. SSL (Secure Sockets Layer)

SSL (*Secure Sockets Layer*) je protokol za sigurno slanje poruka (komunikaciju) putem interneta, koji omogućava slanje poverljivih podataka (npr. broj kreditne kartice) putem interneta u šifriranom i sigurnom obliku. SSL protokol ostvaruje poseban komunikacijski sloj, koji je smešten na pouzdani transportni sloj. Od aplikacijskog sloja prima poruku koju treba poslati, rastavi je u manje delove prikladne za šifriranje, dodaje kontrolni broj, šifrira, eventualno kompresira, a zatim te delove pošalje. Primatelj primi delove, dekompresira, dešifrira, proveri kontrolne brojeve, sastavi delove poruke, pa ih preda aplikacijskom sloju. Na taj način se putem SSL-a ostvaruje zaštićeni kanal prenosa kroz mrežu. Ukoliko su klijent i server neaktivni duže vreme ili razgovor s istim atributima zaštite potraje predugo, atributi se menjaju.

SSL protokol je dizajniran i napravljen u kompaniji Netscape Communications, za upotrebu s Nescape Navigatorom. Prva verzija, 1.0, je razvijena 1994. godine, međutim, to je bila samo probna verzija korištena unutar ove kompanije. Verzija 2.0 je bila prva koja je izdana u javnost i koja je isporučivala s Netscape Navigatorom, verzijama 1 i 2. Poslije verzije SSL 2.0, Microsoft je izdao svoju verziju ovog protokola, koja je imala naziv PCT (*Private Communications Transport*). Najnovija verzija SSL 3.0, je uključila sva poboljšanja Microsoft-ovog PCT-a, i time uklonila slabosti verzije SSL 2.0. U to vreme je, IETF (Internet Engineering Task Force) grupa, koja je osnovana 1996. godine, napravila otvoreni standard za šifriranje zasnovan na SSL-u 3.0. Ovaj protokol je nazvan TLS (Transport Layer Security) verzija 1.0, i objavljen je 1999. godine na RFC (*Request For Comments*) 22461. Očekuje se da će TLS protokol biti standardiziran od strane IETF-a, i može se reći da se on razlikuje od SSL-a u nekoliko detalja. On je adaptiran od strane korisnika i projektanata mobilnih radio uređaja, koji su prilagodili ovaj protokol bežičnim komunikacijama, i nazvali ga WTLS (Wireless Transport Layer Security ).

3.2.1. Vrste potvrda

Postoji više vrsta potvrda. Potvrde je moguće koristiti i u drugim situacijama, ne samo u okviru SSL protokola, ali njihova upotreba izlazi izvan okvira ovog rada.

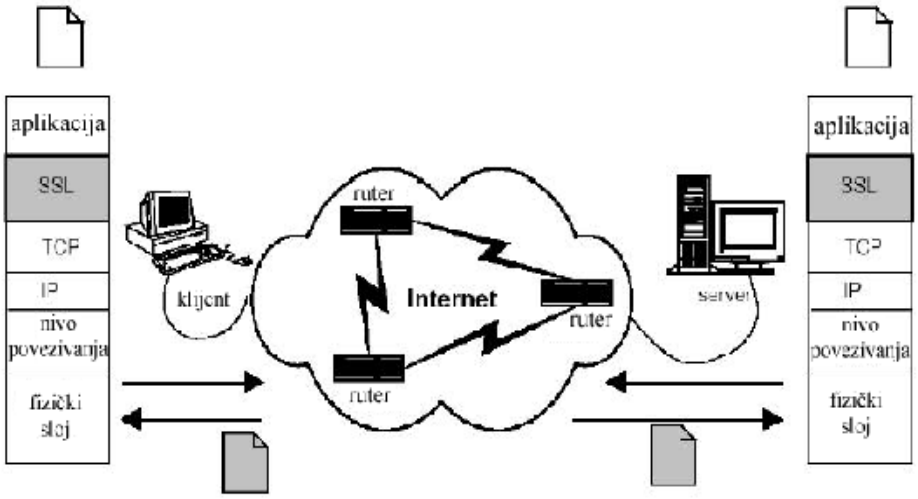
- *Klijentske SSL potvrde ;* Koriste se za identifikaciju klijenta putem SSL protokola. Uobičajeno je poistovjećivanje identiteta klijenta s osobom. Osim za identifikaciju osoba kod pristupa serveru, klijentska potvrda se može koristiti i u druge svrhe, npr. za digitalno potpisivanje digitalnih formulara. Primjer: 1. Banka daje korisniku klijentsku SSL potvrdu koja omogućava serveru banke identifikaciju korisnika i dozvoljava korištenje bankovnog računa. 2. Preduzeće može dati svakom novom zaposlenom klijentsku SSL potvrdu, kojom je moguće dobiti pristup serveru poduzeća.

- *Serverske SSL potvrde;* Koriste se za identifikaciju servera od strane klijenta putem SSL protokola. Identifikacija servera je obavezna u SSL protokolu za ostvarivanje zaštićenog prijenosa podataka dok identifikacija klijenta nije. Primer: Internet poslovanje, npr. *on-line* prodavaonice, najčešće koriste identifikaciju servera preko serverskih SSL potvrda kako bi uspostavili zaštićenu SSL vezu i uverili korisnika da je to odgovarajuće

preduzeće s kojim korisnik želi poslovati. Šifrirana SSL veza osigurava da osetljivi podaci koji se šalju kroz mrežu, kao što su brojevi kreditnih kartica, budu zaštićeni.

### 3.2.2. Opšti prikaz SSL protokola

SSL omogućava razmenu informacija između klijenta i servera, na transparentan način. Ovaj protokol nalazi se između aplikacijskog i transportnog sloja ISO/OSI (*International Standard Organization's Open System Interconnect* ) referentnog modela. Koristeći ovaj pristup, moguće je identificirati SSL protokol kao dio sloja za prezentaciju. Na slici br. 1 se može viđeti mesto SSL-a u okviru TCP/IP protokola.




*Slika br. 1 SSL u okviru TCP/IP protokola*

Međutim, SSL ne funkcioniše na vrhu *User Datagram* protokola, zato što ne nudi pouzdan prenos podataka, što može dovesti do gubitka IP paketa. Zbog toga, SSL ne može pružiti zaštitu za sledeće protokole: SNMP (*Simple Network Management Protocol* ), NFS (*Network File System*), DNS (*Domain Name Service*) kao i za protokol VOIP (*Voice Over Internet Protocol*). SSL se sastoji od dva pod-nivoa: SSL *Record* i SSL *Handshake*, te koristi još 4 podprotokola: 1) SSL *Record*, 2) SSL *Handshake*, 3) *Change Cipher Spec*, i 4) *Alert*. SSL *Record* sloj je odgovoran za prenos blokova informacija, između dva računara. SSL *Handshake* protokol upravlja razmenom ključeva, obaveštenja i promene lozinki. Ovi nivoi se nalaze na vrhu sloja za prenos podataka, koji je obično TCP sloj. Na slici br. 2 vidi se veza između pod-protokola, kao i njihova lokacija, i ostali slojevi SSL-a.