpisnika, da nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika, da direktno bude povezan sa podacima na koje se odnosi i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka, da bude formiran u skladu sa sredstvima za formiranje kvalifikovanog elektronskog potpisa [3]. Provera se vrši na osnovu kvalifikovanog elektronskog sertifikata potpisnika.

Kvalifikovani elektronski potpis, koji zadovoljava prethodno navedne uslove, u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpisni pečat. Podaci za formiranje elektronskog potpisa su podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik koristi za izradu elektronskog potpisa. Sredstva za formiranje elektronskog potpisa predstavljaju odgovarajuća tehnička sredstva kao što su softver i hardver, koja se mogu koristiti za formiranje elektronskog potpisa, uz korišćenje podataka za formiranje elektronskog potpisa. Između ostalog, takođe značajnu ulogu ima i elektronski sertifikat, koji predstavlja elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika. Da bi se izdao elektronski sertifikat, potrebno je odgovorno pravno lice koje izdaje takav sertifikat u skladu sa odredbama zakona, a to je sertifikaciono telo.

Zakon posebno ističe da se elektronskom dokumentu ne može osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku. Da elektronski potpis može imati pravno dejstvo i da se može koristiti kao dokazno sredstvo u zakonom uređenom postupku, osim kada se u skladu sa posebnim zakonom zahteva da samo svojeručni potpis ima pravno dejstvo i dokaznu snagu [3].

2.1 Realizacija elektronskog potpisa

Za formiranje elektronskog poptisa, neophodno je koristiti i posedovati kvalifikovani sertifikat, koji je izdat od strane sertifikacionog tela, koje ispunjava odgovarajuće uslove prema Zakonu o elektronskom potpisu.

U ovom tehnološkom trenutku, da bi se realizovao jedan elektronski potpis, neophodna je primena asimetričnih kriptografskih sistema kao što su na primer *RSA* algoritam i *Hash* algoritam (*MD5* ili *SHA-1* algoritmi), dok se kao sredstva za formiranje elektronskog potpisa uglavnom koriste pametne (*engl. Smart)* kartice. Primer *Hash* algoritma može se videti na slici 1. [2].

Slika 1: *Hashing primer, korišćenjem SH1 klase* [2]

2.2 Tehnologija elektronskog potpisa

U slučaju digitalnog potpisa, sadržaj koji treba da se potpiše prvo se redukuje u otisak poruke (*engl. Message digest*), primenom nekog od metoda za kreiranje otiska poruke, *message-digest* algoritma, u prethodno spomenutim primerima, *MD5* ili *SHA-1* algoritama, a zatim se dobijeni otisak poruke šifruje primenom, *RSA* algoritma, koristeći privatni ključ (*engl. Private key*) potpisnika poruke. Šifrovani otisak poruke predstavlja digitalni potpis date poruke i postaje njen pridruženi deo. Kada ovakva poruka stigne do primaoca kojem je namenjena, izvršava se postupak verifikacije digitalnog potpisa. Ovakav postupak se sastoji od dešifrovanja otiska dobijene poruke primenom *RSA* algoritma, uz upotrebu javnog ključa (*engl. Public key*) pošiljaoca (potpisnika) poruke. Slika 2, prikazuje primer enkripcije podataka *Encryption algorithm* korišćenjem *RSA*, dok slika 3 prikazuje dekripciju (*engl. Decription*) podataka [2].

Slika 2: *RSA algorithm, primenom Encrypt metode* [2]

Slika 3: *RSA algorithm, primenom Decrypt metode* [2]

Po dešifrovanju digitalnog potpisa, primalac poruke izvrši isti **MD5** *(enlg. Message digest)* postupak nad dobijenom porukom. Ukoliko je dobijeni otisak poruke identičan sa dešifrovanom vrednošću otiska, verifikacija se smatra uspešno obavljenom, u suprotnom se smatra negativnom i poruka se odbacuje kao nevalidna. Potpisana elektronska dokumenta se razmenjuju u formi dokumenta u kojima su ugrađeni osnovni podaci o postupku, algoritmu i kvalifikacionom elektronskom sertifikatu potpisnika, kako bi primalac elektronskog dokumenta mogao proveriti kvalifikovani elektronski potpis na bazi usaglašene tehnologije i postupka.

3. PRIMENA ELEKTRONSKOG POTPISA

Sa razvojem digitalizacije i ubrzanim tehnološkim razvojem, javila se potreba da se ujedno smanji i količina papirne dokumentacije koja neminovno prati svaki poslovni proces. Takođe, kako i svaki poslovni dokument prati svojeručni potpis ovlašćenog lica u pravnom licu ili potpis fizičkog lica, to se i sam proces vremenski usporava čekanje da konkretno lice potpiše dokument. Da bi se koristio elektronski potpis, odnosno elektronski pečat potrebno je povezati ga sa određenim licem i identitetom, a to se vrši pomoću navedenog elektronskog sertifikata kao vrste potvrde koje izdaje nadležni organ – jedno od sertifikacionih tela, na osnovu dozvole nadležnog ministarstva ima pravo da izdaje potrebne elektronske sertifikate. Od malog broja ovlašćenih sertifikacionih tela mogu se izdvojiti Privredna komora Srbije i Sertifikaciono telo pri Ministarstvu unutrašnjih poslova Republike Srbije. Privrednoj komori Srbije kao ovlašćenom sertifikacionom telu za izdavanje elektronskog potpisa i pečata, postupak se sprovodi popunjavanjem zahteva za izdavanje sertifikata, a takođe postoji i mogućnost opoziva istog. [1]

3.1 Prednosti primene elektronskog potpisa u kompanijama

Kao osnovne karakteristike primene elektronskog potpisa u kompanijama, izdvajaju se:

1. Značajne promene odnosa između klijenata, zaposleni je u mogućnosti da promeni lokaciju, i putem Interneta, jednim klikom potpiše neki dokument koji će biti validan kao svojeručni potpis,
2. Povećana brzina, promene u digitalnoj ekonomiji i poslovanju se otvaruju velikom brzinom, odnosno koncepti koji su pokazali da doprinose veliki uspeh, veoma brzo se implementiraju na ostalim *Web* lokacijama. Sve više je takvih kompanija koje se ugledaju na uspeh i rast konkuretne kompanije, na primer ukoliko jedna kompanija koristi elektronski potpis kako bi efikasnije obavljala svoja poslovanja, velike su šanse da će to isto uraditi i neka druga kompanija,
3. Udaljenost između kompanija, više nije bitan parametar u poslovanju, ne ubraja se više u opterećujući faktor u uspostavljanju poslovnih odnosa, stvaranju partnerskih odnosa sa udaljenim dobavljačima, poslovanju sa krajnjim korisnicima ili stvaranju sličnih odnosa, [5]
4. Globalno tržište, *Internet* je omogućio stvaranje globalne ekonomije, gde tržište obuhvata neverovatno veliku bazu korisnika povezanih preko ovog medija. Globalna mreža omogućava stvaranje kanala komunikacije između poslovnih partnera, što je veliki značaj za potpisivanje neizostavnih dokumenata prilikom određenih transakcija partnerskih kompanija. [5]

4. IMPLEMENTACIJA ELEKTRONSKOG POTPISA U INFORMACIONOM SISTEMU KOMPANIJE ZA PROIZVODNJU NAFTE I GASA

Implementacija aplikacije elektronskog potpisa jeste klijent-server aplikacija, u kojoj je razdvojen prezentacioni sloj od poslovne logike, jednim delom, upotrebom tehnologije *Web API*. Programski jezik u kojem je pisan kod jeste *C#*, dok je cela implementacija aplikacije napisana u *Microsoft* tehnologijama, alatu *Visual Studio* za deo namenjen serverskom *back-end* delu, dok je sa druge strane deo klijentske strane *front-a* pisan u *Angular-u 5*, alatu *Visual Studio Code*. Za skladištenje podatka korišćena je *MSSQL* baza podataka, kreirana upotrebom *Entity Framework Code First* migracija.

Novokreirani dokument, sastoji se od određenih polja koja su neophodna da čine sastavni deo jednog dokumenta koji se šalje na potpis. Obavezna polja su *Signature field, i Initials field*. Pored navedenih polja, pošiljalac ima mogućnost da doda i polja kao što su *Text field*, ukoliko želi sam nešto da doda, ili podseti primaoca, zatim *Input Field*, ukoliko želi dodatnu poruku od potpisnika dokumenta, kao i polja *Date*, koje predstavlja datum koji unosi pošiljalac dokumenta, i polje *Input Date* koje popunjava primalac, odnosno potpisnik dokumenta. Takođe, kreator dokumenta, ima mogućnost da obriše željeno polje, ukoliko se u toku kreiranja i sastavljanja dokumenta predomisli, ili promeni trenutnu odluku. Pravo brisanja određenog polja, kao i samog dokumenta, ima upravo osoba koja je iste i kreirala.

Sledeći korak pripreme dokumenta, jeste dodavanje korisnika na tačno određeno polje koje je potrebno potpisati. Dokument se smatra validnim, ukoliko pošiljalac dokumenta dobije natrag potpis od svih korisnika kojima je dokument poslat.

Slika 4: *Dijalog za unos svojeručnog potpisa*

```
switch (fieldData.TypeId)
{
    case FieldType.Signature:
    case FieldType.Initials:

        var bitmap = CreateBitmapFromBase64String(fieldData.FieldValue);
        if (bitmap != null)
        {
            using (var bitmapStream = new MemoryStream())
            {
                bitmap.Save(bitmapStream, ImageFormat.Png);

                // Add image to Images collection of Page Resources
                pdfPage.Resources.Images.Add(bitmapStream);

                // Using GSave operator: this operator saves current graphics state
                pdfPage.Contents.Add(new Operator.GSave());

                // Create Rectangle and Matrix objects
                var rectangle = new Aspose.Pdf.Rectangle(lowerLeftX, lowerLeftY + fieldHeight,
                    upperRightX, upperRightY + fieldHeight);
                var matrix = new Matrix(new[]
                {
                rectangle.URX - rectangle.LLX, 0, 0, rectangle.URY - rectangle.LLY,
                rectangle.LLX, rectangle.LLY
            });

                // Using ConcatenateMatrix (concatenate matrix) operator: defines how image must be placed
                pdfPage.Contents.Add(new Operator.ConcatenateMatrix(matrix));
                var ximage = pdfPage.Resources.Images[pdfPage.Resources.Images.Count];

                // Using Do operator: this operator draws image
                pdfPage.Contents.Add(new Operator.Do(ximage.Name));

                // Using GRestore operator: this operator restores graphics state
                pdfPage.Contents.Add(new Operator.GRestore());
            }
        }

        break;
```

Slika 5: *Kod za iscrtavanje potpisanog polja*

Kada primalac dobije dokument, moguće opcije koje može da izabere su*: Approve ili Reject*. Ukoliko se odluči za opciju *Approve*, to bi značilo da je spreman da potpiše dokument na svim mestima gde je pošiljalac naveo, dok akcija *Reject* označava da primalac dokumenta odbija da potpiše pristigli dokument. Prikaz dijaloga, gde primalac može ispisati mišem svojeručni potpis jeste slika 4.

5. ZAKLJUČAK

Korišćenje elektronskog potpisa, dovelo je do mogućnosti fleksibilnije interkomunikacije između sedamnaest kompanija koje rade nezavisne usluge, kao i velike promene u radu. U kombinaciji sa elektronskim poslovanjem i primenom Zakona o elektronskom potpisu, rad kompanija je ubrzan višestruko i samim tim omogućeno efikasnije poslovanje.

Rastom poslovanja, informacioni sistem postaje sve teži za održavanje, što zaposlenima stvara manjak vremena kada je su u pitanju dokumenti koje treba validirati i potpisati. Uvođenje ovakvog tipa aplikacije, ispostavilo se kao prednost i olakšan process poslovanja između kompanija.

Potpisivanje dokumenata elektronskim potpisom, donelo je mogućnost interkomunikacije u sistemu, kao i mogućnost spajanja i boljeg praćenja sistema kao celine. Osim tehnoloških preduslova potrebno je ostvariti i unaprediti i zakonske pretpostavke koji će omogućiti nesmetan razvoj elektronskog poslovanja, zaštitu autorskih prava i privatnosti, i samim tim osigurati univerzalni pristup mreži i adekvatnu politiku određivanja cena za pristup mreži kao i korišćenju informacija.

6. LITERATURA

[1] Web strana sertifikacionog tela MUP-a, http://ca.mup.gov.rs/home.html

[2] https://www.codeproject.com/Articles/14150/Encrypt-and-Decrypt-Data-with-C

[3] ZAKON O ELEKTRONSKOM POTPISU ("Sl. glasnik RS", br. 135/2004).

[4] Jakobsson Markus, Zulfikar Ramzan,(2008) : Crimeware: Understanding New Attacks and Defenses, Addison Wesley Professional

[5] Pleskonjić D., Maček N., Đorđević B., Carić M. (2007) : Sigurnost računarskih sistema i mreža, Beograd.

[6] F. Bonchi et al., „Social Network Analysis and Mining for Business Applications”, ACM Transactions on Intelligent Systems and Technology (TIST), vol. 2, no. 3, 2011.

[7] G. J. Hwang et al., „Criteria, Strategies and Research Issues of Context-Aware Ubiquitous Learning”, Educational Technology & Society, vol. 11, no. 2, pp. 81–91, 2008.

Biografija:

Ana Cvejić rođena je 1992. godine u Šapcu. Godine 2011 obrazovanje nastavlja na Fakultetu tehničkih nauka u Novom Sadu, smer Inženjerski menadžment. Nakon završenih osnovnih akademskih studija, 2016. godine upisuje master akademske studije, program Inženjerstvo informacionih sistema.