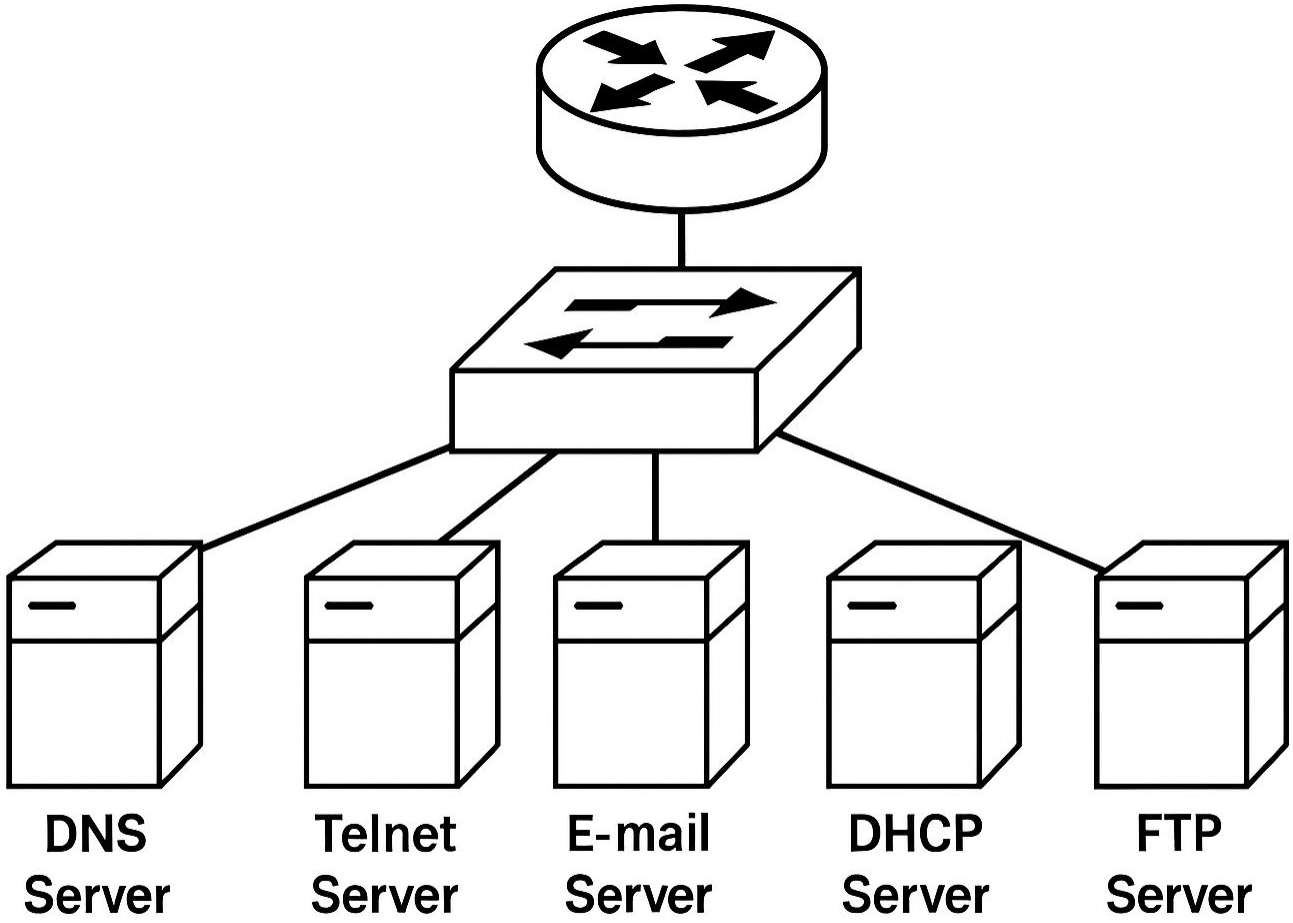
EMAIL SERVIS

Predmet: Mrežni servisi

Predavač: dr Dušan Stefanović

EMAIL SERVIS



EMAIL PROTOKOLI

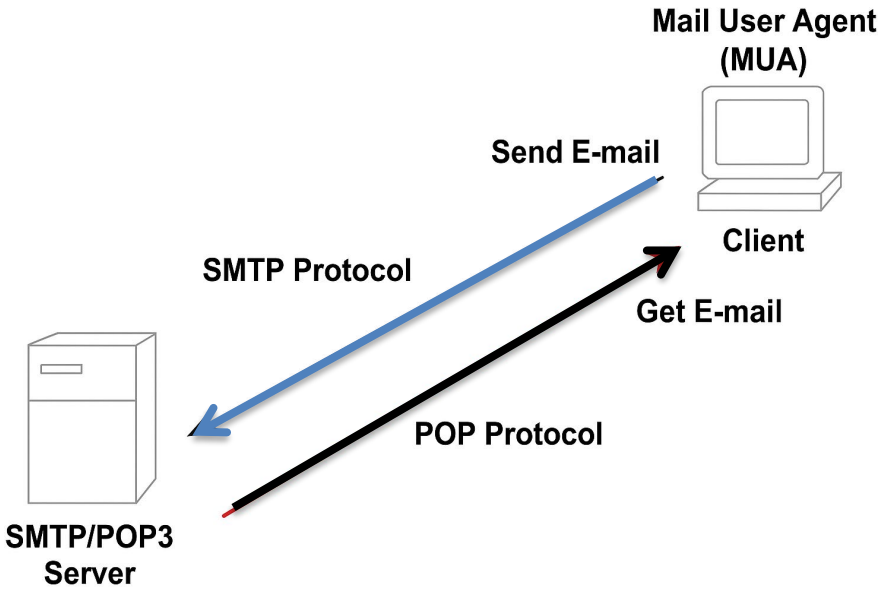
E-mail zahteva dva protokola:

Simple Mail Transfer Protocol (SMTP):

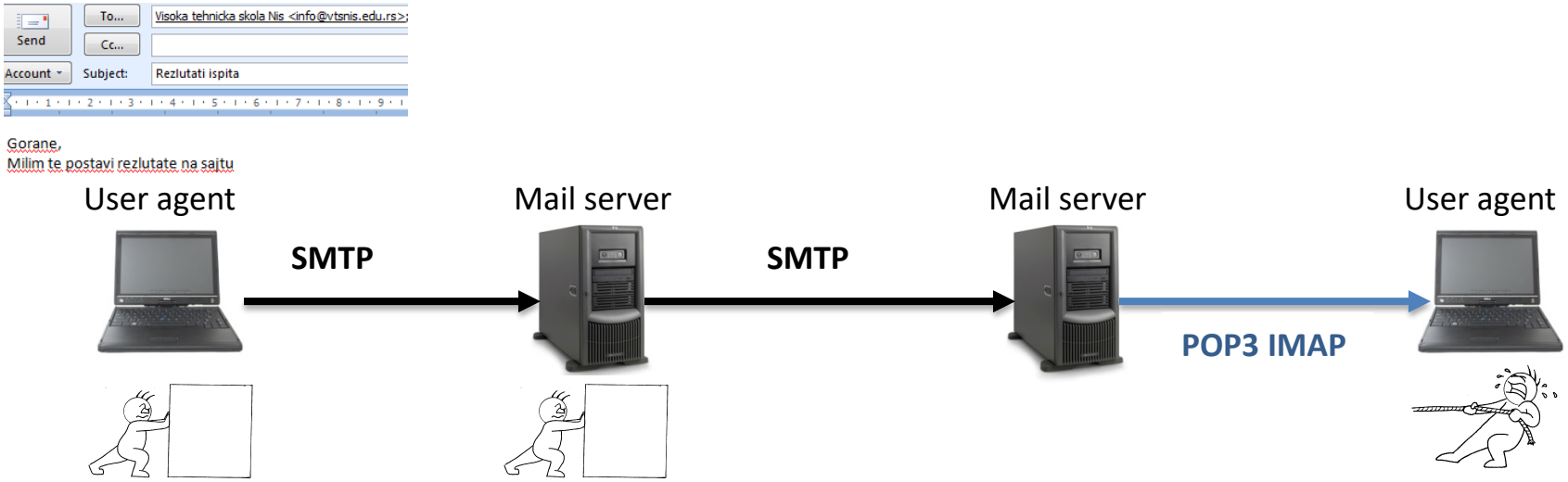
Koristi se da pošalje email poruku i prilog (attachments).

Post Office Protocol (POP) ili **Internet Message Access Protocol (IMAP)**:

Koristi se za primanje email poruka sa email servera.



PUSH VS PULL PROTOKOLI



RFC 2821

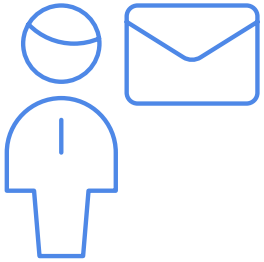
Prosleđuje poruke od **mail servera pošiljaoca** do **mail servera primaoca**

Push protokol, nije pull protokol

Push (od klijenta ka serveru ili od servera ka serveru) - SMTP

Pull (od servera ka klijentu) - POP3, IMAP, HTTP

KOMPONENTE EMAIL SERVISA



Korisnički agent

Aplikacija koja korisniku omogućava čitanje i pisanje e-mail poruka, slanje, prosleđivanje i odgovaranje na poruke i Čuvanje i organizovanje e-mail poruka

Mail server

Čuva mailbox (poštansko sanduče) korisnika, komunicira sa lokalnim user agentom i Komunicira sa drugim mail serverima radi isporuke poruka

SMTP

Protokol na aplikativnom nivou za slanje emailova preko TCP-a.

Protokoli za pristup mailu

POP3, IMAP, HTTP protokoli koji se koriste za pristup mailu.

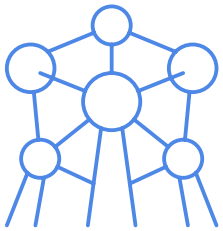
SMTP ATRIBUTI

Puno ime

Puno ime je Simple Mail Transfer Protocol.

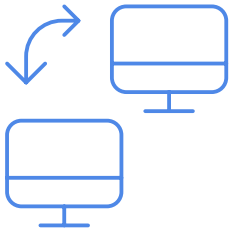
Svrha

Slanje i prosleđivanje e-mail poruka između servera.



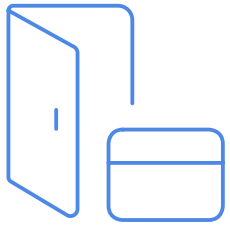
Mrežni sloj

Aplikativni sloj u OSI modelu.



Transportni protokol

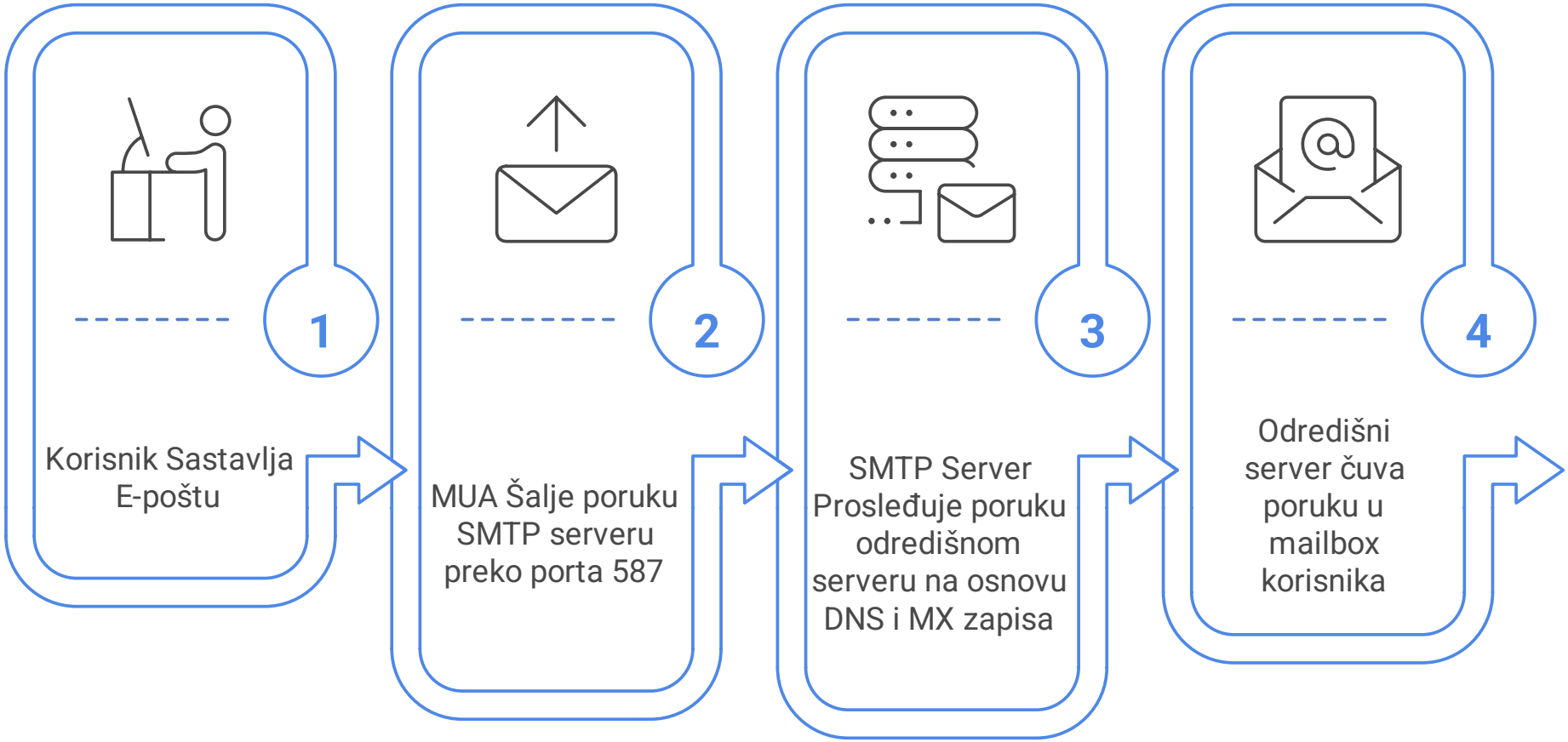
Transmission Control Protocol je transportni protokol.



Standardni portovi

Uključuje portove 25 za komunikaciju između servera, 587 za klijent-server sa autentifikacijom i 465 označen kao "legacy".

PROCES SLANJA EMAIL POŠTE



BEZBEDNOST SMTP PROTOKOLA

Kritična tema

Važnost bezbednosti u SMTP

Presretanje

Rizik od neovlašćenog pristupa porukama

Nebezbedan protokol

Objašnjava inherentne bezbednosne nedostatke SMTP

Falsifikovanje

Mogućnost lažnih poruka

Nešifrovane poruke

Nedostatak šifrovanja u osnovnom SMTP

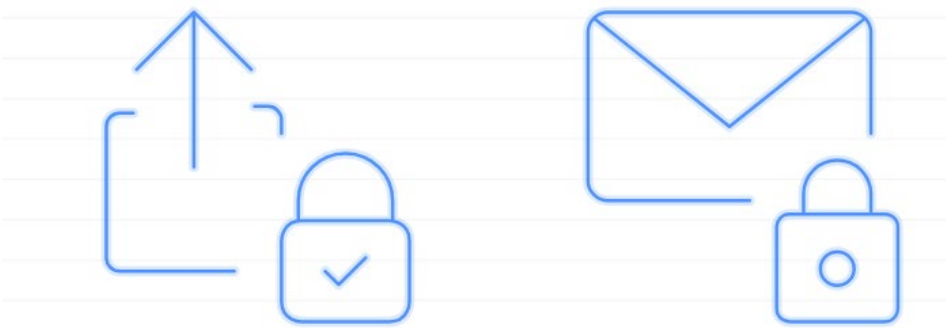
Zloupotreba

Potencijal za zlonamerne aktivnosti

Nedostatak autentičnosti

Odsustvo provere identiteta pošiljaoca

SMTP ENKRIPCIJA



STARTTLS

Štiti podatke od presretanja STARTTLS nije protokol već SMTP ekstenzija kojom se postojeća TCP konekcija unapređuje na TLS enkripciju. Komunikacija počinje kao običan SMTP (npr. port 587), a zatim se šalje STARTTLS komanda. Ako server podržava STARTTLS, obe strane pregovaraju o TLS sesiji.

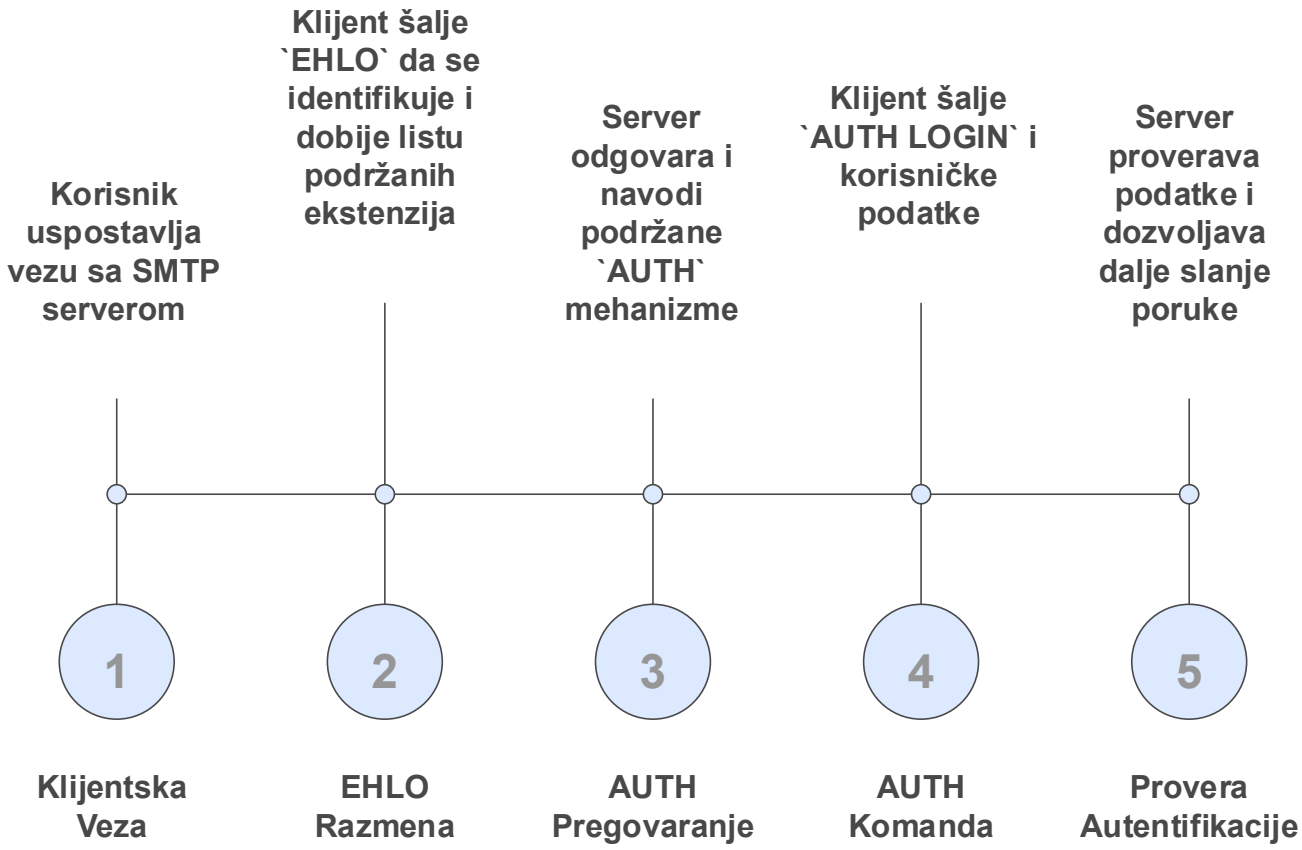
SMTPS

SMTP preko SSL/TLS (port 465) je stariji pristup gde se odmah uspostavlja šifrovana veza. Danas se preferira STARTTLS zbog bolje fleksibilnosti i kompatibilnosti.

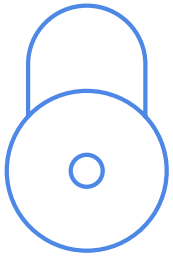
SMTP AUTENTIFIKACIJA

SMTP AUTH (SMTP Authentication) je mehanizam koji omogućava **proveru identiteta korisnika** kada pokušava da pošalje e-mail preko SMTP servera.

Bez ove autentifikacije, bilo ko bi mogao da koristi SMTP server za slanje e-mailova

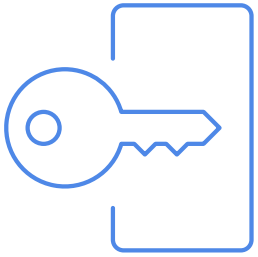


NAČINI AUTENTIFIKACIJE



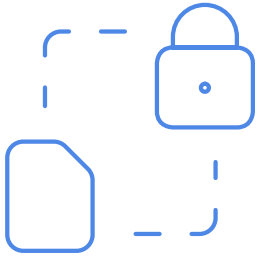
PLAIN mehanizam

Korisničko ime i lozinka se šalju u base64. Bezbedan samo ako se koristi uz TLS.



LOGIN mehanizam

Korisničko ime i lozinka se šalju odvojeno, base64 kodirani. TLS preporučen.

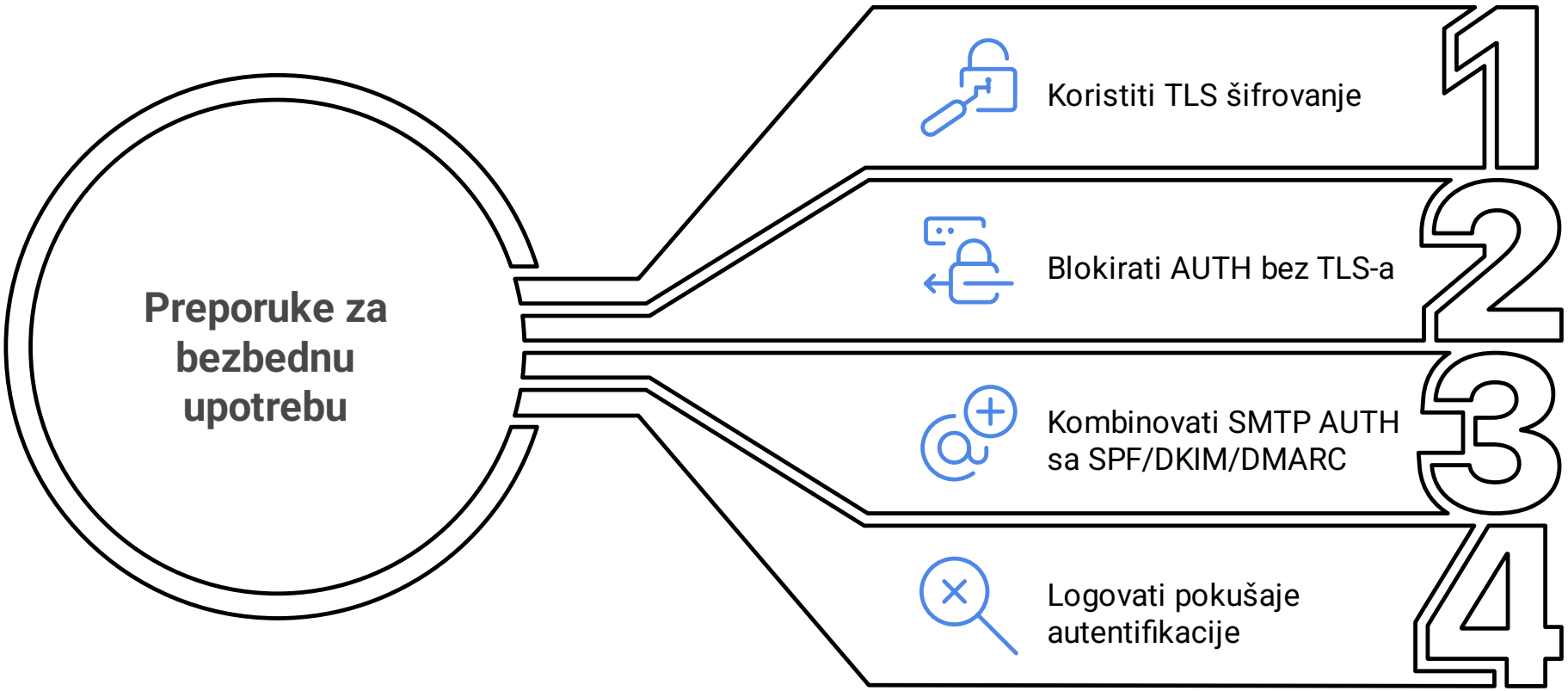


CRAM-MD5 mehanizam

Lozinka se ne šalje direktno, koristi challenge i hash. Bezbedniji ali ređe podržan.

OAUTH2 mehanizam

Koristi token umesto lozinke, za servise poput Gmail. Veoma siguran.


Preporuke za bezbednu upotrebu
Koristiti TLS šifrovanje
1
Blokirati AUTH bez TLS-a
2
Kombinovati SMTP AUTH sa SPF/DKIM/DMARC
3
Logovati pokušaje autentifikacije
4

SPF (SENDER POLICY FRAMEWORK)

SPF je DNS mehanizam za zaštitu od lažiranja pošiljalaca e-pošte (spoofing).

On definiše koje IP adrese imaju dozvolu da šalju mejlove u ime određenog domena.

odseknis.edu.rs. IN TXT "v=spf1 ip4:160.99.37.0/24 -all"

Deo	Značenje
v=spf1	Verzija SPF protokola (uvek počinje ovako)
ip4:160.99.37.0/24	Dozvoljeno slanje mejlova sa bilo koje IP adrese iz ovog opsega
-all	Sve ostale IP adrese su **izričito zabranjene** (hard fail)

"v=spf1 ip4:160.99.37.10 ip4:160.99.37.11 include:_spf.google.com -all"

Dozvoljene IP:160.99.37.10 i 160.99.37.11

Takođe svi koji su u SPF zapisu za google.com (npr. ako se koristi Gmail za slanje)

DKIM (DOMAINKEYS IDENTIFIED MAIL)

DKIM je mehanizam za autentifikaciju e-pošte koji omogućava digitalno potpisivanje poruka tako da primalac može da proveri:

1. da poruka nije izmenjena u transportu
2. da je zaista poslata sa servera ovlašćenog za domen

Pošiljalac (mail server) generiše digitalni potpis iz sadržaja poruke + zaglavlja.

Potpis se dodaje u zaglavlje mejla kao DKIM-Signature:

Primalac vidi DKIM-Signature zaglavlje. Primalac pronalazi javni ključ u DNS zapisu pomoću koga proverava da li se potpis poklapa sa sadržajem poruke

default._domainkey.odseknis.edu.rs. IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GC...QAB"

Element	Opis
v=DKIM1	Verzija DKIM
k=rsa	Algoritam za enkripciju
p=...	Javni RSA ključ koji koristi primalac za verifikaciju potpisa

DMARC

(DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING AND CONFORMANCE)

DMARC (Domain-based Message Authentication, Reporting and Conformance) je mehanizam za autentifikaciju e-pošte koji se nadovezuje na SPF i DKIM i omogućava domenu da:

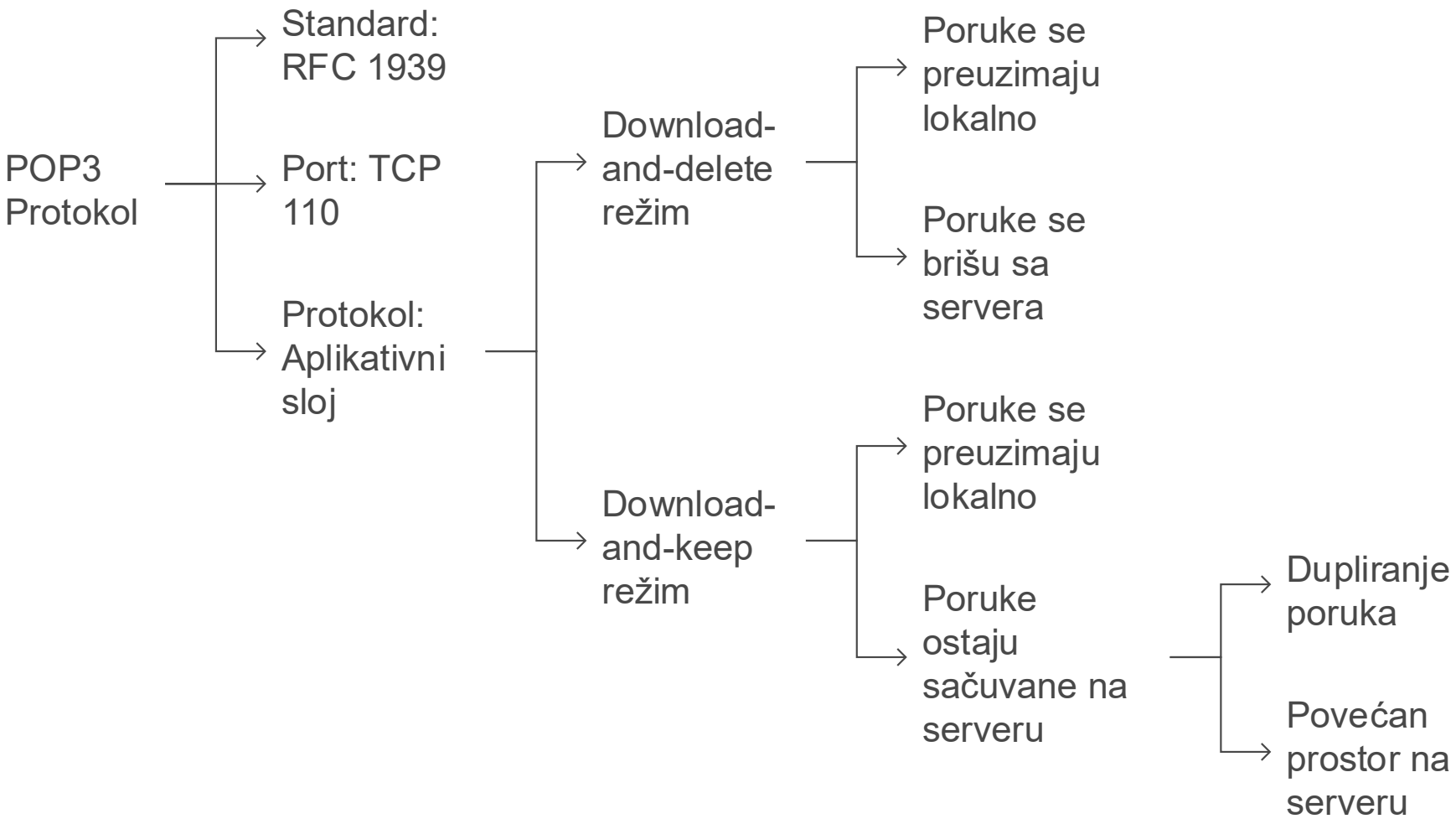
1. Sopšti serverima šta da urade ako SPF i/ili DKIM provera ne uspe (npr. da odbace mejl).
2. Prati i prijavljuje pokušaje zloupotrebe domena za slanje lažnih mejlova (phishing).
3. Štiti brend i korisnike od prevara u e-pošti.

DMARC politika u TXT zapisu za domen odseknis.edu.rs

_dmarc.odseknis.edu.rs. IN TXT
"v=DMARC1; p=reject; rua=mailto:dmarc@odseknis.edu.rs; ruf=mailto:forenzika@odseknis.edu.rs; fo=1"

Element	Značenje
v=DMARC1	Verzija protokola
p=reject	Odbaci mejlove koji ne prođu SPF/DKIM
rua=	Adresa za agregatne izveštaje (ko šalje, koliko, rezultati)
ruf=	Adresa za forenzičke (detaljne) izveštaje
fo=1	Pošalji forenzički izveštaj za bilo koji neuspeh

FUNKCIONALNE KARAKTERISTIKE POP3 PROTOKOLA

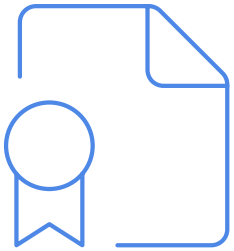


OGRANIČENJA POP3 PROTOKOLA

Ograničenje	Objašnjenje
✗ Nema podrške za **foldere**	Korisnik ne može kreirati ili upravljati folderima na serveru
✗ Nema sinhronizacije	Promene na jednom uređaju nisu reflektovane na drugim
✗ Nema višekorisničke sesije	Samo jedan klijent može istovremeno imati pristup porukama
✗ Ne podržava oznake, zastavice ili tagove	Nema naprednog upravljanja porukama kao što je u IMAP protokolu

Ako se koristi više računara ili mobilnih uređaja, korisnik mora ručno uključiti opciju da poruke ostaju na serveru – u suprotnom, prvi uređaj koji preuzme poruku je jedini koji će je imati.

IMAP KARAKTERISTIKE

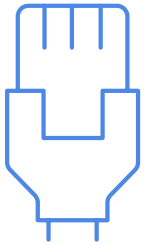


Standard

Definisan u RFC 2060, najnovija verzija RFC 3501.

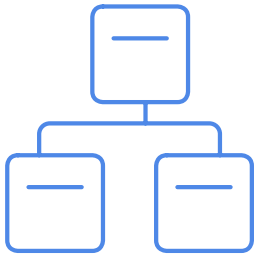
Svrha

Prijem i upravljanje elektronskom poštom na udaljenom serveru.



Port

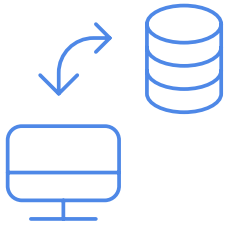
TCP 143 (standardni), 993 (za IMAPS).



Protokol

Aplikativni sloj (OSI Layer 7).

IMAP
OSOBINE

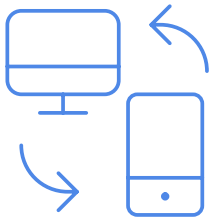


Rad sa serverom

Poruke se ne preuzimaju trajno, već se čitaju direktno.

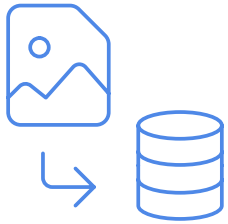
INBOX struktura

Pristup porukama organizovan u poštanskim sandučićima (folderima).



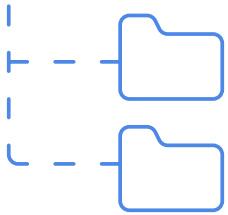
Rad sa više uređaja

Poruke i promene su sinhronizovane između svih klijenata.



Partial fetch podrška

Moguće je privući samo deo poruke.



Upravljanje folderima

Korisnik može kreirati, preimenovati i brisati udaljene foldere.

IMAP SIHRONIZACIJA

Otvori se e-mail na telefonu →

označi se poruka "pročitana" → istog trenutka je i na laptopu označena kao pročitana.

Dvosmerna sinhronizacija

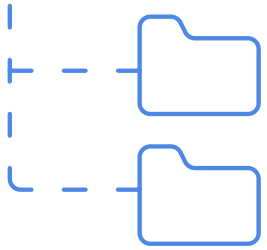
Promene se automatski reflektuju na svim uređajima.

Pohrana na serveru

Poruke ostaju na serveru uvek, a klijent prikazuje njihov sadržaj u realnom vremenu.

Višekorisnički pristup

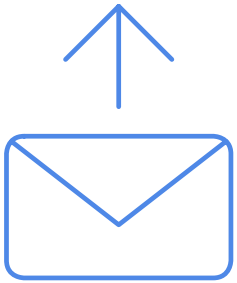
Više korisnika pristupa istom nalogu.



Struktuiranje foldera

Korisnici kreiraju foldere i upravljaju porukama direktno na serveru.

IMAP
FUNKCIONALNOSTI DEFINISANE RFC 3501

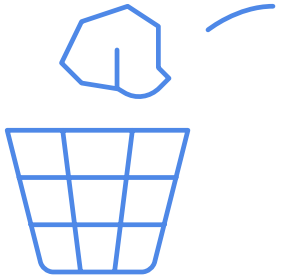


Upravljanje porukama

Čitanje sadržaja, parsiranje zaglavlja, tela i postavljanje zastavica.
\Seen – pročitano
\Answered – odgovoreno
\Flagged – važno
\Deleted – označeno za brisanje
\Draft – nacrt
\Recent – nova poruka

Upravljanje poštanskim sandučićima

Kreiranje, brisanje, preimenovanje sandučića i provera novih poruka.

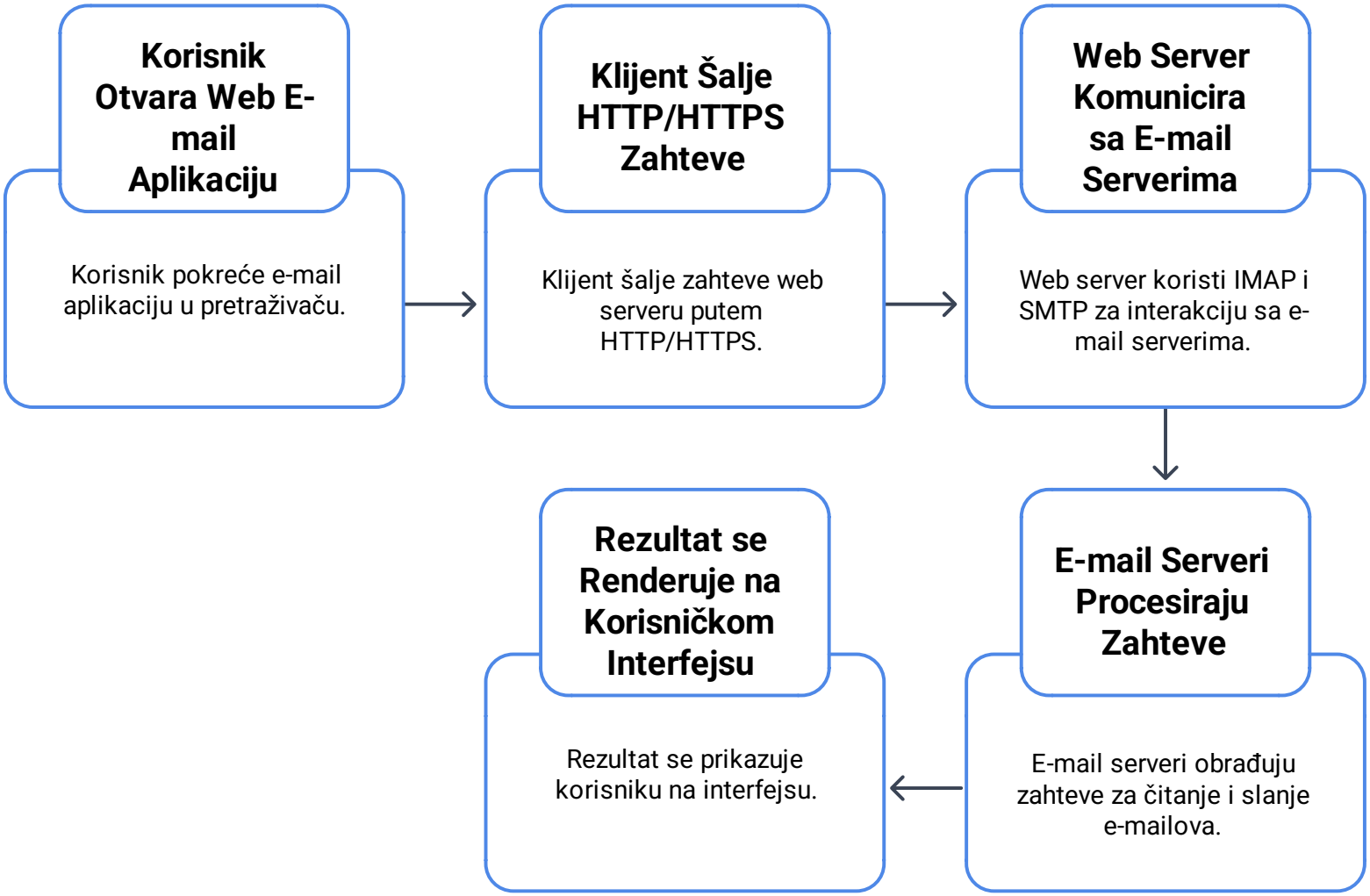


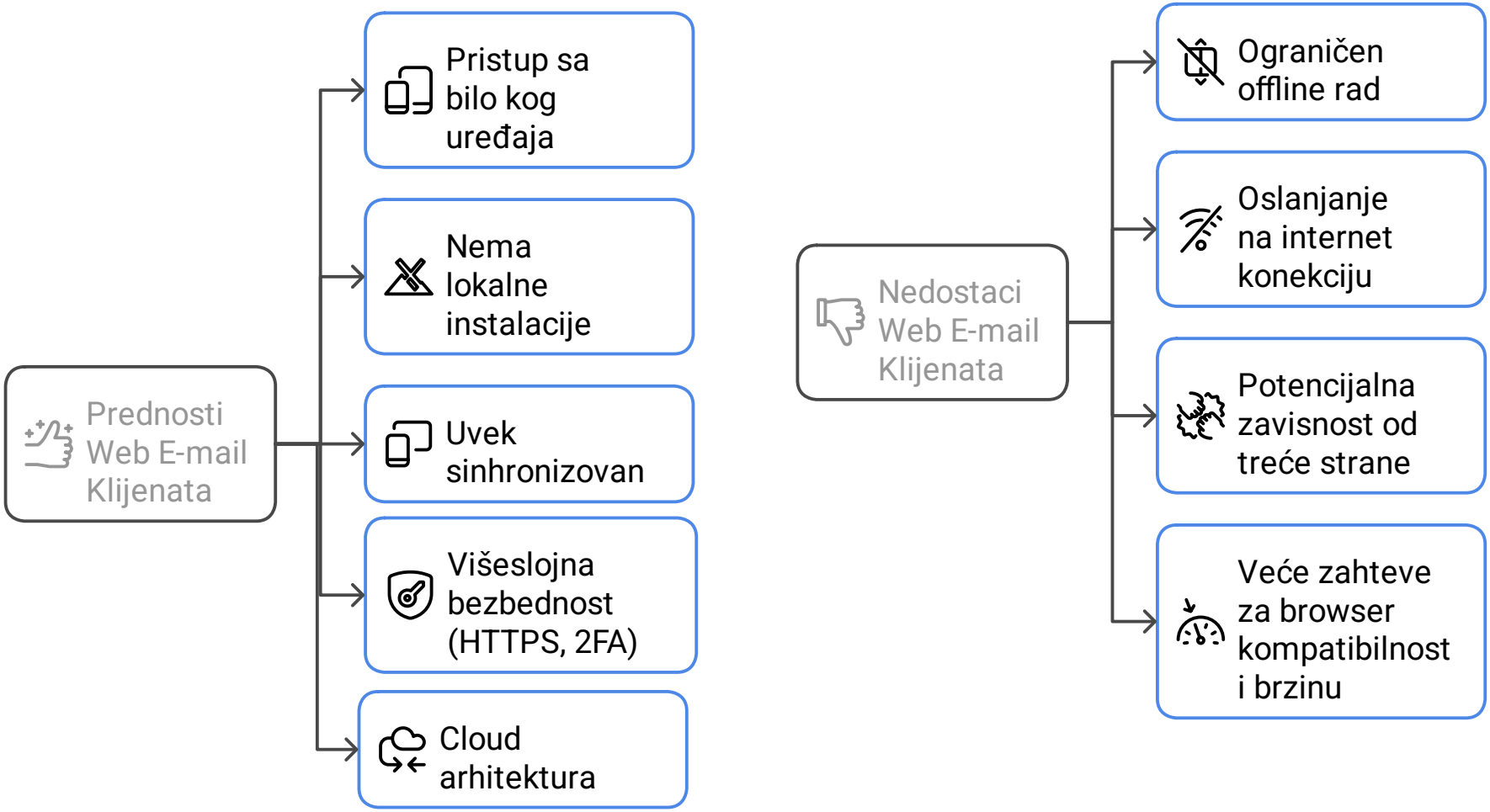
Brisanje i čišćenje

Obeležavanje poruka i trajno uklanjanje iz poštanskog sandučića.

	IMAP	POP3
Upravljanje porukama na serveru	Čuva poruke na serveru	Preuzima i briše poruke
Sinhronizacija uređaja	Sinhronizuje sa više uređaja	Ne sinhronizuje
Podrška za foldere	Podržava foldere i organizaciju	Nema podrške za foldere
Pristup porukama	Omogućava pristup delu poruke	Uvek preuzima celu poruku
Prikladnost klijenta	Pogodan za mobilne i web klijente	Pogodan za lokalnu arhivu

EMAIL WEB KLIJENT

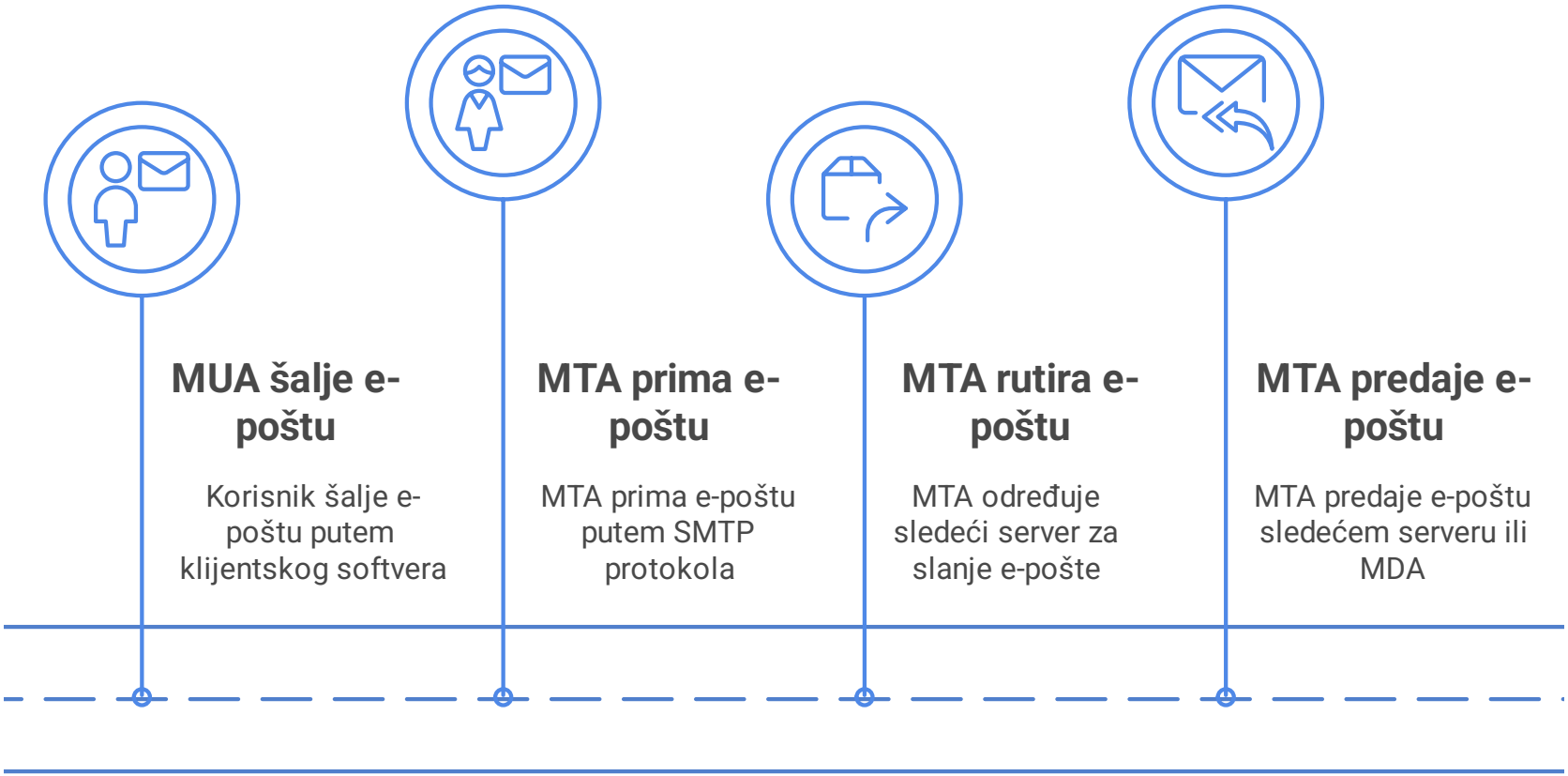



Prednosti Web E-mail Klijenata
Pristup sa bilo kog uređaja
Nema lokalne instalacije
Uvek sinhronizovan
Višeslojna bezbednost (HTTPS, 2FA)
Cloud arhitektura
Nedostaci Web E-mail Klijenata
Ograničen offline rad
Oslanjanje na internet konekciju
Potencijalna zavisnost od treće strane
Veće zahteve za browser kompatibilnost i brzinu

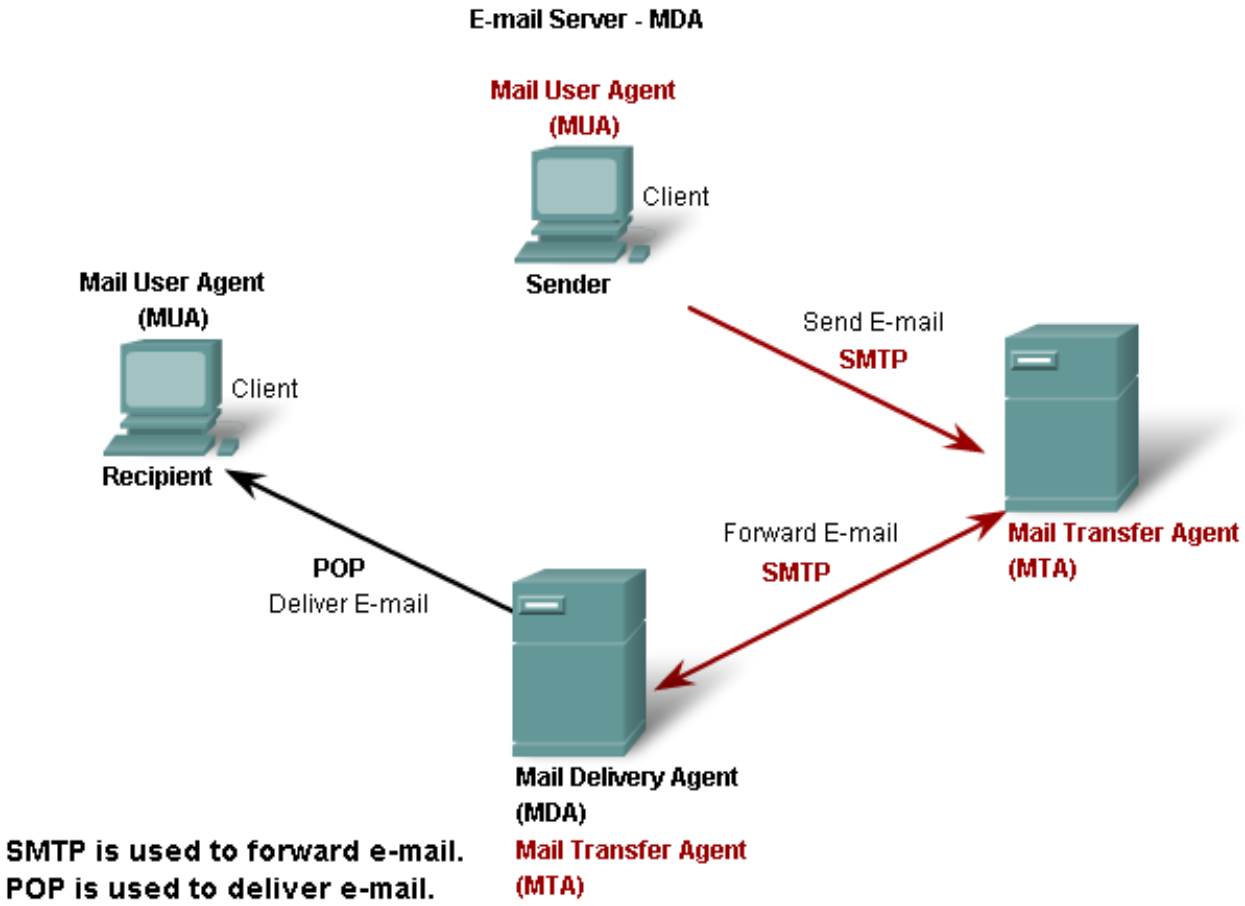
MTA (MAIL TRANSFER AGENT)

MTA je softverska komponenta zadužena za **prijem, rutiranje i prosleđivanje e-mail poruka** sa jednog servera na drugi.

Predstavlja **srce e-mail infrastrukture** i koristi se za **transport e-mailova između domena** i mail servera.



MTA (MAIL TRANSFER AGENT)



TOK SLANJA EMAIL PORUKE