Digital signature (elektronski potpis) u e- bussines

„Elektronski potpis“ je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika.

„Kvalifikacioni elektronski potpis“ je 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.

Kvalifikovani elektronski potpis, mora da zadovolji sledeće uslove:

- isključivo je povezan sa potpisnikom;
- nedvosmisleno identifikuje potpisnika;
- nastaje korišćenje 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 pravo dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat u odnosu na podatke u papirnom obliku.

Kvalifikovani elektronski potpis se formira u skladu sa preporukom PKCS#1, a dužina modula u asimetričnom kriptografskom algoritmu mora biti mimalno 1024 bita.

Slika 1. Digitalni potpis

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

Sredstva za formiranje kvalifikovanog elektronskog potpisa su sredstva koja moraju da obezbede:

• da se podaci za formiranje kvalifikovanog elektronskog potpisa mogu pojaviti smao jednom i da je obezbeđena njihova poverljivost;

• da se iz podataka za proveru kvalifikovanog elektronskog potpisa, ne mogu u razumno vreme i trenutno dostupnim sredstvima, dobiti podaci za formiranje kvalifikovanog elektronskog potpisa;

• da kvalifikovani elektronski potpis bude zaštićen od falsifikovanja, upotrebom trenutno dostupne tehnologije;

• da podaci za formiranje kvalifikovanog elektronskog potpisa budu pouzdano zaštićeni od neovlaščenog korišćenja.

• Sredstva za formiranje kvalifikovanog elektronskog potpisa, prilikom formiranja potpisa, ne smeju promeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke pre procesa formiranja kvalifkovanog elektronskog potpisa.

Elektonski potpis se primenjuje za:

• Elektronsko poslovanje (e-bussiness)

• Elektronsku trgovinu (e-commerce)

• Elektronsko bankarstvo

• Elektronsku upravu (e-government)

• Elektronsko zdravstvo (e-healthcare)

• Platne sisteme na bazi čip kartica (EMV)

„Elektronski sertifikat“ je elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika;

„Kvalifikovani elektronski sertifikat“ je elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene ovim zakonom;

„Sertifikaciono telo“ – pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama zakona

Kvalifikovani elektronski sertifikat je elektronski sertifikat koji izdaje sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata i koji mora da sadrži:

• oznaku o tome da se radi o kvalifikacionom elektronskom sertifikatu,

• skup podataka koji je jedinstveno identifikuje pravno lice koje izdaje sertifikat,

• skup podataka koji jedinstveno identifikuje potpisnika,

• podatke za proveru elektronskog potpisa, koji odgovaraju podacima za izradu kvalifikovanog elektronskog potpisa a koji su pod kontrolom potpisnika;

• podatke o početku i kraju važenja elektronskog sertifikata,

• identifikacionu oznaku izdatog elektronskog sertifikata,

• kvalifikovani elektronski potpis i sertifikacionog tela koje je izdalo kvalifikovani selektronski sertifikat,

• ograničenja vezana za upotrebu sertifikata, ako ih ima.

Slika 2. Prenošenje potpisa u Cyber okruženju

Sadržaj elektronskog sertifikata

• Verzija formata sertifikata (v3)

• Serijski broj sertifikata

• Identifikator algoritma kojim se vrši digitalni potpis

• Naziv sertifikacionog tela koje je izdalo sertifikat

• Rok važnosti sertifikata

• Vlasnik sertifikata

• Javni ključ vlasnika sertifikata

• Određeni specifični podaci koji se odnose na uslove korićenja sertifikata

• Digitalni potpis sertifikata tajnim ključem setrifikacionog tela

Sertifikaciono telo koje izdaje kvalifikovane sertifikate ima obavezu:

1. da obezbedi finansijske resurse za osiguranje od rizika i odgovornosti za moguću štetu nastalu vršenjem usluge izdavanja elektronskih sertifikata,

2. da obezbedi čuvanje svih relevantnih informacija koje se odnose na elektronske sertifikate u propisnaom vremenskom periodu i to u izvornom obliku,

3. da ne čuva i ne kopira podatke za formiranje elektronskog potpisa za lica u čije ime pruža tu uslugu,

4. da obezbedi sistema za fizičku zaštitu uređaja, opreme i podataka, i sigurnosna rešenja za zaštitu od neovlašćenog pristupa,

5. da inormiše lica koja traže izdavanje kvalifikovanog elektonskog sertifikata o tačnim uslovima izdavanja i korišćenja tog sertifikata uključujući bilo koja ograničenja u korišćenju, kao i o postupcima za rešavanje sporova. Takve informacije, koje mogu biti dostavljene elektronski moraju biti napisane i pripremljene u razumljivo obliku na sprskom jeziku. Odgovarajući delovi tih informacija moraju biti raspoloživi na zahtev trećim licima,

6. da koristi pouzdan sistem upravljanja elektronskim sertifikatima, u obliku koji omogućava njihovu proveru kako bi:

- unos i promene radila samo ovlašćena lica
- mogla biti proverena autentičnost informacija iz sertifikata
- elektronski sertifikati bili javno raspoloživi za pretraživanje sam u onim slučajevima za koje je vlasnih sertifikata dao saglasnost.
- bilo koja tehnika promena koja bi mogla da naruši bezbednostne zahteve bila poznata

U skladu sa razvojem našeg društva i potrebom sa usaglašavanjem sa razvijenim državama očekuje se da će elektronski potpis biti standard koji će biti punovažan u svim navedenim područjima primene.