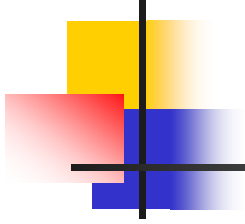


Pravna informatika



- Tema: Elektronski potpis
- Studenti: Nikola Mazic i Aleksandar Campar



Definicije-elektronskog potpisa

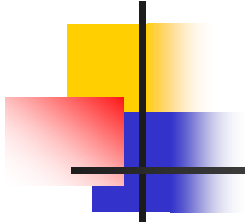
“Elektronski potpis” - skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;

“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 ovim zakonom;



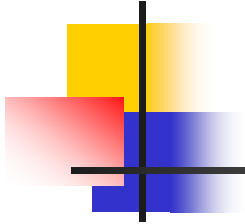
Primjena

- Elektronski(digitalni) potpis se koristi radi:
 - obezbjedjenja sistema elektronskog poslovanja
 - za sigurnu razmjenu podataka elektronskim putem
 - izmedju korisnika koji su fizički udaljeni
 - U tom smislu elektronski potpis u elektronskom poslovanju predstavlja analognu tehniku svojeručnom potpisu u klasičnom poslovanju.



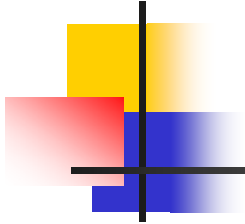
-Najpopularnije aplikacije u kojima se koristi elektronski potpis su:

- zaštićene web transakcije
- zaštićene e-mail poruke
- zaštićen FTP servis
- formiranje VPN (IPSec) mreža
- bezbjedno upravljanje dokumentacijom
- bezbjedna plaćanja putem Interneta



-Najznačajnija polja primjene 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.



E-potpisi mogu biti od pomoći pri rešavanju sporova u slučajevima kada je ugovor doveden u pitanje. Kod zakona o e-potpisu, pitanje o pravnoj sigurnosti i pitanje poverenja su međusobno isprepletena.



Tehnologija elektronskog potpisa

Elektronski potpis se na ovom stepenu tehnološkog razvoja formira na bazi primjene 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



Zakon o elektronskom potpisu

Pravno utemeljenje 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.



Uvod – istorijat donošenja Zakona o elektronskom potpisu

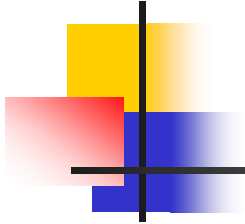
- Zakon o elektronskom potpisu u Crnoj Gori je donesen 12.07.2005 i publikovan u Službenom listu ("Sl.list RCG", br: 55/03 i 31/05)
- Zakon o elektronskom potpisu u Srbiji je izglasan u Narodnoj Skupštini Republike Srbije dana 14.12.2004. i publikovan u Službenom Glasniku Republike Srbije br. 135 od 21.12.2004.
- Time je završena priča koja je započela još u avgustu 2000. godine kada je radna grupa pod okriljem tadašnjeg Saveznog zavoda za informatiku započela izradu Prijedloga Zakona o elektronskom poslovanju i elektronskom potpisu



Zakon o elektronskom potpisu

Zakon se sastoji od sljedećih 7 poglavlja:

- Osnovne odredbe,
- Elektronski potpis i kvalifikovani elektronski potpis,
- Elektronski sertifikati i sertifikaciona tijela,
- Prava, obaveze i odgovornosti korisnika i sertifikacionih tijela,
- Nadzor,
- Kaznene odredbe,
- Prelazne i završne odredbe.



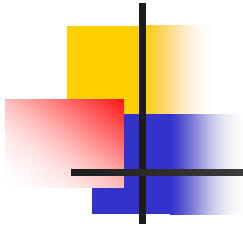
Osnovna uloga Zakona se svodi na dvije najvažnije stvari:

- Da propiše uslove pod kojima je elektronski potpis pravno ekvivalentan svojeručnom potpisu,
- Da propiše uslove koje moraju da ispune Sertifikaciona tela koja izdaju kvalifikovane sertifikate za verifikaciju kvalifikovanih elektronskih potpisa.



Kvalifikovani elektronski potpis

- Kvalifikovani elektronski potpis, mora da zadovolji sljedeće uslove:
 - isključivo je povezan sa potpisnikom;
 - nedvosmisleno identifikuje potpisnika;
 - nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika;
 - direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka;
 - formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa;
 - proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika



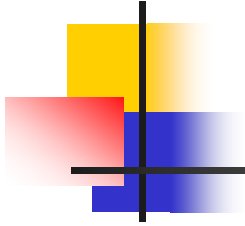
- Kvalifikovani elektronski potpis u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku.

Donošenjem Zakona o digitalnom potpisu, elektronskom poslovanju i pratećih podzakonskih akata u Crnoj Gori normativno je uređena oblast elektronskih transakcija. Takođe su jasno definisani postupci izdavanja i korišćenja digitalnih certifikata, a samim tim i mehanizmi koji se primjenjuju u zaštiti elektronskih transakcija.



Realizacija elektronskog potpisa

Za realizaciju kvalifikovanog elektronskog potpisa neophodno je koristiti sredstva za formiranje kvalifikovanog elektronskog potpisa i posjedovati kvalifikovani elektronski sertifikat, izdat od strane sertifikacionog tijela koje ispunjava odgovarajuće uslove prema Zakonu o elektronskom potpisu.



- Primjena Zakona o elektronskom potpisu je u toku.