Elektronski potpis

Prof. dr Predrag Dimitrijevć

Značenje

- Elektronski potpis predstavlja 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.
- elektronski potpis ima i dodatnu osobinu da štiti integritet elektronski potpisane poruke.
- svojeručni potpis to ne obezbeđuje.

Pravni aspekati elektronskog potpisa

- Direktiva EU 1999/93/EC o elektronskim potpisima (usvojena 13. decembra 1999, a formalno stupila na snagu 19. januara.2000. godine)
- predstavlja pravno utemeljenje elektronskog potpisa i na osnovu nje su doneti
- Zakoni o elektronskom potpisu u svim zemljama EU, kao i u većini ostalih zemalja Evrope.

- Zakonom o elektronskom potpisu koji je donet 2004. godine (Slu-žbeni glasnik RS br. 135/2004) uređuje se upotreba elektronskog pot-pisa u pravnim poslovima, poslovanju i drugim pravnim radnjama, kao i prava, obaveze i odgovornosti u vezi sa elektronskim sertifikatima, ako posebnim zakonima nije drugačije određeno.
- Odredbe ovog zakona primenjuju se na opštenje organa, opštenje organa i stranaka, dostavljanje i izradu odluke organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom - ako je zakonom kojim se uređujetaj postupak propisana upotreba elektronskog potpisa.

- Zakon o elektronskom potpisu u Srbiji, u potpunosti usklađen sa EU Direktivom 1999/93/EC, izglasan je u Narodnoj skupštini Republike Srbije dana 14. decembra 2004.
- publikovan u Službenom glasniku Republike Srbije br. 135 od 21.decembra 2004. godine.

Osnovna uloga

- Osnovna uloga **Zakona o elektronskom potpisu** svodi se na dve najvažnije stvari:
  1. Da propiše **uslove** pod kojima je elektronski potpis pravno ekvivalentan svojeručnom potpisu.
  2. Da propiše uslove koje moraju da ispune sertifikaciona tela koja izdaju kvalifikovane sertifikate za verifikaciju kvalifikovanih elektronskih potpisa.

Definicije

- U Zakonu o elektronskom potpisu navedene su sledeće :
- Elektronski potpis - **skup podataka u elektronskom obliku**, koji su pridruženi ili su logički povezani sa elektronskim dokumentom i služe za identifikaciju potpisnika.
- Kvalifikovani elektronski potpis - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene Zakonom o elektronskom potpisu.

Zakon daje definicije pojedinih izraza

U *Zakonu o elektronskom potpisu* navedene su sledeće definicije:

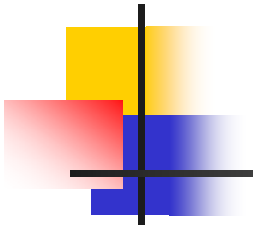
- „**Elektronski dokument**" je dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom.
- „**Elektronski potpis**" je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.

„Kvalifikovani elektronski potpis"

- je elektronski potpiskojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata i onemogućava naknadno poricanje odgovornosti za njihov sadržaj. Kvalifikovani elektronski potpis mora da zadovolji sledeće uslove:

1. isključivo je povezan sa potpisnikom
2. nedvosmisleno identifikuje potpisnika
3. nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika
4. direktno je povezan sa podacima na koje se odnosi i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka
5. formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa
6. proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika.

Kvalifikovani elektronski potpis, koji zadovoljava prethodno navedene uslove, u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpisi 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**" su odgovarajuća tehnička sredstva (softver i hardver) koja se koriste za formiranje elektronskog potpisa, uz korišćenje podataka za formiranje elektron-skog potpisa.
- „**Elektronski sertifikat**" je elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.
- „**Sertifikaciono telo**" je pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama za-kona.

- 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.

Realizacija elektronskog potpisa

- Za realizaciju kvalifikovanog elektronskog potpisa neophodno je koristiti sredstva za formiranje kvalifikovanog elektronskog potpisa i posedovati kvalifikovani elektronski sertifikat, izdat od strane sertifikacionog tela koje ispunjava odgovarajuće uslove prema Zakonu o elektronskom potpisu. U ovom tehnološkom trenutku, kvalifikovani elektronski potpis se realizuje primenom asimetričnih kriptografskih sistema (na primer RSA algoritam) i hash funkcija (MD5 ili SHA-1 algoritmi), dok se kao sredstva za formiranje kvalifikovanog elektronskog potpisa uglavnom koriste smart kartice.

Gde se koristi ?

- Najpopularnije aplikacije u kojima se koristi elektronski potpis su:
- · zaštićene web transakcije
- · zaštićene e-mail poruke
- · zaštićen FTP servis
- · formiranje VPN (IPSec) mreža
- · bezbedno upravljanje dokumentacijom
- · bezbena plaćanja putem Interneta itd.

Najznačajnija polja primene elektronskog potpisa su:

- · elektronsko poslovanje (e-Business)
- · elektronska trgovina (e-Commerce)
- · elektronsko bankarstvo (e-Banking)
- · elektronska uprava (e-Government)
- · elektronsko zdravstvo (e-Healthcare)
- · platni sistemi na bazi čip kartica (EMV) itd.

- Dakle, za primenu kvalifikovanog elektronskog potpisa neophodno je posedovati dva osnovna elementa:

  1. sredstvo za formiranje kvalifikovanog elektronskog potpisa i
  2. kvalifikovani elektronski sertifikat potpisnika.

- Ako bilo koji od ovih elemenata nedostaje, potpis ne zadovoljava uslove da bude kvalifikovan, već je to "samo" elektronski potpis.
- Iako elektronski potpis može prema zakonu biti bilo šta što je "logički povezano sa elektronskim dokumentom i što služi za identifikaciju potpisnika" (na primer, skenirani svojeručni potpis na kraju dokumenta i sl.), elektronskim potpisom se smatra i potpis koji je izvršen sredstvom za formiranje kvalifikovanog elektronskog potpisa ali potpisnik nema kvalifikovani sertifikat.
- Potpisnik koji ima kvalifikovani sertifikat a potpisivanje ne vrši primenom sredstva za formiranje kvalifikovanog potpisa ne može da formira kvalifikovani elektronski potpis koji je pravno izjednačen sa svojeručnim potpisom.

- U našoj zemlji je od 6. januara 2003. uvedeno elektronsko bankarstvo između pravnih i fizičkih lica i skoro svih naših banaka, u kojem se koriste smart kartice za elektronsko potpisivanje finansijskih transakcija.
- Ti potpisi predstavljaju "samo" elektronske potpise, jer korisnici nemaju kvalifikovane sertifikate, a smart kartice koje se koriste nisu verifikovane kao sredstva za formiranje kvalifikovanog potpisa u našoj zemlji.
- Na osnovu svetske prakse, u domenu elektronskog bankarstva neće ni biti obavezno da se koristi kvalifikovani elektronski potpis, jer se to smatra zatvorenom grupom korisnika (gde postoji eksplicitni ugovor između komitenta i banke).
- Na osnovu svetskih i evropskih analiza, prava i najšira primena kvalifikovanog elektronskog potpisa se očekuje u domenu elektronske uprave, kada će građani elektronski poslovati sa javnom upravom, tj. slati elektronske zahteve javnoj upravi (npr. zahtev za izdavanje elektronskog izvoda iz matične knjige, elektronska prijava poreza itd.). Ovi zahtevi moraju biti potpisani kvalifikovanim elektronskim potpisom građana.
- Projekat uvođenja ličnih karata u Srbiji kao elektronskih identifikacionih dokumenata u obliku smart kartice predstavlja pravu podršku za realizaciju pomenutog sistema.
- Očekuje se da će pomenuta elektronska lična karta, biti verifikovana kao sredstvo za formiranje kvalifikovanog elektronskog potpisa.

- Kvalifikovani elektronski potpis se na ovom stepenu tehnološkog razvoja formira na bazi primene asimetričnih kriptografskih algoritama i tehnologije digitalnog potpisa.
- Kvalifikovani elektronski potpis se formira u skladu sa preporukom PKCS#1 (Public Key Cryptographic Standard), a dužina modulusa u asimetričnom kriptografskom algoritmu mora biti minimalno 1.024 bita.
- PKCS#1 standard opisuje metode šifrovanja podataka korišćenjem RSA asimetričnog algoritma i najčešće se koristi za konstrukciju digitalnog koverta i digitalnog potpisa.

Tehnologija elektronskog potpisa

- U slučaju digitalnog potpisa, sadržaj koji treba da se potpiše prvo se redukuje u otisak poruke (message digest) primenom nekog od metoda za kreiranje otiska poruke, message-digest algoritma (na primer, MD5 ili SHA-1 algoritmi), a zatim se dobijeni otisak poruke šifruje primenom, na primer, RSA algoritma, koristeći privatni ključ 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.
- Ovaj postupak se sastoji od dešifrovanja otiska dobijene poruke primenom RSA algoritma, uz upotrebu javnog ključa pošiljaoca (potpisnika) poruke. Po dešifrovanju digitalnog potpisa, primalac poruke izvrši isti message digest postupak nad dobijenom porukom.
- Ako je dobijeni otisak poruke identičan sa dešifrovanom vrednošću otiska, verifikacija je uspela; u protivnom je verifikacija negativna i poruka se odbacuje kao nevalidna.

- Potpisana elektronska dokumenta se razmenjuju u formi dokumenata u kojima su ugrađeni osnovni podaci o postupku, algoritmu i kvalifikovanom elektronskom sertifikatu potpisnika, kako bi primalac elektronskog dokumenta mogao proveriti kvalifikovani elektronski potpis na bazi usaglašene tehnologije i postupaka.