

## Nacrt Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju

### - Komentari AmCham članova -

- Da bi ovaj Zakon omogućio širu upotrebu elektronskog potpisa i unapredio elektronsko poslovanje u celini neophodno je da postane opšti zakon za oblast elektronskog potpisa čija pravila će biti obavezna i u svim drugim oblastima, kao što je bankarski sistem, elektronska trgovina i sl. Na primer, Zakon o zaštiti korisnika finansijskih usluga propisuje da se ugovor o finansijskoj usluzi sačinjava u pismenoj formi ili na drugom trajnom nosaču podataka (član 7. stav 1.). Ovaj Nacrt (član 50. stav 3. tačka 6.), praktično derogira citirane odredbe Zakona o zaštiti korisnika finansijskih usluga, te stoga predlažemo njegovo izostavljanje. I Zakon o elektronskoj trgovini propisuje ugovore, odnosno pravne poslove koji se ne mogu zaključiti u elektronskom obliku (član 10.). Sve navedeno ukazuje na potrebu da ovaj Zakon, kao „krovni“ zakon, *exempli causa* reguliše oblasti, odnosno pravne poslove i transakcije koji bi se mogli zaključiti i realizovati primenom različitih oblika elektronskog potpisa, od kojih svaki podrazumeva različit nivo pouzdanosti, odnosno identifikacije. Sve navedeno važi i za primenu elektronskog pečata čije pravno dejstvo je regulisano članom 51. Nacrta, kao i za dostavljanje različitih akata, odnosno dostavljanje elektronskih dokumenata između organa vlasti i stranaka, što je regulisano članom 15. Nacrta Zakona

### Deo prvi – Osnovne odredbe

- **Član 2, stav 1, tačka 1** – **Pojam elektronskog poslovanja** bi trebalo proširiti i na ugovaranje, davanje jednostranih izjava volja, komunikaciju i vođenje sudskih i upravnih postupaka, s obzirom da se dalje u tekstu uređuju i neke od navedenih oblasti. Zakon bi trebalo jasno da uredi da se sve što se sada radi u "papiru" može raditi i "elektronski", osim izuzetaka koji su dati u članu 50.
- **Član 2, stav 1, tačka 7** – U **definiciju organa javne vlasti** potrebno je dodati i fizičko lice kome je povereno vršenje javnih ovlašćenja kao delatnost.
- **Član 2, stav 1, tačka 15** – Generalno nije dovoljno jasno i precizno definisano šta se smatra pod **uslugama od poverenja i kvalifikovanim uslugama od poverenja**. Potrebno je pojasniti da li je lista koju Nacrt daje u članu 41 samo primer ili konačna lista usluga. U slučaju da je samo primer, nije jasno na koji način bi se mogle prepoznati druge usluge od poverenja.
- **Član 2, stav 1, tačka 21** – **Uvođenje pojma elektronskog pečata** je nepotrebno, a posebno imajući u vidu da pravno lice nije u obavezi da poseduje pečat, te da on nije obavezan na dokumentima. Takođe, u elektronskom potpisu se sadrže podaci o pravnom licu ukoliko je sertifikat izdat na zahtev pravnog lica.

Pečat sam za sebe nema nikakvu funkciju i ne postoji način da se bez neke dublje provere utvrdi koje fizičko lice je stavilo pečat. Jedino što bi moglo da se utvrdi je da određeni skup podataka predstavlja elektronski pečat konkretnog pravnog lica, odnosno preduzetnika, pri čemu bi isti morao biti praćen i elektronskim potpisom ovlašćenog lica.

- **Član 2, stav 1, tačka 23** – Trebalo bi jasnije definisati da se **validacijom potvrđuje da određeni potpis** pripada konkretnom pravnom, odnosno fizičkom licu. Validacijom se ne može potvrđivati sadržina dokumenta koji se pečatira/potpisuje.
- **Član 2, stav 1, tačka 29** – Sa jedne strane nije jasno koji je praktični domašaj **naprednog elektronskog potpisa, a sa druge da li lice koje poseduje kvalifikovani elektronski potpis** istim može potpisivati sve što bi trebalo biti potpisano običnim ili naprednim elektronskim potpisom. Takođe, na osnovu definicije **kvalifikovanog elektronskog potpisa iz člana 2, stav 1, tačka 30** se stiče utisak da postoje i druge vrste naprednog elektronskog potpisa. Isti komentar važi i za član 2, stav 1, tačke 33 i 34. Dalje, budući da pečat ne može imati bilo ko, postavlja se pitanje zbog čega se uvodi i običan i kvalifikovani elektronski pečat, te šta se dešava u slučaju kombinacije običnog i naprednog pečata i potpisa.
- Smatramo da bi stvarni napredak u oblasti elektronskog poslovanja bio postignut ako bi Zakon doveo do **mного šire upotrebe elektronskog potpisa** i značajnog povećanja ponude elektronskih servisa. Da bi se to ostvarilo potrebno je:
  - učiniti da elektronski potpis bude dostupan svima, odnosno širem krugu korisnika;
  - pojednostaviti postupak identifikacije korisnika elektronskog potpisa;
  - smanjiti troškove vezane za izdavanje elektronskog sertifikata.

Optimalni način za ostvarivanje navedena tri cilja, a imajući u vidu inostrana iskustva i okolnost da korišćenje kvalifikovanog elektronskog potpisa zahteva poseban hardver, softer i iziskuje relativno visoke troškove, je **uvođene običnog (nekvalifikovanog) elektronskog potpisa**, odnosno **razlikovanje tri oblika nekvalifikovanog elektronskog potpisa**, koji bi podrazumevali različite nivoe pouzdanosti i, samim tim, različito pravno dejstvo, odnosno različite pravne poslove za čije bi zaključenje bili zahtevani različiti oblici elektronskog potpisa. U tom smislu predlažemo **tri oblika nekvalifikovanog elektronskog potpisa** koja su zasnovana na 3 različita nivoa sigurnosti: običan nivo sigurnosti, srednji nivo sigurnosti i napredni nivo sigurnosti, uz jasno definisanje za koji konkretan pravni posao/transakciju se može koristiti odgovarajući oblik nekvalifikovanog elektronskog potpisa.

Ključno za unapređenje ove oblasti je i propisivanje **mehanizma elektronske identifikacije** umesto tehničkog sredstva za realizaciju elektronskog potpisa. Mehanizme elektronske identifikacije (hardver, softver) potencijalni korisnici elektronskog potpisa već poseduju. Na primer, uz registrovanu sim karticu i PIN kod, koji je poznat samo korisniku, mobilni telefoni bi postali idealno sredstvo elektronske identifikacije jer korisnik već poseduje celokupan harvder i softver. Ukoliko postoje slični mehanizmi koji ispunjavaju gore navedena 3 uslova i njih treba predvideti ovim Zakonom. Bez formalnosti u vezi izdavanja elektronskog sertifikata, uz uštedu vremena i bez troškova, omogućilo bi se značajno povećanje broja korisnika elektronskog potpisa. Pojednostavljenje i mnogo šira primena elektronskog potpisa preduslov je i za realizaciju ideje digitalizacije javne uprave.

- **Član 2, stav 1, tačka 41** – Nije jasno **ko se smatra pružaocem usluge**.
- **Član 2, stav 1, tačka 45** – Nije jasno **šta se podrazumeva pod usklađenošću** kvalifikovanog pružaoca usluga poverenja i kvalifikovanih usluga poverenja koje on pruža.
- **Član 2, stav 1** – Uvodnim definicijama definisati i „znak pouzdanosti“ predviđen članom 39.
- **Član 3** – Zakon **pokriva širu oblast** od one koja je ovde definisana. Član treba dopuniti tako da se jasno definiše da se uređuje i oblast izdavanja elektronskog potpisa, pečata, dozvola za rad i uslova za poslovanje pružaoca usluga, kontrola takvog poslovanja, kao i upotreba potpisa i pečata, te arhiviranje dokumentacije.
- **Član 4, stav 2** – Stav 2 bi trebalo izbrisati (**elektronske transakcije strane se mogu predstavljati pseudonimom ukoliko propisom, ugovorom ili na drugi obavezujući način nije drugačije određeno**). Ukoliko se ugovor, transakcija, zaključuje primenom elektronskog potpisa bitno je da se odmah nedvosmisleno i jasno zna ko su ugovorne strane. Takođe, ne postoji mogućnost vođenja sudskog ili upravnog postupka uz upotrebu pseudonima.
- **Član 5** – Ukoliko je lice izvršilo potpisivanje dokumenta elektronskim potpisom, pravno zainteresovano lice bi trebalo da ima mogućnost vršenja provere. Nije jasno **u kom obliku bi se davala saglasnost**, a posebno na koji način bi istu davala lica sa invaliditetom.
- **Član 6** – Ovaj član (**dostupnost i pristup osobama sa invaliditetom**) potrebno je precizno definisati u skladu sa Zakonom o sprečavanju diskriminacije osoba sa invaliditetom.

### **Deo drugi – Elektronski dokument**

- **Član 11 (overa digitalnog akta)** – Poželjno je predvideti da lice sa pravnim interesom može vršiti digitalizaciju, pri čemu odgovara krivično i materijalno za verodostojnost samog akta ili alternativno uvesti da lice može podneti zahtev nekom od registrovanih pružaoca usluga da izvrši digitalizaciju.
- **Član 12 (overa kopije digitalnog akta)** – Poželjno je predvideti da se overa vrši pred državnim organom ili javnim beležnikom, kao trećom nezavisnom stranom, kako bi svako ko ima potrebu mogao slobodno da pribavi overenu kopiju dokumenta. Fizička lica obično nemaju ovlašćeno lice, te nije jasno kako ono vrši overu. Takođe, postavlja se pitanje šta ako je u pitanju dokument sa više različitih potpisnika, da li je potrebno da svi "overe" dokument? Važeći Zakon o privrednim društvima daje izbor pravnom licu da li će koristiti pečat u svom poslovanju ili ne. Ukoliko je izbor da ne koristi pečat, neće moći da ispuni ovu odredbu.
- **Član 13 (potvrda o prijemu elektronskog dokumenta)** – Potrebno je pojasniti da li će potvrda o prijemu elektronskog dokumenta sadržati elektronski potpis primaoca ili je u pitanju neka sistemski generisana potvrda da je dokument stigao na adresu na koju je upućen? Ovo je u vezi i sa članom 15 i pitanjem kada se smatra da je dostava uredno izvršena, što je posebno važno iz razloga što se na ovaj način može vršiti pismena dostava u sudskim i upravnim postupcima, rešenja i drugih odluka, te drugih pismena čijim prijemom počinje da teče određen rok za ne/postupanje.

- **Član 15 i član 16 (dostavljanje elektronskih dokumenata između organa vlasti i stranaka i dostavljanje elektronskih dokumenata između organa vlasti)** – Svuda gde se pominje „*organ vlasti*“ ispraviti u "*organ javne vlasti*", s obzirom da je to pojam iz člana 2.

Dostupnost bazama podataka državnih organa, odnosno organa uprave, od strane pravnih lica pružalaca usluga, je veoma važna za razvoj ne samo elektronskog poslovanja, već poslovanja uopšte. Tako je, na primer, bankama, uz pisanu saglasnost korisnika, omogućen uvid u Kreditni biro. Nacrt zakona o je i u tom pogledu napravio određeni pomak kroz član 15. Pa ipak, postoje određene nedoumice u pogledu praktične primene ovog člana. Iz navedenog razloga, predlažemo da se član 15. izmeni, odnosno da se kroz posebno poglavlje reguliše dostavljanje podataka i dokumenata od strane državnih organa/organa uprave trećim licima, odnosno da se trećim licima omogući pristup bazama podataka državnih organa/organa uprave uz saglasnost korisnika, odnosno fizičkog lica na koje se podaci odnose, a koja je data u elektronskom obliku putem običnog nekvalifikovanog, elektronskog potpisa sa najnižim nivoom pouzdanosti.

Kroz dostupnost baza podataka bi se mogla obezbediti i pouzdanost izdatih sertifikata, na primer, kroz obavezu Agencije za privredne registre da u slučaju brisanja određenog subjekta iz registra, službenim putem obavesti izdavaoce sertifikata o toj okolnosti, kako bi izdavaoci sertifikata onemogućili korišćenje istog.

### **Deo treći – Elektronska identifikacija**

- Za korišćenje elektronskog potpisa, a u cilju realizacije različitih pravnih poslova/transakcija, svakako je jedan od ključnih elemenata i identifikacija korisnika elektronskog potpisa. Identifikacija korisnika elektronskog potpisa bi se mogla obezbediti ne korišćenjem tehničkog sredstva već putem elektronske identifikacije pomoću sredstava koja potencijalni korisnici elektronskog potpisa već poseduju.  
Različiti oblici nekvalifikovanog elektronskog potpisa, kako je predloženo napred (običan, srednji i napredni ), bi zahtevali različite nivoe pouzdanosti, odnosno načine elektronske identifikacije:
  - a) prvi oblik (običan nivo sigurnosti) bi zahtevao najniži nivo pouzdanosti, odnosno najniži stepen elektronske identifikacije lica - korisnika elektronskog potpisa, na primer unošenjem matičnog broja (jedan element);
  - b) drugi oblik (srednji nivo sigurnosti) bi zahtevao srednji nivo pouzdanosti, odnosno srednji stepen elektronske identifikacije lica - korisnika elektronskog potpisa, na primer putem broja telefona i PIN koda koji je poznat samo korisniku (dva elementa);
  - c) treći oblik (napredni nivo sigurnosti) bi zahtevao najviši nivo pouzdanosti, odnosno najviši stepen elektronske identifikacije lica - korisnika elektronskog potpisa, na primer putem broja telefona, PIN koda koji je poznat samo korisniku i šifre koja bi bila poslata korisniku na telefonski broj koji je korišćen za identifikaciju (tri elementa).
- **Član 22, stav 1 (Bezbednosni uslovi koje treba da ispunjavaju pružaoci usluga elektronske Identifikacije)** – dodati i fizičke mere, a poseban akcenat bi trebalo staviti na kontinuitet u poslovanju.

## Deo četvrti – Usluge od poverenja

- **Član 25, stav 1** – Nije jasno koji je razlog za **ograničenje odgovornosti pružaoca usluga** za štetu koja je uzrokovana namerom i nepažnjom. Predlažemo sledeću alternativnu formulaciju: *Pružalac usluge od poverenja odgovoran je za štetu nastalu usled toga što nije postupio u skladu sa ovim zakonom.*

**Stav 2 i stav 3** treba izbrisati, s obzirom da je drugim zakonom već uređeno na koga pada teret dokazivanja.

**Stav 4** je potrebno precizirati, tj. definisati koji formu treba da ima obaveštenje korisnika usluge od poverenja o ograničenju.

- **Član 26 (Odgovornost korisnika usluga od poverenja za čuvanje sredstava i podataka za formiranje elektronskog potpisa odnosno pečata)** – proširiti dejstvo ovog člana na sve vrste potpisa i pečata.
- **Član 27** – Potrebno je objediniti član 27. i član 22., kako bi se **svi bezbednosni uslovi našli na jednom mestu**. Trebalo bi dodati i periode (na primer od godinu dana) za sprovođenje testiranja da li su bezbednosni uslovi i dalje adekvatni.
- **Član 27, stav 1 (Bezbednosni uslovi koje treba da ispunjavaju pružaoci usluga od poverenja)** – Potrebno je predvideti i fizičke mere.
- **Član 30, stav 2 (Uspostavljanje odnosa između pružaoca i korisnika kvalifikovane usluge od poverenja)** – potrebno je predvideti formu i kojoj će biti obaveštavana lica koja su podnela zahtev za pružanje kvalifikovane usluge od poverenja?

**Član 31, stav 1 (Uslovi za pružanje kvalifikovanih usluga od poverenja)** – Nije jasno na koji način se dokazuje ispunjenost uslova koji se odnose na zaposlene kod pružaoca kvalifikovanih usluga (**tačka 1**), šta se podrazumeva pod rizikom za štetu na osnovu osiguranja (**tačka 2**), u kojoj formi se daje saglasnost lica za javno raspolaganje podacima (**tačka 4**), šta se podrazumeva pod odgovarajućim vremenskim periodom za čuvanje relevantnih informacija - period čuvanja pojedinih dokumenata je dat u različitim zakonima i odgovarajući vremenski period u smislu ovog zakona ne može biti kraći (**tačka 6**). U **tački 5** je potrebno dodati i sprečavanje zloupotrebe. Komentar za **tačku 7** je da podaci da li sertifikat važi, da li je trajno ili privremeno suspendovan, moraju biti dostupni.

- **Član 33, stav 1 (Provera identiteta korisnika kvalifikovane usluge od poverenja)** – Trebalo bi jasnije definisati da se podaci koji će biti sadržani u sertifikatu proveravaju na osnovu javnih isprava i drugih dokumenata.
- **Član 36, stav 1 (Prestanak pružanja usluge izdavanja kvalifikovanih elektronskih sertifikata)** – Potrebno je definisati u kojoj formi je obaveštenje o prestanku obavljanja delatnosti izdavalaca kvalifikovanih elektronskih sertifikata. S obzirom da je ovo posebno navedeno u kaznenim odredbama, objava bi morala da bude na sajtu, novinama i slično. Nemoguće je da isti "obavesti svakog korisnika" bez javne objave.

U stavu 5 je potrebno precizirati u kojim slučajevima se izriče mera privremene zabrane.

### **Deo peti – Pojedine vrste usluga od poverenja**

- Ovakav naslov unosi nesigurnost u smislu da li je lista usluga sadržana u čl. 41. konačna ili je data samo opisno, a da postoje i usluge od poverenja koje ovde nisu izričito navedene. Polazeći od člana 41 i nabiranja usluga od poverenja, stiče se utisak da se pod pružaocem usluga smatra lice koje pruža usluge izdavanja, validacije elektronskog potpisa, pečata, vremenskog žiga i sl. Dilema nastaje zbog toga što, da bi koristila elektronska sredstva u poslovanju, banka ne mora biti registrovana kao pružalac usluga.

- Član 44 (Opoziv i suspenzija kvalifikovanog elektronskog sertifikata) – Nije jasno da li ovo znači da se običan sertifikat ne može opozvati ni suspendovati?

U stavu 1, tačka 2 bi trebalo dodati staratelja i naslednike, s obzirom da izdavalac nema saznanja o nastupanju okolnosti iz tačke 2, dok ga neko o tome ne obavesti.

U stavu 1, tačka 6 bi trebalo dodati sledeći nastavak rečenice "a nije obezbedio prenos sertifikata na drugog pružaoca usluga od poverenja".

U stavu 2 bi trebalo precizirati u kojoj formi se obaveštavaju korisnici o opozivu sertifikata

U stavu 6 nije jasno zbog čega se ne radi javna objava opoziva i suspenzije sertifikata.

- Član 45 (Čuvanje dokumentacije o izdatim i opozvanim kvalifikovanim sertifikatima) – Ovde se opet vraćamo na član 11. Ako je dokument izvorno nastao u elektronskoj formi, ova rečenica je potpuno prihvatljiva, ali ako ne možemo digitalizovati akt u skladu sa čl. 11. to znači da moramo čuvati izvorni, papirni akt i isti arhivirati na način predviđen zakonom kojim se uređuje arhiva. Takođe, treba obezbediti kontinuitet u čuvanju dokumenata u slučaju da se pružalac usluge ugasi.
- Član 46, stav 1, tačka 3 (Kvalifikovana sredstva za kreiranje elektronskog potpisa i pečata) – Bolja formulacija bi bila "Da podaci za kreiranje elektronskog potpisa odnosno pečata budu jedinstveni".
- Član 48 (Postupak validacije kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata) – Nije jasno u kom trenutku se vrši validacija s obzirom da, na primer, prilikom zaključenja ugovora mora biti potpuno jasno da stane imaju odgovarajuća ovlašćenja za potpisivanje i da isto vrše važećim sredstvima.
- Član 50, stav 2 (Kvalifikovani elektronski potpis ima isto pravno dejstvo kao i svojeručni potpis) – Imajući u vidu ovaj stav, postavlja se pitanje koju snagu imaju običan i napredni elektronski potpis. U slučaju da se posebnim zakonom zahteva pisana forma dokumenta, koji potpis bi bio validan?
- Potrebno je precizirati koje vrste vremenskog žiga postoje, koja dokumenta moraju da ih sadrže, način validacije i pravni domašaj (članovi 52 i 53).

- **Član 54 (Uslovi za usluge kvalifikovane preporučene elektronske dostave)** – Ukoliko postoji samo usluga kvalifikovane preporučene elektronske dostave, trebalo bi ujednačiti tekst da ne bi dolazili u nedoumice.
- **Član 55, stav 3 (Potvrda o elektronskoj dostavi)** – Dodati i **parnični postupak**.
- **Član 61, stav 1, tačka 2 (Priprema dokumenata za elektronsko čuvanje dokumenata)** – Nije jasno na koji način se vrši digitalizacija. Član 11. ovde može samo da zakomplikuje pripremu za arhiviranje.
- **Član 65 (Usluga kvalifikovanog elektronskog čuvanja dokumenata)** – Nije jasno zbog čega se pravi ova razlika, tj. koja je njena praktična primena. Pouzdanost bi trebalo da bude garantovana uvek.

### **Deo sedmi – Kaznene odredbe**

- **Član 68, stav 1, tačka 8** – Ovu tačku bi trebalo predefinisati. Nije problem u vršenju vanredne provere, već da je vrši isto lice