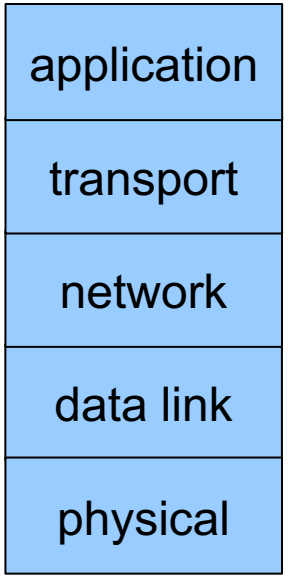
Bezbedna komunikacija u TCP/IP mrežama

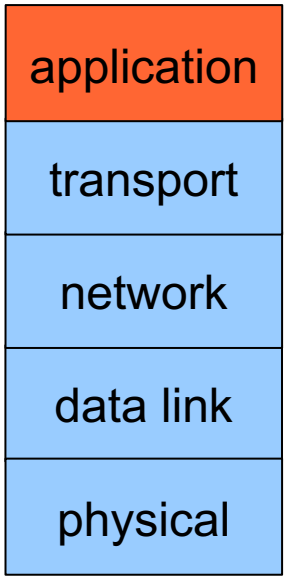
TCP/IP stek i bezbednost

- sigurna komunikacija može da se obezbedi na različitim nivoima TCP/IP steka
- potrebne usluge:
  - poverljivost
  - neporecivost
  - integritet
  - autentifikacija
  - autorizacija
  - upravljanje ključevima (generisanje, čuvanje, razmena)



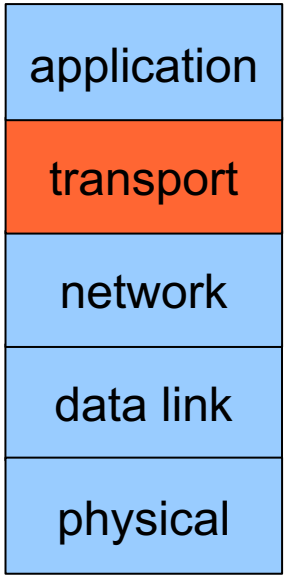
TCP/IP stek i bezbednost

- implementacija sigurnosti na aplikativnom nivou
- dobre osobine
  - implementacija u krajnjim tačkama komunikacije - računarima
  - aplikacija ne mora da se oslanja na sigurnosne servise operativnog sistema
  - kompletan pristup podacima koji se štite
  - jednostavan pristup akreditivima korisnika (npr. tajni ključ)
- loše osobine
  - potrebna je implementacija za svaku aplikaciju posebno
  - komplikovana izmena postojećih aplikacija
  - velika verovatnoća pravljenja greške
- primer
  - PGP: zaštićena email komunikacija
    - email klijent se proširuje funkcijama za pronalaženje javnih ključeva, šifrovanje, dešifrovanje, proveru autentičnosti poruka



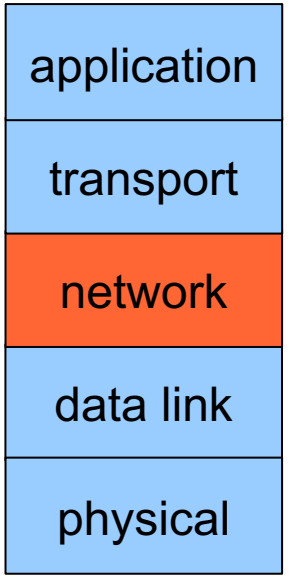
TCP/IP stek i bezbednost

- implementacija sigurnosti na transportnom nivou
- dobre osobine
  - implementacija u krajnjim tačkama komunikacije - računarima
  - ne mora se modifikovati svaka aplikacija
  - kompletan pristup podacima koji se štite
  - sve aplikacije koriste isti stepen sigurnosti
- loše osobine
  - (neznatna) izmena postojećih aplikacija - zahtevanje sigurnosnih usluga od transportnog sloja
- primer
  - TLS: Transport Layer Security
    - usluge provere identiteta, integriteta i poverljivosti preko TCP protokola
    - ne može i za UDP, jer UDP ne održava kontekst tekuće veze



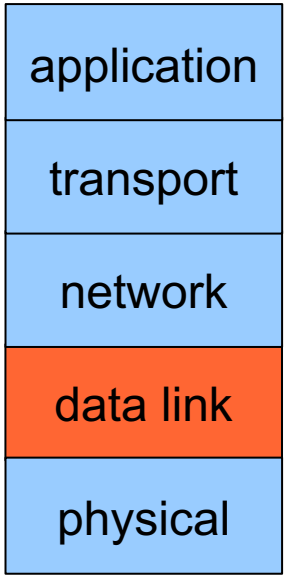
TCP/IP stek i bezbednost

- implementacija sigurnosti na mrežnom nivou
- dobre osobine
  - još manje izmene u aplikacijama
  - svi transportni protokoli koriste istu infrastrukturu
  - mogućnost pravljenja virtuelnih privatnih mreža (VPN)
- loše osobine
  - teško je obezbediti uslugu neporecivosti (mnogo lakše na višim slojevima)
  - teško je obezbediti kontrolu na nivou korisnika na višekorisničkom računaru
- primer
  - IPSec (IP Security)
    - usluge provere identiteta, integriteta i poverljivosti preko TCP protokola



TCP/IP stek i bezbednost

- implementacija sigurnosti na nivou veze
- ako postoji namenska veza između dva uređaja na mreži (računara, rutera)
- ako sav saobraćaj mora da se šifruje
- dobre osobine
  - hardverski uređaj za šifrovanje
  - velika brzina rada
- loše osobine
  - samo za namenske veze - ukoliko su učesnici fizički povezani
- primer
  - veza bankomata sa cetralom putem namenske veze (iznajmljena linija)



PGP

- PGP = Pretty Good Privacy
- nastao 1991. kao reakcija svog autora Filipa Cimermana na predlog zakona koji američkoj vladi omogućava pristup otvorenom tekstu svih poruka na osnovu zahteva prema proizvođačima opreme i komunikacionim provajderima
- sudski proces protiv Cimermana obustavljen 1996.

- tužba od strane RSA Data Security zbog neplaćanja licence za RSA

- prva legalna verzija PGP-a izvan SAD: 1997.
  - sors PGP-a je izvezen u obliku odštampane knjige (to nije zabranjeno - sloboda govora!)
  - potom OCR-om vraćen u elektronski oblik

PGP

- namena PGP-a: zaštita elektronske pošte
  - šifrovanje i digitalni potpisi
- šifrovanje poruka putem PGP-a
  - otvoreni tekst se komprimuje smanjuje se veličina poruke
    - uklanja se očekivani sadržaj u otvorenom tekstu
  - generiše se simetrični ključ (session key), za svaku poruku poseban
  - poruka se šifruje simetričnim algoritmom
  - simetrični ključ se šifruje asimeričnim algoritmom pomoću javnog ključa primaoca
  - primaocu se šalje šifrat otvorenog teksta i šifrat simetričnog ključa

PGP

- digitalno potpisivanje poruka putem PGP-a
  - računa se heš otvorenog teksta
  - heš se potpisuje privatnim ključem pošiljaoca
  - pošiljalac šalje otvoreni tekst i potpisani heš primaocu

PGP

- repozitorijumi javnih ključeva - key servers
  - https://sks-keyservers.net
  - https://keyserver.pgp.com
  - https://keyserver.ubuntu.com
  - https://pgp.key-server.io
  - https://pgp.mit.edu
  - https://keys.openpgp.org
  - ...

- poverenje u javne ključeve: "web of trust" umesto stroge CA hijerarhije
  - vremenom će svaki korisnik prikupiti ključeve drugih ljudi kojima veruje
  - svoj ključ će publikovati uz ključeve ljudi kojima veruje
  - primalac će možda prihvatiti da veruje nekom od tih ključeva
  - ... decentralizovana mreža poverenja otporna na otkaze

  - problem slepog prihvatanja ključeva nije rešen za zadovoljavajući način

PGP

- trenutno podržani algoritmi
  - simetrični: 3DES, IDEA, Blowfish, AES (128, 192, 256), Camellia
  - asimetrični: RSA, ElGamal, DSA, ECDH, ECDSA
  - heš: MD5 (depricated), SHA-1, RIPE-MD, SHA256, SHA384, SHA512, SHA224
  - kompresija: ZIP, ZLIB, BZip2

PGP

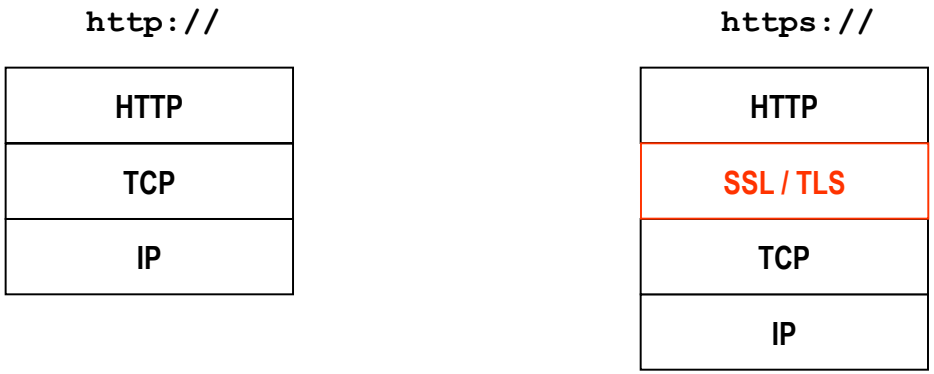
- OpenPGP - rezultat standardizacije u okviru IETF – izbegavanje licenciranja

- RFC 4880
  - definiše standardne formate šifrovanih poruka, potpisa i sertifikata

- različite implementacije (apps, mail app plugins, browser plugins, iOS/Android)
  - GnuPG
  - eM Client
  - The Bat!
  - Outlook
    - gpg4o
    - Gpg4win
    - p≡p
  - Thunderbird
    - Autocrypt
    - Enigmail
  - Apple Mail: GPGTools
  - Canary Mail
  - Mutt
  - Web plugins
    - Mailvelope
    - FlowCrypt (Gmail)
    - Psono
    - **Mailvelope** (Gmail, Yahoo, Outlook)

https://

- bezbedna komunikacija putem HTTP protokola
- sam HTTP protokol se ne menja, već se on oslanja na drugi protokol koji omogućava bezbednu komunikaciju



UDP nije podržan jer nema kontekst

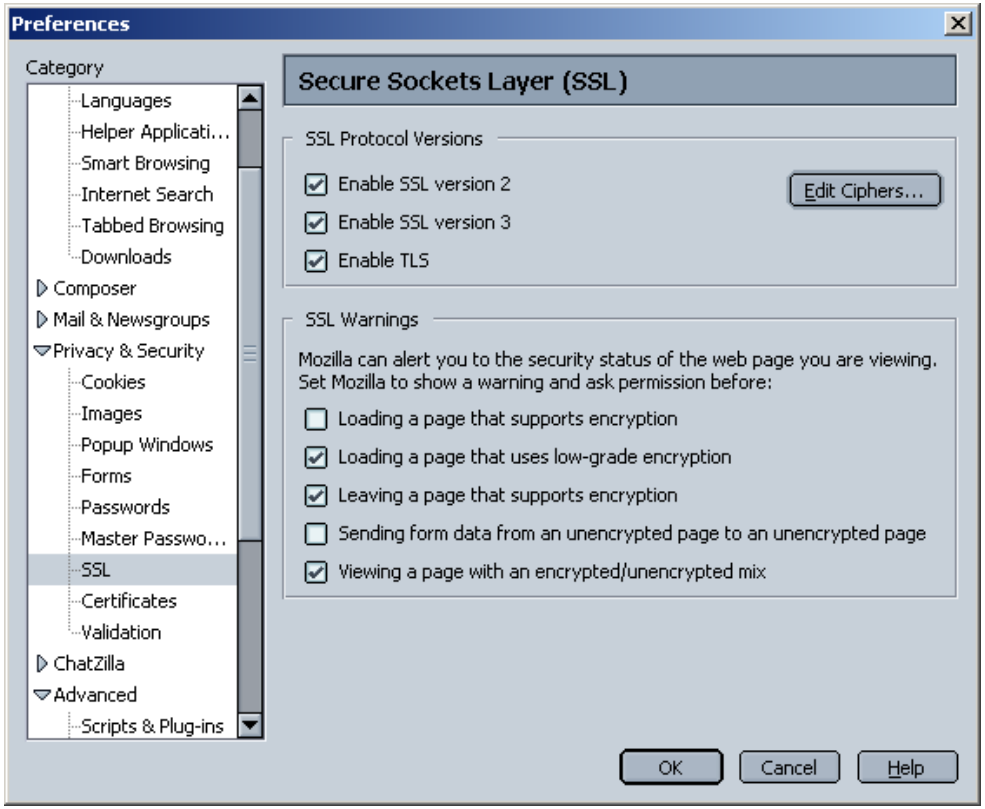
SSL

- komunikacioni protokol razvijen sa ciljem da podrži
  - kriptografsku bezbednost
  - interoperabilnost
    - implementacije različitih proizvođača
  - proširivost
    - različitim kriptografskim algoritmima
  - relativnu efikasnost
    - optimizuje zauzeće procesora i mrežni protok
    - keširanjem komunikacionih parametara za uspostavljene veze

- SSL = Secure Sockets Layer
  - prozvod Netscape-a
  - SSL v2: prva prihvaćena verzija
    - imala je bezbednosnih nedostataka
  - SSL v3: de facto standard od 1996.
    - nikad nije zvanično standardizovan

TLS

- TLS = Transport Layer Security
  - standardizacija SSL protokola u okviru IETF
  - RFC 2246
  - podrška u savremenim browserima



TLS

- dva sloja
  - Record Protocol
  - Handshake Protocol / Alert Protocol / Change Cipher Spec Protocol

- TLS Record Protocol
  - oslanja se na TCP i daje podršku za protokole višeg nivoa
  - koristi simetrične algoritme za šifrovanje
  - prenos poruka obuhvata i proveru integriteta pomoću hash funkcija

- TLS Handshake Protocol
  - autentifikacija klijenta i servera i dogovor oko korišćenih algoritama i ključeva
  - provera identiteta pomoću asimetričnih algoritama
  - dogovor oko session ključa je siguran od prisluškivanja
  - postupak dogovaranja obezbeđuje detekciju man-in-the-middle napada

TLS Record Protocol

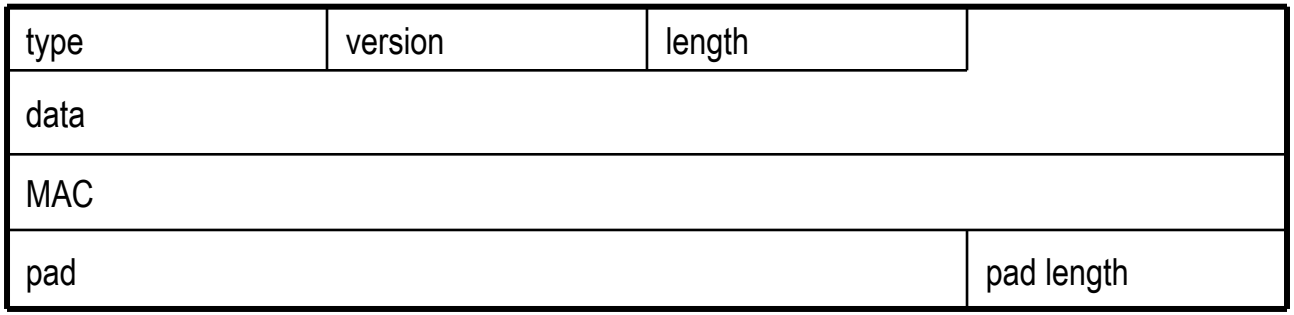
- protokol nižeg nivoa koji omogućava prenos poruka drugih protokola:
  - handshake protocol
  - alert protocol
  - change cipher spec protocol
  - protokol aplikativnog nivoa (npr. HTTP)

- TLS Record protokol prati stanje konekcije
  - stanje se sastoji iz
    - izabranog algoritma za kompresiju
    - izabranog algoritma za šifrovanje
    - izabranog heša za proveru integriteta poruka
    - parametara ovih algoritama
      - simetrični ključ
      - IV ako se koristi blok algoritam u CBC modu

TLS Record Protocol

- slanje poruke
  1. poruka se kompresuje
  2. poruci se dodaje hash
  3. poruka se šifruje simetričnim algoritmom i session ključem

- struktura

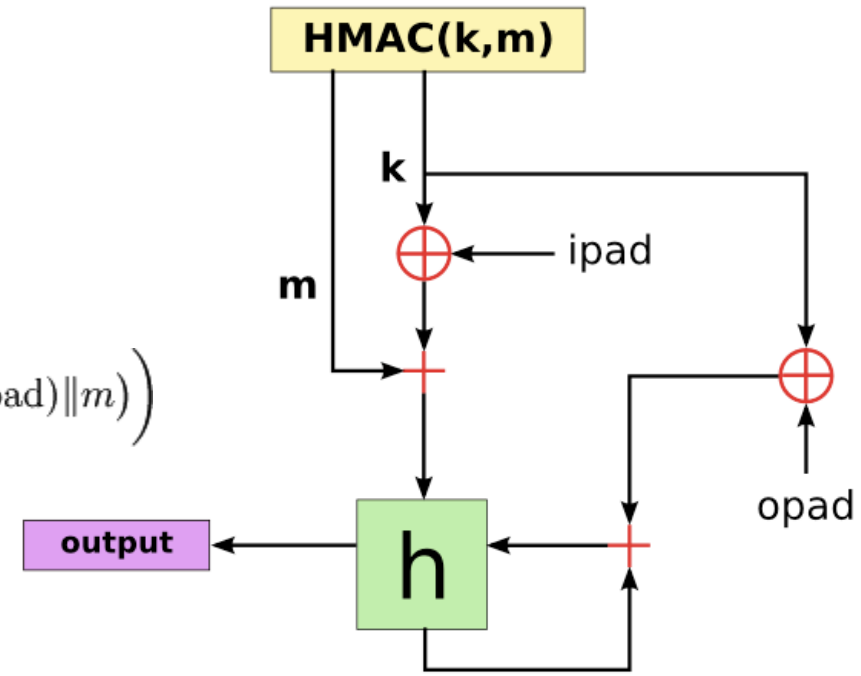


type:
20 - ChangeCipherSpec
21 - Alert
22 - Handshake
23 - Application protocol

TLS Record Protocol

- MAC = message authentication code
  - provera integriteta i provera autentičnosti pošiljaoca
  - ulazna poruka + ključ ⟶ vrednost fiksne dužine
- konstrukcija pomoću heš funkcije: HMAC
  - h: heš funkcija
  - K: tajni ključ dopunjen nulama do dužine bloka heš funkcije
  - m: poruka
  - ||: konkatenacija
  - $\oplus$: XOR
  - opad: 0x5c5c5c... (u dužini bloka)
  - ipad: 0x363636... (u dužini bloka)

$$\mathrm{HMAC}_K(m) = h\Big((K \oplus \mathrm{opad}) \| h\big((K \oplus \mathrm{ipad}) \| m\big)\Big)$$



TLS Handshake Protocol

- namenjen za uspostavljanje komunikacione sesije
- sesija je skup parametara
  - identifikator sesije
    - niz bajtova koji jedinstveno identifikuje sesiju (dogovaraju ga klijent i server)
  - potvrda identiteta drugog učesnika u komunikaciji
    - X.509.v3 sertifikat
  - algoritam za kompresiju
    - kompresija podataka, ako se koristi, vrši se pre šifrovanja
  - cipher spec
    - simetrični algoritam
    - heš funkcija (za MAC)
  - master secret
    - 48-bajtni tajni niz koga dele klijent i server - koristi se za generisanje simetričnih ključeva
  - resumable
    - da li se sesija može koristiti za uspostavljanje novih konekcija

- jedna sesija može da sadrži više konekcija
  - browser može da prenosi više fajlova istovremeno kroz više konekcija sa istim parametrima

TLS Handshake Protocol

- cipher suite: skup kriptografskih protokola korišćen u komunikaciji
- sastoji se od:
  - alogritma za razmenu simetričnog ključa
  - algoritma za autentifikaciju
  - alogritma za šifrovanje podataka
  - MAC/hash algoritma
- razvijaju se took vremena – nove verzije novi protokoli
- opcije za TLS 1.2:

Key exchange/agreement	Authentication	Block/stream ciphers	Message authentication
RSA	RSA	RC4	Hash-based MD5
Diffie–Hellman	DSA	Triple DES	SHA hash function
ECDH	ECDSA	AES	
SRP		IDEA	
PSK		DES	
		Camellia	

TLS Handshake Protocol

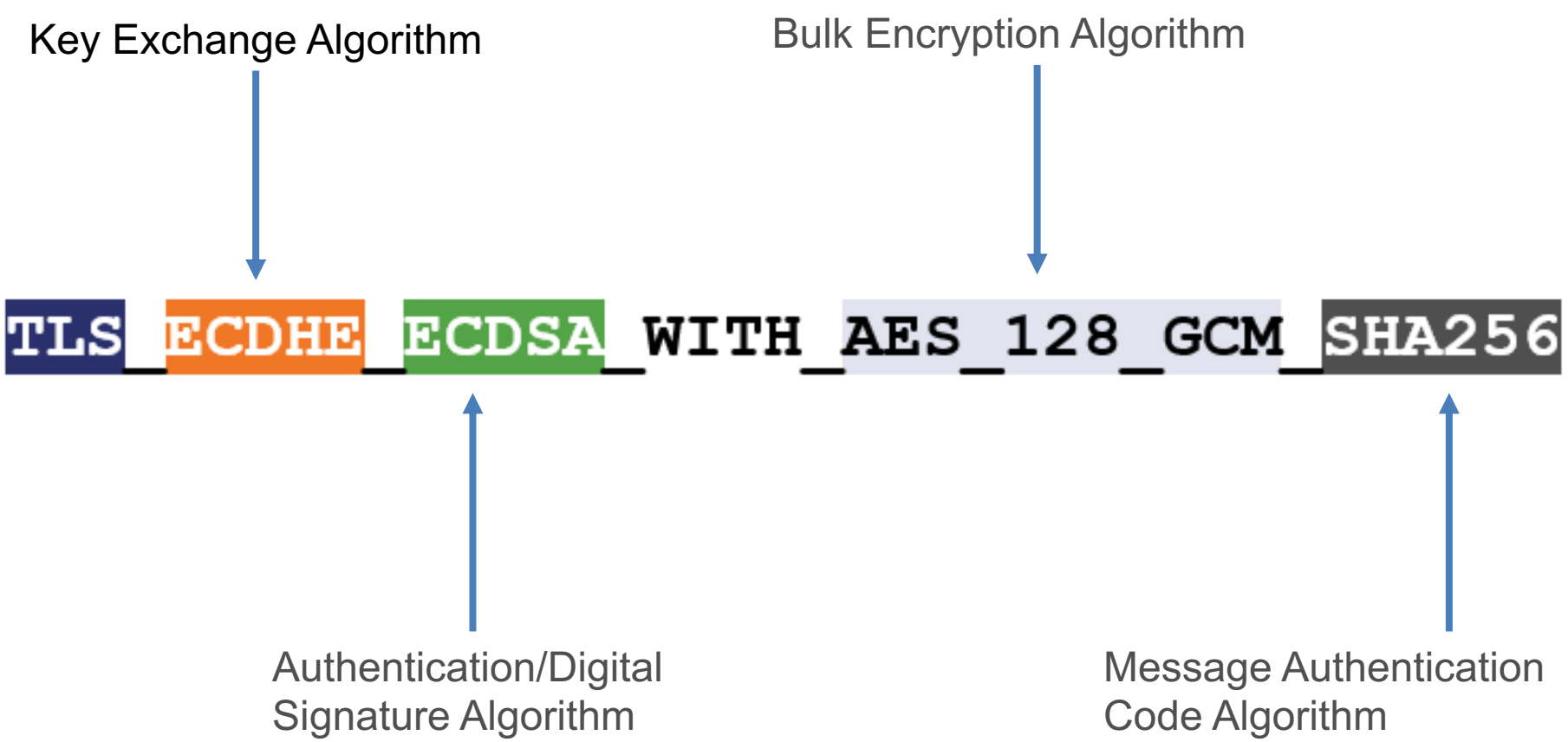
- cipher suite: primeri

TLS_NULL_WITH_NULL_NULL
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_WITH_IDEA_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_DSS_WITH_DES_CBC_SHA
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_RSA_WITH_DES_CBC_SHA
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA
TLS_DH_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA
TLS_DH_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DH_DSS_WITH_AES_128_CBC_SHA256
TLS_DH_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA

TLS Handshake Protocol

- cipher suite – string

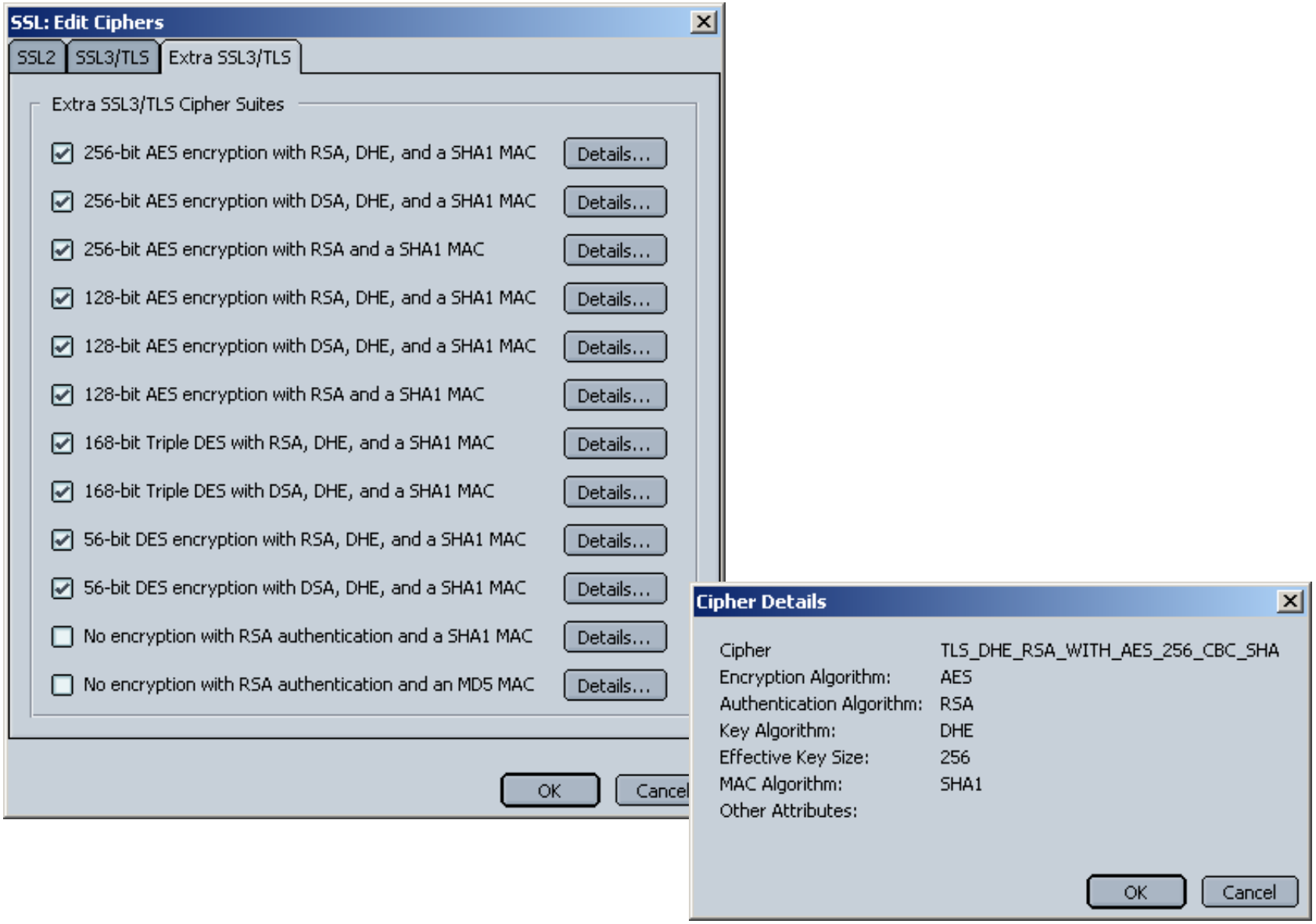


TLS Handshake Protocol

- cipher suite – razložen

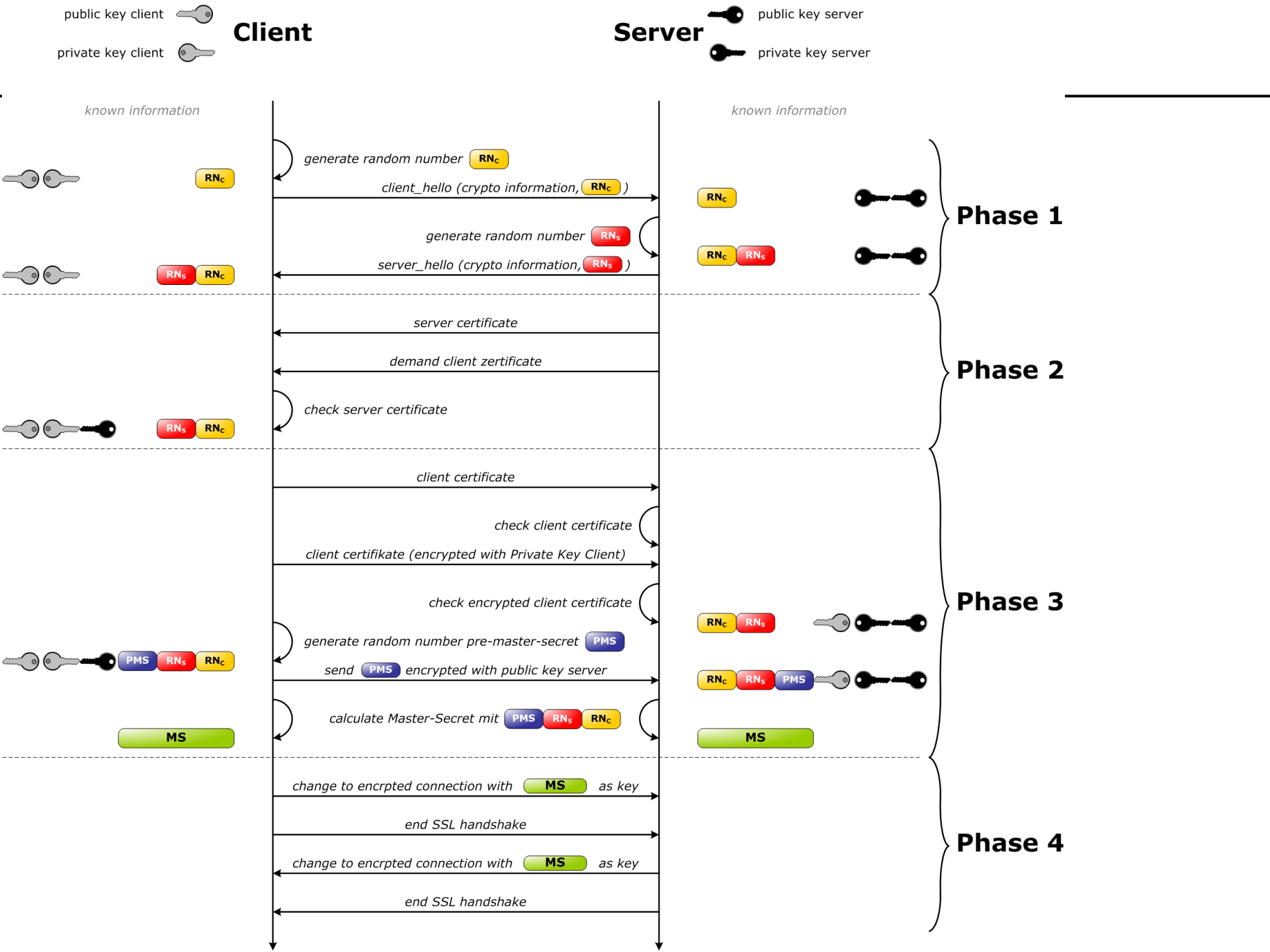
Key Exchange Algorithm	Authentication Algorithm	Bulk Encryption Algorithm	Mac Algorithm
Elliptic Curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 256 in Galois Counter Mode (AES256-GCM)	SHA384
Elliptic Curve Diffie–Hellman (ECDH)	RSA	AES 256 in Galois Counter Mode (AES256-GCM)	SHA384
Elliptic curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	ChaCha20 (CHACHA20)	POLY1305
Elliptic curve Diffie–Hellman (ECDH)	RSA	ChaCha20 (CHACHA20)	POLY1305
Elliptic Curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 128 in Galois Counter Mode (AES128-GCM)	SHA256
Elliptic curve Diffie–Hellman (ECDH)	RSA	AES 128 in Galois Counter Mode (AES128-GCM)	SHA256
Elliptic Curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 256 (AES256)	SHA384
Elliptic curve Diffie–Hellman (ECDH)	RSA	AES 256 (AES256)	SHA384
Elliptic curve Diffie–Hellman (ECDH)	Elliptic Curve Digital Signature Algorithm (ECDSA)	AES 128 (AES128)	SHA256
Elliptic curve Diffie–Hellman (ECDH)	RSA	AES 128 (AES128)	SHA256

TLS Handshake Protocol



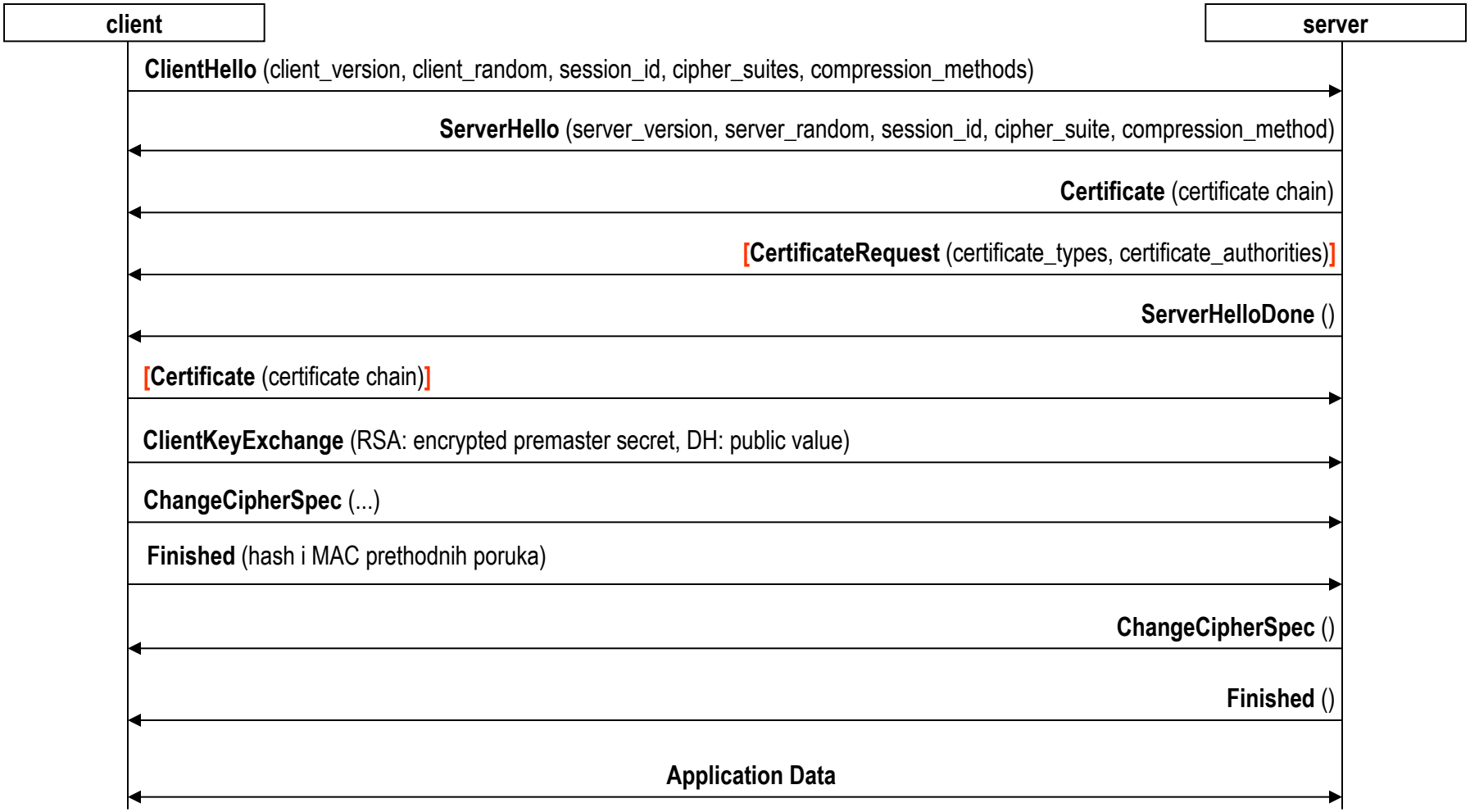
TLS Handshake Protocol

- tok komunikacije - osnovni
  - klijent otvara vezu i šalje spisak podržanih šifara i heš funkcija
  - server od ponuđenih bira najjaču kombinaciju i obaveštava klijenta
  - server šalje svoju identifikaciju u obliku sertifikata
  - klijent može kontaktirati CA radi provere sertifikata - to nije obuhvaćeno TLS protokolom!
  - klijent šifruje slučajan broj javnim ključem servera i šalje mu ga
  - na osnovu slučajnog broja klijent i server generišu session ključ


public key client
private key client
Client
Server
public key server
private key server
known information
known information
generate random number RNc
client_hello (crypto information, RNc)
generate random number RNs
server_hello (crypto information, RNs)
Phase 1
server certificate
demand client zertificate
check server certificate
Phase 2
client certificate
check client certificate
client certifikate (encrypted with Private Key Client)
check encrypted client certificate
generate random number pre-master-secret PMS
send PMS encrypted with public key server
calculate Master-Secret mit PMS RNs RNc
MS
MS
Phase 3
change to encrpted connection with MS as key
end SSL handshake
change to encrpted connection with MS as key
end SSL handshake
Phase 4

TLS Handshake Protocol

- tok komunikacije - osnovni

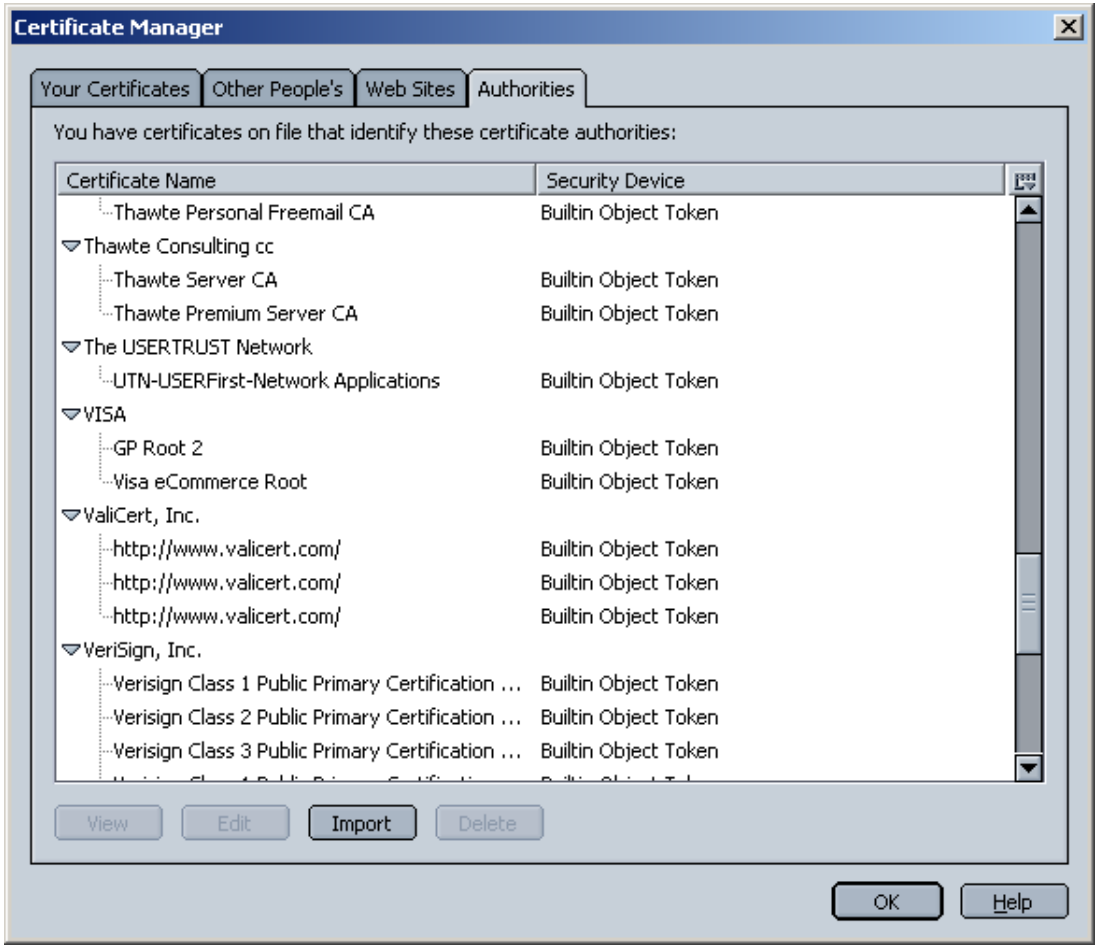


Alert Protocol

- dva polja u poruci
- level
  - 1: warning - veza ili sigurnost može biti nestabilna
  - 2: fatal - veza ili sigurnost mogu biti ugroženi, ili je nastupila neotkloniva greška
- description
  - ...
  - 10: unexpected message
  - ...
  - 20: bad record MAC
  - ...
  - 44: certificate revoked
  - 45: certificate expired
  - ...

Sertifikati

- “root CA” je self-signed
- browseri sadrže “root CA” sertifikate
- svaki sertifikat sadrži “CA flag”
  - da li vlasnik ima pravo da izdaje nove sertifikate, tj. da li je vlasnik takođe CA



Sertifikati

- Internet Explorer 5.0-6.0 bag
  - ne proverava da li posrednički sertifikati imaju pravo da izdaju sertifikate
  - na primer
    - kupimo sertifikat za nastyattacker.com
    - iskoristimo ga za potpisivanje sertifikata za amazon.com
    - presrećemo saobraćaj sa amazon.com i podmećemo svoj lažni sertifikat
  - primer kako mali bag može da sruši sistem čija izgradnja košta puno $M

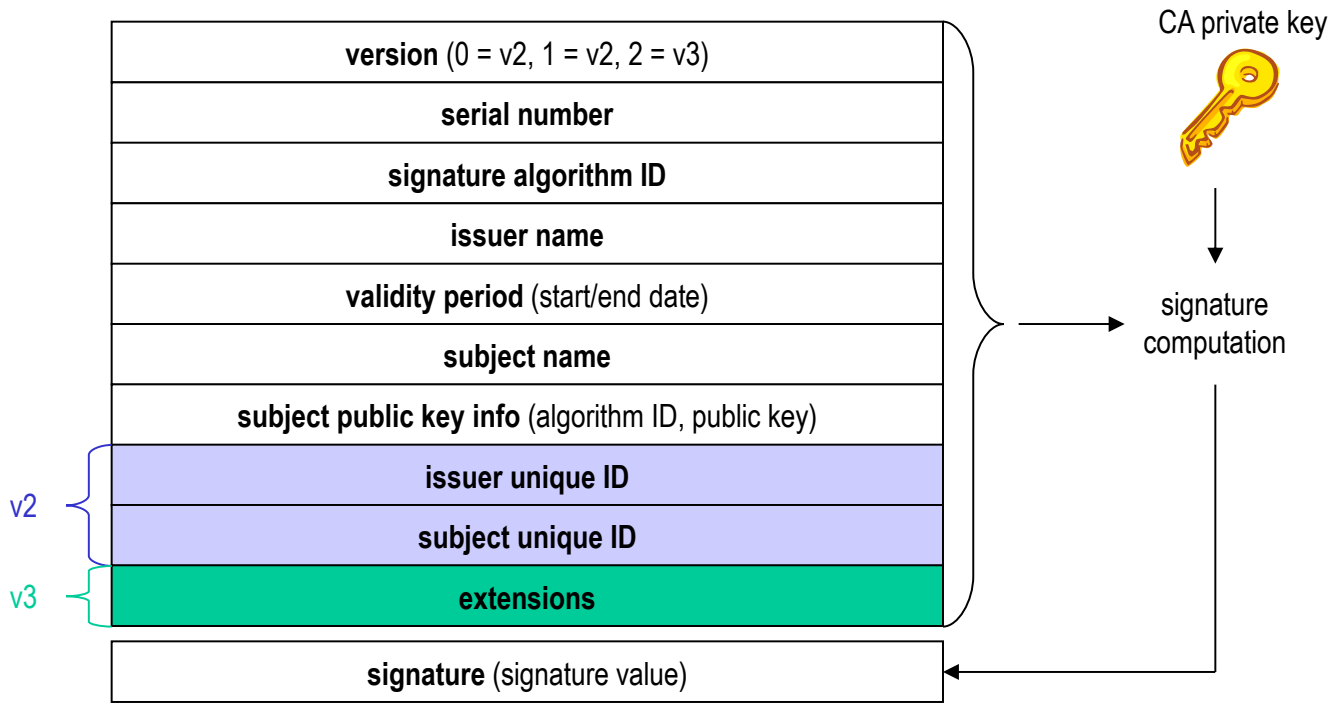
Sertifikati

- Kako postati “root CA”
  - troškovi oko $0.5M
  - finansijski, regulatoroni, politički uslovi
- Kupovina sertifikata kod CA
  - slično reketiranju

> “...If you fail to renew your Server ID prior to the expiration date, operating your Web site will become far riskier than normal […] your Web site visitors will encounter multiple, intimidating warning messages when trying to conduct secure transactions with your site. This will likely impact customer trust and could result in lost business for your site....”

Sertifikati

- X.509 standard



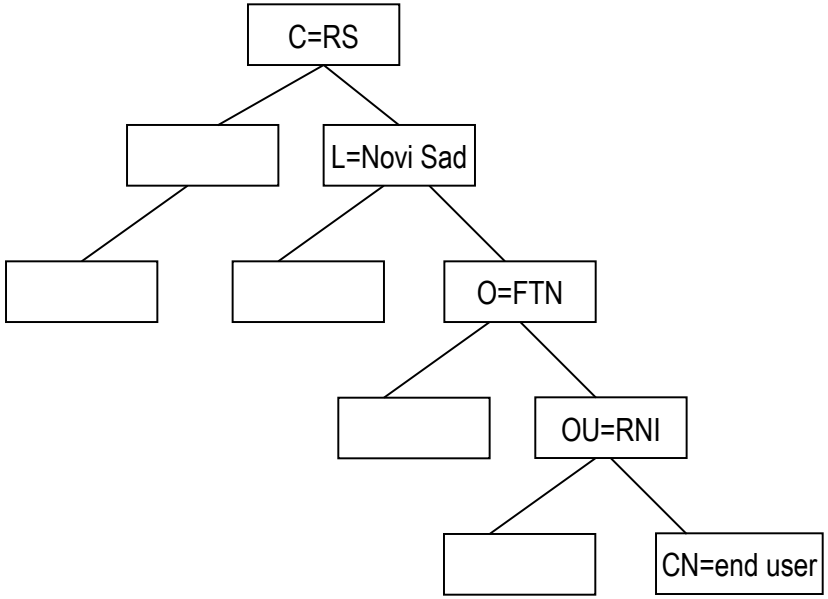
Sertifikati

- X.509 standard
  - primer sertifikata

Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=CS, L=Novi Sad, O=FTN, OU=Odeljenje za sertifikate, CN=FTN CA, Email=ca@ftn.uns.ac.rs
Validity:
Not Before: Jun 8 10:00:00 2004 GMT
Not After: Jun 7 10:00:00 2005 GMT
Subject: C=CS, L=Novi Sad, O=FTN, OU=Katedra za informatiku, CNGoran Sladiić, Email=sladicg@uns.ac.rs
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit): 00:b3:4e:75:76:fc:4c:c3:bd:61:6c:14:41:8f:47:...
Exponent: 65537 (0x10001)
X.509v3 Extensions:
X.509v3 Basic Constraints
CA: false
Netscape Comment:
OpenSSL Generated Certificate
X.509v3 Subject Key Identifier:
a6:db:b8:78:19:7a:c4:67:23:de:03:a3:ee:d4:26:5e:78:14:71:61
Signature:
9f:15:a8:cb:6c:a9:0d:d4:61:24:b9:7a:bc:29:e4:29:8b:4c:...

Sertifikati

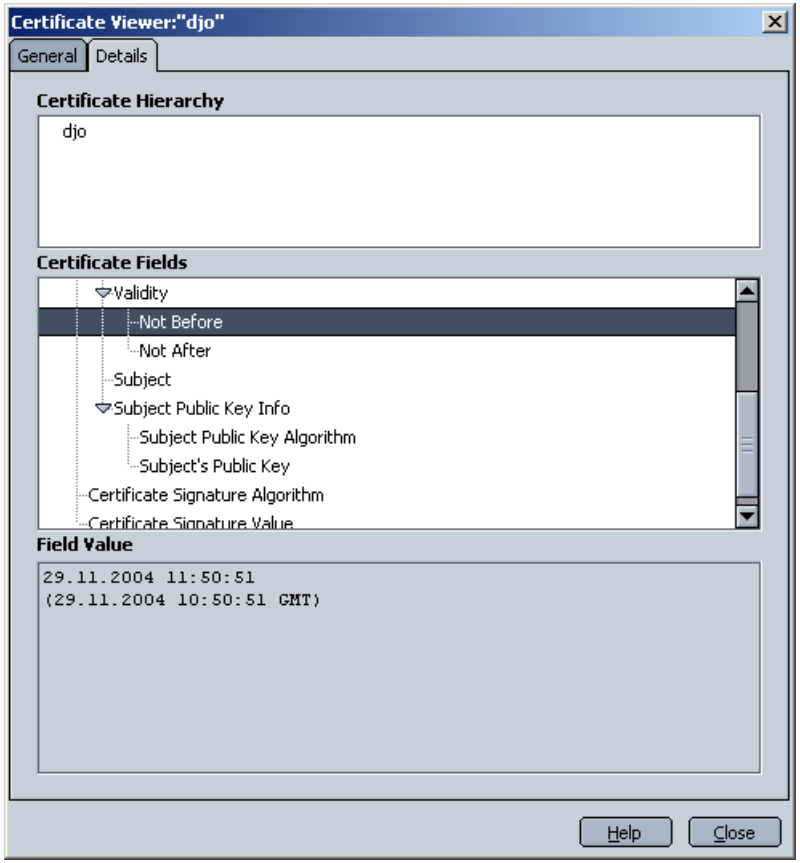
- X.509 standard
  - hijerarhijska organizacija imena (C=RS, L=Novi Sad, O=FTN, ...) potiče od X.500 standarda, sveobuhvatnog direktorijumskog servisa



  - oznaka čvora: Relative distinguished name (RDN)
  - puna identifikacija čvora: Distinguished name (DN)
    - DN = konkatenacija svih RDN od korena do datog čvora
  - atributi za opisivanje organizacija i osoba su definisani u X.520 i X.521

Sertifikati

- X.509 standard
  - problem distribucije ključeva pretvoren je u problem distribucije imena
    - ljudi sa istim imenom i prezimenom u istoj organizaciji
    - kreiranje jedinstvenih naziva – pretraživanje po imenu više nema smisla
      - John Smith 1 vs John Smith 2 vs John Smith 3



Sertifikati

- X.500 nije zaživeo
  - organizacija možda ne želi da otkrije svoju internu strukturu

- X.509 sertifikati mogu biti vezani za
  - X.500 distinguished name (prethodni primer)
  - alternative name: email adresa, DNS ime
- X.509 obuhvata i standard za CRL
  - Online Certificate Status Protocol (OCSP)
  - browseri mogu, ali i ne moraju proveravati validnost sertifikata preko CRL ili OCSP-a!

IPSec

- skup proširenja IPv4 koji obezbeđuje privatnost, integritet, proveru identiteta i neporecivost
- integralni deo IPv6
- na mrežnom sloju TCP/IP steka
- uređaji na putu između krajnjih čvorova ne moraju podržavati IPSec

IPSec

- koristi sledeće komponente
  - Diffie-Hellman za razmenu ključeva
  - algoritme za digitalno potpisivanje komunikacije pri DH razmeni ključeva
    - radi potvrde identiteta učesnika u komunikaciji - sprečava se man-in-the-middle napad
  - DES, 3DES, AES za šifrovanje
  - MD5 i SHA kao osnova za HMAC funkcije
  - sertifikate koje potpisuje CA

IPSec protokoli

- dva nezavisna protokola:

- AH (authentication header)
  - usluge integriteta, provere identiteta i neporecivosti

- ESP (encapsulated security payload)
  - integritet, identitet, neporecivost *i poverljivost* podataka

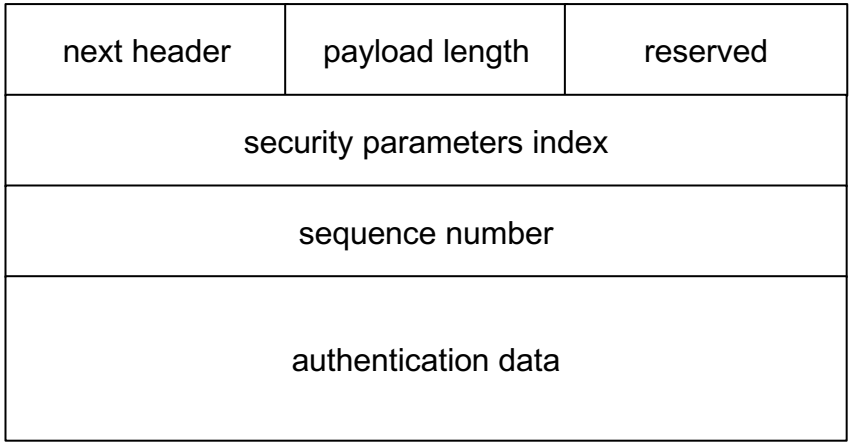
IPSec / Authentication Header

- RFC 2402
- AH zaglavlje se smešta između IP zaglavlja i podataka koji slede

- ne enkapsulira podatke iz protokola kojima pruža uslugu!

IPSec / Authentication Header

- polja u AH zaglavlju:
  - *next header*: tip podataka koji sledi posle AH zaglavlja (npr. 6 - TCP, 17 - UDP, 50 - ESP)
  - *payload length*: dužina podataka u 32-bitnim rečima umanjena za 2
  - *reserved*: 16 bita rezervisano za buduće potrebe, vrednost 0
  - *security parameters index*: skup parametara veze koji se definišu prilikom uspostave veze
  - *sequence number*: povećava se prilikom svakog slanja paketa sa istim parametrima veze
    - zaštita od napada ponavljanjem paketa
  - *authentication data*: vrednost na osnovu koje se proverava integritet i autentičnost
    - MAC vrednost IP zaglavlja, AH zaglavlja postavljenog na 0, i svih podataka protokola višeg sloja

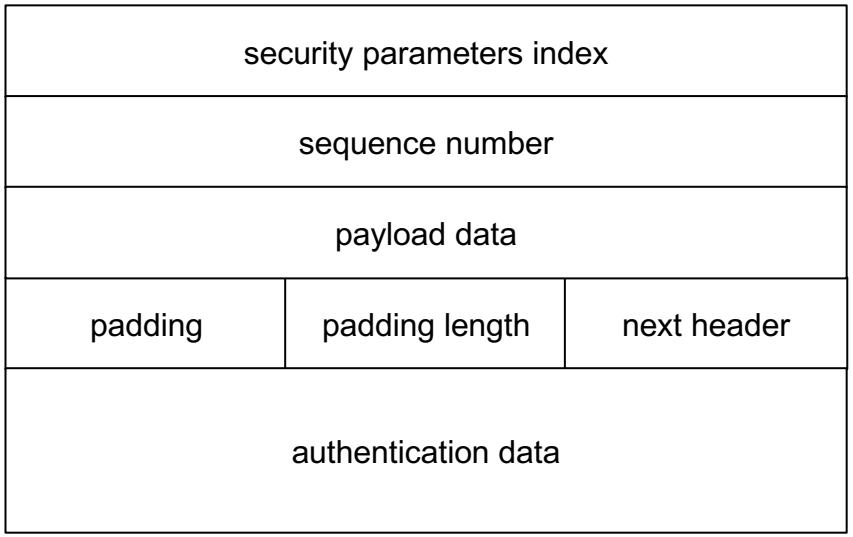


IPSec / Encapsulated Security Payload

- RFC 2406
- smešta se posle IP zaglavlja
- enkapsulira sve podatke iz protokola višeg sloja
- dodaje završni slog u koji se mogu smestiti podaci za proveru identiteta

IPSec / Encapsulated Security Payload

- polja u EPS zaglavlju:
  - *security parameters index*: skup parametara veze, isto kao kod AH
  - *sequence number*: brojač paketa sa istim parametrima veze, isto kao kod AH
  - *payload data*: podaci iz protokola višeg sloja i
  - *padding*: dopuna paketa (zbog šifrovanja blokova fiksne dužine ili zbog razloga implementacije)
  - *padding length*: dužina dopune
  - *next header*: tip podataka koji sledi posle ESP zaglavlja, isto kao kod AH
  - *authentication data*: samo kada se koristi provera identiteta; MAC se računa na osnovu celog ESP paketa osim ovog polja

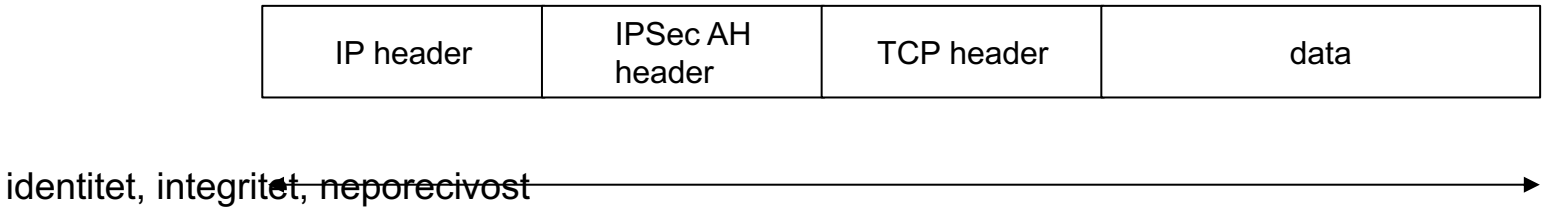


IPSec

- dva režima rada
  - transportni režim
    - šifruju se samo podaci u IP paketu, dok se IP zaglavlje ne menja
    - svakom paketu se dodaje samo nekoliko okteta
    - ruteri vide source i destination IP
  - tunelovanje
    - poseban oblik IP paketa
    - tunel čine klijent i server koji su konfigurisani da koriste IPSec tunelovanje
    - unapred dogovoreni mehanizmi za enkapsulaciju i šifrovanje kompletnih IP paketa
    - siguran prenos preko javnih ili privatnih mreža

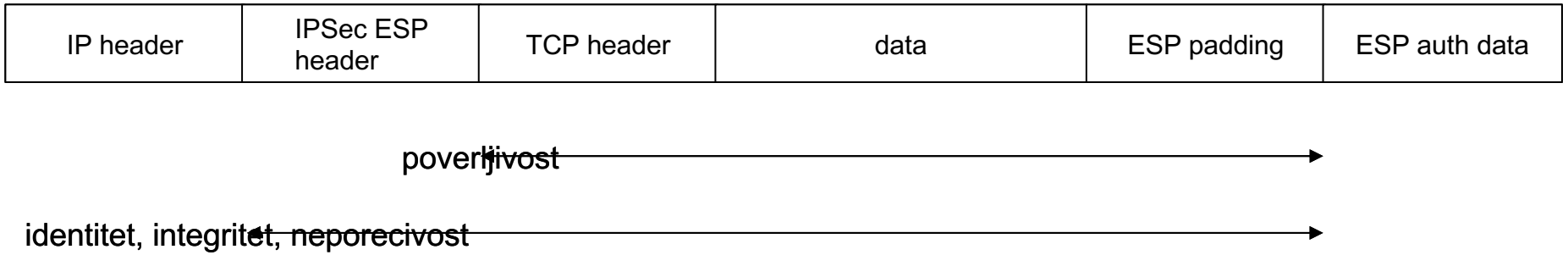
IPSec / transportni režim

- ako se koristi AH



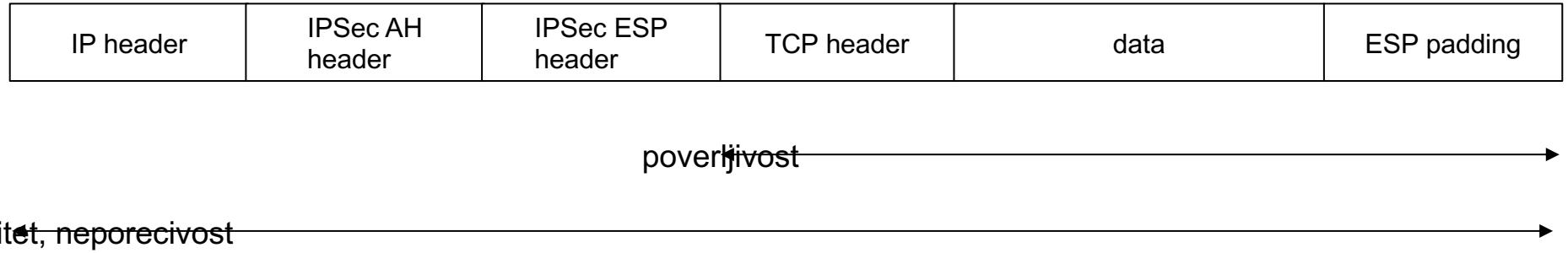
IPSec / transportni režim

- ako se koristi ESP
  - svi podaci iz višeg sloja su šifrovani
  - ESP proverava integritet svog zaglavlja i podataka, ali ne i IP zaglavlja
    - moguće izmene IP zaglavlja



IPSec / transportni režim

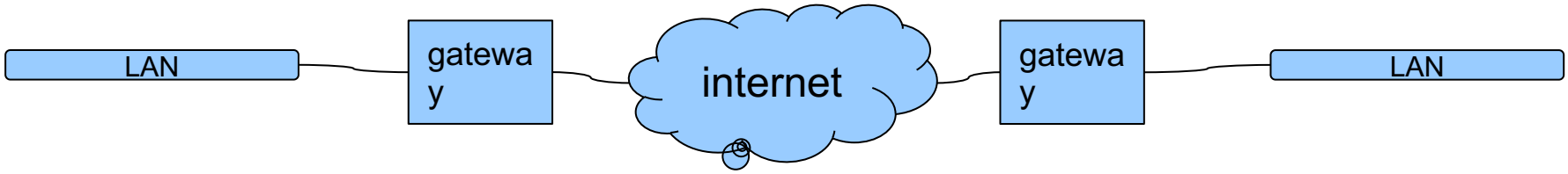
- ako se koristi ESP + AH
  - AH za integritet, identitet i neporecivost *celog* IP paketa
  - ESP za poverljivost
  - prvo se formira ESP deo, potom AH
  - ESP ne sadrži polje *auth data*, već to radi AH



IPSec / tunelovanje

- sigurna komunikacija gateway-to-gateway između dve mreže
- VPN (virtual private network)
- u gateway-to-gateway varijanti krajnji čvorovi u komunikaciji ne moraju podržavati IPSec
  - moguća je i komunikacija računar-gateway ili računar-računar, tada moraju podržavati IPSec

- formira se novi IP paket koji enkapsulira originalan IP paket

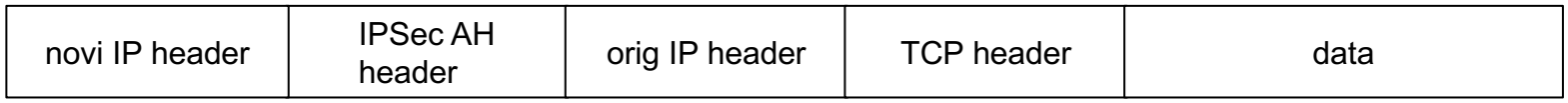


IPSec / tunelovanje

- tok komunikacije
  - pošiljalac formira IP paket i šalje ga svom gateway-u
  - gateway enkapsulira primljeni paket u novi paket (po RFC 2003) i formira AH i ESP zaglavlja
  - tako formirani novi paket se šalje drugom gateway-u
  - tamo se uklone dodatna zaglavlja, (ako treba) dešifruje paket i proveri njegov integritet
  - originalni IP paket se isporučuje odredištu

IPSec / tunelovanje

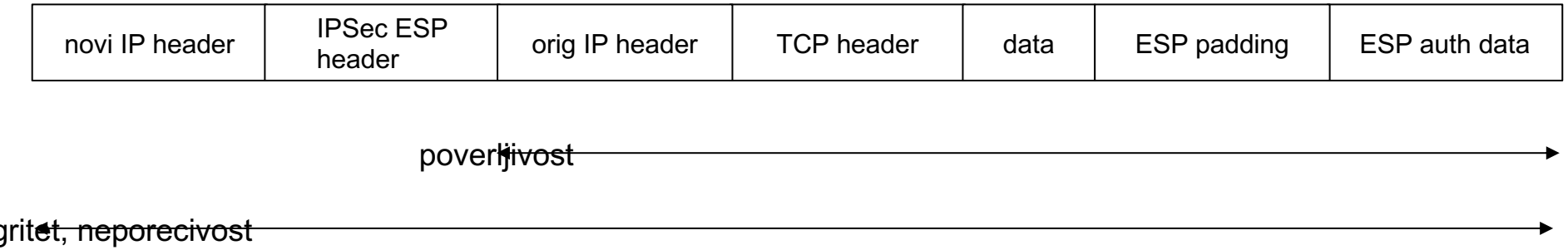
- ako se koristi AH
  - integritet, identitet, neporecivost
  - originalni IP paket se enkapsulira u novi kome se dodaje AH zaglavlje



et, integritet, neporecivost

IPSec / tunelovanje

- ako se koristi ESP
  - integritet, identitet, neporecivost i poverljivost
  - šifruje se ceo enkapsulirani IP paket



IPSec / tunelovanje

- ako se koristi AH + ESP
  - nije predviđeno po RFC 2401

IPSec / uspostava veze

- IPSec ne definiše mehanizam za uspostavljanje parametara veze
- protokoli zasnovani na Diffie-Hellman algoritmu
  - Photuris
  - SKIP (Simple Key Management for Internet Protocols)
- raširenији postupci
  - ISAKMP (Internet Security Association and Key Management Protocol)
  - IKE (Internet Key Exchange)

IKE

- RFC 2409
- kombinuje
  - ISAKMP: infrastruktura za proveru identiteta i razmenu ključeva
  - Oakley: način razmene ključeva
  - SKEME: način razmene ključeva i obezbeđuje anonimnost

- uspostava veze po IKE ima dve faze
  - uspostavljanje IKE SA (Security Association) parametara
  - uspostavljanje IPSec SA parametara

IKE / uspostavljanje IKE SA

- parametri IKE veze (SA)
  - algoritam za šifrovanje
  - heš funkcija
  - metoda provere identiteta
    - RSA/DSA digitalni potpisi
    - tajni ključ (*preshared key*)
    - puna PKI infrastruktura (eliminiše man-in-the-middle napad)
  - Oakley grupa koja definiše DH razmenu ključeva (RSA ili eliptične krive)

IKE / uspostavljanje IKE SA

- dva režima rada
  - main mode
    - zaštita identiteta učesnika u komunikaciji
    - razmenjuje se šest poruka tokom uspostave IKE SA
  - aggressive mode
    - nema zaštite identiteta učesnika
    - razmenjuje se tri poruke - brža uspostava veze

IKE / uspostavljanje IKE SA

- ključevi u IKE
  - glavni ključ koji se koristi za generisanje ostalih ključeva
  - ključ koji IKE SA koristi za šifrovanje poruka
  - ključ koji IKE SA koristi za proveru identiteta i integriteta
  - ključ koji služi za generisanje IPSec SA

- cookies: heš vrednost na osnovu
  - IP adresa, port, protokol, time stamp, secret value

IKE / uspostavljanje IPSec SA

- izvodi se u quick mode
  - koristi se prethodno uspostavljen IKE SA skup parametara
  - IPSec SA se određuje na osnovu IKE SA

IPSec i potrošnja resursa

- dodatno procesorsko vreme za kriptografske operacije
- povećan mrežni saobraćaj
  - dodatna zaglavlja
  - padding
  - inicijalizacioni vektor za šifrovanje u CBC režimu