# **Kriptografski protokoli**
(SSL, IPSec, Kerberos)

# Sadržaj

- Kriptografski protokoli
- Protokol Secure Socket Layer (SSL)
- Protokol SSH i OpenSSH implementacija
- IPSec
- Kerberos

# Kriptografski protokoli

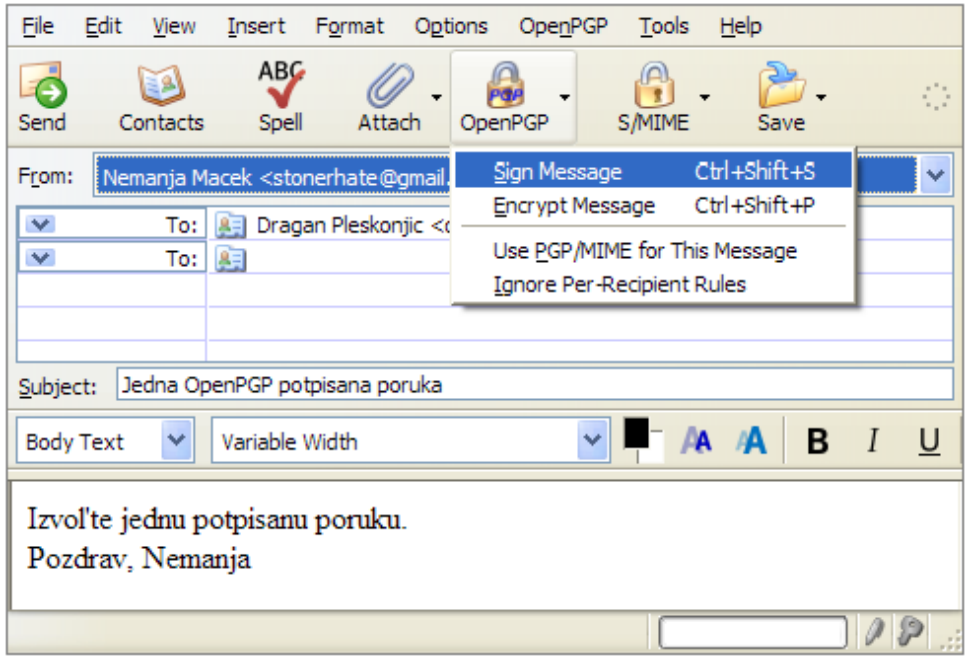
- Protokol je skup pravila i konvencija koji definiše komunikacioni okvir između dva ili više učesnika u komunikaciji.
  - Uspostava veze
  - Održavanje veze
  - Raskid veze
  - Oporavak u slučaja prekida veze
  - Učesnici u komunikaciji: krajnji korisnici, procesi ili računarski sistemi.
- Ukoliko je bar jedan deo poruke šifrovan, protokol se može smatrati **kriptografskim**.
- **Kriptografski protokoli** su protokoli koji se oslanjaju na kriptografske metode zaštite kako bi učesnicima u komunikaciji obezbedili usluge **poverljivosti**, **integriteta** i **neporecivosti**.
- Postoji mnoštvo protokola koji pružaju sigurnost na različitim nivoima skupa protokola TCP/IP.
- Prednosti i lose strane implementacije na različitim slojevima ilustrujemo na primeru:
  - aplikacionog sloja,
  - мrežnog sloja.

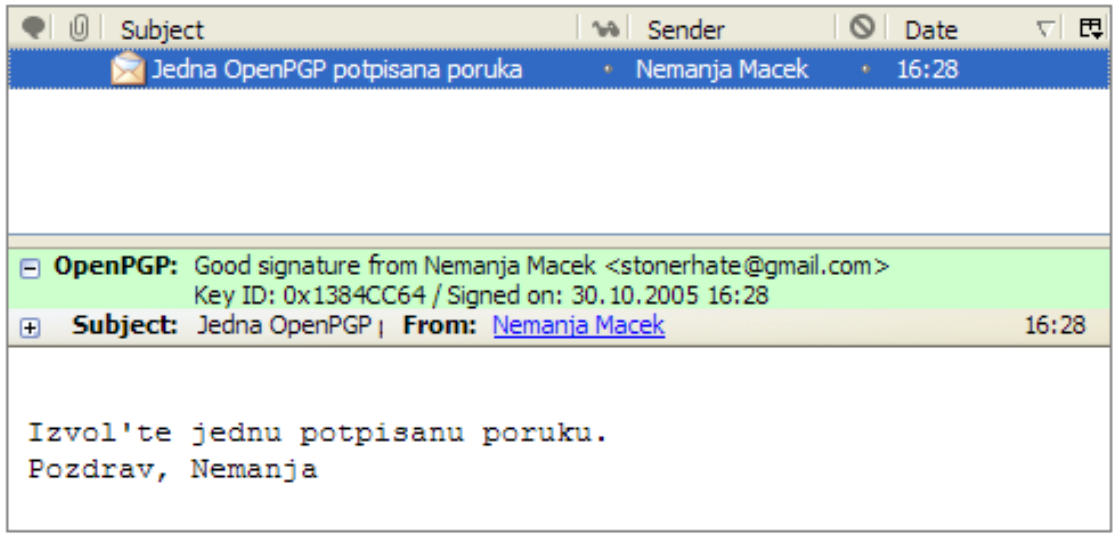
# Kriptografski protokoli

- **Kriptografski protokoli na sloju aplikacije**.
- Moraju biti implementirani u krajnjim tačkama komunikacije (najčešće, na računarima).
- Prednosti:
  - Aplikacija može da se proširi bez oslanjanja na sigurnosne usluge koje obezbeđuje OS.
  - Kompletan pristup podacima koje korisnik želi da zaštiti.
    - Olakšano obezbeđivanje sigurnosnih usluga (na primer, neporecivosti).
    - Lak pristup akreditivima korisnika (poput privatnih ključeva).
- Loše strane i potencijalni problemi:
  - Sigurnosni mehanizami moraju se projektovati za svaku aplikaciju posebno.
    - To znači da se postojeće aplikacije moraju izmeniti i/ili proširiti.
  - Projektovanje više različitih sistema $\rightarrow$ veća verovatnoća greške i sigurnosnih propusta.

# Kriptografski protokoli

- **Kriptografski protokoli na sloju aplikacije**.
- Primer: OpenPGP
  - Klijent e-pošte „proširuje“ se procedurama za pronalaženje javnih ključeva korisnika, šifrovanje i dešifrovanje i proveru autentičnosti poruka.



# Kriptografski protokoli

- **Kriptografski protokoli na mrežnom sloju**.
- Prednosti:
  - Premašenje izazvano razmenom ključeva značajno je smanjeno.
  - Svi transportni protokoli i aplikacije sada dele infrastrukturu upravljanja ključem koju obezbeđuje mrežni sloj.
  - Promene aplikacija su značajno manje (minimalne) u odnosu na prethodni slučaj.
  - Mogućnost izgradnje virtuelne privatne mreže (VPN-a).
- Loše strane i potencijalni problemi:
  - Teško obezbeđivanje usluge neporecivosti.
    - Znatno lakše se ostvaruje na višim slojevima!
  - Teško ostvarivanje kontrole na nivou korisnika na višekorisničkom računaru.
  - Rešenje problema: uvođenje dodatnih mehanizama na krajnjim računarima.

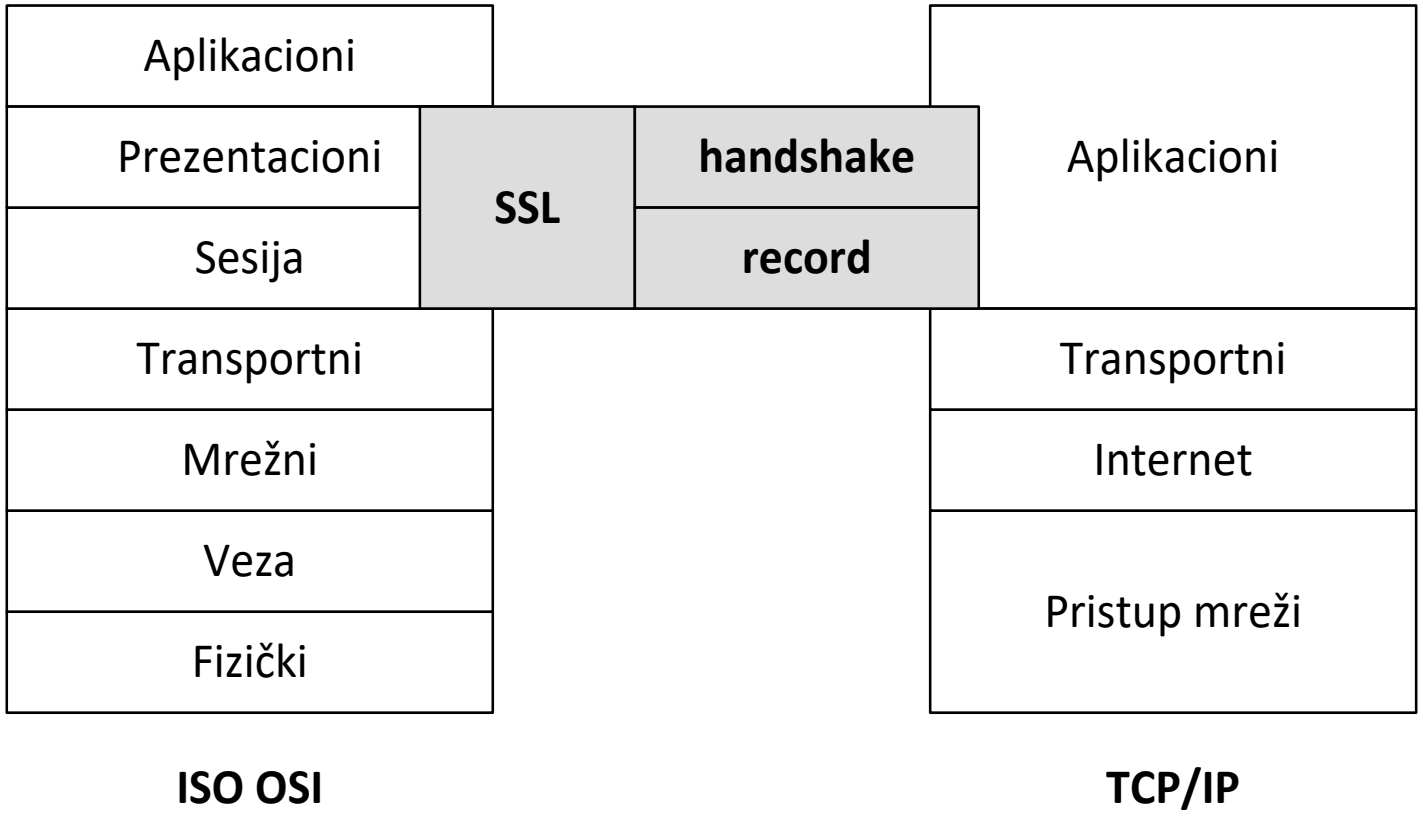
# Protokol Secure Sockets Layer (SSL)

- Protokol SSL obezbeđuje mehanizme za identifikaciju dva sagovornika povezana računarskom mrežom i zaštićeni prenos podataka između njih.
- **Kriterijumi projektovanja**.
  - Kriptografska zaštita.
  - Nezavisnost od softvera i hardvera.
    - Dva različita programa koji koriste SSL (npr. Web server i Web čitač) mogu razmeniti parametre šifrovanja, bez međusobnog poznavanja koda.
  - Proširivost.
    - U okvir se u slučaju potrebe mogu uklopiti novi algoritmi.
    - Nema potrebe za projektovanjem novih protokola $\rightarrow$ manja šansa pojavljivanja novih sigurnosnih propusta i grešaka.
  - Efikasnost.
    - SSL kešira komunikacione parametre ostvarenih veza.
    - Manji broj veza koje mora ponovo da uspostavlja $\rightarrow$ manje se opterećuje procesor.

# Protokol Secure Sockets Layer (SSL)

- **Zadatak SSL protokola** je da ostvari zaštićeni prenos podataka kroz mrežu.
- SSL obezbeđuje mehanizme za:
  - identifikaciju serveram
  - identifikaciju klijenta,
  - šifrovanu razmenu podataka između njih.
- To čini potpuni sistem zaštićene komunikacije dva mrežna entiteta.
- Za ostvarivanje zaštićenog prenosa, protokol SSL moraju podržavati i klijent i server.
- **Svojstva SSL-a**:
  - privatnost (šifrovanje podataka simetričnim algoritmima),
  - provera identiteta (provera identiteta klijenta, odnosno servera, javnim ključem),
  - pouzdanost (provera integriteta primljenih podataka).

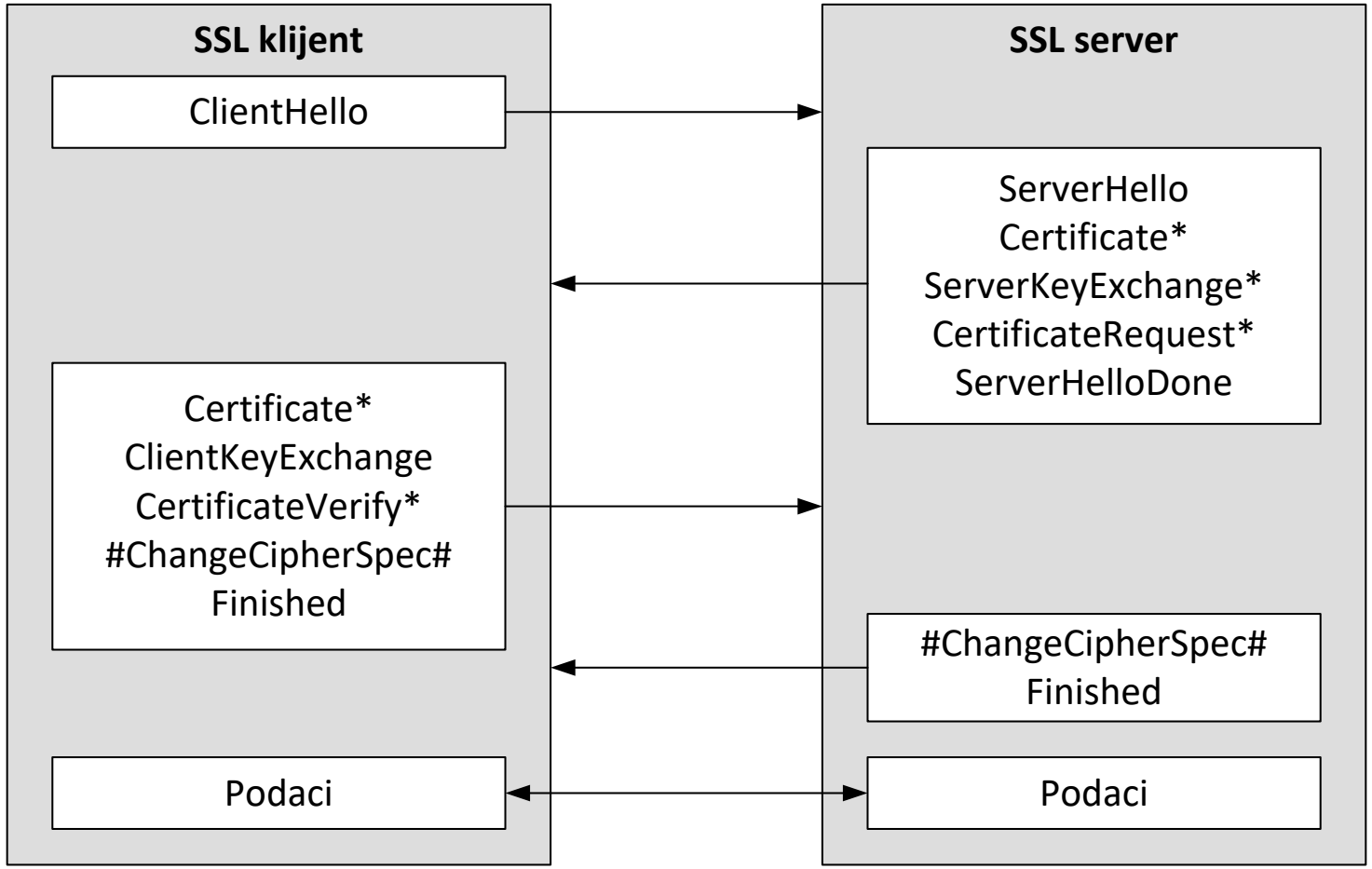
# Protokol Secure Sockets Layer (SSL)



# Protokol Secure Sockets Layer (SSL)

- SSL se sastoji od dva protokola:
- **SSL Handshake protokol** (protokol za rukovanje, tj. uspostavljanje sesije).
  - Međusobna identifikacija klijenta i servera.
    - Očekivani minimum: identifikacija servera slanjem svog sertifikata klijentu.
      - Za identifikaciju servera koristi se javni ključ i digitalni potpis servera.
      - Komunikacija servera ili klijenta sa CA nije deo protokola SSL!
      - Određena je drugim preporukama i standardima.
    - SSL može uspostaviti sesiju bez identifikacije klijenta i servera.
      - Tada je nivo zaštite prenosa podataka vrlo nizak.
      - Podaci se štite samo simetričnim šifrovanjem.
      - Ključ je nezaštićenom komunikacijom dogovoren između klijenta i servera.
  - Razmena parametara za prenos (odabir algoritma i ključeva).
- **SSL Record protokol** (protokol za zapise).
  - Zadužen za šifrovanje i prenos poruka.

# SSL Handshake



# SSL Handshake

- K → S: Pozdravna poruka `ClientHello`.
- S → K: Pozdrav `ServerHello` (ako ovog nema, sledi prekid komunikacije).
  - Pozdravne poruke koriste se za uspostavljanje atributa sesije.
    - Klijent u svom pozdravu nudi serveru listu mogućih načina šifrovanja i komprimovanja.
    - Server bira najbolju kombinaciju koju može da prihvati.
- S → K: Sertifikat (`Certificate`).
  - Server može tražiti klijentov sertifikat (`CertificateRequest`) ako je to u skladu sa dogovorenim algoritmima šifrovanja.
  - U tom slučaju on očekuje ili sertifikacionu poruku ili izveštaj da klijent nema sertifikat.
- S → K: Poruka o kraju pozdrava (`ServerHelloDone`).
- K → S: Novi atributi (`#ChangeCipherSpec#`) kojima će slati šifrovane podatke.
  - Klijent postavlja nove attribute za aktivne.
- K → S: Izveštaj o kraju slanja šifrovan aktivnim atributima (`Finished`).
- S → K: Server šalje svoje attribute i izveštaj o kraju slanja šifrovan novim atributima.

# SSL Handshake

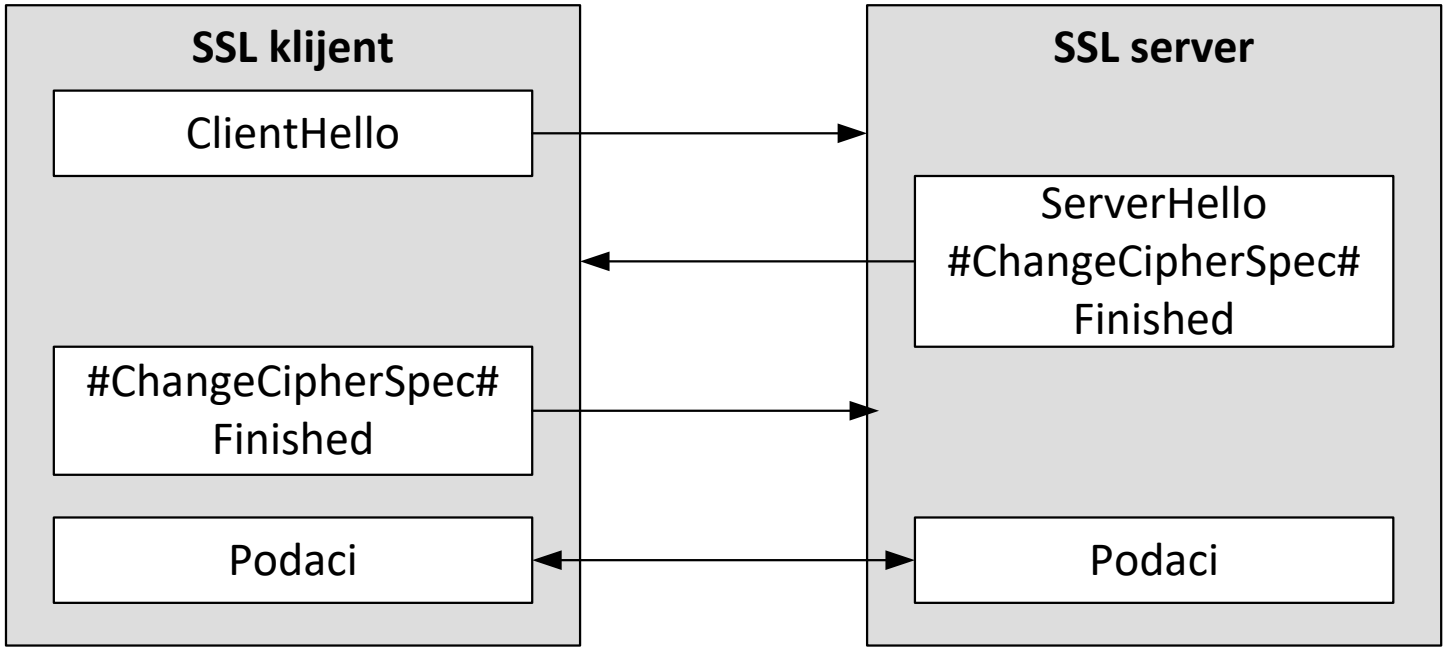
- Kada SSL protokol za rukovanje identifikuje server i/ili klijent i dogovori načine šifrovanja kažemo da je uspostavljena **sesija** (engl. *session*).
- **Atributi kojima je opisana sesija** se dogovaraju prilikom uspostavljanja sesije (engl. *handshake*):
  - Identifikator sesije.
    - Niz bajtova koji ugovaraju klijent i server i koji jedinstveno identifikuje tu sesiju.
  - Potvrda entiteta.
    - Ako je sesija uspostavljena bez identifikacije klijenta i servera, atribut je NULL.
  - Algoritam kompresije.
    - Ako se kompresija ne obavlja, atribut je NULL.
  - Kriptografski algoritmi (algoritam za simetrično šifrovanje i jedna heš funkcija).
  - Zajednička tajna.
    - Koristi se za generisanje simetričnih ključeva i izračunavanje MAC vrednosti.
  - Proširivost.
    - Oznaka koja pokazuje može li se unutar date sesije uspostaviti nova veza.

# SSL Handshake

- Često klijent i server žele paralelno da uspostave više sesija.
  - Primer: prenos datoteke i čitanje sadržaja Web stranice.
- Zato je omogućeno da se unutar jedne sesije uspostaviti više **veza** (engl. *connection*).
- **Atributi SSL veze** su:
  - Slučajne vrednosti klijenta i servera.
    - Koriste se za šifrovanje i moraju biti različite.
  - Serverova i klijentova MAC tajna.
    - Koriste se za identifikaciju poruka koje šalje server, odnosno klijent.
  - Serverov i klijentov simetrični ključ.
    - Ključ kojima server šifruje, a klijent dešifruje poruke, i obrnuto.
  - Redni brojevi poruka.
    - I klijent i server moraju da vode računa o rednim brojevima poslatih i primljenih poruka.
    - Ako se u toku veze promene načini šifrovanja, redni brojevi se postavljaju na nulu.
    - Promenom atributa sesije i veze za vreme njihovog trajanja postiže se **viši nivo zaštite**.

# Obnavljanje SSL sesije

- Klijent i server imaju mogućnost da nastave razgovor ukoliko su ranije već komunicirali.
- Time se preskače provera verodostojnosti i dogovaraju se samo nužni novi atributi.



# SSL Record

- Na strani **pošiljaoca** SSL protocol za zapise:
  - Prima podatke s višeg sloja.
  - Deli podatke na na blokove fiksne dužine.
    - Više poruka može biti spojeno u jedan fragment ili jedna poruka podeljena u više fragmenata.
  - Komprimuje fragmente (ukoliko je to dogovoreno).
  - Šiti fragmente simetričnim algoritmom (privatnost) i MAC algoritmom (integritet poruke),
  - Šalje poruku nižim slojevima.
- Na strani **primaoca** SSL protokol za zapise:
  - Dešifruje primljeni fragment.
  - Izračunava MAC vrednost i upoređuje je sa onom koju je generisao pošiljalac.
    - Ukoliko su ove MAC vrednosti identične, poruka se prihvata.
    - U suprotnom vraća se izveštaj o grešci.

# SSL izveštaji

- Izveštaj je posebna vrsta poruka koju SSL koristi za osiguravanje ispravnog toka sesije.
- Dve vrste izveštaja:
- **Izveštaj o kraju veze**.
  - Služi za dogovor o kraju veze pre samog prekida veze.
  - Kraj može inicirati bilo koji učesnik.
- **Izveštaj o grešci**.
  - Ako jedan od učesnika ustanovi grešku prilikom komunikacije, obavestiće o tome sagovornika pomoću izveštaja o grešci.
  - Ako greška ugrožava sigurnost prenosa oba sagovornika istovremeno prekidaju vezu.
  - Komunikacija preko drugih veza unutar sesije može se nastaviti.
    - Neophodno je da se promeni identifikator sesije.

# SSL izveštaji

- **Izveštaj o grešci**.
  - Neočekivana poruka.
    - Rezultuje prekidom veze (SSL sumnja na napad tipa fabrikovanje podataka).
  - Neispravna MAC vrednost.
    - Rezultuje prekidom veze (SSL sumnja na napad tipa izmena podataka).
  - Greška prilikom dekompresije.
  - Greška u fazi uspostavljanja sesije.
    - Pošiljalac nije u mogućnosti da se uskladi sa atributima zaštite koji su mu predloženi.
    - Rezultuje prekidom sesije (u ovom slučaju veze još nisu uspostavljene).
  - Greške vezane za sertifikate.
    - Nema sertifikata, nevažeći sertifikat, poništen sertifikat, …
  - Nevažeći parameter
    - Vrednost nekog atributa nalazi se van dozvoljenih vrednosti ili je nekonsistentna s ostalim vrednostima.
    - Rezultuje prekidom veze.

# Protokol SSH i OpenSSH implementacija

- **Secure Shell** (SSH) je popularan protokol za šifrovanje komunikacionih kanala, koji se najčešće koristi za obezbeđivanje sigurnih sesija udaljenog prijavljivanja na sistem.
- **OpenSSH**.
  - Besplatna verzija SSH familije kriptografski zaštićenih mrežnih protokola.
  - Omogućava udaljeno prijavljivanje na sistem, pristup komandnoj liniji i prenos datoteka između računara.
- Serverska OpenSSH komponenta (`sshd`) osluškuje (podrazumevano na portu 22).
- Server odgovara shodno klijentskoj aplikaciji koja je poslala zahtev sa udaljenog računara:
  - Zahtev šalje `ssh` klijent.
    - OpenSSH server podešava pristup komandnoj liniji nakon autentifikacije.
  - Zahtev šalje `scp` klijent.
    - OpenSSH server pokreće servis sigurnog kopiranja datoteka nakon autentifikacije.

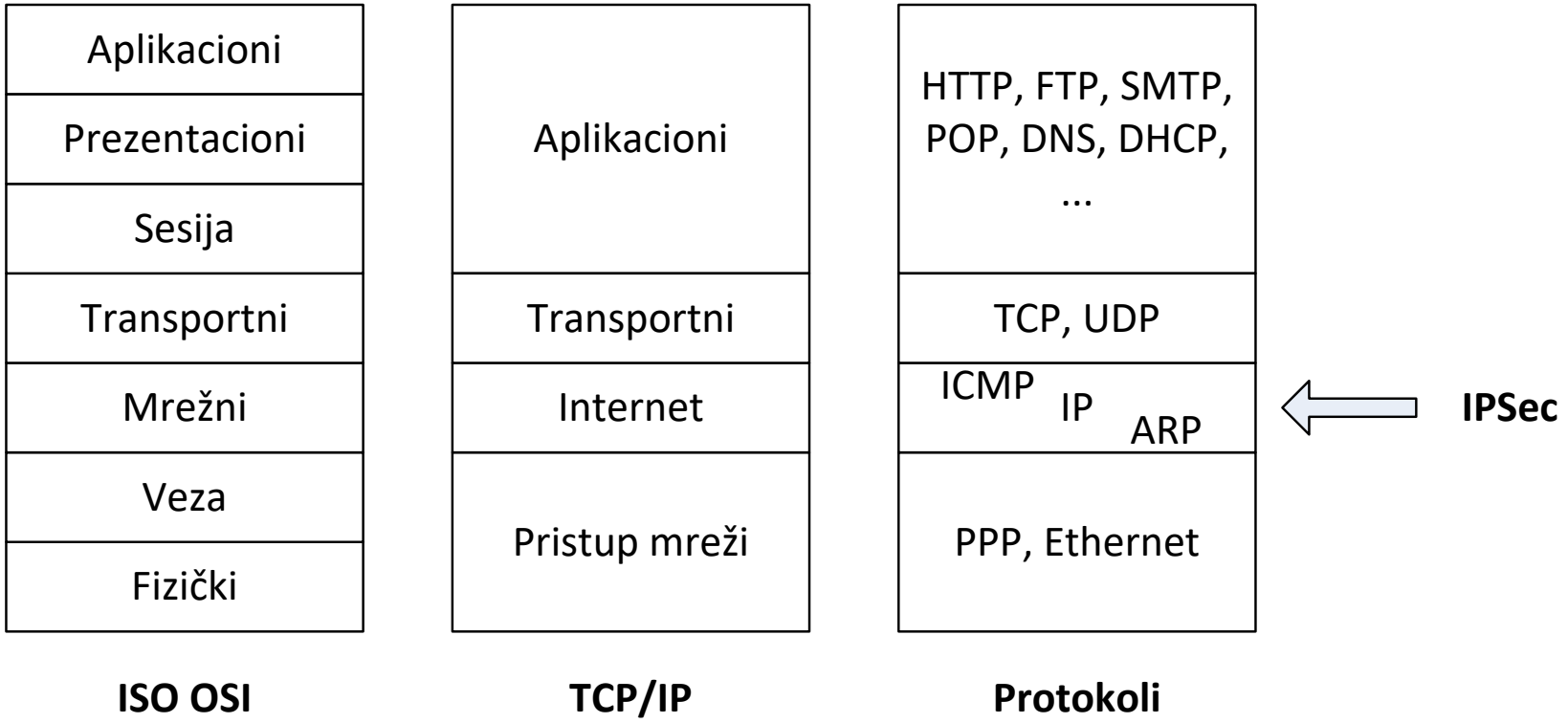
# Protokol SSH i OpenSSH implementacija

- OpenSSH koristi nekoliko metoda autentifikacije:
  - lozinka,
  - kriptografski ključevi,
  - Kerberos tiketimi,
  - PAM moduli (poput OTPW).
- Autentifikacija pomoću ključeva:
  - Prednosti:
    - "*To be as hard to guess as a normal SSH key, a password would have to contain 634 random letters and numbers*."
    - Sprečavaju se napadi pogađanjem lozinki, uključujući i društveni inženjering!
  - Mane:
    - Možete prijaviti samo sa računara sa kog je prethodno dozvoljen SSH pristup.
    - Pristup nije moguć ukoliko slučajno obrišete ključ sa računara kom je dozvoljen pristup.
    - Šta ćemo da radimo ako zabranite lokalni login a ostane ključ?

# IPSec

- **IPSec** (IP Security) je skup proširenja protokola IPv4 i integralni deo protokola IPv6.
- IPSec NIJE protokol.
  - To je skup protokola, algoritam i opšti okvir (engl. *framework*).
- IPSec obezbeđuje:
  - privatnost,
  - integritet,
  - proveru identita,
  - neporecivost.
- IPSec implementira sigurnosne mehanizme mrežne komunikacije na mrežnom sloju OSI referentnog modela (Internet sloj TCP/IP skupa).
  - Upotreba IPSec protokola transparentna je za više slojeve skupa protokola TCP/IP.
  - To znači da aplikacije koriste ove usluge bez obzira na svoju funkcionalnost.
- Primena: povezivanje udaljenih ogranaka firme sa centralom sigurnom vezom preko javnih (nesigurnih) mreža, siguran pristup sa udaljenih lokacija preko javne mreže, itd.

# IPSec

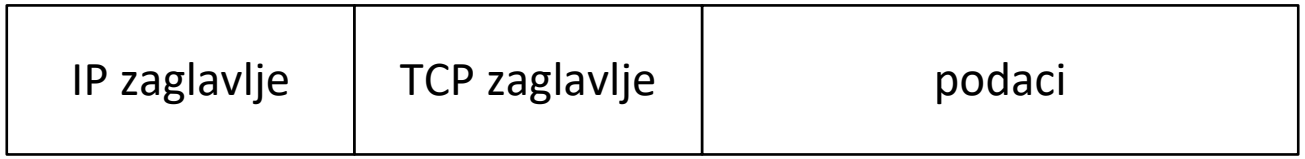

Aplikacioni
Prezentacioni
Sesija
Transportni
Mrežni
Veza
Fizički
ISO OSI
Aplikacioni
Transportni
Internet
Pristup mreži
TCP/IP
HTTP, FTP, SMTP, POP, DNS, DHCP, ...
TCP, UDP
ICMP IP ARP
PPP, Ethernet
Protokoli
IPSec

# IPSec režimi rada

- **Prenosni režim** (engl. *transport mode*).
  - Šifruju se samo podaci a IP zaglavlja ostaju u obliku otvorenog teksta.
  - Zaglavlja viših slojeva (na primer, sloja aplikacije) su šifrovana.
  - Potrebno je da obe krajnje tačke komunikacije (izvor i odredište) podržavaju IPSec.
  - U ovom načinu rada adrese izvorišta i odredišta poruka su vidljive (napadač može delimično da analizira mrežni saobraćaj).
- **Tunelovanje** (engl. *tunnel mode*).
  - Potpuno siguran prenos preko javnih ili privatnih mreža.
  - Tunel = klijent + server (koji su konfigurisani da koriste IPSec tunelovanje).
  - Enkapsulacija i šifrovanje kompletnih IP paketa.
    - Šifrovani podaci se spajaju sa odgovarajućim nešifrovanim IP zaglavljima.
    - Formiraju se IP paketi koji se na kraju tunela dešifuju i oblikuju u IP pakete namenjene krajnjem odredištu.

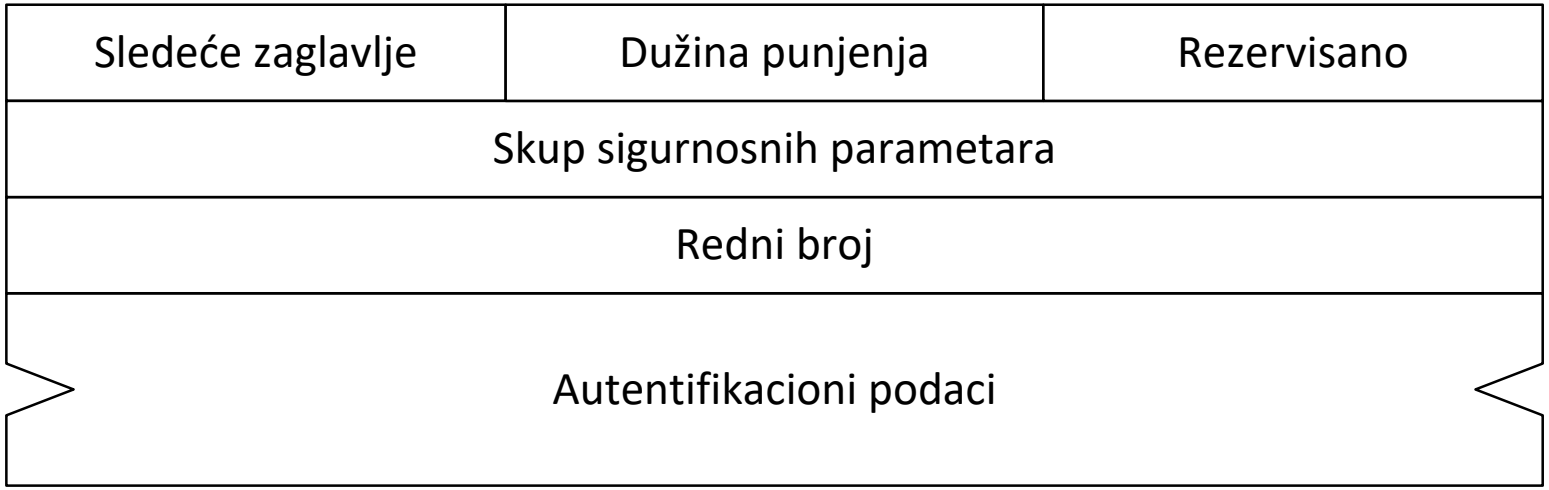
# IPSec protokoli

- IPSec se implementira pomoću dva međusobno nezavisna protokola.
- **AH** (*authentication header*) obezbeđuje usluge:
  - integriteta,
  - provere identiteta,
  - neporecivosti.
- **ESP** (*encapsulated security payload*) osim toga obezbeđuje i privatnost podataka.
- Oba protokola, AH i ESP, modifikuju standardni oblik IP paketa.



# Protokol AH

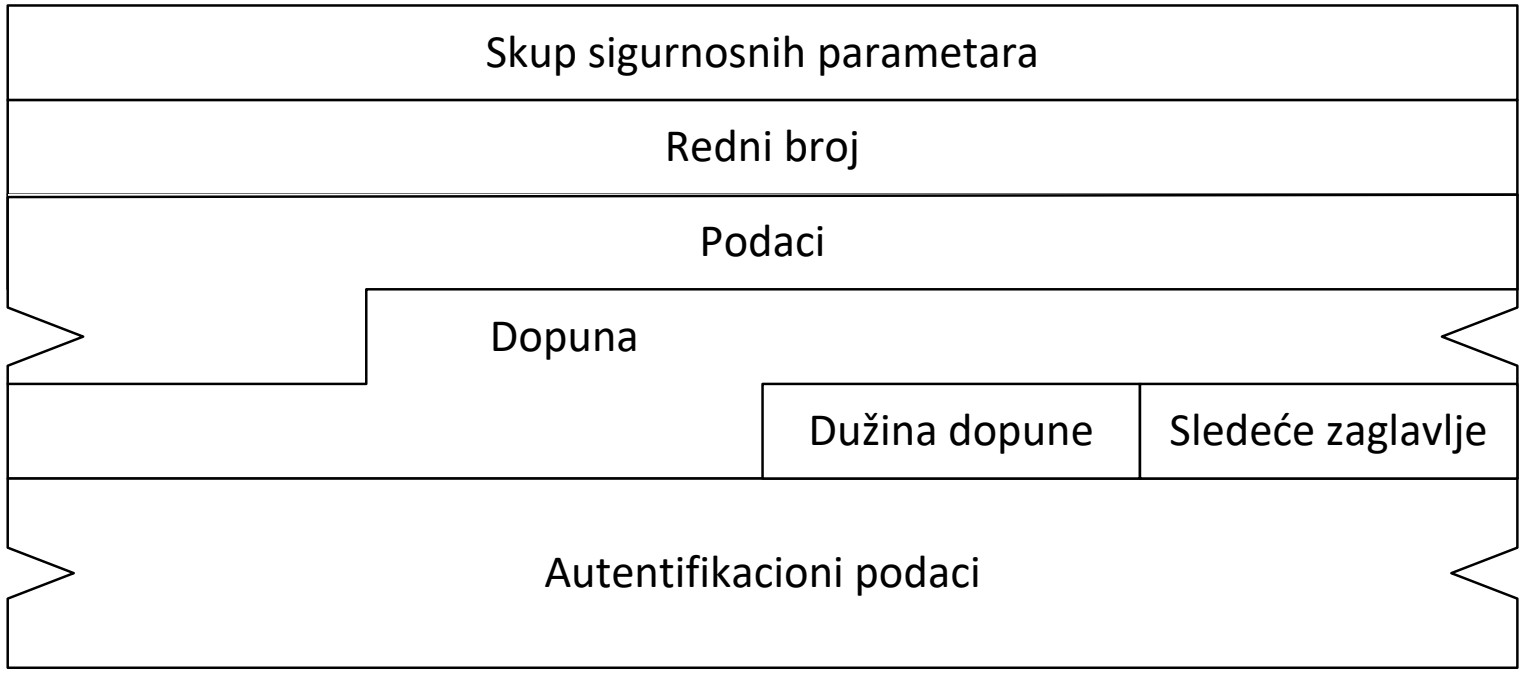
- Obezbeđuje usluge provere identiteta, integriteta i neporecivosti IP paketa ali ne i privatnost.
- Protokolom je definisano zaglavlje koje se smešta između IP zaglavlja i podataka koji slede.
- Specifičnost AH je u tome što ne enkapsulira podatke protokola kojima pruža uslugu.




AH zaglavlje

# Protokol ESP

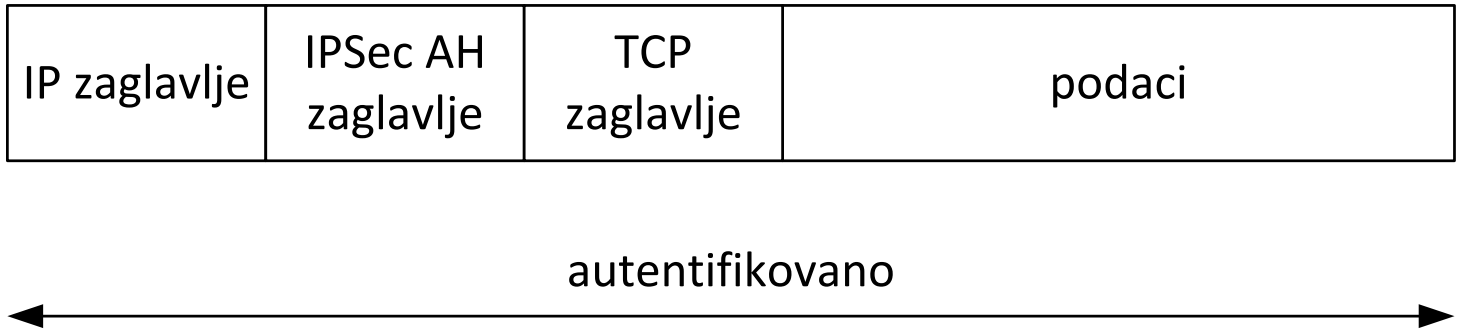
- Obezbeđuje usluge provere identiteta, integriteta, neporecivosti i privatnosti podataka.
- Definiše ESP zaglavlje koje se u IP paket smešta posle IP zaglavlja, enkapsulira sve podatke protokola višeg sloja i dodaje završni slog u koji se mogu smestiti podaci za proveru identiteta.




ESP paket

# AH u transportnom režimu rada

- Polje „protokol“ u IP zaglavlju sadrži vrednost 51 (AH).
- Polje „sledeće zaglavlje“ u AH zaglavlju sadrži vrednost koja odgovara protokolu višeg sloja čiji su podaci enkapsulirani (na primer, 6 za TCP segment).
- Obezbeđuje se provera identiteta, integritet i neporecivost celog IP paketa.

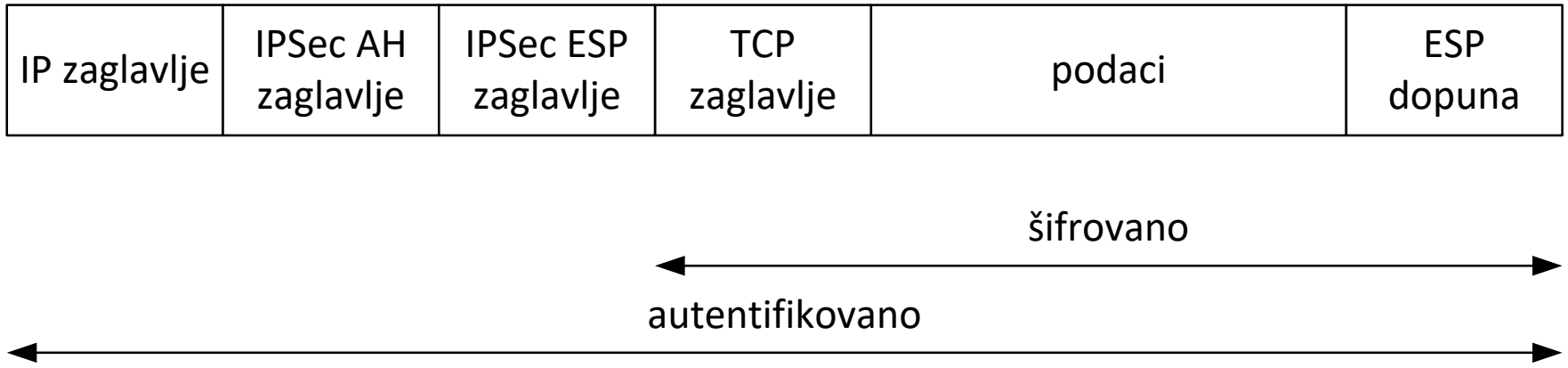


# ESP u transportnom režimu rada

- Polje „protokol“ u IP zaglavlju sadrži vrednost 50 (ESP).
- Polje „sledeće zaglavlje“ u ESP zaglavlju ima funkciju istu kao i u AH zaglavlju.
- Ukoliko je u skupu sigurnosnih parametara specificirana i provera identiteta dodaje se polje „podaci za proveru identiteta“.
- Obezbeđuje se integritet, proveru identiteta, neporecivost i privatnost podataka.

# ESP + AH u transportnom režimu rada

- Polje „protokol“ u IP ima vrednost 51 (AH).
- AH zaglavlje, polje „sledeće zaglavlje“ sadrži vrednost 50 (ESP).
- ESP zaglavlje,  polje „sledeće zaglavlje“ sadrži vrednost koja označava protokol višeg sloja.
- AH obezbeđuje integritet, proveru identiteta i neporecivost celog IP paketa.
- ESP obezbeđuje privatnost podataka, i opciono integritet, proveru identiteta i neporecivost podataka i ESP zaglavlja.



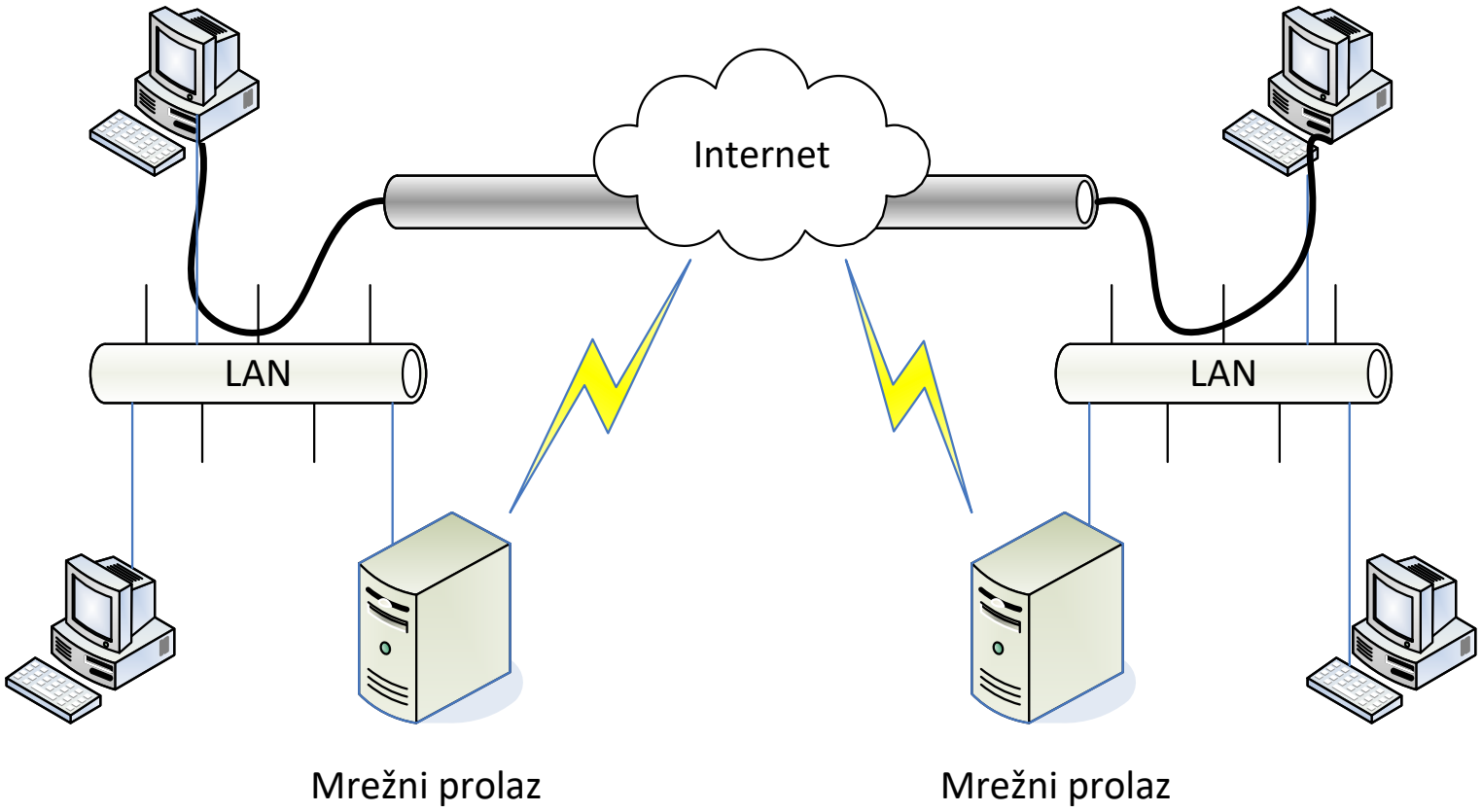
# Tunelovanje

- IPSec služi za uspostavljenje sigurne komunikacije između **mrežnih prolaza** (engl. *gateway*) na udaljenim mrežama (tzv. *gateway-to-gateway*).
- Time se uspostavlja **VPN mreža** (engl. *Virtual Private Network*) između udaljenih lokacija.
  - Krajnji entiteti u komunikaciji ne moraju da podržavaju IPSec.
  - Za njih je komunikacija transparentna jer sve operacije obavljaju mrežni prolazi.
  - Mrežni prolazi predstavljaju krajnje tačke sigurnog komunikacionog kanala.
  - Oni formiraju siguran tunel kroz nesiguran medijum (Internet).
- Tunelski način rada moguć je i u komunikaciji računar-računar ili računar-mrežni prolaz.
  - Tada krajnji entiteti (odnosno entitet) moraju podržavati IPSec.

# Tunelovanje

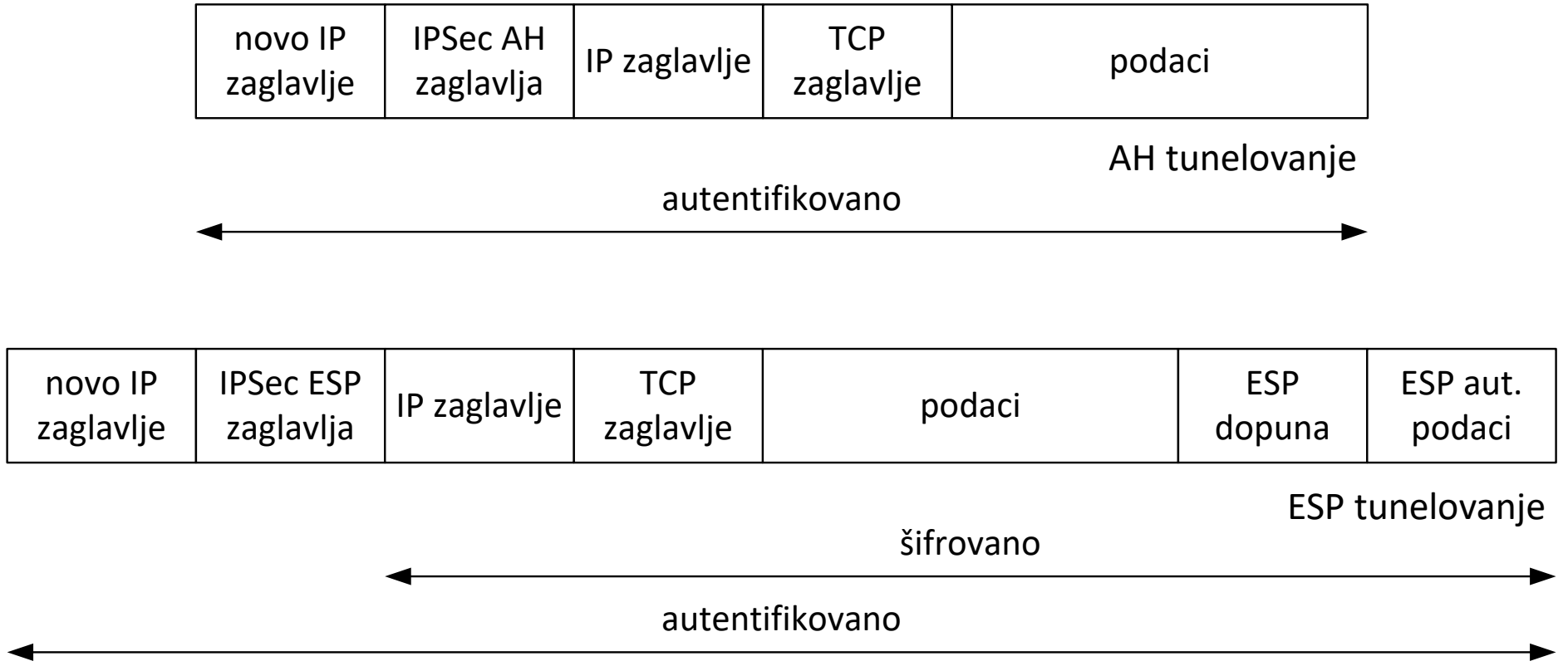
- Pri tuneliovanju se formira nov IP paket koji **enkapsulira kompletan originalni IP paket**.
- Dva entiteta komuniciraju na sledeći način:
  - Pošiljalac formira IP paket i šalje ga preko lokalne mreže lokalnom mrežnom prolazu.
  - Mrežni prolaz enkapsulira originalni IP paket u nov paket i formira odgovarajuća AH, odnosno ESP zaglavlja.
  - Paket se šalje preko uspostavljenog tunela do mrežnog prolaza na udaljenoj mreži.
  - Drugi mrežni prolaz uklanja dodatna zaglavlja, po potrebi dešifruje paket i provera njegov integritet.
  - Originalni IP paket se isporučuje odredištu.

# Tunelovanje



# AH i ESP u režimu tunelovanja

- NAPOMENA: kombinacija AH i ESP u tunelskom režimu rada nije predviđena.



# Uspostavljanje IPSec komunikacije

- IPSec ne sadrži mehanizam za uspostavljanje komunikacije i ne specificira konkretne kriptografske algoritame koji će se koristiti u IPSec komunikaciji.
- Neophodno je da entiteti koji žele da komunikaciju pomoću IPSec protokola dogovore skup sigurnosnih parametara komunikacije (engl. ***Security Association***, **SA**):
  - Kriptografske metode koje će se koristiti
  - Način provere identiteta strana u komunikaciji
  - Razmena kriptografskih ključeva potrebnih za tako dogovorenu komunikaciju.
- Postoji nekoliko načina za uspostavljanje IPSec komunikacije:
  - Teoretski je moguće ručno podešavanje skupa sigurnosnih parametara (neprihvatljivo!)
  - **ISAKMP** (*Internet Security Association and Key Management Protocol*)
  - **IKE** (*Internet Key Exchange*).
    - Implementiran kombinovanjem postojećih protokola: ISAKMP, Oakley i SKEME.
    - Sastoji se od dve osnovne faze:
    - Uspostavljanja IKE SA skupa sigurnosnih parametara.
    - Uspostavljanja IPSec SA skupa sigurnosnih parametara korišćenjem IKE SA.

# Protokoli za proveru identiteta

- **Provera identiteta** je sigurnosna usluga kojom se od svakog korisnika zahteva da se predstavi sistemu pre nego što nešto uradi.
- Cilj provere identiteta je da obezbedi odgovarajući mehanizam pomoću koga će se potvrditi da je objekat (neko ili nešto) zaista „ono za šta se izdaje“.
- Provera identiteta korisnika je veoma značajna sigurnosna usluga!
- Međutim, da bi bila praktično upotrebljiva, mora da zadovolji još neke uslove:
  - jednostavnost upotrebe i održavanja,
  - finansijsku isplativost.
- Na primer, iris skeneri nude visok nivo sigurnosti, ali su skupi i zbog toga još uvek nisu široko rasprostranjeni kao mehanizmi za proveru identiteta.

# Kerberos

- **History lesson**:
- Kerber (*Κέρβερος*) – što znači demon iz jame – u grčkoj mitologiji predstavlja troglavog psa čuvara ulaza u podzemlje (Had).

# Kerberos

- Jedan od najpoznatijih protokola za proveru identiteta korisnika.
- Centar za distribuciju ključeva, poput mitskog bića, ima tri „glave“:
  - bazu,
  - server za proveru identiteta,
  - server za izdavanje karata.
- Prijavljivanje tipa „**prijavi-se-samo-jednom**“ (engl. *Single Sign On*):
  - jednom se prijavi na sistem,
  - nakon toga, imaš pristup resursima u skladu sa svojim ovlašćenjima.
- Razrešava se problem upravljanja velikim brojem korisničkih naloga i lozinki, a smanjuje se i vreme potrebno za pristup pojedinačnim servisima
- Kerberos korisničke lozike nikad ne šalje preko mreže u obliku otvorenog teksta, što ga čini otpornim na pasivne napade tipa prisluškivanja i analize mrežnog saobraćaja.

# Kerberos: osnovni pojmovi i koncepti

- Svaki **entitet** (korisnik, računar, server ili mrežni servis) opisan je odgovarajućim **imenom** u bazi KDC servera.
- Ovo ime čini **deo principala** koji jednoznačno identifikuje entitet u Kerberos sistemu.
- Struktura principala: `identity/instance@realm`.
  - `identity` (obavezno polje). Opisuje ime Kerberos entiteta.
  - `instance` (polje nije obavezno).
    - U slučaju principala koji opisuju mrežne servise: polje sadrži ime računara na kom je servis pokrenut (tako se razlikuju dva ista servisa pokrenuta na različitim računarima).
    - U slučaju korisničkih naloga ovo polje može da opiše grupu kojoj korisnik pripada.
  - `realm` (oblast, obavezno polje) – jedinstveni domen definisan za svaku za zasebnu instalaciju Kerberos sistema.
    - Opisuje sistem i razgraničava ga od bilo kog drugog Kerberos okruženja.
    - Najčešće odgovara DNS imenu domena organizacije ali se označava velikim slovima.
    - Primer: oblast za DNS domen `viser.edu.rs` označava se kao `VISER.EDU.RS`
- Ovim je omogućeno jednoznačno definisanje i korišćenje svih entiteta u Kerberos okruženju.

# Kerberos: osnovni pojmovi i koncepti

- Primeri Kerberos pricipala u  hipotetičkoj Kerberos oblasti VISER.EDU.RS:
  - Korisnik nmacek koji je član grupe webadmin
    - `nmacek/webadmin@VISER.EDU.RS`
  - SSH servis na računaru server.viser.edu.rs
    - `ssh/server.viser.edu.rs@VISER.EDU.RS`
  - Računar nicotine.viser.edu.rs
    - `novilaptop/nicotine.viser.edu.rs@VISER.EDU.RS`

# Centar za distribuciju ključeva

- KDC server je entitet kome svi veruju i kome se svi obraćaju za potrebe provere identiteta.
- Sadrži tri komponente najčešće integrisane u jednom servisu koji se izvršava na serveru.
- **Baza principala**.
  - Sadrži sve principale Kerberos oblasti sa odgovarajućim tajnim ključevima.
  - Konkretna implementacija baze zavisi od operativnog sistema koji se izvršava na serveru.
    - Linux KDC $\rightarrow$ podaci se čuvaju u okviru LDAP baze.
    - MS Windows Server KDC $\rightarrow$ podaci se čuvaju u Aktivnom Direktorijumu.
  - Baza sadrži tajne ključeve svih entiteta!
    - Kompromitovanje baze ugrožava sigurnost celog Kerberos Sistema.
- **Server za proveru identiteta** (engl. *Authentication Server*, AS).
  - Izdaje *Ticket Granting Ticket* kartu klijentima koji žele da se prijave na sistem.
  - TGT karta se generiše prilikom prijavljivanja na sistem.
  - Klijentima daje pravo da kasnije traže karte za pristup raznim mrežnim resursima.
- **Server za dodelu karata** (engl. *Ticket Granting Server*, TGS).
  - TGS izdaje karte za pristup mrežnim resursima.

# Centar za distribuciju ključeva

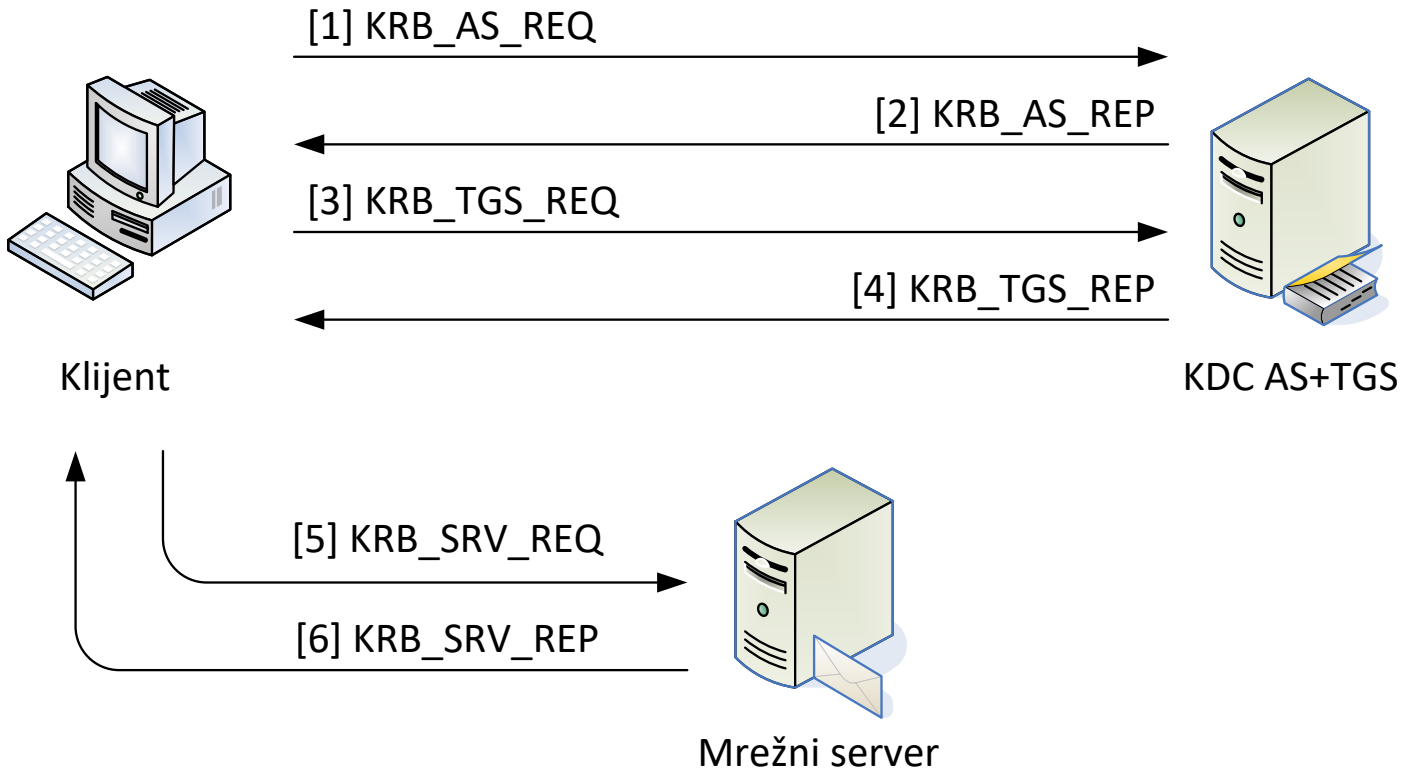
- KDC mora biti stalno dostupan kako bi sistem normalno funkcionisao.
- Ukoliko server otkaže (na primer, usled kvara):
  - Nijedan entitet ne može da se prijavi  u sistem.
  - Ne mogu da se koriste  mrežni servisi u Kerberos sistemu.
- Ulogu centra za distribuciju ključeva može obavljati više servera.
- Time se obezbeđuje neprekidno funkcionisanje sistema u slučaju otkaza jednog servera.
  - Osim **primarnog** (*master KDC*) uvodi se jedan ili više **sekundarnih** KDC servera (*slave KDC*).
  - Sekundarni KDC će preuzeti ulogu u slučaju nedostupnosti primarnog servera.
- U ovom slučaju važno je obezbediti **sinhronizaciju** svih KDC servera u sistemu!
  - Primer: MIT implementacija sekundarnih servera.
    - Sekundarni KDC serveri sadrže kopiju podataka sa primarnog KDC servera.
    - Nad kopijom imaju samo pravo čitanja.
    - Mogu izdavati karte korisnicima (prijavljivanje na sistem i pristup resursima)
    - Sve promene u bazi mogu obaviti isključivo na primarnom serveru.

# Kerberos karte

- Svaka Kerberos karta sadrži sledeće podatke:
  - ime principala koji zahteva pristup,
  - ime principala za koji se traži pristup,
  - vremensku oznaku (engl. *timestamp*),
  - tok važenja karte,
  - listu IP adresa s kojih je moguća upotreba karte,
  - tajni ključ za komunikaciju sa traženim resursom.
- Vremenska oznaka i rok važenja karte su parametri koji obezbeđuju dodatni nivo sigurnosti komunikacije!
  - Ovi vremenski parametri štite sistem od **napada ponavljanjem**.
  - Sprečava se scenario po kome neovlašćeni korisnik najpre presreće i „snima“ mrežni saobraćaj a zatim ga ponavlja i ostvaruje pristup resursu ili sistemu.

# Kako se odvija komunikacija?

- Kerberos  je najvećim delom zasnovan na Needham-Schroeder protokolu za proveru identiteta.
- Kasnije su dodate funkcionalnosti koje sprečavaju napad „čovek u sredini“ na N-S protokol.



# Kako se odvija komunikacija?

- **KRB_AS_REQ zahtev** (klijent → KDC AS).
- Postupak provere identiteta klijenta.
- Ova poruka se šalje u obliku otvorenog teksta i sadrži:
  - ime principala Kerberos klijenta koji inicira zahtev,
  - vremensku oznaku (lokalno vreme na strani klijenta u momentu generisanja zahteva),
  - ime principala TGS servera,
  - traženo vreme trajanja karte.

# Kako se odvija komunikacija?

- **KRB_AS_REP odgovor** (KDC AS → klijent).
- AS server proverava da li navedeni klijentski principal postoji u bazi podataka.
  - Ako principal ne postoji zahtev se odbija.
  - Ako principal postoji server proverava vremensku oznaku na zahtevu.
  - Server računa razliku između vremenske oznake i lokalnog vremena.
    - Ako je razlika van okvira zahtev se odbija a klijentu se šalje poruka o grešci.
    - Ako je razlika u okvirima server vraća klijentu odgovor šifrovan tajnim ključem.
      - Tajni ključ je poznat samo KDC serveru i tom korisniku.
- KRB_AS_REP odgovor sastoji se od dva dela.
- **Prvi deo KRB_AS_REP** odgovora.
- Šifrovan je tajnim ključem klijenta (engl. *client key*) i sadrži:
  - ključ sesije za komunikaciju sa TGS serverom (engl. *client-TGS session key*) – klijent nakon dešifrovanja dela primljenog odgovora kešira ovaj ključ,
  - ime principala TGS servera,
  - vreme trajanja karte.

# Kako se odvija komunikacija?

- **Drugi deo KRB_AS_REP** odgovora.
- Sadrži TGT kartu šifrovanu tajnim ključem koji dele KDC AS i TGS server (engl. *TGS key*).
  - Ovaj deo poruke klijent ne može da dešifruje.
  - Klijent kešira šifrovanu TGT kartu i koristi prilikom slanja zahteva za pristup resursima.
- Šifrovana TGT karta sadrži:
  - ključ sesije za komunikaciju sa TGS serverom (engl. *client-TGS session key*),
  - ime principala Kerberos klijenta,
  - vreme trajanja karte i vremensku oznaku KDC servera,
  - IP adresu klijenta koja se dobija iz inicijalnog AS_REQ zahteva.
- NAPOMENA:
  - TGT karta se generiše  prilikom prijave korisnika u sistem.
  - Kada TGT karta istekne klijent mora da zatraži novu TGT kartu od AS servera.
    - Mora da generiše nov KRB_AS_REQ zahtev.

# Kako se odvija komunikacija?

- **KRB_TGS_REQ** (klijent → KDC TGS).
- Klijent koji želi da pristupi nekom resursu šalje zahtev koji sadrži:
  - ime principala resursa kom klijent želi da pristupi,
  - traženo vreme trajanja karte,
  - TGT kartu keširanu u prethodnom koraku,
  - autentifikator (obezbeđuje jedinstvenost svakog zahteva za pristup resursu i potvrđuje da korisnik ima tajni ključ sesije dogovoren u prethodnim fazama komunikacije).

# Kako se odvija komunikacija?

- **KRB_TGS_REP** (klijent → KDC TGS).
- KDC TGS formira odgovor sa novim ključem sesije (engl. *client-service session key*).
- Ovaj ključ klijent koristi za razmenu poruka sa resursom za koji traži pristup.
- **Prvi deo poruke** je šifrovan ključem client-TGS session ključem i sadrži:
  - ime principala resursa kom klijent želi da pristupi
  - vreme trajanja karte
  - ključ sesije za razmenu poruka sa resursom kom klijent želi da pristupi.
- **Drugi deo poruke** je TGS karta za pristup resursu šifrovana tajnim ključem koji dele KDC server i resurs (*service key*) kom klijent traži da pristupi:
  - **ključ sesije** za razmenu poruka sa resursom kom klijent želi da pristupi,
  - ime principala klijenta,
  - vreme trajanja karte i vremensku oznaku KDC servera,
  - IP adresu klijenta.
- Klijent dešifruje primljenu poruku *client-service session* ključem
- Klijent kešira TGS kartu i novi ključ sesije.

# Literatura


1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić (2007): Sigurnost računarskih sistema i mreža. Mikro knjiga, Beograd.
2. M. Stamp (2006): Information Security. John Wiley and Sons.

# Hvala na pažnji

**Pitanja su dobrodošla.**