

# Vještine komuniciranja u inženjerstvu

## Elektronička pošta (E-mail)



Predrag Pale

# E-mail: za koga, kada?

- danas je prihvaćen kao **medij poslovne komunikacije**
- na FER-u se očekuje da i **studenti** i nastavnici **koriste** svoje **račune** (eng. *mail account*)

**@FER.hr**

*ime.prezime@fer.hr*

- moguće je imati **više računa**
  - kod raznih pružatelja usluga (eng. *provider*)
  - svaki za neku drugu svrhu
  - za privatne i službene potrebe
  - a **upravljati** njima **iz jedne aplikacije**

- za razliku od drugih oblika elektroničkog komuniciranja e-mail ima
  - naslov (subject),
  - poruku (message body),
  - privitak (attachement)
- poruka se može **zaštititi kriptiranjem**
- može se uključiti **potvrda isporuke i prijema** (čitanja)
- **lagano** se šalje **na više primatelja**
  - s laganom kontrolom popisa primatelja
  - koji jedni drugima mogu biti vidljivi, ili nevidljivi
- mogu se stvarati **funkcionalne adrese**
  - koje se proslijeđuju na račun jedne ili više osoba
- mail se može **preusmjeriti u program**
  - ili poslati iz programa
  - što ga čini prikladnim sredstvom za Internet of Things (IoT)
    - a tu komunikaciju čovjek može lagano nadzirati

fer@fer.hr



# ADRESIRANJE



# Oblik e-mail adrese

- oblik adrese je

**primatelj@domena**



- **primatelj** je

- ili oznaka poštanskog sandučića: pperic12
- ili ime osobe: Pero.Peric, PeroPeric, pero\_peric

- **domena** je adresa na kojoj se nalazi poštanski sandučić (*eng. mailbox*):

- najčešće adresa **organizacije**: **fer.hr**
- ili adresa **računala**: **mailman.fer.hr**

- sustavi **ne razlikuju** mala i velika slova

Pero.Peric@FER.hr ≡ pero.peric@fer.hr

- dozvoljeni znakovi su:

a-z A-Z 0-9 . \_ -

! # \$ % & ' \* + - / = ? ^ \_ ` { | } ~ smiju, ali se ne preporuča  
mogući su i dijakritički znakovi (ćčđšž)

- ali još ih ne podržavaju svi sustavi u svijetu

# Vaše e-mail adrese

- osim službene: *Ime.Prezime@FER.hr*
- možete ih imati koliko želite
- popularne su:  
@gmail.com, @yahoo.com, @hotmail.com, @zg.tcom.hr
- ali možete imati i **vlastitu domenu**,  
**besplatno, zauvijek**  
*ime-prezime.from.hr*
  - <https://dns.hr/portal/register/free-fromhr>
- glavna **prednost** je da
  - možete se seliti (po cijelom svijetu)
  - možete mijenjati providera za svoj sandučić
  - **vaša se adresa neće promijeniti**

# Marko Sršan [FER 2014] – Tech Stars



- Iako sam se e-mailom na faksu služio dosta, tek kada sam počeo raditi u Londonu shvatio sam kolika se masa komunikacije odvija putem e-maila
- Kroz posao sam upoznao mnogo ljudi i bivao upoznat s mnogo ljudi
- I sve se odvijalo putem e-maila, kada bi me moj kolega upoznao s drugim kolegom
- Problem kod upoznavanja (*make an introduction*) je što upoznavatelja nije briga što se dalje događa nakon inicijalnog povezivanja
- Njemu je samo važno da je osoba koju je predstavio odgovorila, da vidi odgovor, i da je nadalje ispušten iz tog e-mail lanca
- Tome služi **Bcc**, a mnogo ljudi ne razumije da bi bilo dobro, dapače, poželjno upoznavatelja staviti u **Bcc** i time ga poštediti od daljnjih razgovora
- Zvuči nevažno, no ukoliko dnevno dobiješ prosječno 150-ak mailova, 20 mailova u kojima se dvoje ljudi dogovara gdje i kada će se naći na kavi, a nakon što si ih spojio, predstavlja višak.
- Poanta priče: **Bcc je važan!**

- tj. čemu služe **To:**, **Cc:** i **Bcc:** polja i koga se u njih stavlja?
- **To:** polje
  - glavna **osoba kojoj je poruka namijenjena**
  - od nje se **očekuje da reagira** na sadržaj poruke
    - **obavi** traženo
    - **odgovori**, ako treba
  - zato je dobro da se u nju **ne stavlja više od jedne osobe**
    - osim ako sve trebaju napraviti isto
- **Cc:** polje
  - svi **koji trebaju znati** za komunikaciju između vas i **To:** primatelja
  - od njih se, u načelu, **ne očekuje da išta poduzmu**
  - odgovaraju samo ako je to bitno: za ispraviti ili dodati vašoj poruci
- **Bcc:** polje
  - svi navedeni u **To:** i **Cc:** poljima **su vidljivi svima** koji prime poruku
  - navedeni u **Bcc:** **nisu vidljivi nikome** tko je primio poruku
  - tu se navode oni koji trebaju znati za komunikaciju, ali za njih nitko ne treba ili ne smije znati



# Kako odgovarati na poruke?

- naredbom “Reply” ili “Reply all”

- **“Reply”**

- šalje odgovor samo onome tko je poruku poslao

- tko je u **From:** polju



- **“Reply all”**

- šalje odgovor još i svima koji su bili u **To:** i **Cc:** poljima

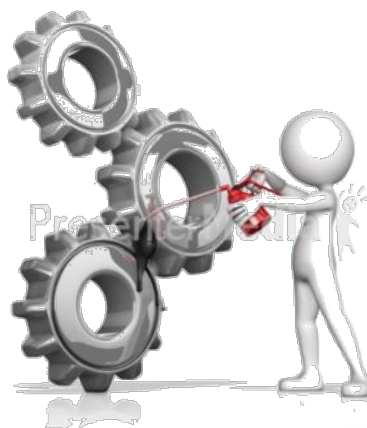
- ali ne i onima u **Bcc:**

- koristite **jedino ako** zaista **SVI** trebaju vidjeti vaš odgovor

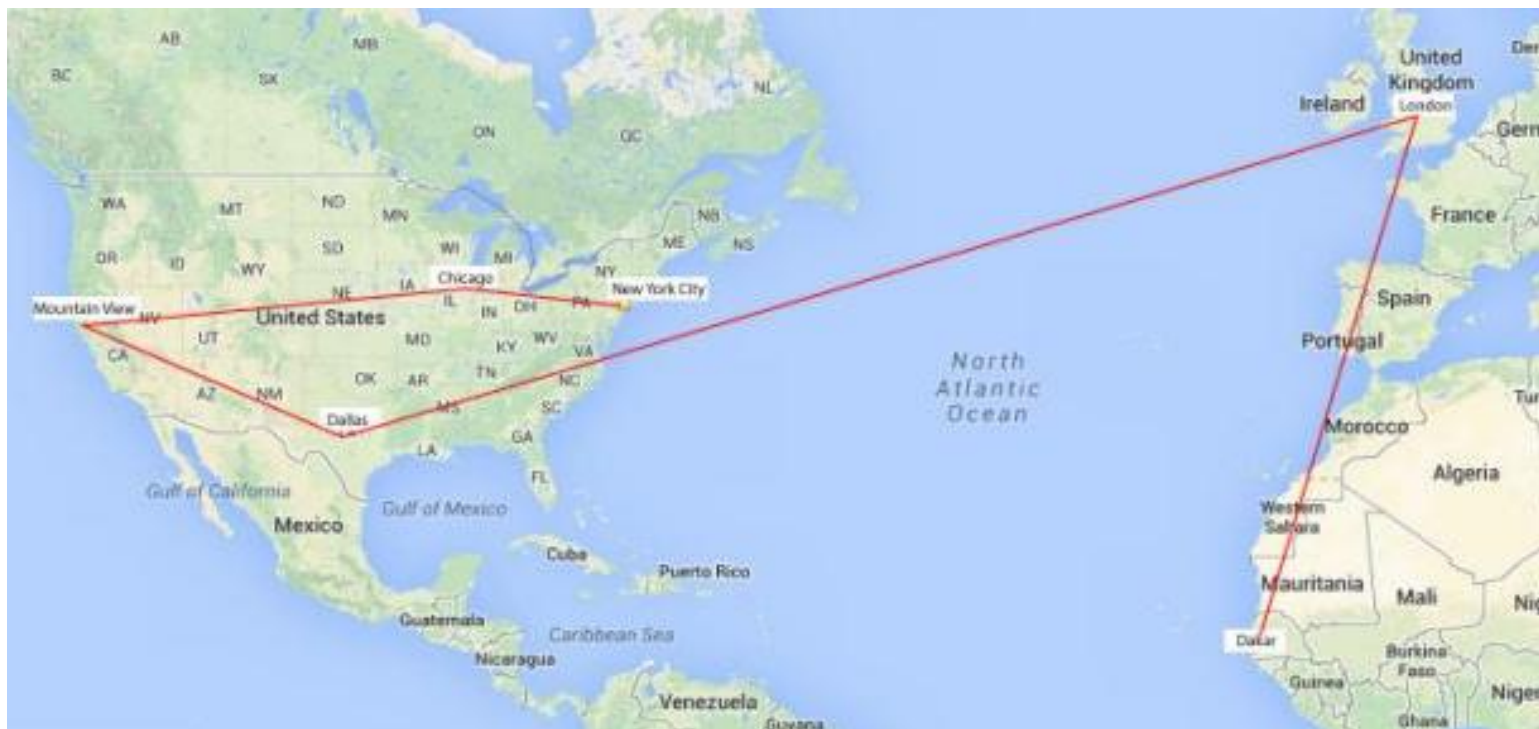


# Još o To:, Cc: i Bcc:

- **virusi** koji napadaju računala
  - pregledaju vaše **mailove**
  - i **napadaču pošalju sve adrese** koje u njima nađu
  - adrese iz **Bcc: ne mogu naći**
- kad šaljete “**kružnu obavijest**” (eng. *circular message*)
  - **sve** primatelje stavite u **Bcc:** polje
  - osim ako svi moraju znati tko je sve dobio poruku
    - tada ih sve stavite u **Cc:** polje
- **onaj tko je u Bcc:**
  - **neće dobiti “Reply all”** poruke svih koji su bili u To: i Cc:
  - i u pravilu **oni niti ne žele** dobivati niz poruka koji slijedi
    - ako im trebaju ti odgovori, onda ih stavite u **Cc:**



# TEHNIKA



# KAKO E-MAIL PUTUJE



10.10.2018.

Computer forensics - Email



# E-mail sustav čine

## 1. message **user** agent (MUA) – “e-mail klijent”

- **komunicira s korisnikom**
- **komunicira s MTA**
  - kako bi **poslao** e-mail **primatelju**
  - **dohvaća primljene poruke** koje je primio i čuva MTA
- **popularni agenti:**
  - mail, mailx, pine, elm, mutt
  - Outlook, Thunderbird, Eudora ...
  - web based agents
    - Squirrel mail, RoundCube
    - Gmail, Yahoo, Hotmail



**SquirrelMail**  
WEBMAIL FOR NUTS

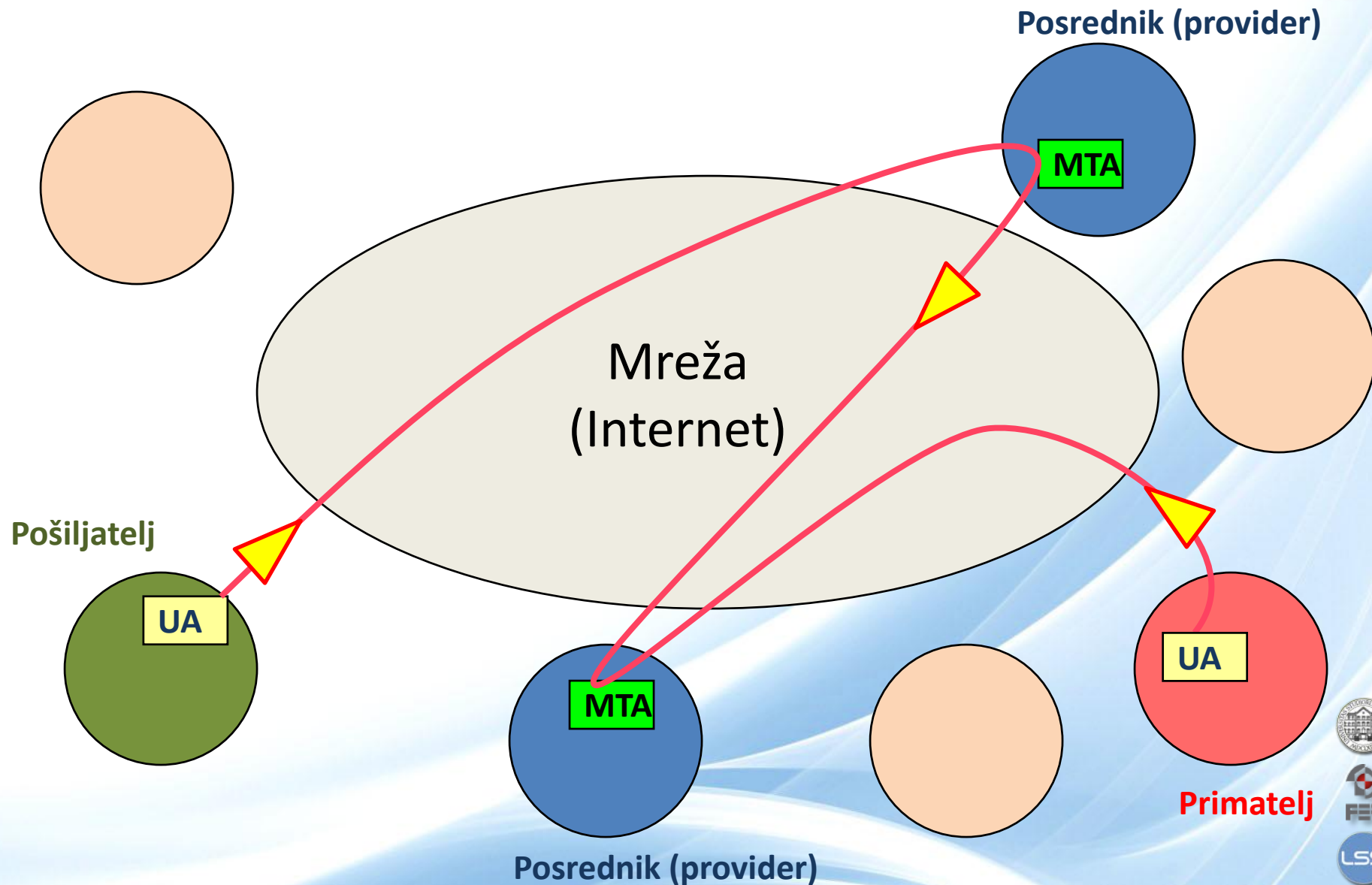


## 2. message **transfer** agent (MTA)

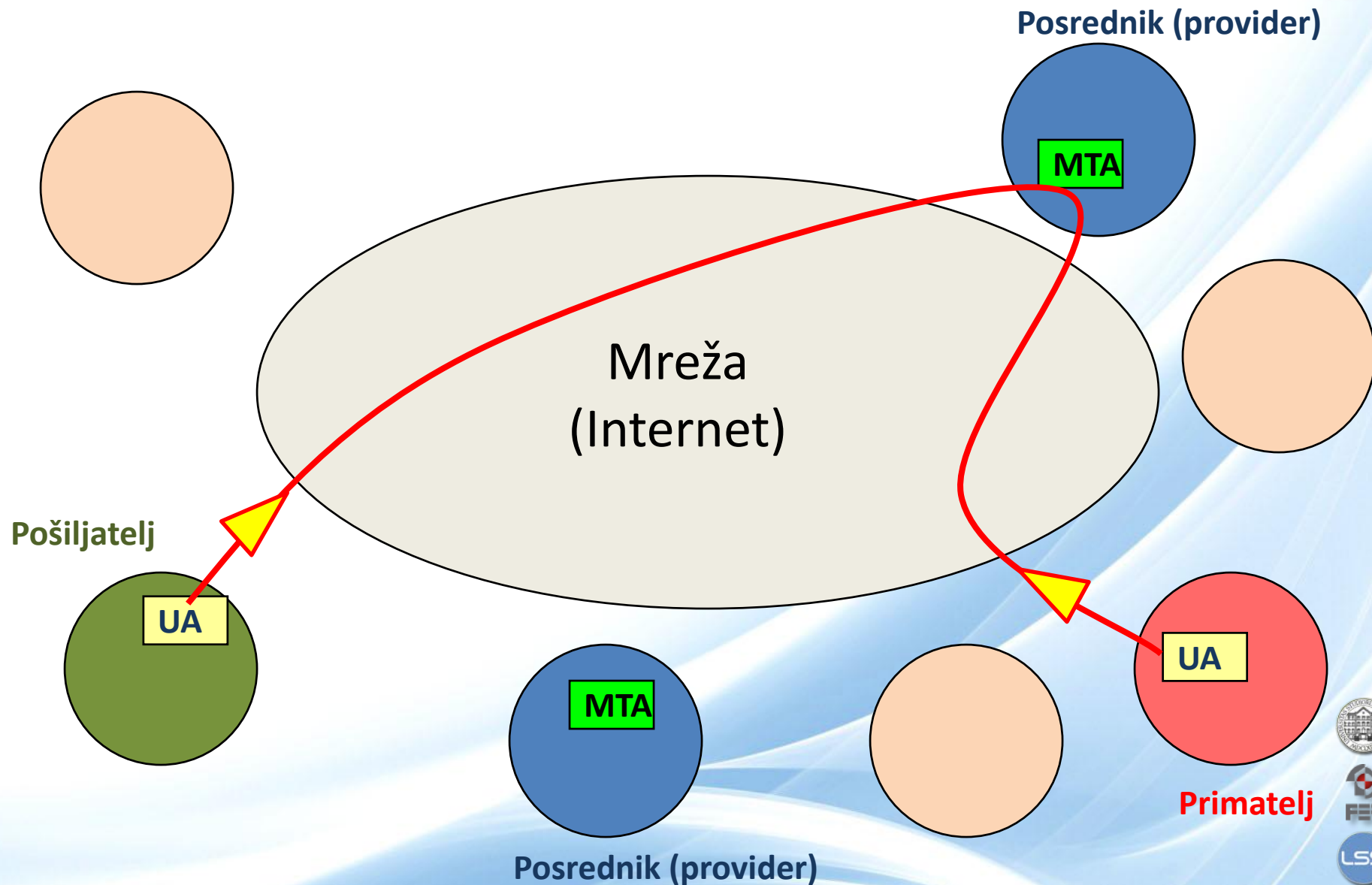
- mail transfer agent, mail relay
- mail exchanger, mail server, MX host ...
- **on zapravo razmjenjuje poruke**, s drugim MTA
- **popularni MTA:**
  - postfix, exim, sendmail
  - MS Exchange
  - IBM Domino (Lotus Notes)



# Indirektni prijenos – nekoliko MTA



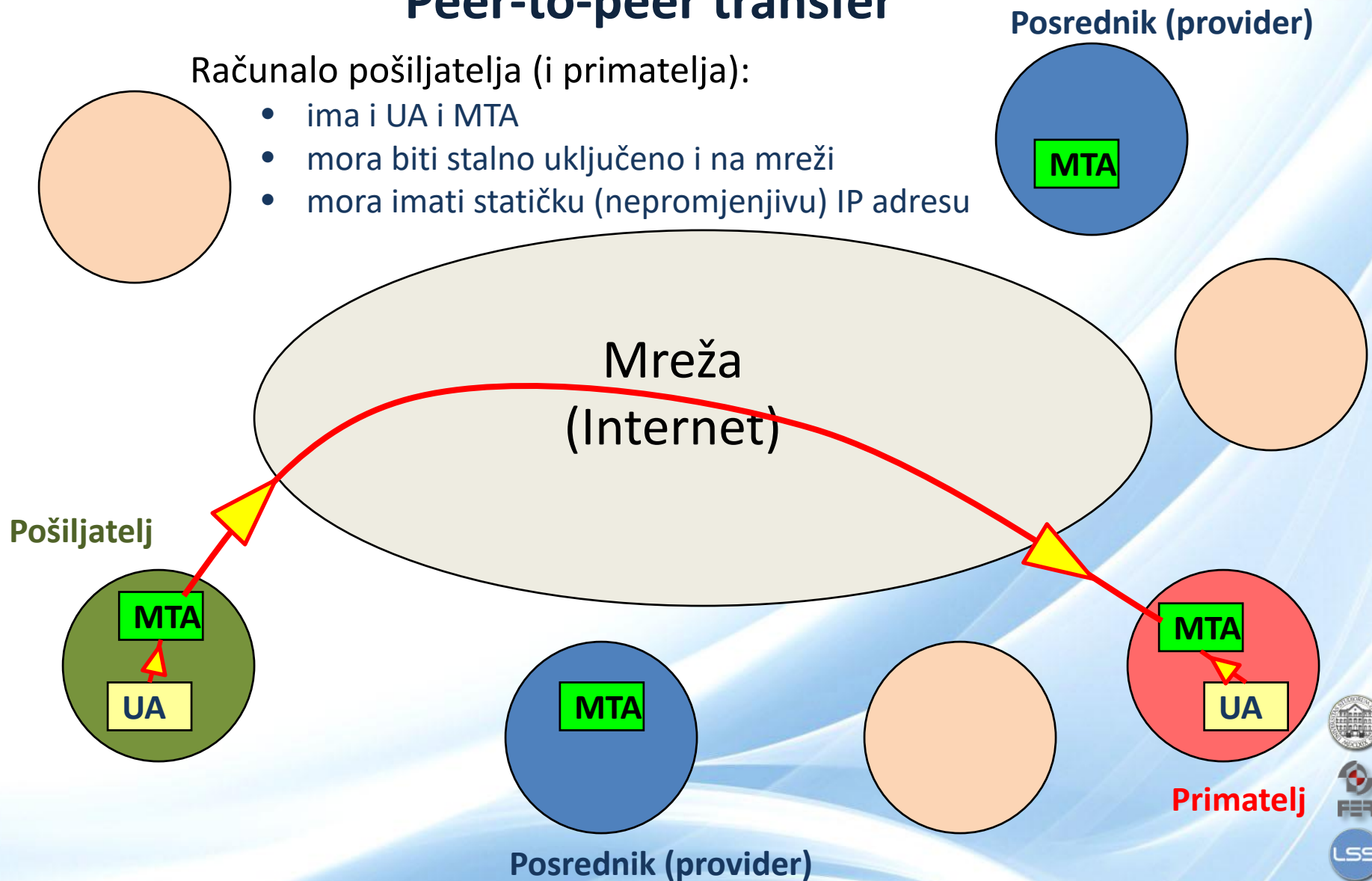
# Indirektni prijenos – jedan MTA



## Peer-to-peer transfer

Računalo pošiljatelja (i primatelja):

- ima i UA i MTA
- mora biti stalno uključeno i na mreži
- mora imati statičku (nepromjenjivu) IP adresu





# Mail klijenti: web based ili desktop

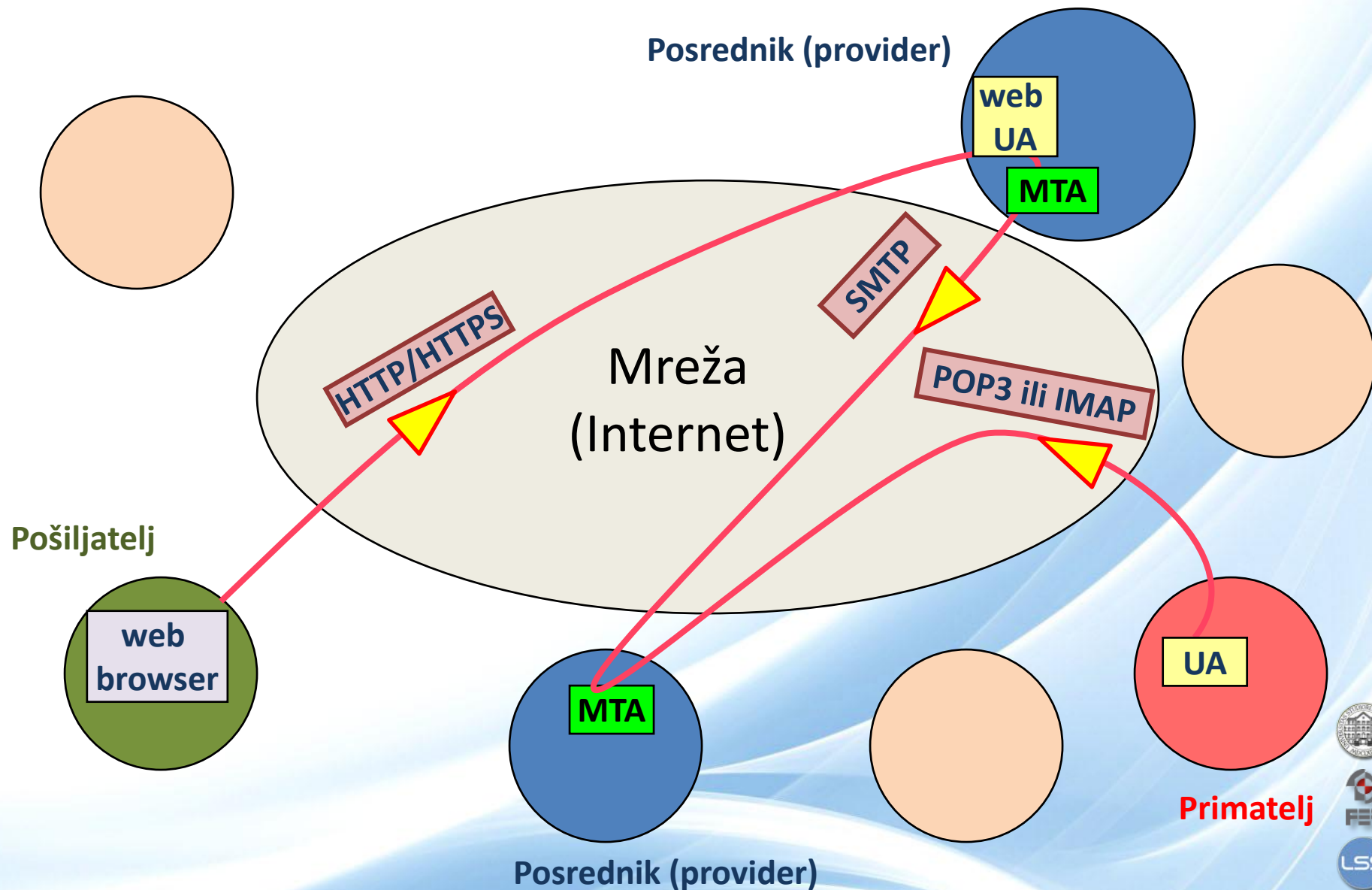
- popularni su **web** klijenti
  - **ne možete** mailove **čitati off-line**
  - i ako imate više mail računa za svakog **morate** koristiti **odvojeni** klijent





- zato se koriste **desktop** klijenti
  - za desktop računala, laptope, tablete i smartphone
  - Mozilla **Thunderbird**, MS-**Outlook** i drugi
  - “istovremeno” možete upravljati **neograničen broj računa**
  - **mailovi** mogu biti **pohranjeni** na vašem računalu, **lokalno**
  - možete **integrirati mail s programima**
    - koji će **automatski** primiti i/ili slati mailove



# Web ili desktop UA?





- **e-mail**, u pravilu, **dolazi** u sandučić (eng. mailbox) na **poslužitelju** vašeg providera
- vaš desktop **klijent mora pristupiti** sandučiću
  - i preuzeti poštu
- **POP3** poslužitelj
  - **preuzima poštu** s poslužitelja
  - i **pohranjuje ju lokalno**, na vaše računalo
  - problem: ako poštu želite čitati s više različitih računala (doma, ured, putno ...)
    - nećete ju vidjeti osim na jednom računalu
- **IMAP**
  - **ostavlja poruke** na poslužitelju (providera)
  - pa se mogu **čitati sa svih računala**
  - a može se napraviti i lokalna kopija
    - koja se prvom prilikom sinkronizira s poslužiteljem

# Što je to “Plain text”, a što “HTML”?

- E-mail se razmjenjuje protokolom SMTP (*Simple Mail Transfer Protocol*)
  - koji je napravljen u **70-tim godinama**
  - **prenosi samo ASCII znakove i samo 7 bita**
- zato SMTP **ne može prenijeti**
  - ćčđšžäöüß ....
  - niti fotografije, zvuk, video, programe ....
  - niti slova mogu biti u bojama, različitim veličina i fontova
- da bi se to moglo, takav **sadržaj se mora kodirati**
  - **da izgleda kao da je 7bit ASCII**
  - a vaš mail **klijent** program mora znati **interpretirati** taj kod
- danas se **za kodiranje sadržaja** poruke koristi **HTML**
  - bez kodiranja je “**plain text**”
    - neki “command line” mail klijenti na Linuxu
    - još i danas znaju prikazati samo mail koji je u “plain text” formatu
- **svi privici poruci (attachement)**
  - se **kodiraju** metodom “**base 64**”
  - i **dodaju na kraj** tekstualnog dijela **poruke**

Ovo je “Plain text”.  
Sva slova jednako izgledaju  
Nema grafike.  
Svako slovo je 1 Byte.



**base64 encode**





# Kako e-mail poruka izgleda “iznutra”?

Delivered-To: ppale@maja.zesoi.fer.hr

Received: from maja.zesoi.fer.hr ([127.0.0.1])

by localhost (maja.zesoi.fer.hr [127.0.0.1]) (amavisd-new, port 10024)

with ESMTTP id WuKEIzdOXP5t for <ppale@maja.zesoi.fer.hr>; Sun, 9 Oct 2016 19:14:12 +0200 (CEST)

Received: from vlasta1.WIN.LSS.HR ([2002:a135:400a::a135:400a]) by

vlasta1.WIN.LSS.HR ([2002:a135:400a::a135:400a]) with mapi; Sun, 9 Oct 2016 19:15:27 +0200

From: Marko Martinjak <marko.martinjak @lss.hr>

To: Predrag Pale <Predrag.Pale@lss.hr>

CC: "Juraj Petrovic" <juraj.petrovic@fer.hr >

Subject: Logo za Vjestine komuniciranja

Date: Sun, 9 Oct 2016 17:15:18 +0000

Predrag,

Samo ovaj logo imam

[VjeKom-logo-25%.png]

u prilogu je veliki logo.

Marko

# Slike unutar poruke ...

--\_005\_FEF4C524D59556418993C16A5A3CA70E0196D4F91CDBvlasta1WINL\_

Content-Type: **image/png;** name="image001.png"

Content-Description: image001.png

Content-Disposition: **inline;** filename="image001.png"; size=1292;

creation-date="Sun, 09 Oct 2016 17:15:26 GMT";

modification-date="Sun, 09 Oct 2016 17:15:26 GMT"

Content-ID: <image001.png@01D22261.790FDAE0>

Content-Transfer-Encoding: **base64**

iVBORw0KGgoAAAANSUhEUgAAABYAAAAUCAYAAACJfM0wAAAAAXNSR0IArs4c6QAAAAAwSF  
xAAADsQBlSsOGwAAABl0RVh0U29mdHdhcmUATWljcm9zb2Z0IE9mZmljZX/tNXEAAASMSUR

...

...

...

1evldTjt/N7e3vE7YJyrzLbTOYKFtDJhAHJcmikisQ8TTGHVtDFqzgOVSQVaFn8mkSfVM4K  
dZx6ESsnoFRfLJcNs1AI/P8AcIcshELwmlwAAAAASUVORK5CYII=

--\_005\_FEF4C524D59556418993C16A5A3CA70E0196D4F91CDBvlasta1WINL\_--

# Privitak (attachement) ...

--\_006\_FEF4C524D59556418993C16A5A3CA70E0196D4F91CDBvlasta1WINL\_

Content-Type: **image/png** name="VjeKom-logo.png"

Content-Description: VjeKom-logo.png

Content-Disposition: **attachment;** filename="VjeKom-logo.png";  
**size=12259;**

creation-date="Sun, 09 Oct 2016 17:15:15 GMT";

modification-date="Sun, 09 Oct 2016 17:11:11 GMT"

Content-Transfer-Encoding: **base64**

iVBORw0KGgoAAAANSUhEUgAAAIIsAAACACAYAAAAA73po8AAAAAXNSR0ICQMB9xQAAAA1wSF  
EgAAFxIBZ5/SUGAAABl0RVh0U29mdHdhcmUATWljcm9zb2Z0IE9mZmljZX/tNXEAAC9jSU  
7V15fFNV9mccdXRmHMD11HF+47gwLuNa9jRL2wChpEuSppRV2QoIlCZpSAWhyAiCrAVEEB

...

...

LEFFdcT9E+RIq9ZG0Qjoz+k5qD5e8hmGSDjOuuF7YOfrx9H78yQ7doanJ5yAim12glJ58d  
xks0/XlSY+TrImuNlmim5yNe5Pk/zZszNbsCP9oviAYEx4aC5YaW/wecj2OulPpylAAAAAB  
rkJggg==

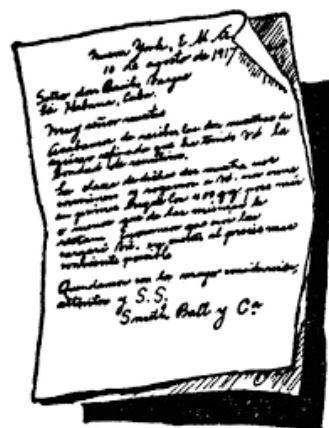
--\_006\_FEF4C524D59556418993C16A5A3CA70E0196D4F91CDBvlasta1WINL\_

# Potvrda predaje i prijema poruke

- za svaku poruku (ili za sve poruke) koje šaljete **moguće je uključiti**
- **potvrdu predaje** poruke (*delivery receipt*)
  - potvrdu će vam poslati **poslužitelj**
    - na kojem je sandučić primatelja
  - **automatski**, čim primi poruku
  - i primatelj to **ne može spriječiti**
- **potvrdu prijema** poruke (*read receipt*)
  - mail klijent primatelja će od njega tražiti da potvrdi da je pročitao poruku
    - u trenutku dok čita poruku
  - primatelj to **može zaobići**
    - iako **neki mail klijenti** imaju postavku da se potvrda šalje automatski, **bez pitanja korisnika**







# SADRŽAJ

# A sadržaj? Učinkovita poruka:

- pazite na **oslovljavanje** primatelja
  - Poštovani ...
- uvijek se primjereno **potpišite**
  - puno ime i prezime
  - funkcija
    - student, voditelj projekta, predsjednik udruge, član tima ...
- **Subject:** neka privuče pažnju i bude jasan
- **ne očekujte da** primatelj
  - **zna** (sjeti se) **tko ste**
  - samo zbog Vaše funkcije **zna o čemu je riječ**
  - **prati medije** i zna što se događa
- budite **ljubazni**
  - poštuju primateljevo vrijeme
  - i činjenicu da prima puno poruka
- budite **strpljivi** čekajući odgovor
  - nikad ne očekuje odgovor za nekoliko sati ili minuta!



- **5 obveznih dijelova** poruke
  - kad se obraćate po prvi put
  - ili nakon jako dugog vremena
  - ili u potpuno novoj ulozi
    - vašoj ili primateljevoj



# Oslovljavanje primatelja – prvi put

Poznata „VI“ osoba	Poštovani gospodine Horvat, Poštovani Hrvoje,	Dear Mr. Smith, Dear John,
Nepoznati	Poštovani gospodine Poštovana gospođo Poštovani,	Dear Mr. Dear Ms. (umjesto Mrs. ili Miss) Dear Madam or Sir
Bilo tko nadležan	Poštovani,	To whom it may concern
Prof.dr.sc.	Poštovani profesore Poštovani profesore Horvat Profesore (u drugoj i ostalim porukama u nizu)	Dear Professor Dear Professor Smith Professor Smith
Dr.sc. PhD	Poštovani doktore Poštovani doktore Horvat Doktore Horvat	Dear doctor Smith

Ako se potpiše formalno	Nastavite kao i prvi put	
Ako <b>imate</b> neformalni odnos i ako se potpiše samo imenom	Profesore, Doktore, Gospodine Horvat	Professor, Doctor, John,
Ako <b>nemate</b> neformalni odnos (velika razlika u godinama ili statusu) čak <b>iako</b> se potpiše imenom	Poštovani profesore Poštovani profesore Horvat	Dear Professor Dear Professor Smith Professor Smith





# Pet obveznih dijelova poruke

- primatelju morate **kratko i nedvojbeno** objasniti:

1. tko je **on**

- u kojoj **njegovoj ulozi** mu se obraćate
  - (vaš) profesor, ima informaciju, ugled, novac ...

2. tko ste **vi**

- njegov student, zainteresiran, voditelj tima ...

3. o čemu je riječ

- organizirate predavanja, trebate sponzora, tražite posao ...

4. što **želite**

- da održi predavanje, financira, da informaciju ...

5. što da **napravi** ako se slaže: neka ...

- **dođe** DD.MM.GGG u HH:MM na lokaciju XYZ
- **uplati** KKK kuna na račun broj RRRR
- **predloži** termin sastanka
- ...



**Napišite** to kao **uputu** koju primatelj može dati ili pokazati svom **pomoćniku** koji će to onda izvršiti.

# Primjer dobre poruke

Poštovani akademice,

- 1 vjerujemo da nema mnogo onih kojima nije poznat **Vaš rad** na teoriji repunziranja.
- 2 Mi smo **udruga** za **promicanje znanosti kod mladih**.
- 3 Organiziramo susrete **mladih s hrvatskim vrhunskim znanstvenicima**.  
Smatramo da **osobni kontakt** najbolje može motivirati mlade.
- 4 Mislimo da bi bilo jako korisno, a nama bi bila velika čast, kad biste imali interesa i vremena **održati predavanje** u okviru naše ljetne škole.
- 5 Ako biste mogli, molimo Vas da nam **javite datum i vrijeme** kad bi Vam najviše odgovaralo da održite predavanje u periodu 15.-19. lipnja.

S poštovanjem,

Anja Radišić

Predsjednica udruge Repunzel







- što ako će primatelju **trebati više informacija**, da donese **odluku**, da **djeluje**?
- možete ih **staviti u prilog** (*eng. attachment*)
  - radije u **više manjih** datoteka, nego jedna “enciklopedija”
  - pazite **da ne pretrpate** primateljev sandučić
  - pazite da **prilog nije prevelik** (1MB, 2MB, ...)
- ali je **bolje** u tekst poruke **staviti poveznice** (*eng. link*) na prava mjesta
  - pazite da ne pretjerate!



# Što napisati u “Subject:” ?

- u mail klijentima, u popisu poruka se vidi samo:

- pošiljatelj
- datum slanja i
- “Subject:”

	Tomislav Žganec	RE: vjekom.her.hr	čet 6.10.2016 15:21
	Matija Matoković	još novosti	čet 6.10.2016 16:04
	Dino Bartošak	Re: Vještine komuniciranja	čet 6.10.2016 16:09
	Vesna Kezdorf	FW: materijali za INU	čet 6.10.2016 16:55
	goran Popović	Detekcija boja	čet 6.10.2016 19:34
	Nikola Banić	RE: Detekcija boja	čet 6.10.2016 20:19

- o sadržaju “Subject:” polja ovisi **hoće li primatelj otvoriti** poruku i početi ju čitati

- stoga, iz njega **mora biti jasno**

- o čemu je riječ
- što se od primatelja očekuje

- primjeri

- **zamolba za predavanje** o repunziranju
- udruga za vrtne patuljke **treba novčanu pomoć**
- student cinguliranja treba **više informacija**
- ...

Ako mislite da će “otkrivanje” što tražite smanjiti šansu da primatelj otvori mail, onda pokušajte privući pažnju:

- “Serija predavanja o repunziranju”
- “Predavanja za napredne učitelje”
- “Sjajni rezultati udruge za vrtne patuljke”
- “Dodatne informacije o cinguliranju”



# Emocije u e-mailu - emotikoni

- E-mail poruka je **komunikacijski štura**

- nema **naglasaka**

- nema **emocija**

- pokušaj dopune su emotikoni (“smajlići” eng. *smile*)

- ☺ ☹

- koristite ih **štedljivo**

- i samo osnovne: ☺ ☹

- jer rijetki razumiju ostale, naročito ako nisu grafičke, već

;-) :) :-) :D :-P :-D :D :-P :-O

- ne dopustite rasplamsavanje emocija u e-mail porukama jer onda najčešće **dolazi do nesporazuma**

- upotrijebite telefon ili Skype





- Moji su klijenti daleko od Zagreba
  - Istočna obala Amerike je na -6h, zapadna obala na -9h
  - kad je njima jutro, oko 8-10h prije podne, nama je to oko 14-16h ili 17-20h
  - Malen broj radnih sati u danu nam se preklapa, pa je komunikacija asinkrona.
- Na primjer, završavaš s poslom oko 18h, klijent još nije ni došao na posao, a tebi je bas bitno izvuci informacije iz njega kako bi znao što raditi idući dan.
- Pošalješ klijentu e-mail s pitanjima i očekuješ da te sutra čeka e-mail s odgovorima
  - Klijent ce imati cijeli dan za odgovoriti ti na taj e-mail
- Bitno je taj e-mail zato napisati kvalitetno
  - da nema dvostrukog značenja, da klijent shvati sto ga ti zapravo tražiš, s kojim informacijama raspolažeš
  - Tu želite izbjeći da vas ujutro čeka e-mail od klijenta s brdom pitanja, jer vas nije dobro shvatio
  - Izgubit ćete cijeli novi dan kako bi se razjasnilo što se uopće treba raditi.
- Napiši sve činjenice bitne za problem/pitanja koja imaš za klijenta.
  - Nemojte imati pretpostavke i ne napisati neke stvari, samo zato jer vi mislite da se one podrazumijevaju
  - Ne mora značiti da i klijent podrazumijeva iste stvari.
- Na primjer, ako radiš na klijentskoj mobilnoj aplikaciji, koja trenutno komunicira s develop verzijom servera, a tebe baš zanima nešto u vezi servera
  - naglasi u tom e-mailu da si to i to testirao na develop verziji servera.
- Takve sitnice ne koštaju puno za napisati, a s druge strane smanjuju broj nepoznanica onome tko ih čita. U suprotnom te ujutro može čekati odgovor od klijenta "na kojoj verziji servera si to testirao?", bez odgovora na ijedno tvoje pitanje.

# Brzina komunikacije

- mnogi će vaši **korespondenti** biti “negdje” u svijetu
  - koja je njegova vremenska zona ?
  - kad će on pročitati i odgovoriti ?
  - kad ćete vi pročitati odgovor?
- zato u poruci
  - budite **konkretni**
  - dajte **sve** potrebne **informacije** koje su dovele do vašeg pitanja ili zaključka
- **ne očekujte** odgovor **odmah**, u minutama i satima
  - čak ni od susjeda
  - jer **ne čitaju svi** e-mail na mobitelu
  - **imaju** ljudi i drugog **posla**
  - a ako je vaše pitanje **zaista važno**



**Ako** na odgovor **čekate** koji **dan** ili **tjedan**:

- napravite “**Forward**” svoje poslane poruke na originalnog primatelja (To:)
- i napišite da **samo provjeravate** je li poruka stigla u redu
- **uključite potvrdu** predaje i prijema poruke



# SIGURNOST E-MAIL KOMUNIKACIJE



# Vjerodostojnost E-mail-a

- **SMTP** je 40 godina **star**
- **nije** napravljen s razmišljanjem o **zlouporabi**
- cjelokupna **poruka**
  - i sadržaj i zaglavlje
  - **je otvorena**, u ASCII obliku
- čuva se u datoteci i na poslužitelju i na klijentu
  - **svatko** (s pristupom računalu) **ju može mijenjati**



- **sva polja** u zaglavlju (koja prikazuje klijent) **se mogu falsificirati**

From:            To:            Date:            Subject:



- **jedino rješenje je**
  - **digitalni potpis i**
  - **kriptiranje sadržaja**



# Analiza zaglavlja (*header*) poruke

**Delivered-To:** predrag.pale@gmail.com

**Received:** by 10.64.56.166 with SMTP id b6csp1745238ieq; Sat, 14 Nov 2015 13:34:29 -0800 (PST)

**Return-Path:** <Albert.Zweistein@physics.world.org>

**Received:** from maja.zesoi.fer.hr (maja.zesoi.fer.hr. [2001:b68:16:70::64:3]) by mx.google.com with ESMTP id 200si15266292wmk.102.2015.11.14.13.34.29 for <predrag.pale@gmail.com>; Sat, 14 Nov 2015 13:34:29 -0800 (PST)

**Received-SPF:** neutral (google.com: 2001:b68:16:70::64:3 is neither permitted nor denied by best guess record for domain of

Albert.Zweistein@physics.world.org) client-ip=2001:b68:16:70::64:3;

**Received:** from localhost (localhost [127.0.0.1]) by maja.zesoi.fer.hr (Postfix) with ESMTP id 80195B00C8 for <predrag.pale@gmail.com>; Sat, 14 Nov 2015 22:33:37 +0100 (CET)

**Received:** from maja.zesoi.fer.hr ([127.0.0.1]) by localhost (maja.zesoi.fer.hr [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id YsNLov-uYHD7 for <predrag.pale@gmail.com>; Sat, 14 Nov 2015 22:33:35 +0100 (CET)

**Received:** from pero (dhcp-91.zesoi.fer.hr [161.53.64.91]) by maja.zesoi.fer.hr (Postfix) with SMTP id CC2F0B00BC for <predrag.pale@gmail.com>; Sat, 14 Nov 2015 22:33:35 +0100 (CET)

**To:** Mickey.Mouse@disneyland.org

**From:** joker@joking.com

**Subject:** An offer you can't refuse

**Sender:** Ms.Monneypenny@james.bond.com

**Date:** Thu, 21 May 2060 05:33:29 -0700

**Message-Id:** <20151114213337.80195B00C8@maja.zesoi.fer.hr>

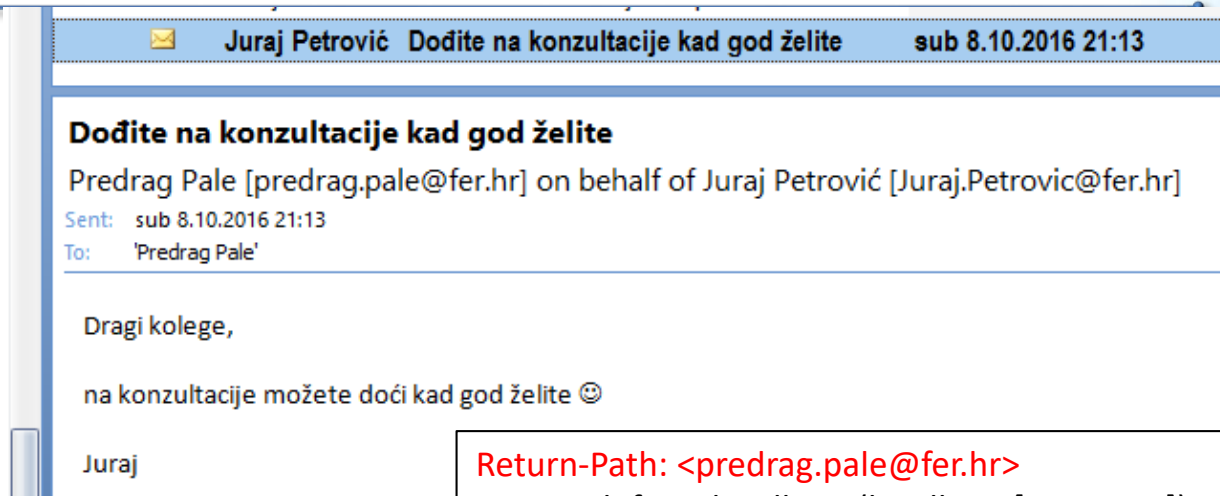
?!

Tražite prvi (najniži na popisu)  
"Received:" zapis.  
To je **PRAVI** pošiljatelj!

# Slanje u ime nekog (legalno)

- “On behalf of” omogućava da
- pomoćnik šalje
  - u ime šefa
- fizička osoba
  - u ime liste
  - funkcionalne adrese

- Iako u zaglavlju poruke piše:
  - From: juraj.petrovic@fer.hr
- nalaze se i:
  - Return-Path: predrag.pale@fer.hr
  - Sender: predrag.pale@fer.hr
- “Reply” na takvu poruku će otići na
  - juraj.petrovic@fer.hr



Return-Path: <predrag.pale@fer.hr>  
Received: from localhost (localhost [127.0.0.1])  
by maja.zesoi.fer.hr (Postfix) with ESMTP  
for <ppale@maja.zesoi.fer.hr>; Sat, 8 Oct 2016 18:56:26 +0000  
Received: from EUR01-DB5-obe.outbound.protection.outlook.com (191.23.253.100)  
by maja.zesoi.fer.hr (Postfix) with ESMTP  
for <Predrag.Pale@lss.hr>; Sat, 8 Oct 2016 18:56:26 +0000  
From: Juraj Petrović <juraj.petrovic@fer.hr>  
Sender: predrag.pale@fer.hr  
To: Predrag Pale <Predrag.Pale@lss.hr>  
Subject: Dođite na konzultacije kad god želite  
Date: Sat, 8 Oct 2016 18:56:26 +0000

Dragi kolege,

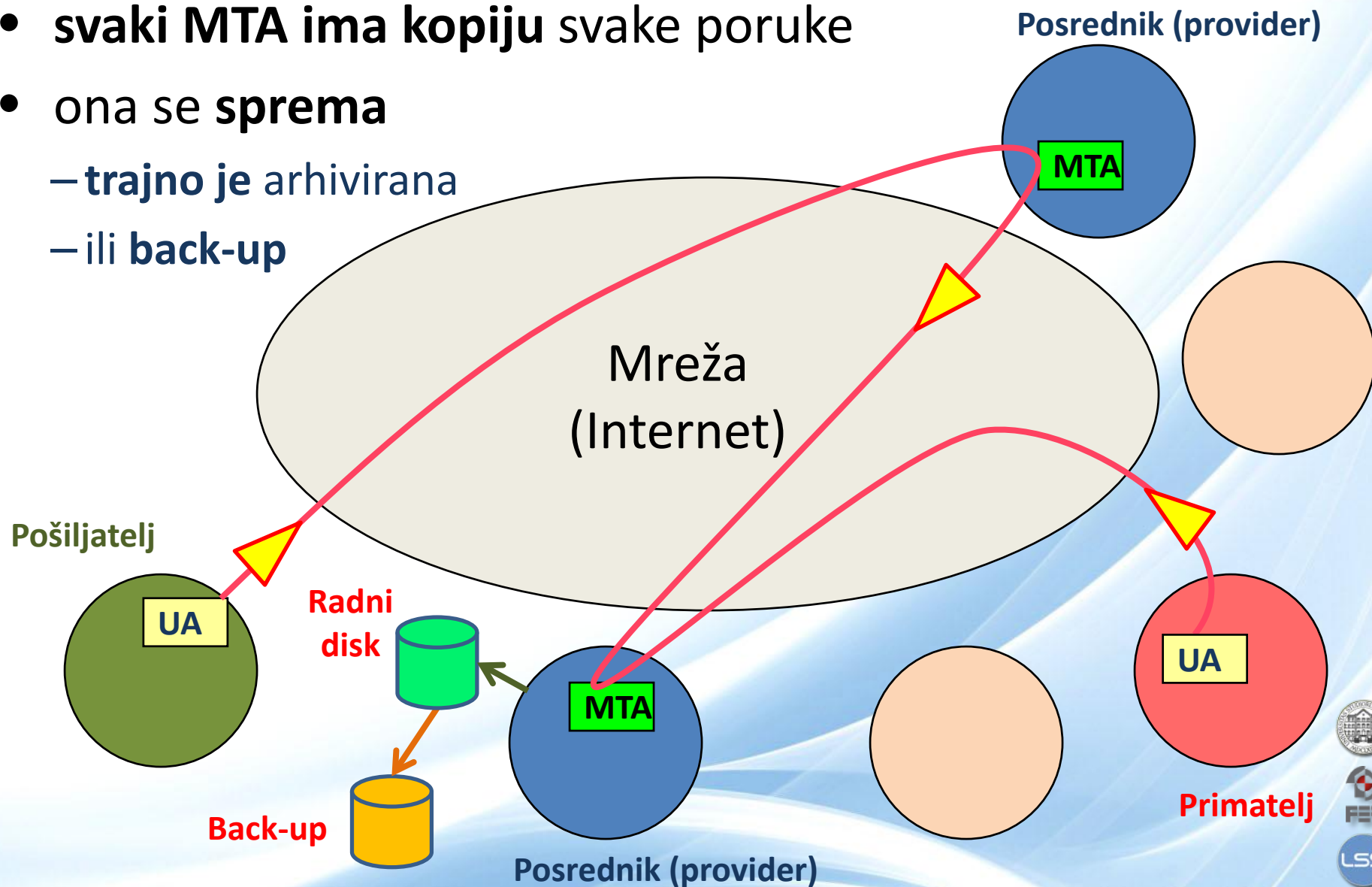
na konzultacije možete doći kad god želite :)

Juraj

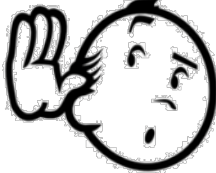


# Sigurnost poruke

- **svaki MTA ima kopiju** svake poruke
- ona se **sprema**
  - **trajno je** arhivirana
  - ili **back-up**





- **e-mail** se prenosi (SMTP) **nezaštićen**
  - kroz sve komunikacijske **putove** i **uređaje**
- **prisluškivanjem** komunikacija 
  - moguće je **vidjeti sadržaj** poruke
- različiti **napadi** na sigurnost sustava (npr. *man-in-the-middle*)
  - mogu i **izmijeniti sadržaj** poruke
- poruka se i **sprema** na svim MTA kroz koje prolazi
  - i završava u **arhivama** i **back-upu**
- kriptografski **postupci** i **alati** omogućavaju
  - **skrivanje** sadržaja
  - **čuvanje integriteta** sadržaja (potpun i neizmijenjen)
  - **jamče autorstvo** poruke
- malo poboljšanje su:
  - HTTPS, POP3S, IMAPS
  - između korisnika i poslužitelja **poruke se prenose kriptirane**



# Kriptografski alati za e-mail

- mail klijenti podržavaju **kriptiranje** i **potpisivanje**
- morate **stvoriti svoj** digitalni **potpis**
  - za svaki vaš e-mail račun treba novi potpis
    - sastoji se od dva uparena (povezana) ključa
  - **javni ključ** dajete svima i oni ga koriste da
    - kriptiraju svoje poruke vama i dekriptiraju vaše koje im šaljete
  - **tajni ključ** dobro čuvate i koristite za
    - dekriptiranje njihovih poruka vama i kriptiranje vaših poruka njima

Javni ključ



Tajni ključ



- najpopularniji alati su:

- S/MIME
- OpenPGP



**S/MIME**  
Secure E-Mail for Everyone

- da biste s nekim **razmjenili kriptiranu poruku**
  - vi trebate njegov, a on treba vaš ključ



- za **razmjenu ključeva** mogu se koristiti

- **komercijalni** servisi
- **polu-komercijalni** (dio usluge besplatan) poput Comodo
- ili **vlastiti** servis poput Kleopatra



- E-mail je **jedino** opće **prihvaćeno sredstvo** službene/**poslovne elektroničke komunikacije**
- E-mail adresa **ne razlikuje velika i mala slova**
- **možete imati vlastitu, vječnu, besplatnu domenu**

*ime-prezime.from.hr*

- **nije svejedno** koga stavljamo u **To:, Cc:, Bcc:**
  - ni korištenje “Reply” i “Reply all”
- **izbjegavati emocije** u porukama
- **5 obveznih dijelova** poruke
- mail klijenti: i web based i desktop
- protokoli **POP3 i IMAP**
- **plain text i HTML**
- pazite na **vremenske zone**
- **poruke se mogu lažirati**
- **poruke je moguće kriptirati**







**VJEKOM@ZESOI.FER.HR**

**PREDRAG.PALE@FER.HR**

