DOI: 10.7251/GFP2111186M

UDC: 351.755.62:57.081.1][:004.738.5

Pregledni naučni rad

Datum prijema rada:
14. maj 2021.

Datum prihvatanja rada:
30. jun 2021.

Pravna prihvatiljivost nivoa bezbjednosti sistema elektronske identifikacije

Apstrakt: Sajber prostor se profiliše kao dominantna globalna arena za posredovanje u razmjeni roba i usluga. Sajber prostor zauzima sve veću ulogu u zadovoljavanju socijalnih potreba savremenog čovjeka. Usluge koje pružaju organi javne uprave se pomjeraju prema internetu i savremenim informaciono-komunikacionim tehnologijama. U takvom okruženju sve više dolazi do izražaja neophodnost i potreba da se pojedinac pouzdano identifikuje i da se potvrdi veza između stvarnog identiteta i identiteta koji se predstavlja u sajber prostoru. Elektronska trgovina, kao i elektronsko poslovanje u najvećem broju slučajeva podrazumjeva posjedovanje kretne kartice kao instrumenta bezgotovinskog platnog prometa. Kreditna kartica je, dakle, prepoznata i kao instrument kojim se potvrđuje identiteta pojedinca u okviru elektronskih interakcija, a banka se može posmatrati i kao pružalac usluga povjerenja u postupcima elektronske identifikacije. U velikom broju elektronskih transakcija u sajber prostoru se, često, ne javlja potreba za potvrdom identiteta putem kreditne kartice, jer se ne vrši nikakva finansijska transakcija. Istovremeno se javlja potreba da se pouzdano utvrdi identitet pojedinca u sajber prostoru. Intenzivan razvoj interneta, te transfer velikog broj poslovnih, ali i socijalnih aktivnosti u ono što se naziva sajber prostor doveo je do potrebe prilagođavanja pravnih rješenja kojima se oblikuje i reguliše internet, odnosno gore pomenuti sajber prostor. Tako se razvio i sistem pouzdanog digitalnog ovjeravanja transakcija i prepoznavanja identiteta pojedinca kod pojave u sajber prostoru. U Republici Srpskoj, ali i Bosni i Hercegovini usvojila zakonska regulativa kojiom se prepoznaju elektronski potpis, te usluge povjerenja i elektronske identifikacije. Evropska unija je, još 1999 godine usvojila regulativu vezanu za digitalne potpise koja je zamjenjena Regulativom o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutrašnjem tržištu broj 910/14, popularno nazvana eIDAS. Pored toga što se eIDAS regulativnom izjednačava pravna valjanost elektronskog dokumenta i elektronskog poslovanja sa tradicionalnim dokumentom i poslovanjem, uvode se i pravno definišu nivoi elektronske identifikacije. U okviru rada su, upravo i obrađeni nivoi elektronske identifikacije, te moguća rješenja u zakonodavstvu i praksi u R. Srpskoj i Bosni i Hercegovini.

Ključne riječi: usluga povjerenja, elektronska identifikacija, kvalifikovani digitalni potpis, napredni digitalni potpis, jednostavan digitalni potpis, uređaj za izradu pečata i potpisa.

Siniša Macan
Doktor nauka iz oblasti računarstva i informatike

1. UVODNI DEO

Razmjena robe, usluga i kapitala, ali i veliki broj socijalnih aktivnosti dobija potpuno novu dimenziju razvojem informaciono-komunikacionih tehnologija koja se desila u poslednjih trideset godina i zaživljavanjem sajber prostora. U poslednjoj deceniji, obim maloprodaje putem elektronske trgovine se povećao 3,2 puta. Globalni obim elektronske trgovine u 2014 godini je iznosio 1336 milijardi američkih dolara, dok je u 2020 godini povećan na 4280 milijardi američkih dolara[1], sa projektovanim trendom rasta do 2023 do cca 5900 milijardi dolara. Istovremeno, statistike pokazuju[2] da je broj korisnika interneta u svijetu oko 4,5 milijardi ljudi, dok društvene mreže koristi cca 3,8 milijardi ljudi.

Navedene cifre pokazuju izuzetan potencijal sajber prostora, ali otkrivaju i potrebu za pouzdanijom identifikacijom pojedinaca i smanjenjem rizika od raznih vrsta zloupotreba. U ovom kontekstu treba posmatrati i tržište u Republici Srpskoj i Bosni i Hercegovini. Korisnik usluge, kupac robe, ali i svaki pojedinac koji pristupa internetu ili društvenim mrežama iz Republike Srpske jeste dio globalnog sajber prostora sa svim prednostim i rizicima koje nosi ovaj prostor. U takvim novim uslovima sajber prostora javila se potreba za regulisanjem ponašanja, posebno u domenu identiteta i pristupa globalnoj mreži kod obavljanja raznih vrsta transakcija.

Sa aspekta zaštite prava i zakonitosti, izuzetno bitno je da se uspostavi nedvosmislena relacija između stvarnog i digitalnog identiteta prilikom obavljanja elektronskog poslovanja, ali i kod učešća na globalnim mrežama ili u transakcijama koje obavljaju javni organi sa građanima i pojedincima.

Republika Srpske, odnosno Bosna i Hercegovina se nalaze u postupku integracije sa Evropskom Unijom. Sporazum o stabilizaciji i pridruživanju između Evropske Unije, odnosno država članica, s jedne strane, i Bosne i Hercegovine, s druge strane potpisan je u Luksemburgu 16. juna 2008. godine. Sporazum je stupio na snagu 1. juna 2015. godine.[3] Sporazuma o stabilizaciji i pridruživanju je pravno obavezujući u Bosni i Hercegovini i u Republici Srpskoj, tako da postoji obaveza usklađivanja propisa u BiH sa propisima Evropske unije.[4]

Digitalne usluge, te reforma tržišta roba i usluga koje promoviše elektronsko poslovanje i trgovinu predstavlja jedan od prioriteta Evropske unije. U reformama koje su sprovedene na prostoru Evropske unije se značajno transformisalo zakonodavstvo vezano za digitalne identiteta, posebno u kontekstu bezbjednost. Transformacije koje su se dešavale su bazirane na naučno-tehnološkom razvoju što predstavlja jedan od temelja Ugovora o funkcionisanju Evropske unije.[5]

---

[1] Dostupno na: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/, (12.5.2021).

[2] Dostupno na: https://wearesocial.com/digital-2020, (12.5.2021).

[3] Dostupno na: https://www.dei.gov.ba/bs/stabilization-agreement, (12.5.2021).

[4] Čl. 70, st. 1 Sporazuma o stabilizaciji i pridruživanju između Bosne i Hercegovine i Evropske Unije glasi: „1. Strane priznaju važnost usklađivanja postojećeg zakonodavstva Bosne i Hercegovine sa zakonodavstvom Unije, kao i njegovog efikasnog provođenja. Bosna i Hercegovina će nastojati osigurati postepeno usklađivanje svojih postojećih zakona i budućeg zakonodavstva s pravnom tekovinom (acquisem) Unije. Bosna i Hercegovina će osigurati propisnu primjenu i provođenje postojećeg i budućeg zakonodavstva."

[5] Čl. 114 Ugovora o funkcionisanju Evropske Unije navodi u stavu 3: „Komisija, u svojim predlozima iz stava 1 koji se odnose na zdravlje, bezbjednost, zaštitu životne sredine i zaštitu potrošača, uzima za polaznu osnovu visoki nivo zaštite, naročito vodeći računa o svakom novom razvoju zasnovanom na naučnim činjenicama. I Evropski parlament i Savjet, u okviru svojih nadležnosti, teže postizanju ovog cilja."

Tržište digitalnih usluga, ali i društvene mreže i druge aktivnosti koje se ostvaruju putem interneta zahtjevaju oprezno regulisanje sajber prostora u kome su povezani računarski sistemi. „Sajber prostor je nefizički prostor u kome, prema trenutnom važećem zakonodavstvu, ne postoje nacionalne granice i uspostavljaju se nova pravila, bazirana na tehničkim mogućnostima računarskih sistema“[6]. „Sajber prostor je nova vrsta prostora koji se sastoji od Interneta, World Wide Web[7], odnosno osnovne infrastrukture i informacija o internetu i WWW, nakon poznatih i tradicionalnih četiri vrste prostora: kopno, more (okean), vazdušni prostor (atmosferski prostor, ili unutrašnji prostor) i svemir. Sajber prostor je zapravo peti prostor u kome savremeni čovjek živi, radi, igra se i posluje.“[8] U okviru sajber prostora, a posebno prilikom obavljanja digitalnih transakcija koje zahtjevaju određen nivo pouzdanosti, neophodno je da se obezbjede mehanizmi provjere identiteta lica.

Zemlje članice Evropske unije su u prethodnih 25 godina prepoznale potrebu za pouzdanom identifikacijom prilikom obavljanja transakcija u sajber prostoru, pa je tako 1999 godine usvojena prva direktiva koja se bavi digitalnim identitetima, odnosno digitalnim potpisima[9]. Kroz višegodišnju primjenu Direktive o elektronskim potpisima uspostavljeni su sistemi za digitalnu identifikaciju u zemljama članicama, ali su se javili problemi usklađenosti i interoperabilnosti sistema između država članica. Ovo je dovelo do potebe reforme propisa vezanih za digitalnu identifikaciju, kako bi se stvorili jednaki uslovi u svakoj zemlji članici. Shodno navedenom, usvojena je Uredba o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutrašnjem tržištu broj 910/14 (u daljem tekstu: *eIDAS*). Uredbom *eIDAS* je, prevashodno stvoren pravni osnov za uspostavu sistema elektronske identifikacije i usluga povjerenja koje će biti unificirane i priznate jednako u svim zemljama članicama Evropske unije. Definisani su postupci koji obezbjeđuju da se kroz proces akreditacije[10] postigne cilj da svaki pružalac usluge povjerenja, odnosno certifikaciono tijelu zadovoljava tehničke uslove u skladu sa standardima i preporukama. Postupak akreditacije se provodi na unificiran način[11], što garantuje ujednačene uslove na cijeloj teritoriji Evropske Unije.

Ono što je bitno jeste da su Uredbom 910/14 definisani i određeni nivoi bezbjednosti, a na osnovu kojih se utvrđuje pravna snaga usluge povjerenja elektronske identifikacije, odnosno digitalnog potpisa[12]

Bosna i Hercegovina, odnosno Republika Srpska imaju pravnu obavezu da usklađuju svoje zakonodavstvo sa zakonodavstvom Evropske unije.

---

6 Macan, S. (2020). Procjena usklađenosti u postupku primjene zakona o digitalnom potpisu Republike Srpske i usaglašenost sa eIDAS regulativom. *Godišnjak Fakulteta pravnih nauka*, 10, 241-255.

7 World Wide Web – usluga interneta koja se najčešće koristi i koja omogućava pristup dokumentima putem linkova i otvaranjem novih stranica, skraćeno WWW. U osnovi, to je mreža stranica koje su povezane

8 Song, Y. Y. (2019). *Cybercryptography: Applicable Cryptography for Cyberspace Security*. Springer Nature Switzerland, https://doi.org/10.1007/978-3-319-72536-9;

9 Direktiva 1999/93/EZ Evropskog parlamenta i Savjeta od 13. decembra 1999. o okviru Unije za elektronske potpise.

10 U Odjeljku 2, eIDAS Uredbe broj 910/14 definisana je obaveza provjere usklađenosti, koju zahtjeva Nadzorno tijelo.

11 Uredba (EZ) br. 765/2008 o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište.

12 Shodno članu 3. eIDAS-a, digitalni potpis se definiše se kao “podaci u elektronskom obliku koji se prilažu ili logički povezuju s drugim podacima u elektronskom obliku i koje potpisnik koristi za potpisivanje”

U radu se obrađuju nivoi bezbjednosti elektronske identifikacije, uz pregled prakse u Bosni i Hercegovini, te susjednim zemljama. Istraživanje se vrši kroz analizu zakonskih i podzakonskih akata, regulative Evropske unije, te praksi koje se primjenjuju.

2. NIVOI POUZDANOSTI I BEZBJEDNOSTI KOD UTVRĐIVANJA DIGIRALNOG IDENTITETA

Pružanje usluga elektronske identifikacije[13] i elektronskih potpisa[14] ima za cilj da omogući pouzdanu identifikaciju kod pristupa sajber prostoru. Uredbom *eIDAS* je regulisano između ostalog i sledeće: [15]

- Utvrđivanje uslova pod kojima države članice priznaju sredstva elektronske identifikacije fizičkih i pravnih lica koja su obuhvaćena prijavljenim sistemom druge države članice,
- Utvrđuju se pravila za usluge povjerenja, posebno za elektronske transakcije,
- Uspostavlja se pravni okvir za elektronske potpise, elektronske pečate, elektronske vremenske žigove, elektronske dokumente, usluge elektronske preporučene dostave i usluge certificiranja za autentikaciju mrežnih stranica.

Kako bi se prikazala suština potrebe za elektronskom identifikacijom, neophodno je definisati pojmove realnog identiteta, odnosno pravnog i digitalnog identitata.

Svaki pojedinac se u realnom svijetu identifikuje i prepoznaje na osnovu svog porijekla, odnosno imena i prezimena, te datuma i mjesta rođenja. Realan identitet pojedinca čini skup svih podataka koji određuju tog pojedinca, a organi javne uprave kroz zakonom utvrđen postupak na osnovu skupa poznatih podataka o ličnosti utvrđuju jedinstvene identifikatore za svakog pojedinca. Ovako utvrđen identetet se naziva pravni identitet. Pravni identitet predstavlja podskup od svih podataka o nekom pojedincu, a na osnovu kojih se taj pojedinac identifikuje. Kao posljedica ovakvog postupka organi javne uprave pojedincima izdaju identifikacione dokumente.

Realni i pravni identitet se mogu opisati na sledeći način":[16]

1. Ličnost po rođenju dobija određene karakteristike koje mogu biti fizičke, geografske, vremenske i slično
2. Na osnovu karakteristika se kreira identitet ličnosti
3. Identitet ličnosti je skup podataka koji jedinstveno određuju ličnost, kao što su:
   a. Ime, prezime,
   b. Podaci o roditeljima i podaci o rođenju

---

[13] Elektronska identifikacija je postupak korištenja ličnim identifikacionim podacima u elektronskom obliku koji nesporno predstavljaju fizičko ili pravno lice ili fizičko lice odgovorno u pravnom licu, prema eIDAS

[14] Elektronski potpis predstavljaju podaci u elektronskom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektronskom obliku i koje potpisnik koristi za potpisivanje, prema eIDAS

[15] Macan, S., Karan, S. (2019). Ustavnopravni osnov primjene EU uredbe o elektronskoj identifikaciji i uslugama povjerenja u Republici Srpskoj. *Godišnjak Fakulteta pravnih nauka*, 9, 160-175.

[16] Macan, S. (2018). *Registri za identifikaciju građana – Zaštita ljudskih prava i efikasna državna uprava* (doktorska disertacija), Fakultet pravnih nauka Panevropskog univerziteta Apeiron, Banja Luka.

c. Fizički podaci o ličnosti i podaci koji se nadleđuju
d. Zdravstveni podaci
e. Socijalni podaci
f. Vještine ličnosti
g. Sklonosti su podaci koji karakterišu navike lica

4. U realnom svijetu su dostupni resursi kojima ličnost ima interes da pristupa
5. Ličnost dokazuje svoj identitet na osnovu dokumenta koje izdaje ovlašteni organ, odnosno identifikacionog dokumenta
6. U postupku prepoznavanja, odnosno autentikacije u realnom svijetu, se utvrđuje da li lice sa određenim identitetom (odnosno identifikacionom dokumentom) ima pravo da pristupi određenim resursima"
7. Pojavom sajber prostora javila se potreba da se ličnosti iz realnog svijeta identifikuju u digitalnom svijetu, te se na taj način kreira digitalni identitet. Prilikom obavljanja aktivnosti u sajber prostoru neophodno je stvoriti određen nivo pouzdanosti, odnosno povjerenja u digitalni identitet i njegovu vezu sa stvarnim identitetom. U realnom svijetu, te kod obavljanja određenih stvarnih transakcija ili traženja određenih usluga se često traže različiti nivoi identifikacije. Nekada je dovoljno da se pojedinac samo pojavi i traži određenu uslugu. Pružalac usluga uopšte nema potrebu da utvrđuje stvarni identitet, odnosno uspostavlja odnos povjerenja bez dodatnih provjera. Međutim, određene transakcije koje se dešavaju u stvarnom svijetu zahtjevaju utvrđivanje identiteta lica, a nekada je potrebno da se određene aktivnosti obavljaju uz prisustvo treće strane koja je, najčešće ovlaštena od strane države. Tako, kada se lice pojavi u prodavnici da kupuje određenu robu, uopšte se ne traži identifikacija lica. Ukoliko se na primjer, podnosi zahtjev za izdavanje dokumenta ili neku drugu uslugu, onda je potrebno da lice pokaže lični dokument i dovoljno je da se potpiše. Međutim, kod određenih poslovnih ili privatnih transakcija, kao što su zaključenje ugovora većih vrijednosti ili prodaja nekretnina, potrebno je da se identitet potvrdi ličnim dokumentom, a takve transakcije ovjerava notar. U realnom svijetu se, dakle, javlja potreba za različitim nivoima bezbjednosti kod identifikacije.

Analogno gore navedenom, u okviru *eIDAS* regulative su prepoznati različiti nivoi digitalne identifikacije[17]. Shodno potrebama iz realnog svijeta, gdje se, kod obavljanja ra-

[17] U preambuli 16 eIDAS regulative se već govori o nivoima identifikacije: „Nivo osiguranja identiteta trebale bi označivati stepen pouzdanosti u sredstva elektronske identifikacije pri utvrđivanju identiteta pojedinca, te na taj način osigurati da pojedinac koja se predstavlja pod određenim identitetom stvarno jest pojedinac kojoj je taj identitet dodijeljen. Nivo bezbjednosti zavisi od stepena pouzdanosti koji sredstvo elektronske identifikacije pruža u odnosu na traženi ili utvrđeni identitet pojedinca uzimajući u obzir postupke (na primjer dokazivanje identiteta i verifikaciju te autentikaciju), aktivnosti upravljanja (na primjer organ koje izdaje sredstva elektronske identifikacije i postupak izdavanja takvih sredstava) i provedene tehničke kontrole. Postoje različite tehničke definicije i opisi nivoa bezbjednosti koje su posljedica pilot-istraživanja finansiranih sredstvima Unije, kao i normiranja i međunarodnih aktivnosti. Posebno, opsežni pilot-projekti STORK i ISO 29115 odnose se, između ostalog, na nivoe 2, 3 i 4, o čemu bi trebalo voditi u najvećoj mogućoj mjeri računa pri određivanju minimalnih tehničkih zahtjeva, normi i postupaka za nizak, značajan i visok nivo bezbjednosti u smislu ove eIDAS, osiguravajući

zličitih transakcija ili radnji zahtjeva različit nivo identifikacije, u okviru Uredbe *eIDAS* se definišu tri nivoa bezbjednosti sredstava elektronske identifikacije[18]:

1. Nizak nivo bezbjednosti[19]
2. Značajan nivo bezbjednosti[20]
3. Visok nivo bezbjednosti[21]

Elektronski potpis predstavlja, shodno članu 3 *eIDAS* „podatke u elektronskom obliku koji se prilažu ili logički povezuju s drugim podacima u elektronskom obliku i koje potpisnik koristi za potpisivanje". Dakle i običan potpis u elektronskoj poruci zadovoljava navedenu definiciju elektronskog potpisa. Međutim, shodno nivoima bezbjednosti sredstava elektronske identifikacije, u odnosu na pravnu snagu, možemo definisati sledeće nivoe elektronske identifikacije:

1. Jednostavne elektronske potpise[22], koji predstavljaju bilo koji potpis u digitalnom obliku, kao što je potpis elektronske pošte. Ovakav potpis nema nikakvu pravnu težinu i može se posmatrati analogno situaciji iz realnog svijeta u kome pojedinac izvrši svoje predstavljanje bez pružanja ikakvih dokaza.
2. Napredne elektronske potpise[23], potpise kojim se može napraviti veza sa stvarnim identitetom. Jedinstven je za stvarnog korisnika, međutim nema pravnu snagu. Česta tehnička rješenja su vezana za upotrebu biometrijskih podataka kod identifikacije ili kod identifikacije korisnika korišćenjem nekih autentikacionih metoda.
3. Kvalifikovani elektronski potpis[24] je napredni elektronski potpis koji se kreira na kvalifikovanim sredstvima za izradu potpisa i kvalifikovanom certifikatu. Ima istu snagu kao svojeručan ovjeren potpis pojedinca. Kvalifikovanim elektronskim potpisom povećava se nivo sigurnosti u odnosu na napredni elektronski potpis

pri tome dosljednu primjenu eIDAS, posebno u pogledu visokog nivoa bezbjednosti koja se odnosi na dokazivanje identiteta za izdavanje kvalifikovanih certifikata. Utvrđeni zahtjevi trebali bi biti tehnološki neutralni. Neophodne bezbjedonosne zahtjeve trebalo bi biti moguće ispuniti primjenom različitih tehnologija.

[18] Čl, 8, st. 2 eIDAS.

[19] Čl. 8, st. 2, tač. a) eIDAS: „nizak nivo bezbjednosti odnosi se na sredstva elektronske identifikacije u kontekstu sistema elektronske identifikacije, koja pruža ograničen stepen pouzdanosti u odnosu na traženi ili utvrđeni identitet pojedinca, te se upućuje na tehničke specifikacije, norme i povezane postupke, uključujući tehničke kontrole čija je svrha smanjenje rizika zloupotrebe ili promjene identiteta"

[20] Čl. 8, st. 2, tač. b) eIDAS: „značajan nivo bezbjednosti se odnosi na sredstva elektronske identifikacije u kontekstu sistema elektronske identifikacije, koja pruža značajan stepen pouzdanosti u odnosu na traženi ili utvrđeni identitet pojedinca, te se upućuje na tehničke specifikacije, norme i povezane postupke, uključujući tehničke kontrole čija je svrha smanjenje rizika zloupotrebe ili promjene identiteta"

[21] Čl. 8, st. 2, tač. c) eIDAS: „visok nivo bezbjednosti se odnosi na sredstva elektronske identifikacije u kontekstu sistema elektronske identifikacije, koja pruža viši stepen pouzdanosti u odnosu na traženi ili utvrđeni identitet pojedinca, te se upućuje na tehničke specifikacije, norme i povezane postupke, uključujući tehničke kontrole čija je svrha smanjenje rizika zloupotrebe ili promjene identiteta"

[22] *Simple Electronic Signature* (SES)

[23] *Advanced Electronic Signature* (AdES)

[24] *Qualified Electronic Signature* (QES)

imajući u vidu da je certifikat izdat od tijela koje je prošlo postupak akreditacije i dobilo neophodne dozvole od strane organa vlasti. U postupku akreditacije izvršena provjera usklađenosti[25], te je potvrđena tehnička ispravnost i sigurnost opreme i postupaka od strane Nadzornih tijela[26] zemlje članice.

4. Elektronski potpisi imaju različite nivoe bezbjednosti, a pravna lica pružaju različite usluge, shodno utvrđenom nivou bezbjednosti u postupku identifikacije lica koje traži određenu elektronsku uslugu.

Shodno navedenom, elektronske usluge mogu biti dostupne shodno različitim nivoima identifikacije, a u zavisnosti od neophodne sigurnosti i zaštite podataka, odnosno povjerenja koja se očekuje kod pružanja usluga. Najveći nivo povjerenja se očekuje od kvalifikovanih digitalnih potpisa, te je u sledećem poglavlju obrađen postupak kojim se utvrđuje kako pravna lica stiču pravo da izdaju kvalifikovane digitalne potpise.

2.1. Pravna snaga kvalifikovanog digitalnog potpisa

Razvojem digitalnog tržišta, javila se potreba za stvaranjem jednakih uslova za izdavanje kvalifikovanih digitalnih potpisa, koji imaju jedinstvenu pravnu snagu kao i svojeručni potpisi. Takva potreba zahtjeva uspostavljanje takve zakonske regulative koja će garantovati da se na određenom tržištu izdaju kvalifikovani digitalni potpisi pod istim i sličnom uslovima, odnosno na opremi i uređajima koji garantuju zahtjevani nivo sigurnosti. Činjenica je da tržište Evropske unije predstavlja jedinstveno tržište, tako da je i u slučaju digitalnog tržišta neophodno obezbjediti interoperabilnost[27] sistema elektronske identifikacije što je jedan od ciljeva *eIDAS* regulative. Obavezu svake države članice EU jeste da prihvata sisteme kvalifikovane elektronske identifikacije u postupcima obavljanja elektronskog poslovanja, ali i pružanja elektronskih usluga, čime se postiže identično pravno tretirnje elektronskih dokumenata sa papirnim dokumentima.

Kako bi kvalifikovani digitalni potpis na cijeloj teritoriji Evropske unije, ali i u zemljama koje su u postupku pridruživanja imao identičnu pravnu snagu kao svojerečni potpis, neophodno je uspostaviti proces provjere tehničkih uslova i sigurnosti opreme

---

[25] U čl. 17, st. 4, tač. e) eIDAS je navedeno da je zadatak nadzornih tijela: obavljanje revizija ili zahtijevanje od tijela za proocjenjivanje usklađenosti da provede procjenjivanje usklađenosti kvalificiranih pružatelja usluga povjerenja u skladu s čl. 20, st. 2. eIDAS;

[26] eIDAS regulativom je definisana obaveza uspostavljanja Nadzornih organa čija je uloga, shodno članu 17 stav (3) uredbe sledeća: (a) da nadzire kvalifikovane pružaoce usluga povjerenja s poslovnim sjedištem na području države članice koja ga određuje kako bi se osiguralo, putem prethodnih (ex ante) i naknadnih (ex post) aktivnosti nadzora, da ti kvalifikovani pružaoci usluga povjerenja i kvalifikovane usluge povjerenja koje oni pružaju ispunjavaju zahtjeve utvrđene u ovoj Uredbi; (b) da, prema potrebi, preduzima mjere u odnosu na nekvalifikovane pružaoce usluga povjerenja s poslovnim sjedištem na području države članice koja ga određuje, putem naknadnih (ex post) aktivnosti nadzora, kada primi obavijest da ti nekvalifikovani pružaoci usluga povjerenja ili usluge povjerenja koje oni pružaju navodno ne ispunjavaju zahtjeve utvrđene u ovoj Uredbi.

[27] U preambuli Uredbe eIDAS, u tačkama 19, 20 i 54 se definišu obaveze vezane za interoperabilnost, dok se članom 12 Uredbe definišu obaveze zemalja članica prilikom prihavljivanja sistema elektronske identifikacije.

putem kojih ovlaštena pravna lica[28] izdaju kvalifikovane digitalne potpise. Postupak u okviru koga se provjeravaju uslovi se naziva provjera usklađenosti. Provjeru usklađenosti vrše ovlaštena akreditaciona tijela[29] koja provode identične postupke i na objektivan način utvrđuju da li su ispunjeni svi uslovi da se digitalni certifikati koje izdaju ovlaštena pravna lica mogu smatrati pouzdanim kako bi izdavli kvalifikovane digitalne certifikate. Prema *eIDAS* regulativi su uspostavljena nadzorna tijela u svakoj državi članici i ova nadzorna tijela, angažuju akreditaciona tijela koja treba da, kroz proces provjere usklađenosti[30] utvrde tehničke, organizacione i sigurnosne uslove stvorene u pravnom licu koje treba da izdaje kvalifikovane digitalne certifikate.

Upravno proces akreditacije omogućava da se napravi razlika između naprednih digitalnih potpisa i kvalifikovanih digitalnih potpisa. Česta je situacija da i napredni i kvalifikovani digitalni potpisi koriste slična tehnološka rješenja. Međutim, kvalifikovani digitalni potpis su prošli dodatne provjere od strane ovlaštenih laboratorija i potpisi izdati na ovakvim uređajima imaju identičnu pravnu snagu kao svojeručni potpisi i mogu se koristiti u bilo kakvih digitalnim transakcijama, sa punom pravnom snagom. Dokumenta potpisana sa ovakvim kvalifikovanim potpisima i u sudskim postupcima imaju identičnu pravnu snagu kao klasična dokumenta. Napredni digitalni potpisi se mogu koristiti da se podigne nivo povjerenja između pravnih subjekata kod elektronskog poslovanja.

Na ovakav način je omogućeno da se, u zavisnosti od potrebe, koriste različiti nivoi bezbjednosti kod elektronske identifikacije, što će se opisati u sledećem poglavlju.

U Bosni i Hercegovini postoji obaveza usklađivanja regulative sa regulativom Evropske unije, a shodno ustavnoj strukturi nadležnost je Republike Srpske, odnosno entiteta u Bosni i Hercegovine za usluge elektronske identifikacije[31]. Prema gore navedenom, u Republici Srpskoj je usvojn zakon o elektronskom potpisu[32] u kome su uvedeni pojmovi koji su definisani *eIDAS* uključujući i kvalifikovani elektronski potpis[33]. Shodno pravnoj regulativi u Republici Srpskoj, postoji obaveza u kojoj pravna lica da bi izdavala kvalifikovane

---

[28] Pravna lica koja izdaju kvalifikovane digitalne potpise se nazivaju certifikaciona tijela, odnosno *certification authorities* (CA)

[29] U preambuli 15 Uredbe (EZ) br. 765/2008 o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta se navodi: „Imajući u vidu da je svrha akreditacije osigurati adekvatnu izjavu o osposobljenosti određenog pravnog lica za izvođenje aktivnosti vezanih za procjenu usklađenosti, države članice ne trebaju imati više od jednog akreditacionog tijela i trebaju osigurati da to tijelo bude organizovano tako da se garantuje objektivnost i nepristranost njegovih djelatnosti. Pomenuta državna akreditaciona tijela trebaju djelovati nezavisno od komercijalne djelatnosti procjenjivanja usklađenosti. Zbog toga je potrebno predvidjeti da države članice osiguraju da se smatra da državna akreditaciona tijela u vršenju svojih provode javna ovlaštenja bez obzira na njihov pravni status.“

[30] U čl. 17, st. 4, tač. e) eIDAS je navedeno da je zadatak nadzornih tijela: obavljanje revizija ili zahtijevanje od tijela za proocjenjivanje usklađenosti da provede procjenjivanje usklađenosti kvalificiranih pružatelja usluga povjerenja u skladu s čl. 20, st. 2. eIDAS;

[31] Čl. 3, st. 3, tač. a) Ustava Bosne i Hercegovine glasi: „a) Sve funkcije i ovlaštenja koja nisu ovim Ustavom izričito povjerena institucijama Bosne i Hercegovine pripadaju entitetima.“. Oblast elektronske identifikacije i usluga povjerenja nije povjerena institucijama BiH.

[32] Zakonom o elektronskom potpisu Republike Srpske (*Službeni glasnik Republike Srpske*, br. 106/15 i 83/19).

[33] Zakonom o elektronskom potpisu Republike Srpske, članom 4 definiše kvalifikovani elektronski potpis.

digitalne potpise moraju da dobiju dozvolu resornog ministarstva[34], a na osnovu izvještaja Komisije[35] koja provjerava uslove kod tog pravnog lica. Ova odredba zakonodavstva u R. Srpskoj je u suprotnosti sa *eIDAS*[36].

U sledećem poglavlju su navedeni primjeri iz Republike Hrvatske i Republike Srbije vezano za nivoe identifikacije, odnosno mogućnosti provjere identiteta kod pružanja usluga povjerenja.

2.2. Primjeri nivoa bezbjenosti digitalnog potpisa

Pravna lica, te organi javne uprave prikupljaju i obrađuju podatke o građanima shodno zakonskoj regulativi. Ovakav način obrade podataka omogućava kreiranje usluge povjerenja elektronske identifikacije. Pravna lica koja obrađuju podatke o građanima mogu da pružaju usluge elektronske identifikacije, te da omoguće da se, uz određene metode autentikacije vrši provjera identiteta na osnovu koje se vrši pristup uslugama.

Bankarski sistem i regulatorni okvir koji se uspostavlja omogućio je da se na relativno pouzdan način prikupljaju podaci o građanima. Dalje, kroz kartično poslovanje je omogućeno da se koriste postupci provjere identiteta kod pružanja elektronskih usluga i plaćanje. Na ovaj način je omogućeno da se podaci iz banaka mogu koristiti kod pružanja usluga povjerenja.

Ovakav pristup, uz adekvatno zakonsko regulisanje koje ima osnov u *eIDAS* regulativi je omogućio da se na fleksibilan način omogući pružanje digitalnih usluga povjerenja.

Tako imamo primjer u Republici Hrvatskoj u kojoj je podignuta platforma „e Građani – informacije i usluge“[37]. Uspostavljen je Nacionalnog Identifikacioni i Autentifikacioni Sistem (NIAS) koji „posreduje između pojedinih usluga u sistemu e-Građani i izdavaoca potvrda – elektronskih potvrda identiteta krajnjih korisnika koji se služe tim uslugama. NIAS provjerava korisnikov identitet i omogućuje mu pristup pojedinim e-uslugama javnog sektora. Ujedno mu omogućuje pojedinačnu i jedinstvenu odjavu iz usluga koje koristi.“[38]

Sistemom e-Građani u Republici Hrvatskoj je kreirana jedinstvena platforma koja, shodno *eIDAS* regulativi omogućava različite nivoe sigurnosti pristupa. Tako su definisani sledeći nivoi pristupa u Republici Hrvatskoj[39]:

1. Visok nivo bezbjednosti je definisan za ukupno pet sistema pristupa i u pitanju su

[34] Čl. 22, st. 1 Zakona o elektronskom potpisu Republike Srpske glasi: „Certifikaciono tijelo iz člana 21. ovog zakona, koje izdaje kvalifikovane elektronske certifikate, može da obavlja usluge na osnovu dozvole koju izdaje Ministarstvo za naučnotehnološki razvoj, visoko obrazovanje i informaciono društvo“

[35] Čl. 22, st. 2 Zakona o elektronskom potpisu Republike Srpske glasi: „(2) Na osnovu zahtjeva certifikacionog tijela za izdavanje dozvole, ministar imenuje Komisiju za provjeru ispunjenosti uslova za obavljanje usluga izdavanja kvalifikovanih elektronskih certifikata (u daljem teksu: Komisija), koja ima tri člana.“

[36] Macan (2020), 241-255.

[37] Dostupno na: www.gov.hr, (4.5.2021).

[38] Dostupno na: https://nias.gov.hr/authentication/Step1, (4.5.2021).

[39] Dostupno na: https://nias.gov.hr/Authentication/Step2, (4.5.2021).

kvalifikovana certifikaciona tijela regustrovana u Republici Hrvatskoj[40]

2. Značajan nivo bezbjednosti, gdje se nalazi ukupno dvanaest pružaoca usluga povjerenja[41]. Uglavnom su u pitanju banke. Ovakva vrsta autentikacije je dozvoljena, s tim što nije moguće pristupati uslugama koje zahtjevaju kvalifikovan digitalni potpis
3. Nizak nivo bezbjednosti, gdje se nalaze ukupno četiri pružaoca usluge digitalne identifikacije[42]
4. Shodno gore navedenom, Republika Hrvatska je omogućila pristup elektornskim servisima putem 21 pružaoca usluga elektronske identifikacije u momentu pisanja rada. Sitaucija sa pružaocima usluga povjerenja se mijenja protokom vremena. U zavisnosti od zahtjevanog nivoa sigurnosti, omogućava se pristup određenim servisima.

Republika Srbija je uspostila platformu eUprava[43]. Prijava na usluge je moguća na tri načina[44]:

1. Kvalifikovanim digitalnim certifikatom, koji „predstavlja najviši nivo pouzdanosti i korisnicima koji se prijavljuju na ovaj način dostupne su sve usluge. Korisnici koji se prijavljuju na ovaj način mogu samostalno da generišu niže nivoe poverenja (osnovni i srednji nivo pouzdanosti) kao i da elektronski potpisuju dokumenta i zahjteve."
2. Dvofaktorska autentikacija, „prijava mobilnim telefonom (dvofaktorska autentikacija) predstavlja srednji nivo pouzdanosti i korisnicima koji se prijavljuju na ovaj način dostupno je 98% usluga. Prednost ovog načina prijavljivanja jeste u tome što korisnicima nisu potrebni kvalifikovani elektronski sertifikati, već instalirana aplikacija na njihovim pametnim uređajima (mobilni telefon ili tablet)." Međutim, na ovaj način nije moguće vršiti pravno verifikovane transakcije.
3. Prijava korisničkim imenom i lozinkom, „predstavlja osnovni nivo pouzdanosti i ovim korisnicima dostupan je ograničen broj usluga."
4. U Republici Srbiji, dakle, nisu još uvjek prepoznate banke ili druge institucije kao pružaoci usluga povjerenja.

Bosna i Hercegovina je susjedna zemlja Republike Srbije i Republike Hrvatske, sa kojima vrši veliki obim robne razmjene i koje pripadaju Evropskoj uniji, odnosno CEFTA sporazumu[45]. Interes Bosne i Hercegovine i Republike Srpske je da ima slične uslove za

---

[40] Na stranici https://nias.gov.hr/Authentication/Step2 se nalazi pet kvalifikovanih sistema elektronske identifikacije među kojima je elektronska lična karta, FINA kvalifikovani potpis, FINA kvalifikovani pečat i drugi kvalifikovani pružaoci usluga povjerenja (4.5.2021).

[41] Na stranici https://nias.gov.hr/Authentication/Step2, se nalazi ukupno dvanaest banaka, među kojima su Erste banka, Zagrebačka banka, OTP banka, Istarska banka, Zavod zdravstvenog osiguranja i drugi, (4.5.2021).

[42] Na stranici https://nias.gov.hr/Authentication/Step2, se nalazi ukupno četiri pružaocu usluga povjerenja niskog nivoa bezbjednosti, među kojima su pošta i telekom, (4.5.2021).

[43] Dostupno na: https://euprava.gov.rs/, (2.5.2021).

[44] Dostupno na: https://prijava.eid.gov.rs/, (2.5.2021).

[45] Republika Srpska i Bosna i Hercegovina najveći deo svoje poslovne razmene obavlja sa tržištem Evropske unije i zemalja CEFTA sporazuma. Prema podacima Spoljno-trgovinske komore

pristup digitalnim uslugama kao susjedne zemlje, odnosno kao zemlje Evropske unije. U sledećem poglavlju je dat kratak pregled po pitanju mogućnosti pouzdane digitalne identifikacije u BiH.

3. DIGITALNA IDENTIFIKACIJA U REPUBLICI SRPSKOJ

Članom 3. Ustava Bosne i Hercegovine su navedene direktne nadležnosti Bosne i Hercegovine.[46] Sve što nije nadležnost Bosne i Hercegovine jeste nadležnost entiteta. Usluge povjerenja i elektronska identifikacija jesu u nadležnosti Republike Srpske[47]. Slično kao u susjednim zemljama, pravna regulativa, ali i praksa u Republici Srpskoj treba da omogući uslove za efikasnu elektronsku identifikacije. Kako je ranije navedeno, u Republici Srpskoj je usvojen zakon o elektronskom potpisu[48], a ranije je usvojen i zakon na nivou Bosne i Hercegovine.[49]

U Republici Srpskoj postoji pravni osnov za vođenje registara kvalifikovanih certifikacionih tijela[50]. Također, shodno pravnoj regulativi u Republici Srpskoj, postoji osnov da MUP Republike Srpske pruža usluge kvalifikovane elektronske identifikacije[51].

Banke u Republici Srpskoj i Bosni i Hercegovini provode procedure kojima se na pouzdan način utvrđuje identitet klijenata.

Međutim, u Republici Srpskoj nisu uspostavljeni servisi pouzdane elektronske identifikacije niti je uspostavljena praksa slična praksama u susjednim zemljama ili zemljama Evropske unije.

4. ZAKLJUČAK

Intenzivan razvoj informaciono-komunikacionih tehnologija je indukovao prilagođavanje pravne regulative i propisa vezanih za pružanje digitalnih usluga. U poslednjih trideset godina se kreirao specifičan nematerijalni prostor koji je nazvan sajber prostor, kome savremeni čovjek pristupa, obavlja poslovne transakcije, ali i zadovoljava različite socijalne potrebe.

Bosne i Hercegovine, od ukupne robne razmene u 2016 godini, 65.18% se odnosi na zemlje Evropske Unije, a 13.5% na zemlje CEFTA ugovora. Dostupno na: http://www.mvteo.gov.ba/izvjestaji_publikacije/izvjestaji/default.aspx?id=8622&langTag=bs-BA, (27.3.2018.).

[46] Čl. 3, st. 1 Ustava Bosne i Hercegovine glasi: Sledeća pitanja su u nadležnosti institucija Bosne i Hercegovine: a) Spoljna politika, b) spoljno-trgovinska politika, c) Carinska politika, d) Monetarna politika, kao što je predviđeno članom VII Ustava, e) Finansiranje institucija i međunarodnih obaveza Bosne i Hercegovine, f) Politika i regulisanje pitanja imigracije, izbjeglica i azila, g) Provođenje međunarodnih i međuentitetskih krivičnopravnih propisa, uključujući i odnose sa Interpolom, h) Uspostavljanje i funkcionisanje zajedničkih i međunarodnih komunikacijskih sredstava, i) Regulisanje međuentitetskog transporta, j) Kontrola vazdušnog saobraćaja

[47] Macan, Karan (2019). 160-175.

[48] Zakonom o elektronskom potpisu Republike Srpske. *Službeni glasnik Republike Srpske,* br. 106/15 i 83/19.

[49] Zakon o elektronskom potpisu Bosne i Hercegovine. *Službenom glasniku BiH*, br. 91/06

[50] Čl. 22, st. 1 Zakona o elektronskom potpisu Republike Srpske glasi: „Certifikaciono tijelo iz člana 21. ovog zakona, koje izdaje kvalifikovane elektronske certifikate, može da obavlja usluge na osnovu dozvole koju izdaje Ministarstvo za naučnotehnološki razvoj, visoko obrazovanje i informaciono društvo“

[51] Macan, S. (2019). Evropski okvir za pružanje usluga povjerenja i uloga MUP Republike Srpske u pružanju usluga povjerenja u Republici Srpskoj. *Časopis MUP Republike Srpske Bezbjednost, policija, građani*, 2.

Identifikacija u ovakvom prostoru i pouzdana potvrda da je stvarni i pravni identitet jednak digitalnom identitetu koji se pojavljuje u sajber prostoru se profilisala kao potreba koja garantuje određen nivo bezbjednosti digitalnih usluga.

Radom je prikazan kratak pregled razvoja digitalnih usluga i metoda digitalne identifikacije koja je prepoznata kroz pravnu regulativu Evropske unije. Iskazujući volju da se pristupi Evropskoj uniji i Bosna i Hercegovina je preduzela pravne obaveze da uskladi svoje zakonodavstvo sa zakonodavstovom Evropske unije. Tako je u zakonodavstvu Evropske unije prepoznat različit nivo realizacije elektronske identifikacije, u zavisnosti od tehničkih rješenja, ali i potreba bezbjednosti u postupku elektronske identifikacije.

Određene usluge koje se pružaju u sajber prostoru zahtjevaju izuzetno visok nivo pouzdanosti, tako da je uspostavljen pravni osnov za korišćenje kvalifikvanih digitalnih certifikata. Ovakvi certifikati se izdaju od pravnih lica koje ispunjavaju određene uslove i koji se posebno provjeravaju i dobijaju dozvole države da vrše pružanje usluga identifikacije. Svi elektronski dokumenti i postupci koji se dešavaju u sajber prostoru, a koji su verifikovani ovakvim certifikacima imaju identičnu paravnu snagu kao i svojeručno potpisano i ovjereni dokumenti i postupci.

Često postoji potreba za uslugama u kojima se ne zahtjeva visok nivo sigurnosti, tako da su pravno prepoznati i ovakvi nivoi identifikacije.

U radu su prikazani primjeri iz susjednih zemalja, gdje je vidljivo da se koriste različiti nivoi identifikacije, te se omogućava pristup određenim uslugama elektronskim putem. Usluge su dostupne u zavisnosti od zahtjevanog nivoa bezbjednosti, za različite metode elektronske identifikacije. Tako da se za određene usluge traži kvalifikovani digitalni potpis, a za određene usluge ne postoji takav zahtjev. Ono što je ključno, jeste činjenica da je građanima omogućen određen nivo fleksibilnosti i dostupnosti usluga, shodno njihovim potrebama.

U Bosni i Hercegovini i u Republici Srpskoj ne postoje uspostavljeni sistemi elektronske identifikacije, niti prepoznati nivoi pouzdanosti koji su definisani zakonodavstvom Evropske unije. Shodno navedenom, građani Bosne i Hercegovine nemaju isti nivo usluga koje postoje u susjednim zemljama, te u zemljama Evropske unije.

LITERATURA

Monografije, članci

Song, Y. Y (2019). *Cybercryptography: Applicable Cryptography for Cyberspace Security*. Springer Nature Switzerland, https://doi.org/10.1007/978-3-319-72536-9;

Dijck, J. V., Jacobs, B. (2020). *Electronic identity services as sociotechnical and political-economic constructs*. New media and sociati, Sage. 22(5), 896-914.

Macan, S. (2020). Procjena usklađenosti u postupku primjene zakona o digitalnom potpisu Republike Srpske i usaglašenost sa eIDAS regulativom. *Godišnjak Fakulteta pravnih nauka*, 10, 241-255.

Macan, S. (2019), Evropski okvir za pružanje usluga povjerenja i uloga MUP Republike Srpske u pružanju usluga povjerenja u Republici Srpskoj. *Časopis MUP Republike Srpske Bezbjednost, policija, građani*, 2.

Macan, S. (2018). *Registri za identifikaciju građana – Zaštita ljudskih prava i efikasna državna uprava* (doktorska disertacija), Fakultet pravnih nauka Paneveropskog Univerziteta Aperiron, Banja Luka.

Macan, S., Karan, S. (2017). Ustavno pravo na privatnost, slobodu kretanja i prebivalište korišćenjem biometrijskih podataka, *Godišnjak fakulteta pravnih nauka*.

Macan, S., Karan, S. Đajić, G. (2018). Ustavnopravni aspekt primjene EU standarda o upotrebi elektronskog potpisa u Republici Srpskoj. *Godišnjak fakulteta pravnih nauka*, 8.

Cohen, J. E. (2007). *Cyberspace As/And Space*. Georgetown University Law Center.

Pravni izvori

Evropski parlament i Evropske Savjet, Uredba o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutrašnjem tržištu (eIDAS) broj 910/14

Zakonom o elektronskom potpisu Republike Srpske. *Službeni glasnik Republike Srpske,* br. 106/15 i 83/19.

Zakon o elektronskom potpisu Bosne i Hercegovine. *Službeni glasnik BiH,* br. 91/06.

Zakon o elektronskom dokumentu Republike Srpske. *Službeni glasnik Republike Srpske,* br. 106/15

Uredba (EZ) br. 765/2008 o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište Bosna i Hercegovina i Evropska Komisija, Sporazum o stabilizaciji i pridruživanju, 2008

www.wearesocial.com/digital-2020

www.statista.com

www.vladars.net

www.mnrvoid.net

https://europa.eu/european-union/

www.dei.gov.ba

www.gov.hr

www.nias.gov.ba

https://euprava.gov.rs/

Legal Acceptability of the Security Level of the Electronic Identification System

Summary: Cyberspace is becoming the dominant global arena for the exchange of goods and services. In addition, cyberspace is playing an increasing role in meeting the social needs of the modern human being. Services provided by public administrations are moving to the Internet and modern information and communication technologies. In such an environment, the need for reliable identification of an individual in cyberspace becomes increasingly demanding. E-commerce, as well as e-business in most cases implies the possession of bancing cards as an instrument of non-cash payment transactions. Therefore, a banking card is recognized as an instrument that confirms the identity of an individual within electronic interactions, and the bank can also be seen as a provider of trust services in electronic identification procedures. In a large number of electronic transactions in cyberspace, there is often no need for identity verification via credit cards, because no financial transaction. At the same time, there is a need to reliably determine the identity of an individual in cyberspace. The intensive development of the Internet, the transfer of a large number of business and social activities in cyberspace has led to the need to adapt legal solutions that regulate some activities on the Internet, or the mentioned cyberspace. Thus, a system of reliable digital authentication of transactions and recognition of an individual's identity when appearing in cyberspace has been developed. In the Republic of Srpska, but also in Bosnia and Herzegovina, legislation has been adopted that recognizes electronic signatures, as well as trust and electronic identification services. Back in 1999, the European Union adopted a regulation for digital signatures, which was replaced by the Regulation on electronic identification and trust services for electronic transactions in the internal market number 910/14, popularly called eIDAS. eIDAS regulations legally regulate the met-

hods of digital identification, as well as the legal validity of electronic documents and electronic business with traditional documents and business. The paper studies the levels of electronic identifications, possible solutions in legislation and practice in the Republic of Srpska and Bosnia and Herzegovina and presents examples from neighboring countries.

Key words: trust service, electronic identification, qualified digital signature, advanced digital signature, simple digital signature, devices for creation of digital signature and digital stamp.