**DIGITALNI POTPIS**

Digitalni potpis (eng. Digital Signature) je skup podataka u elektronskom obliku koji su dodati ili logički pridruženi elektronskim porukama ili dokumentima i služe kao metod za identifikaciju potpisnika. Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke (dokaz da poruka nije promenjena na putu od pošiljaoca do primaoca), kao i da obezbedi garantovanje identiteta pošiljaoca poruke.

Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljalac primenom kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (pr. 512 ili 1024 bita) koji u potpunosti oslikava sadržaj poruke. To znači da svaka promena u sadržaju poruke dovodi do promene potpisa. Dakle, pošiljalac kreira digitalni potpis na osnovu poruke koju želi da pošalje. Šifruje ga svojim tajnim ključem i šalje zajedno sa porukom. Primalac po prijemu poruke dešifruje potpis pošiljaoca njegovim javnim ključem. Zatim kreira potpis na osnovu poruke koju je primio i upoređuje ga sa primljenim potpisom. Ako su potpisi identični, može biti siguran da je poruku zaista poslao pravi pošiljaoc (jer je njegovim javnim ključem uspešno dešifrovao potpis) i da je ona stigla nepromenjena (jer je utvrđeno da su potpisi identični).

Dakle, digitalni potpis je elektronska zamena rukom pisanog potpisa, a ne digitalna slika ručnog potpisa. Digitalni potpis omogućava identifikaciju učesnika u komunikaciji i integritet podataka. Za proveru identiteta i integriteta koristi se javni ključ sadržan u digitalnom sertifikatu.

Digitalni potpis se koristi za [potvrdu verodostojnosti](javascript:AppendPopup(this,'432272511_1')) digitalnih informacija – poput dokumenata, e-poruka i makroa – korišćenjem računarskog šifrovanja. Digitalni potpisi pomažu u uspostavljanju sledećih garancija:

* **Autentičnost**     Digitalnim potpisom se garantuje identitet potpisnika.
* **Integritet**     Digitalnim potpisom se garantuje da sadržaj nije promenjen ili neovlašćeno izmenjen nakon digitalnog potpisivanja.
* **Nemogućnost poricanja porekla sadržaja**     Digitalnim potpisom se dokazuje poreklo potpisanog sadržaja. Poricanje porekla sadržaja predstavlja postupak potpisnika u kome on poriče sve veze sa potpisanim sadržajem.

Da biste dobili ove garancije, autor sadržaja mora digitalno potpisati sadržaj korišćenjem potpisa koji zadovoljava sledeće kriterijume:

* Digitalni potpis je [važeći](javascript:AppendPopup(this,'678677478_2')).
* [Certifikat](javascript:AppendPopup(this,'645425458_3')) povezan sa digitalnim potpisom je tekući (nije mu istekao rok važenja).
* Osoba ili organizacija koja je potpisala sadržaj, odnosno izdavač je [pouzdan](javascript:AppendPopup(this,'512465720_4')).
* Pouzdani [autoritet za izdavanje certifikata (CA)](javascript:AppendPopup(this,'875886355_5')) izdaje certifikat povezan sa digitalnim potpisom za izdavača koji potpisuje sadržaj.

## DIGITALNI SERTIFIKAT

Digitalni (elektronski) sertifikat (digital certificate) je elektronski dokument koji izdaje sertifikaciono telo (Certification Authority - CA). Digitalni sertifikat može da se shvati kao digitalna lična karta, jer sadrži podatke o korisniku sertifikata i podatke o izdavaocu sertifikata. To je uverenje kojim se potvrđuje veza između podataka za verifikaciju elektronskog potpisa i identiteta potpisnika, koji je izdat od strane akreditovanog sertifikacionog tela.

U okviru digitalnog sertifikata koji se izda korisniku nalazi se pored ostalog i korisnikov javni kriptografski ključ (Public Key), koji je par njegovom tajnom kriptografskom ključu (Private Key). Sertifikacioni autoritet garantuje tačnost podataka u sertifikatu tj. garantuje da javni ključ koji se nalazi u sertifikatu pripada korisniku čiji su podaci navedeni u tom istom sertifikatu. Zbog toga, ostali korisnici na Internetu ukoliko imaju poverenje u sertifikaciono telo, mogu da budu sigurni da određeni javni ključ zaista pripada korisniku koji je vlasnik pripadajućeg tajnog ključa.

Digitalni sertifikat je elektronski dokument koji je javno dostupan na Internetu. zbog toga što se u okviru sertifikata nalaze javni ključevi korisnika sertifikata, distribucijom sertifikata se distribuiraju i javni ključevi. Iz tog razloga, omogućena je pouzdana razmena javnih ključeva posredstvom Interneta između korisnika koji se nikada nisu sreli, uz mogućnost verifikovanja identiteta korisnika. Digitalni sertifikat je nemoguće falsifikovati jer je potpisan tajnim kriptografskim ključem (Private Key) sertifikacionog tela. Za verifikovanje valjanosti digitalnog sertifikata koristi se javni ključ tj. sertifikat sertifikacionog tela.

**SSL PROTOKOL**

Secure Sockets Layer – SSL

* + Bezbedna veza između dva porta aplikacija
  + Uveden je 1995. godine od strane Netscape-a (vodeći brauzer iz tog doba)
  + Koristi se i u Internet Exploreru

Većina trgovine na Internetu se temelji na SSL protokolu. Zadatak ovog protokola je uspostavljanje sigurne komunikacije između klijenta i servera na primer, Web servera i Browsera. Zadatak SSL protokola je da ostvari zaštićeni prenos podataka kroz mrežu. SSL obezbeđuje mehanizme za identifikaciju servera, identifikaciju klijenta i šifrovanu razmenu podataka između njih.

SSL obezbeđuje tri svojstva zaštite:

* **Privatnost** – Podaci šifrovani simetričnim algoritmom (DES, RC4)
* **Provera identiteta** – Identitet se proverava javnim ključem koristeći RSA
* **Integritet** – Za proveru primljenih podataka koristi se SHA ili MD5

SSL je smešten iznad transportnog sloja, a ispod aplikacionog. Pošiljalac prima poruku sa aplikacionog sloja, rastavlja je na delove koji se šifruju, zatim dodaje kontrolni broj i eventualno komprimuje te delove. Na drugoj strani primalac prima delove poruke, po potrebi ih dekomprimuje, proverava kontrolne brojeve, dešifruje i šalje ih ka aplikacionom sloju. SSL protokol je nezavisan od aplikacionog sloja. SSL se sastoji od dva “podprotokola”

* **SSL Handshake** – uspostavljanje sesije koja omogućava klijentu i serveru međusobnu identifikaciju i odabir algoritma i ključeva
* **SSL Record** – šifrovanje i prenos poruka

Pri uspostavljenju zaštićenog prenosa SSL zahteva identifikaciju servera. To se događa pri uspostavljanju sesije slanjem sertifikata. Za identifikaciju se koristi javni ključ i digitalni potpis servera. Posle identifikacije razmena podataka odnosno šifrovanje se vrši uz upotrebu simetričnog algoritma. Sertifikaciono telo može da posluži za izdavanje sertifikata, ali komunikacija sa CA serverom nije deo protokola SSL. Uspostavljanje sesije između klijenta i servera može da se vrši i bez identifikacije između klijenta i servera, pri čemu je sigurnost podataka koji se prenose na znatno nižem nivou.

Komunikacija između klijenta i servera se odvija uz pomoć poruka. Poruke odnosno njeni formati su unapred definisani:

* **Alert** – obaveštava entitete u komunikaciji o mogućem sigurnosnom propustu ili grešci u komunikaciji
* **ApplicationData** – podaci koje dve strane razmenjuju, šifrovani su, autentifikovani i verifikovani su od strane SSL-a
* **Certificate** – poruka koja prenosi sertifikat sa javnim ključem
* **CertificateRequest** – zahtev servera klijentu za klijentovim sertifikatom
* **CertificateVerify** – poruka kojom klijent potvrđuje da ima tajni ključ koji odgovara javnom ključu u sertifikatu
* **ClientHello** – poruka od strane klijenta kojom obaveštava server o sigurnosnim servisima koje želi i koje podržava
* **ClientKeyExchange** – klijentova poruka koja sadrži kriptografske ključeve za komunikaciju
* **Finished** – obaveštenje da su svi koraci pregovora gotovi i da je uspostavljena sigurna komunikacija
* **HelloRequest** – zahtev servera klijentu za početak pregovora oko sigurnosnih parametara u komunikaciji
* **ServerHello** – poruka kojom server javlja koji će sigurnosni servisi biti korišćeni
* **ServerHelloDone** – obaveštenje servera da je poslao sve zahteve klijentu za uspostavljanje komunikacije
* **ServerKeyExchange** – poruka servera koja sadrži kriptografske ključeve za komunikaciju

Najčešće se koristi pri plaćanju kreditnom karticom. Za ovakve transakcije SSL nudi zadovoljavajući nivo sigurnosti. SSL omogućava proveru integriteta pomoću sertifikata. Koristi asimetričnu i simetričnu kriptografiju. Za uspešnost SSL protokola važan je davaoc sertifikata, odnosno sertifikaciono telo. Korisnici veruju sertifikatima koji su najčešće izdati od strane poznatih kompanija koje se bave distribucijom istih. Atributi uspostavljeni tokom sesije se menjaju usled neaktivnosti sagovornika u zaštićenoj komunikaciji. SSL je relativno brzo postao standard za sigurnu komunikaciju.

### ELEKTRONSKO BANKARSTVO

Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja. Glavni cilj je postao da se bez obzira na geografske distance što brže i efikasnije povežu klijenti i tokovi informacija. U uslovima vrlo jake konkurencije gdje postepeno nestaju razlike između banaka, investicionih banaka, brokerskih firmi i osiguravajućih kompanija, finansijske organizacije su pod stalnim pritiskom da zadrže korisnike svojih usluga, smanje troškove, upravljaju rizikom i koriste tehnologiju kao izvor konkurentske prednosti. Model globalne organizacije i jake konkurencije zahteva novu koncepciju pristupa banaka u njihovom poslovanju, o čemu svedoče sve veća ulaganja u specijalizovanu i prema klijentu orijentisanu tehnologiju. Internet je jedna od tih tehnologija.  
  
Elektronsko bankarstvo, kao specifičan deo elektronskog poslovanja, ima mnoge prednosti u odnosu na klasično poslovanje: Smanjenje troškova transakcija; Brži obrt sredstava; Siguran i bezbedan platni promet; Ušteda vremena; Mogućnost obavljanja transakcija sa radnog mesta; Stalni uvid u stanje na računu i promet.  
  
Primarni cilj uvođenja sistema elektronskih plaćanja bio je rešavanje problema sistema plaćanja zasnovanih na papiru, korišćenjem potencijalnih prednosti primene informacione tehnologije. Praksa je kasnije pokazala da ovi procesi znače mnogo više od zamjene papirnih dokumenata i njihovog fizičkog prenosa elektronskim putem, odnosno da efikasno i ekonomično korišćenje ove tehnologije zahtijeva reinženjering poslovnih procesa i međuodnosa učesnika. Pojava elektronskog novca nametnula je potpuno novu filozofiju u bankarstvu koja se zasniva na elektronskoj razmeni podataka i sredstava (EFT-Electronic Funds Transfer), koja je pojmovno određena kao elektronsko bankarstvo. Sa porastom potreba korisnika bankarskih usluga, raste i očekivani kvalitet usluge. Dobra strana automatizacije bankarskog poslovanja je što je omogućeno korišćenje usluga 24 časa dnevno. Očekivani kvalitet usluge uključuje i različite dimenzije usluga. U poslednje vrijeme se javljaju korisnički zahtevi za boljom kontrolom i upravljanjem finansijama. Internet je omogućio masovni protok informacija i natjerao banke da se više pozabave kvalitetom i dostupnošću informacija.  
  
Procenjuje se da će u SAD, u narednim godinama, gotovo 30% profita sektora stanovništva biti ostvareno korišćenjem Internet bankarstva. U Francuskoj je, na primer, država učestvovala u finansiranju razvoja informatičke infrastrukture, pa je i širenje on-line bankarstva išlo veoma brzo, što je rezultiralo u većem broju elektronskih usluga koje nude banke:  
  
Informacije o računu: kupovine kreditnim/debitnim karticama, stanje na računu, korišćenje kreditnih linija, obračuni.  
  
Tekući i štedni ulozi: prezentiranje računa i plaćanja, kretanje sredstava.  
  
Hartije od vrednosti: preporuke u vezi kupovine/prodaje, cijene akcija, osnovne informacije o hartijama od vrednosti, cijene fondova, informacije o kupovini/prodaji za prethodnu godinu, informacije o primljenim dividendama i kuponima, kupovine i otkupi fondova.  
  
Razvojem elektronskog prenosa sredstava, znatno se mijenjaju finansijski instrumenti i tehnologija poslovanja. Finansijske transakcije mogu da se prenesu na neograničenu udaljenost u minimalnom vremenskom razmaku putem postojećih komunikacionih mreža u zemlji i inostranstvu, bez tradicionalnog pripremanja naloga i ostale prateće dokumentacije. EFT transfer omogućava transfer sredstava u momentu plaćanja sa računa dužnika na račun korisnika. Ovim načinom plaćanja eliminiše se plaćanje čekovima i drugim oblicima bezgotovinskog plaćanja.  
  
Elektronski sistem plaćanja (Electronic Payment System-EPS), sve je dominantnija alternativa plaćanju čekom. Pojedine zemlje razvile su posebne sisteme usluga interbankarskog transfera sredstava, u okviru mreže unutrašnjeg platnog prometa. Pored toga razvijen je: Bezgotovinski transfer na mikro nivou i, Elektronski transfer sredstava na mestu prodaje.  
  
U razvoju je, a u znatnoj meri i primjeni, niz novih bankarskih tehnologija, kao što je: Elektronska trgovina, Samouslužno (self-service) bankarstvo, Kućno i kancelarijsko bankarstvo, Pozivni centri, Kartičarstvo.  
  
Bankomati ili samouslužni šalteri, koriste se od strane banaka sa ciljem da povećaju kvalitet svojih usluga, orijentisanih prema klijentima, koje se uglavnom odnose na rutinske bankarske operacije. Bankomati nude vlasnicima platnih kartica sledeće usluge: podizanje gotovine (cash dispenser), polaganje depozita, transfer sredstava sa računa na račun, uplate na račune, naručivanje i primanje izveštaja.  
  
Elektronski transfer sredstava na mestu prodaje kao bezgotovinski sistem plaćanja, ostvaruje se preko trgovačkih, uslužnih i ostalih organizacija. Terminali ili registar kase, u ovim organizacijama povezani su sa bankarskom kompjuterskom mrežom. Korisnici ovakvog sistema transfera sredstava su u mogućnosti da na mestu kupovine, ili korišćenjem usluga vrše plaćanje prenosom iznosa, sa svog računa na račun poslodavca, preko terminala, gde se obavlja trgovina ili koristi usluga.  
  
Elektronska trgovina omogućava klijentu kupovinu i plaćanje preko kućnog PC-a. Porudžbina se obavlja preko Interneta, a prilikom plaćanja klijent se poziva na svoju platnu karticu. Za kupce, trgovine i banke, elektronska trgovina je pogodna i efikasna zbog relativno niskih troškova održavanja istih.  
  
Samouslužno bankarstvo, kao poseban vid inovacija, omogućuje korisnicima automatsku uslugu u ekspozituri, bez ljudske intervencije. Za ovakav vid usluge ekspoziture treba da su opremljene "self service terminalima". Ovi terminali su povezani sa informacionim sistemima banke, tako da zamjenjuju šalterske službenike.  
  
Kućno i kancelarijsko bankarstvo (telebanking), kao vrsta samouslužnog bankarstva, razvijeno je nakon razvoja i primjene samouslužnih šaltera i prodajnih terminala. Ova vrsta samouslužnog bankarstva nastala je sa željom da se komitenti iz svojih stanova direktno uključe u elektronski transfer sredstava, poznat kao kućno bankarstvo (home banking), odnosno da se privrednom sektoru omogući obavljanje finansijskih usluga iz svojih poslovnih prostorija poznat kao sistem kancelarijskog bankarstva.  
  
Pozivni centar kao nova tehnologija u bankarstvu, pruža komitentu mogućnost da pozivanjem banke, dobije niz informacija telefonom, bez kontakta sa službenicima banke.  
  
Platne kartice, kao savremeni instrumenti bezgotovinskog plaćanja, koriste se za identifikaciju izdavaoca i korisnika kartice, na aparatima za izvođenje finansijskih transakcija, u cilju obezbeđenja unosa podataka za te transakcije. Dve su vrste platnih kartica - debitne i kreditne. Vrlo često se misli na debitnu karticu kada se pomene platna, ili obrnuto. Međutim, razlika je jasna. Dok je platna kartica sredstvo plaćanja (ili jednostavnije-to je mala plastična kartica kojom se mogu plaćati roba i usluge), debitna i kreditna kartica su njene podvrste. U zavisnosti od toga za koju se platnu karticu klijent banke opredijeli, na raspolaganju će mu biti prateći programi i važiće potpuno različiti propisi njenog korišćenja. Kada se koristite debitnim karticama po pravilu morate na računu imati novac koji želite da potrošite. Kod kreditne kartice je potpuno suprotno-po pravilu nemate novac koji trošite, već na kraju meseca (ili nekog drugog perioda plaćanja koji banka odredi) plaćate iznos koji ste potrošili u potpunosti ili djelimično. Kreditna kartica sigurno zvuči bolje, ali je isto potrebno reći da kreditnu karticu ne može dobiti svako. U inostranstvu koje je daleko odmaklo kada je u pitanju ovaj način plaćanja, praćenjem kreditnog ponašanja pojedinaca bave se kreditni biroi. Oni, na zahtev banaka koje su primile molbe od potencijalnih klijenata, sastavljaju izveštaj o tome kako se određena osoba ponašala prethodnih godina u smislu finansijske odgovornosti-da li je plaćao račune na vrijeme, da li je imao stabilan posao, posjeduje li ili iznajmljuje kuću/stan, ima li mobilni telefon i slično. Ako banka smatra da je klijent dovoljno pouzdan, izdaće mu kreditnu karticu i dozvoliti mu da troši njen novac (što će kasnije platiti), jer je rizik prihvatljiv. U suprotnom, ponudiće mu debitnu karticu.  
  
Kartica se definise kao mali komad kartona ili plastike koji sadrzi neko srestvo za indetifikaciju, sto omogucava osobi na koju kartica glasi da kupuje robu ili usluge na teret svog racuna. Prvu univerzalnu karticu izdao je Diners Club 1950 godine. Kasnije su se pojavili bankarski sistemi kreditnih kartica u kojima banka odobrava racun trgovcu odmah po prijemu racuna o prodatoj robi, prikuplajuci racune koji ce biti zaracunati vlasniku kartice nakon dogovorenog vremenskog perioda.  
  
Smart kartica je plastična kartica koja po izgledu podseća na običnu karticu s tim da poseduje jedan detalj koji je odvaja od njih, a to je integrisano kolo ili čip na kojem se nalazi procesor i memorija. Na čipu se na siguran način mogu čuvati odredjeni podaci. Najveća snaga SmartKard tehnologije jeste u raznovrsnosti mogućih primena. Zahvaljujući inteligenciji kartice, moguće je razviti raznovrsne aplikacije u oblastima kao što su: zaštita pristupa računaru ili mreži, indetifikacija, mobilna telefonija, digitalan potpis, kupovina, zaštita autorskih prava, elekronska kupovina, ...  
  
Naglo širenje interneta u poslednjoj deceniji i njegovo sve veće korišćenje u poslovne svrhe nametnuli su potrebu za promjenama u funkcionisanju svjetske mreže. Sve je veći broj povjerljivih podataka koji se prenose internetom kao i porast trgovine putem interneta stavili su u prvi plan problem sigurnosti komunikacije. Naročito aktuelan problem je sigurnosti komunikaciji je web servera i clienta. Standardni protokoli za komunikaciju ne nude rješenje za ove probleme. Zato je razvijeno više protokola koji obezbedjuju sigurnu komunikaciju prije svega na internetu. Neki od njih su na aplikativnom nivou poput secure HTTP-a ili Secure Socket Layera, protokol koji je defakto standard za sigurnu komunikaciju. Problem tajnosti u računarskim komunikacijama rješava se kriptovanjem podataka na izvoru i dekriptovanjem na odredištu. Savremene metode kriptovanja zasnivaju se na javno dostupnim algoritmima, a tajnost podataka je garantovana tajnošću ključa.  
  
Elektronsko bankarstvo predstavlja segment digitalne ekonomije u sferi elektronskog platnog prometa i transfera novčanih sredstava, a u međuvremenu se razvilo na sve vidove poslovanja banaka, kako unutar njene organizacije tako i na njene komitente. Institucionalno bankarstvo i finansijska tržišta imaju za poslovno okruženje sve privredne i poslovno aktivne subjekte, koji su najdirektnije upućeni na međusobnu poslovnu saradnju. Preko usluga koje bankarski sektor obavlja za svoje komitente i klijente, i preko finansijskih inovacija koje je neophodno nuditi u tržišnim uslovima, sve više dolazi do izražaja poslovna saradnja, zasnovana na savremenim informacionim i telekomunikacionim tehnologijama, što ima za rezultat transformaciju načina rada i poslovne saradnje ka elektronskom poslovanju i digitalnoj ekonomiji.