SVEUČILIŠTE U ZAGREBU
Fakultet elektrotehnike i računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2022./2023.

Sigurnost elektroničke pošte

Creative Commons

- **slobodno smijete:**
  - **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
  - **remiksirati** — prerađivati djelo
- **pod sljedećim uvjetima:**
  - **imenovanje**. Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
  - **nekomercijalno**. Ovo djelo ne smijete koristiti u komercijalne svrhe.
  - **dijeli pod istim uvjetima**. Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, preradu možete distribuirati samo pod licencom koja je ista ili slična ovoj.

U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Tekst licencije preuzet je s http://creativecommons.org/.

Incidenti vezani uz elektroničku poštu

- 4 vrste sigurnosnih incidenata
  - neprikladno ponašanje koje nije specifično samo za elektroničku poštu
    - prijetnje, otkrivanje povjerljivih informacija, prevare
  - zlonamjerne poruke s neželjenim posljedicama po računalo korisnika
    - virusi, crvi...
  - zloupotreba usluge
    - spam, hoax
    - društveni inžinjering
  - gubitak privatnosti i anonimnosti
    - web bug
    - kompromitiranje poruka u mreži

Gubitak privatnosti i anonimnosti

- web bug
  - klijent elektroničke pošte prikazuje HTML
  - pošiljatelj može uključiti link na sliku koja kontaktira njegov web-poslužitelj
  - “tko je pročitao mail?”
- kompromitacija poruke
  - *store-and-forward*
  - poruke prolaze kroz niz mail-poslužitelja – vide je svi na putu
  - rješenja:
    - zahvati u infrastrukturi sustava, mreže, usmjeravanja
    - šifriranje s kraja na kraj
      - S/MIME
      - PGP

Simple Mail Transfer Protocol

- definiran je 1982. godine u RFC 821 → RFC 2821 →RFC 5321
- specificira način prijenosa poruka između dva računala
  - ne ovisi o mrežnom protokolu
  - omogućuje prosljeđivanje poruka kroz raznovrsne mreže
- strogo definira sintaksu i redoslijed odvijanja transakcije
  - koristi retke teksta za razmjenu informacija
  - polazno računalo šalje SMTP naredbe, na koje ciljno računalo odgovara kodovima koji mogu označavati uspjeh ili pogrešku
  - svaka naredba pošiljatelja mora dobiti odgovor primatelja
- naredbe
  - obavezne: HELO, MAIL, RCPT, DATA, RSET, VRFY, NOOP, QUIT
  - neobavezne: SEND, SOML, SAML, EXPN, HELP, TURN
- čvorovi
  - MUA (*Mail User Agent*)
  - MTA (*Mail Transfer Agent*)

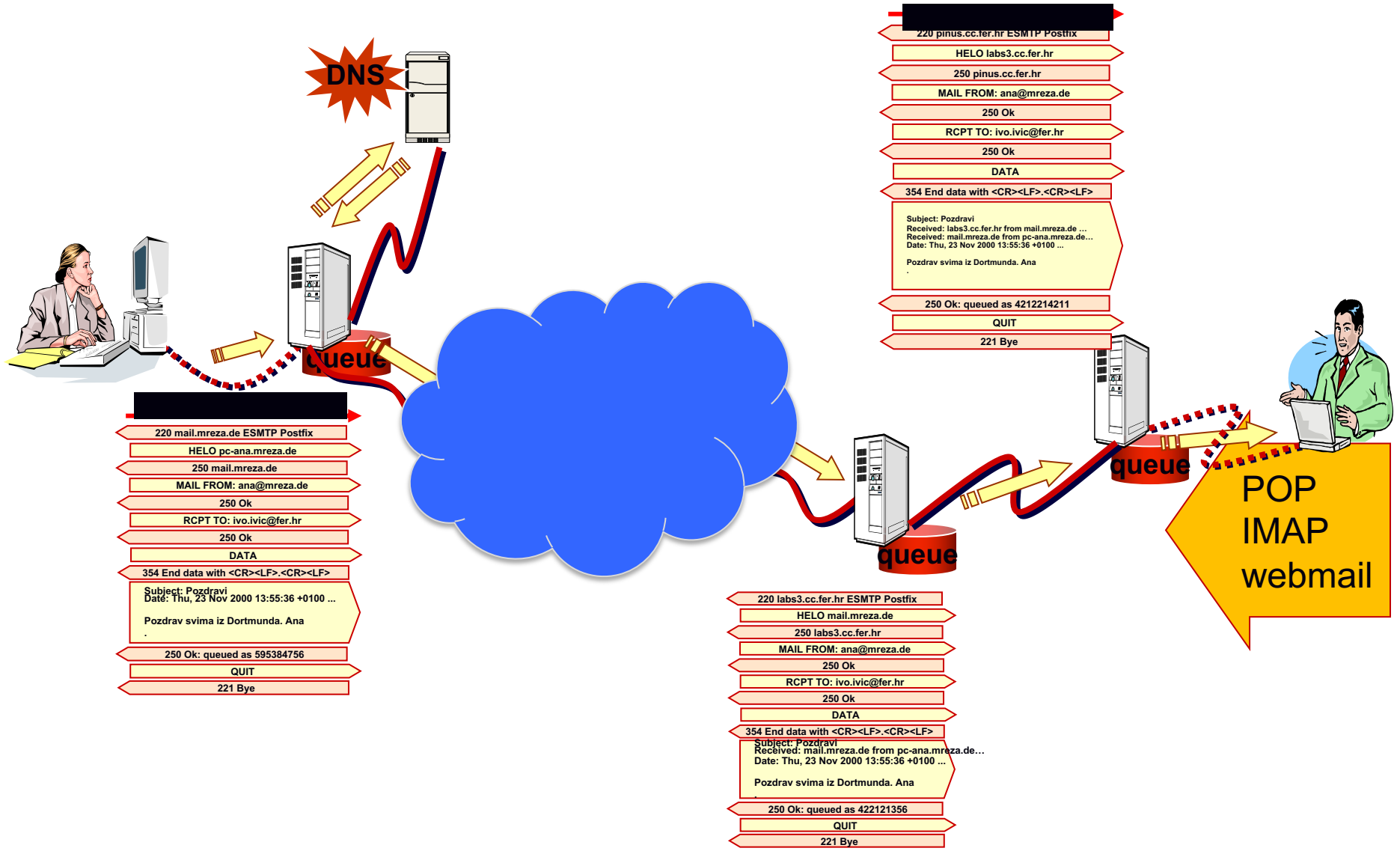
Simple Mail Transfer Protocol - primjer

```
dave@Mint ~ $ telnet 192.168.254.167 25
Trying 192.168.254.167...
Connected to 192.168.254.167.
Escape character is '^]'.
220 smtp-sink ESMTP
HELO localhost
250 smtp-sink
MAIL FROM: sender@domain.com
250 2.1.0 Ok
RCPT TO: recipient@domain.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: This is the subject!
This is the test message body of this email!
.
250 2.0.0 Ok
Quit
221 Bye
Connection closed by foreign host.
```

slika preuzeta: http://dfirdave.blogspot.com/

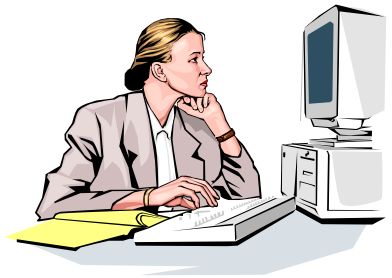
više na: http://www.yuki-onna.co.uk/email/smtp.html

Mehanizam slanja elektroničke pošte



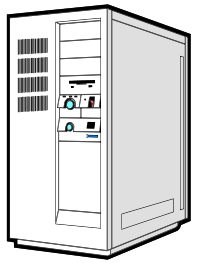
SMTP – komunikacija MUA i MTA

ana@mreza.de



pc-ana.mreza.de

uspostavlja vezu spajanjem na port 25



mail.mreza.de

220 mail.mreza.de ESMTP Postfix

HELO pc-ana.mreza.de

250 mail.mreza.de

MAIL FROM: ana@mreza.de

250 Ok

RCPT TO: ivo.ivic@fer.hr

250 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

Subject: Pozdravi
Date: Thu, 24 Nov 2011 13:55:36 +0100 ...

Pozdrav svima iz Dortmunda. Ana.
.

250 Ok: queued as 595384756

QUIT

221 Bye

From:
ana@mreza.de
To: ivo.ivic@fer.hr
Subject: Pozdrav*i*

Pozdrav svima iz Dortmunda.

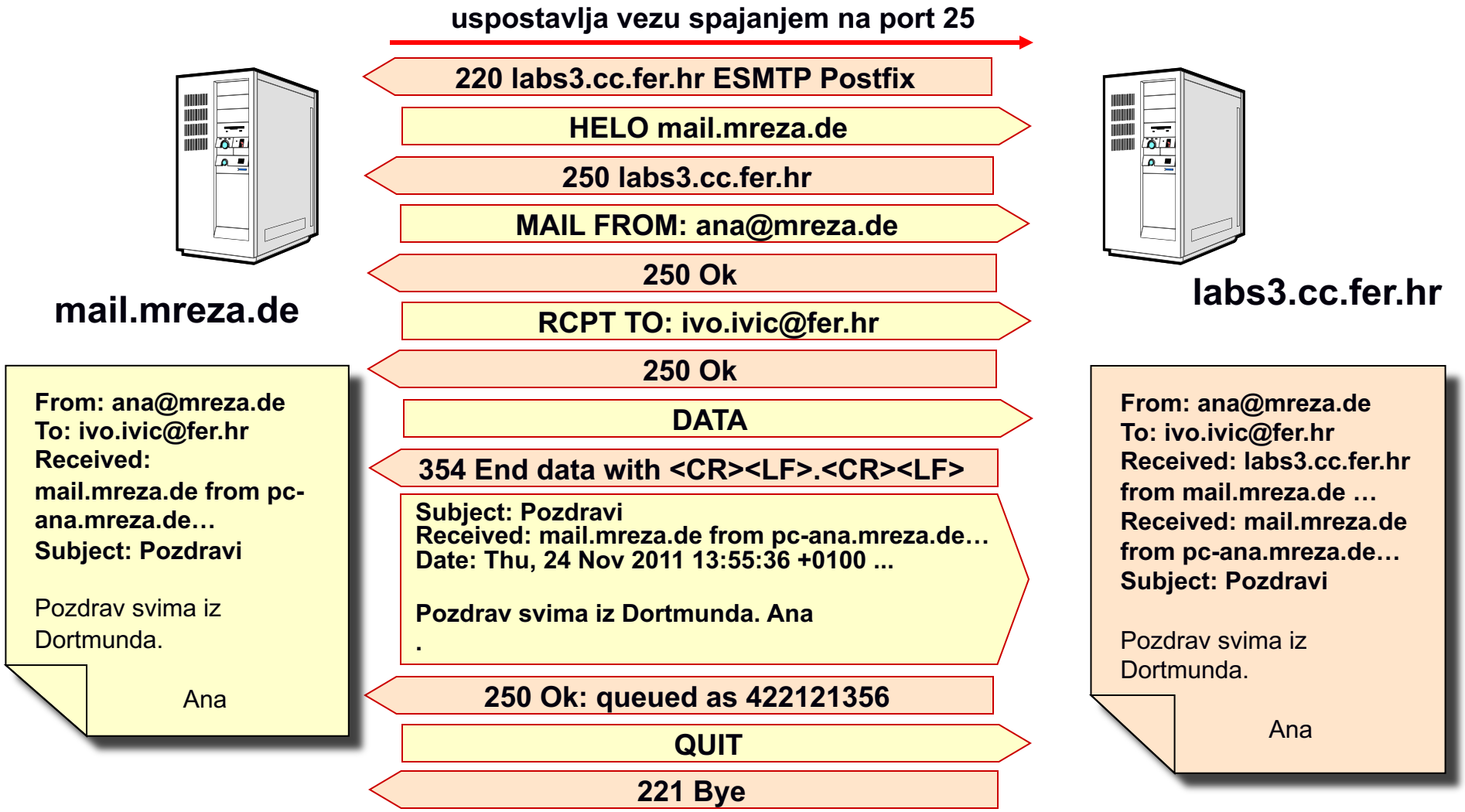
Ana

From: ana@mreza.de
To: ivo.ivic@fer.hr
Received: mail.mreza.de from pc-ana.mreza.de…
Subject: Pozdravi

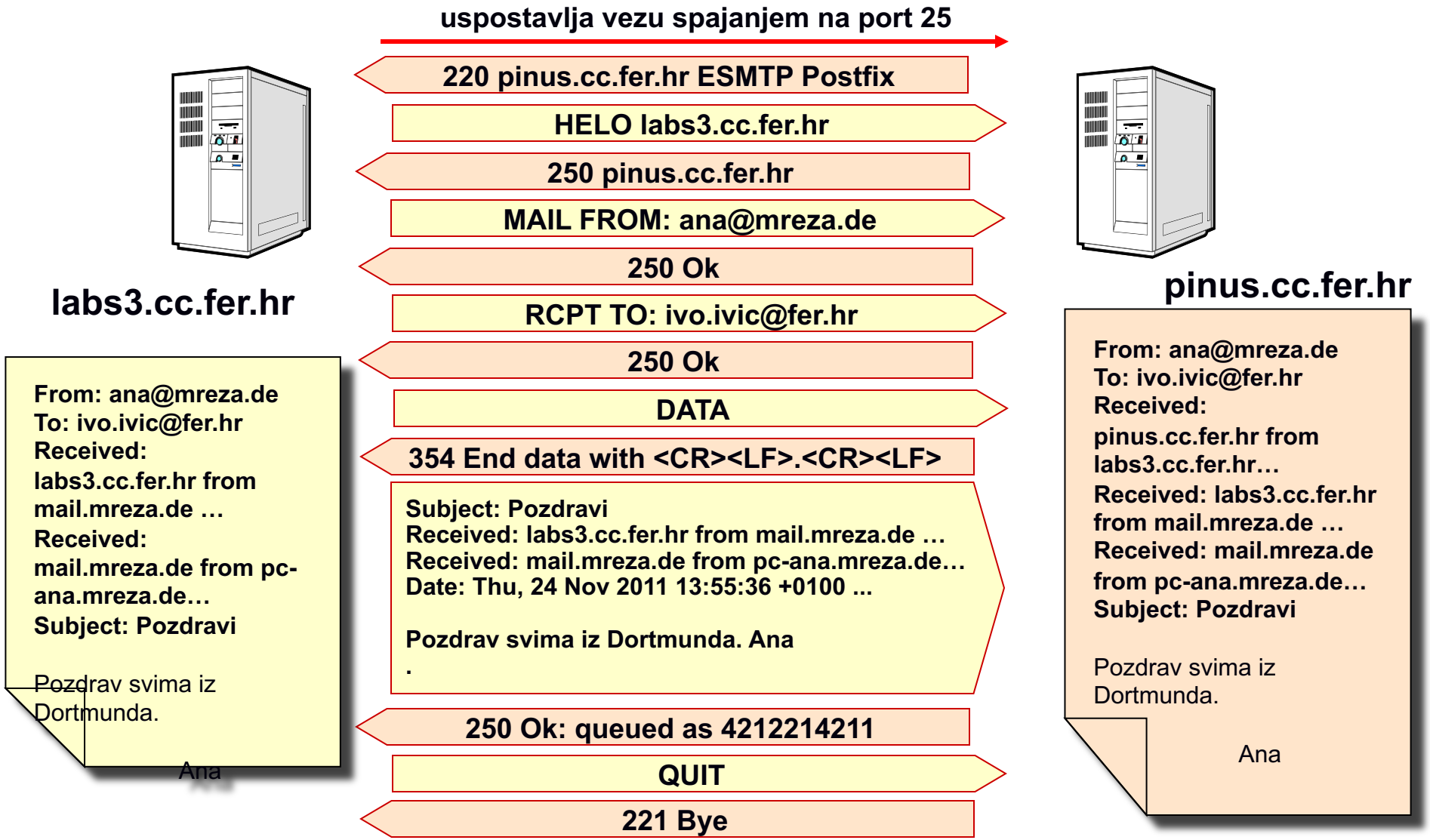
Pozdrav svima iz Dortmunda.

Ana

SMTP – komunikacija MTA i MTA



SMTP – komunikacija MTA i MTA



Sigurnosni problemi SMTP-a

- uopće nema sigurnosnih mehanizama!
- otvoren i u tekstualnom obliku
- nema autentifikacije
- podrazumijeva se povjerenje i suradnja
  - otvoreni mail relay
  - ne provjerava se tko se spaja na poslužitelj
  - prihvaća se pošta za korisnika koji nije na lokalnoj mreži

Borba protiv neželjene pošte

- autentifikacija i reputacija korisnika
- izazov/odgovor
- zaštitne sume
- crne liste temeljene na DNS-u
- striktno pridržavanje RFC-ova
  - mora se čekati odgovor poslužitelja prije slanja podataka
  - sive liste (privremeno se odbacuje pošta koja stiže od nepoznatih SMTP poslužitelja, generira se greška 4xx)
  - provjera sintakse HELO i EHLO
  - višestruki nedohvatljivi MX-zapisi na DNS-u
  - detekcija raskida veze naredbom QUIT
- honeypot
- prepoznavanje uzoraka...

Moguća rješenja problema sigurnosti

- provjera IP adrese klijenta
  - pristup moguć samo onima na popisu
- ograničena upotreba nekih naredbi
  - nakon autentifikacije
- ograničena upotreba naredbi za pristup do korisničkih adresa
  - EXPN, VRFY – je li adresa ili lista valjana? - SPAM!
- provjera valjanosti podataka u zaglavljima
  - envelope, MAIL From:
- ograničenje veličine poruke
- ograničenje broja poruka u zadanom vremenu
- vođenje logova

- većina ovih rješenja nisu dio standarda SMTP

Autentifikacija korisnika

- POP-before-SMTP ili SMTP-after-POP
  - poruke je moguće slati tek nakon “dokaza” da ih se može i preuzeti
- SMTP-AUTH (RFC 2554) – port 587
  - pregovaranje oko protokola – nove naredbe
- ESMTP (RFC 5321 + RFC 5336)
  - Simple Authentication and Security Layer - SASL
- Microsoft: Secure Password Authentication – SPA putem SMTP-AUTH

- ne pomažu u rješavanju spama!
- zamjena SMTP-a nije praktična

Extended SMTP – ekstenzije

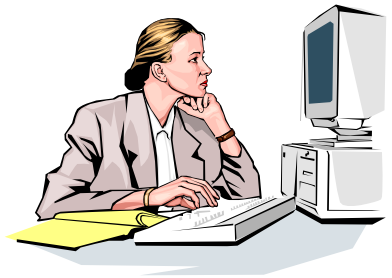
- 8BITMIME — 8-bitni prijenos podataka, RFC 1652
- ATRN — autentificirani TURN za On-Demand Mail Relay, RFC 2645
- SMTP-AUTH — autentificirani SMTP, RFC 4954
- CHUNKING — cjepkanje velikih poruka, RFC 3030
- DSN — obavijest o dostavi, RFC 3461
- ETRN — udaljeni TURN, RFC 1985
- HELP — pomoć, RFC 821
- PIPELINING — slanje više naredbi odjednom, RFC 2920
- SIZE — deklaracija veličine poruke, RFC 1870
- STARTTLS — Transport layer security, RFC 3207
- UTF8SMTP — korištenje UTF-8 u zaglavljima, RFC 5336

SMTP-AUTH – primjer komunikacije

```
S: 220-smtp.example.com ESMTP Server
C: EHLO client.example.com
S: 250-smtp.example.com Hello client.example.com
S: 250-AUTH GSSAPI DIGEST-MD5
S: 250-ENHANCEDSTATUSCODES
S: 250 STARTTLS
C: STARTTLS
S: 220 Ready to start TLS ... nastavlja se šifrirana
komunikacija...
C: EHLO client.example.com
S: 250-smtp.example.com Hello client.example.com
S: 250 AUTH GSSAPI DIGEST-MD5 PLAIN
C: AUTH PLAIN dGVzdAB0ZXN0ADEyMzQ=
S: 235 2.7.0 Authentication successful
```

Mail Relay

*.dsl.t-com.hr



uspostavlja vezu spajanjem na port 25

220 mail.tel.fer.hr ESMTP Postfix

HELO gazda.predsjednik.hr

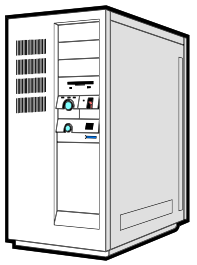
250 mail.tel.fer.hr

MAIL FROM: kolinda@predsjednik.hr

250 Ok

RCPT TO: trump@whitehouse.gov

550 Relaying Denied



mail.tel.fer.hr

From: kolinda@predsjednik.hr
To: trump@whitehouse.gov
Subject: Pozdravi

Dragi kolega, primite puno pozdrava od ...

mail.tel.fer.hr prihvaća poštu samo:

- od lokalnih korisnika za vanjske korisnike
- od vanjskih korisnika za lokalne korisnike
- od lokalnih korisnika za lokalne korisnike

lokalno: *@tel.fer.hr

Povjerljivost komunikacije

S/MIME

Kako osigurati povjerljivost

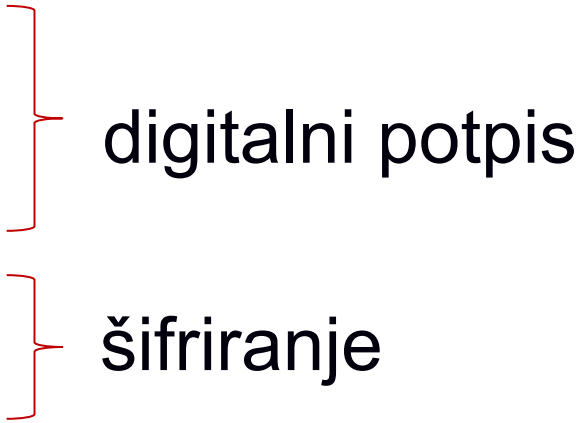
- s kraja na kraj?
- od čvora do čvora?
- nekoliko raznih rješenja
  - Privacy-enhanced Electronic Mail – PEM (RFC 1421-1424)
    - nije zaživjelo, ovisilo o PKI s jednim korijenom
    - nametanje središnjeg autoriteta
  - Pretty Good Privacy – PGP
    - Web of Trust – PKI
    - OpenPGP, GnuPGP
  - proširenja standarda MIME
    - Mime Object Security Services – MOSS (RFC 1848)
    - S/MIME (RFC 5751)

S/MIME

- sigurnosno proširenje standarda MIME
  - Multipurpose Internet Mail Extension
- nije ograničeno samo na elektroničku poštu!
  - koristi se i za druge protokole – npr. HTTP
- komercijalna primjena i poslovni svijet
  - korisnicima za osobnu upotrebu “bolji” PGP
- povijest:
  - S/MIME v1, 1995. – RSA Security, Inc.
  - S/MIME v2, 3/1998. – informativni RFC 2311 i 2312
  - S/MIME v3, 6/1999. – IETF S/MIME Email Security WG – RFC 2630-2634
    - 9/2009 - RFC 5652 - CMS
    - 1/2010 - RFC 5751 – v3.2

Usluge kriptozaštite koje nudi S/MIME

- autentifikacija
- cjelovitost poruke
- neporecivost
- privatnost
- sigurnost podataka



- no, što je MIME?
  - *Multipurpose Internet Mail Extensions*

Zašto je potreban MIME?

- RFC 822 definira format elektroničke poruke
  - kasnije RFC 2822, 5322
- ograničenja formata elektroničke pošte prema RFC 822:
  - prijenos binarnih datoteka (npr. izvršnih)
  - duljina retka 1000 znakova (998 + CR-LF)
  - poruke pisane nacionalnim jezicima (samo 7-bitni ASCII)
  - prijevod iz ASCII u EBCDIC
  - neke implementacije ne drže se specifikacije iz RFC 822
- ograničenja SMTP-a
  - odbijaju se prevelike poruke
  - mijenja, briše ili mijenja raspored CR/LF
  - reže ili cijepa retke duže od 76 znakova
  - miče tabove i razmake na kraju retka ili poruke
  - dopunjava retke da budu iste veličine
  - pretvara tab u razmake

Standard MIME

- omogućuje:
  - korištenje svih znakova, uključivo i 2-oktetne znakove (istočnjačka pisma)
  - definiranje strukture poruke i vrste poruke
  - dodavanje jedne ili više binarnih, HTML ili višemedijskih datoteka u poruku (paziti na duljinu takvih poruka – RFC 1870)
  - nije u konfliktu sa specifikacijama u RFC 821 i 822
  - neki dijelovi standarda MIME mogu se koristiti i za druge primjene (HTTP)
- jedini zahtjev
  - klijent mora biti kompatibilan sa standardom

Korištenje standarda MIME

- uvodi se 5 novih polja u zaglavlje poruke
  - daju dodatnu informaciju o tijelu
- definirani su formati sadržaja
  - standardizira se reprezentacija sadržaja i daje podrška za višemedijske poruke
- definiraju se metode kodiranja pri prijenosu
  - čuvaju sadržaj od mogućih promjena tijekom prijenosa

- MIME standardizira način na koji se upravlja informacijama i sadržajem u višemedijskoj okolini

Nova zaglavlja

- MIME-Version `[MIME-Version: 1.0 ]`
  - verzija MIME standarda, trenutno samo 1.0 (RFC 2045, 2046)
- Content-Type `[Content-Type: text/plain; charset=UTF-8]`
  - opisuje vrstu podataka u pojedinom MIME entitetu (tip i podtip)
- Content-Transfer-Encoding `[Content-Transfer-Encoding: quoted-printable]`
  - definira način kodiranja podataka u MIME poruci
- Content-ID `[Content-ID: <E796FD66-8942-41B1-9C78-BAA583C156FD>]`
  - jednoznačno definira MIME entitet, slično kao Message-ID: poruku
- Content-Description `[Content-Description: slicica]`
- dodatno Content-Disposition `[Content-Disposition: attachment; filename="file.pdf"]`
  - definira kako treba tretirati MIME entitet, kao dio poruke (inline) ili vanjski dodatak (attachment), tek od RFC 2183

Primjer zaglavlja MIME

```
...
MIME-Version: 1.0
Content-Type: multipart/mixed;
       boundary="----=_NextPart_000_002F_01C1C57E.29CC71A0"

This is a multi-part message in MIME format.

------=_NextPart_000_002F_01C1C57E.29CC71A0
Content-Type: multipart/alternative;
       boundary="----=_NextPart_001_0030_01C1C57E.29CC71A0"

------=_NextPart_001_0030_01C1C57E.29CC71A0
Content-Type: text/plain;
       charset="iso-8859-2"
Content-Transfer-Encoding: quoted-printable
...
```

Content-Type: tipovi i podtipovi podataka

Tip	Podtip	Content-Type
Text	Plain, enriched, html	text/plain, text/enriched, text/html
Image	Jpeg, tiff, gif	image/jpeg, image/tiff, image/gif
Audio	Basic, mpeg	audio/basic, audio/mpeg
Video	Mpeg, quicktime	video/mpeg, video/quicktime
Application	Octet-stream, postscript, pdf, zip, msword	application/pdf, application/zip
Message	Rfc822, partial, external-body	message/rfc822, message/partial
Multipart	Mixed, alternative, digest, parallel	multipart/mixed, multipart/digest

Multipart

- omogućuje da se u tijelu jedne poruke šalje više MIME entiteta
- dijelovi su odvojeni graničnim nizom znakova koji je definiran u zaglavlju glavne poruke

```
Content-Type: multipart/mixed; boundary=zxf918

This is a MIME-encapsulated message.

--zxf918
Body part1
--zxf918
Body part2
--zxf918--
```

Content-Transfer-Encoding

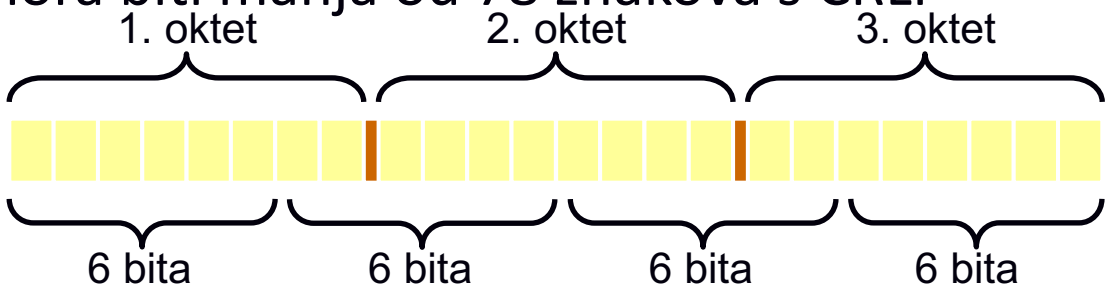
- 7bit
  - poruka se sastoji od linija ne dužih od 998 okteta 7-bitnih podataka, koji završavaju s CRLF
- 8bit
  - poruka se sastoji od linija ne dužih od 998 znakova, koji završavaju s CRLF
- binary
  - poruka se sastoji od niza 8-bitnih znakova bez ograničenja na duljinu linije ili dozvoljene znakove
- quoted-printable
  - uglavnom ASCII, prepoznatljivo
- base64
  - ASCII, neprepoznatljivo

Content-Transfer-Encoding: quoted-printable

- ako su podaci koji se kodiraju većinom 7-bitni ASCII znakovi, kodirani oblik ostaje većinom razumljiv čitateljima
  - svaki posebni znak može se zamijeniti s odgovarajućim dvoznamenkastim heksadecimalnim ekvivalentom tako da se ispred njega doda znak “=“
  - linije ne smiju biti dulje od 76 znakova (+ CRLF)
- kompromis između čitljivosti, učinkovitosti i robustnosti
- nije striktno definiran i postoje odstupanja u izvedbama
- Elektronička pošta -> Elektroni=C4=8Dka po=C5=A1ta

Content-Transfer-Encoding: base64

- Content-Transfer-Encoding: base64
  - koristi se podskup US-ASCII (7-bitnih) znakova koji sadrži 65 znakova
  - grupe od 3 okteta kodiraju se u 4 znaka (svaki znak 6 bitova)
  - duljina linije mora biti manja od 78 znakova s CRLF



GIF89 (71 73 70 56 57 : decimal)

01000111 01001001 01000110 00111000 00111001 (Octet stream)

010001 110100 100101 000110 001110 000011 1001

010001 110100 100101 000110 001110 000011 100100

17 52 37 6 14 3 36

R 0 1 G O D K

R01GODK=

"Non ASCII" znakovi u zaglavljima

- postoje tehnike kojima se omogućuje kodiranje ne-ASCII teksta u zaglavljima prema RFC 822
- =?charset?encoding?text?=
  - charset: us-ascii, iso8859-1 do iso8859-9
  - encoding: B ili Q
    - Q: inačica quoted-printable kodiranja, space se kodira s _
    - B: kodiranje prema base64
  - text: niz ASCII znakova koji se podvrgava pravilima kodiranja
- kodirana riječ ograničena je na 75 znakova
    - From: =?iso-8859-2?Q?Alen_Ba=BEant?= <alen.bazant@fer.hr>
    - From: =?iso-8859-2?Q?Martina_Jel=E8i=E6?= <martina.jelcic@fer.hr>
    - Subject: =?euc-kr?B?x9Gx28GmuPEgKE1JTUUgdGVzdCk=?=

Zaključno o standardu MIME

- neizbježan pri prijenosu podataka Internetom
- objektno-orijentirana struktura poruke po standardu MIME omogućuje mu da bude višenamjenski standard
- primjenom standarda MIME moguće je prenositi poruke između sustava koji koriste različite formate

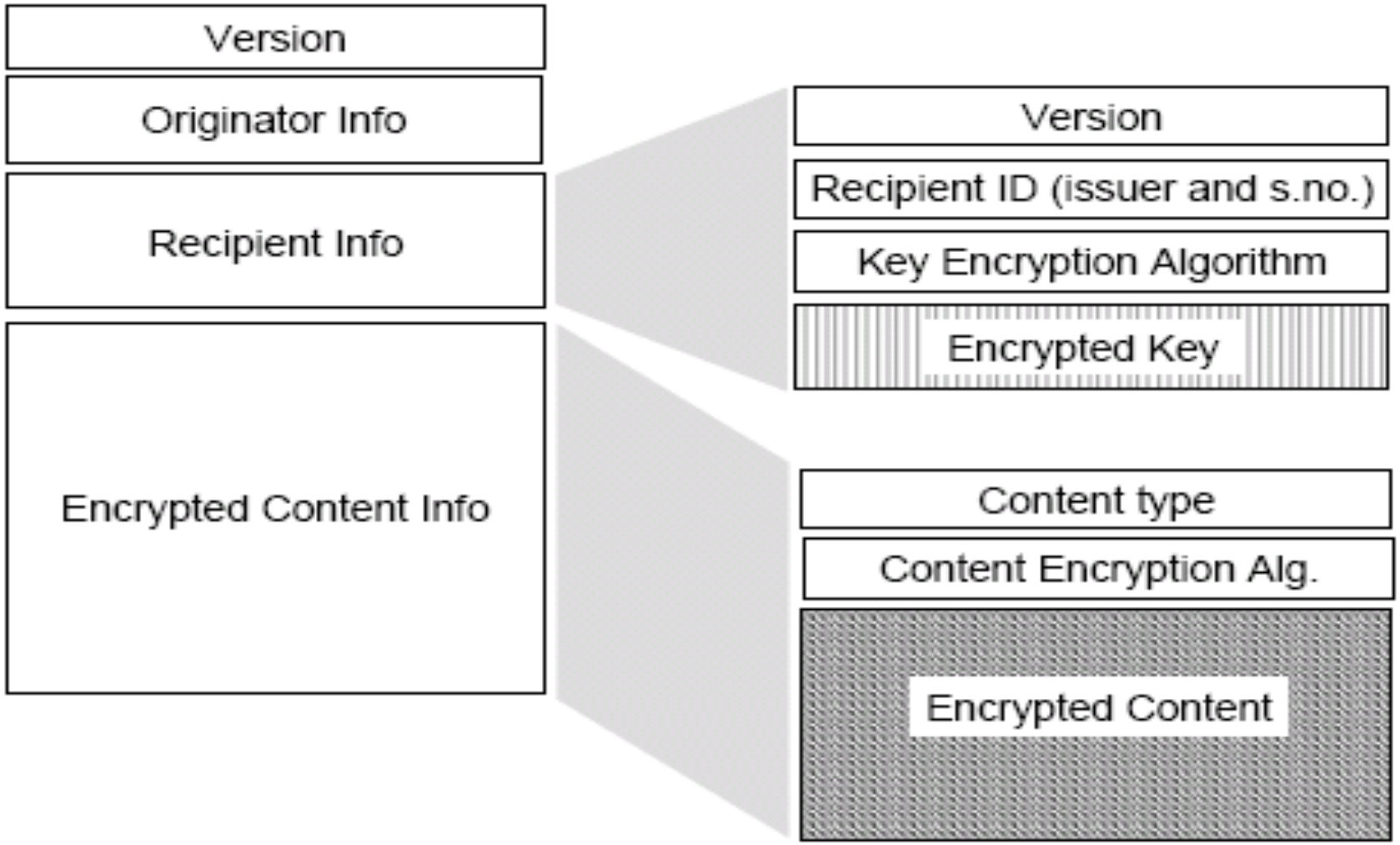
Cryptographic Message Syntax

- S/MIME se temelji na Cryptographic Message Syntax (CMS)
  - RFC 5652 (ali i RFC 5911 – ASN.1)
  - standard IETF-a za prijenos šifriranih poruka
  - digitalni potpis, sažetak, autenfitikacija, šifriranje bilo kojeg oblika podataka
  - temeljen na sintaksi standarda RSA Security (PKCS#7)
- arhitektura temeljena na upravljanju ključevima i certifikatima

Funkcije: *enveloped-data*

- šifrirani sadržaj bilo kojeg tipa i šifrirani ključevi za jednog ili više korisnika
  - digitalna ovojnica
- način rada:
  - stvara se jednokratni ključ za šifriranje za RC2/40 ili DES
  - taj se ključ šifrira za svakog primatelja njegovim javnim ključem
  - sve potrebne informacije (certifikat pošiljatelja, algoritam, šifrirani ključ) pohrane se u vrijednost *RecipientInfo*
  - sadržaj se šifrira jednokratnim ključem za šifriranje (moguće uz *padding*)
  - vrijednosti *RecipientInfo* za sve primatelje prikupe se i uz šifrirani sadržaj postave u vrijednost *EnvelopedData*
- funkcija osigurava privatnost i sigurnost podataka

Enveloped data



Primjer šifrirane poruke

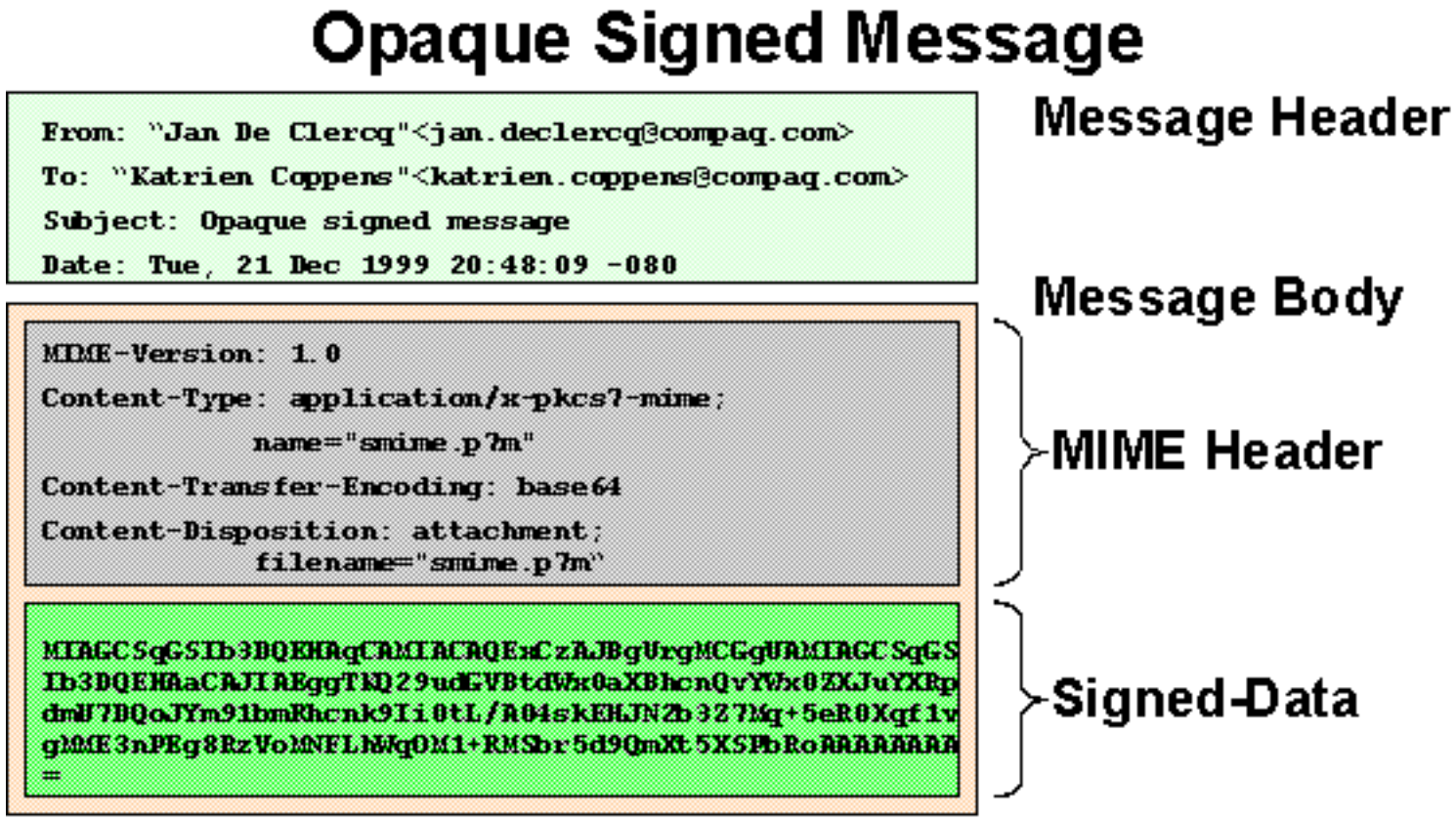
```
Content-Type: application/pkcs7-mime;
      smime-type=enveloped-data;
      name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQ
pfyF467GhIGfHfYT67n8HHGghyHhHUujhJh4VQpf
yF467GhIGfHfYGTrfvbnjT6jH7756tbB9Hf8HHGT
rfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghy
HhHUujpfyF4 0GhIGfHfQbnj756YT64V
```

Funkcije: *signed-data*

- sadržaj bilo kojeg tipa + jedan ili više digitalnih potpisa
  - obično jedan sadržaj + jedan potpis
- digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja
  - moguće i više potpisnika, paralelno
  - podaci o potpisniku (certifikat, identifikator algoirtma, šifrirani sažetak) pohranjuju se u vrijednost *SignerInfo*
- sadržaj i sažetak (saželi) kodiraju se prema base64 u vrijednost SignedData
- funkcija osigurava autentičnost, cjelovitost i neporecivost
- korisnik mora podržavati S/MIME za čitanje i verificiranje potpisa

Signed data



http://windowsitpro.com/exchange-server/advanced-security-exchange-2000-part-2

Potpisana poruke: application/pkcs7-mime

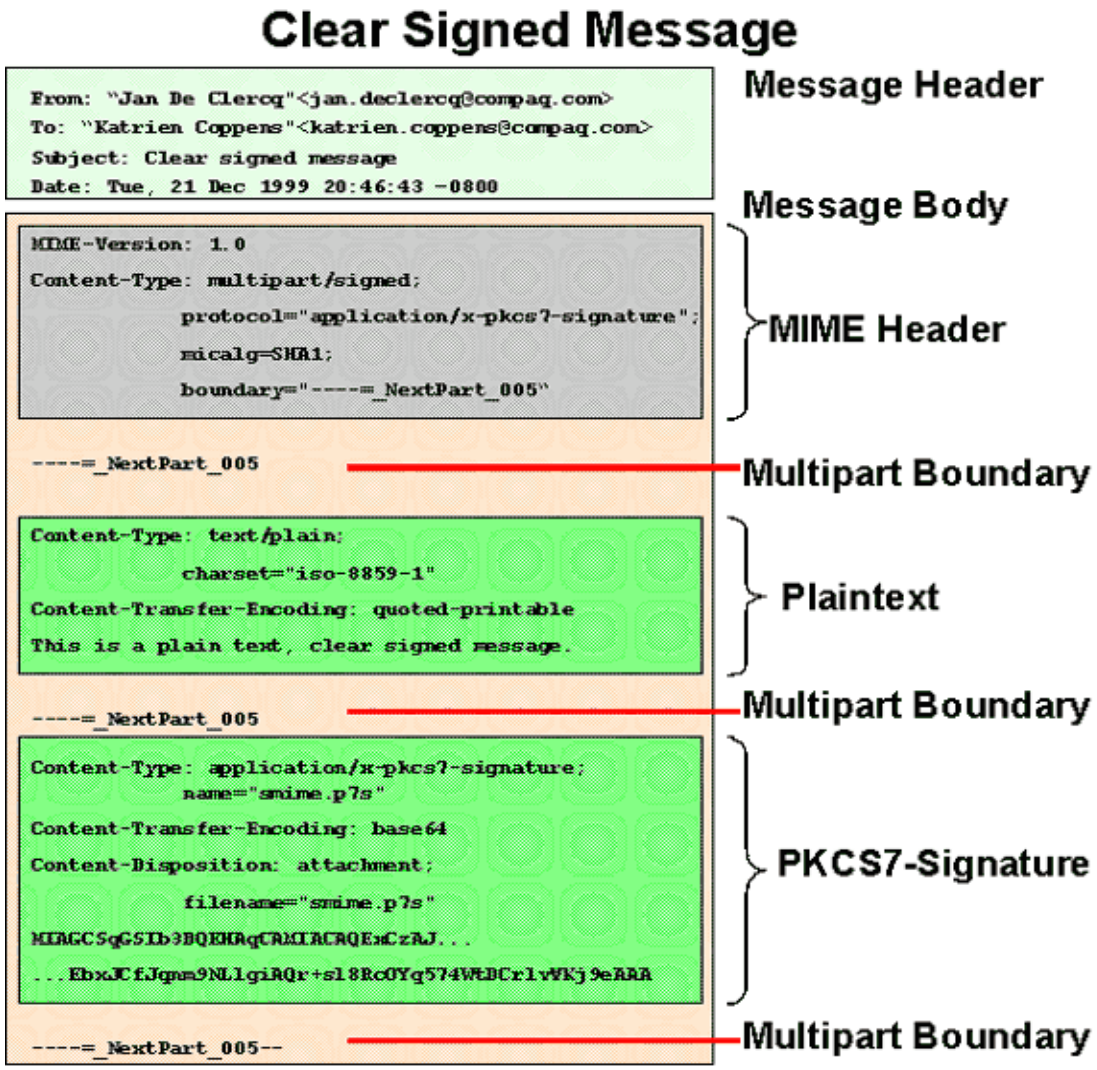
```
Content-Type: application/pkcs7-mime;
      smime-type=signed-data;
      name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhj
H776tbB9HG4VQbnj777n8HHGT9HG4VQpfyF467Gh
IGfHfYT6rfvbnj756tbBghyHhHUujhJhjHHUujhJ
h4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
7n8HHGghyHh6YT64V0GhIGfHfQbnj75
```

Funkcije: *clear-signed-data*

- digitalni potpis formira se potpisivanjem sažetka poruke i šifriranjem tog sažetka privatnim ključem pošiljatelja
  - moguće i više potpisnika, paralelno
  - podaci o potpisniku pohranjuju se u vrijednost *SignerInfo*
  - *SignedData* je prazan
- samo se sažetak (sažeci) kodira prema base64
  - sadržaj se kodira ako je neprikladan za prijenos, ali posebno
- korisnik koji ne podržava S/MIME može čitati, ali ne može verificirati potpis

Clear - signed data



http://windowsitpro.com/exchange-server/advanced-security-exchange-2000-part-2

Primjer potpisane poruke

```
Content-Type: multipart/signed; protocol="application/pkcs7-
signature";
        micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

Ovo je potpisana poruka s tekstom u čitljivom obliku.

--boundary42

Content-Type: application/pkcs7-signature;  name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT64VQpfyF467Gh
IGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnjn8HHGTrfvhJhjH776tbB9HG4
VQbnj7567GhIGfHfYT6ghyHhHUujpfyF47GhIGfHfYT64VQbnj756

--boundary42--
```

Kriptografski algoritmi kod S/MIME-a

- MUST/SHOULD
- hash: preporuka SHA-1, obavezno podržavati MD5
- digitalni potpisi: DSS i RSA
- šifriranje privremenih ključeva: ElGamal i RSA
- šifriranje poruka: 3DES, RC2/40 i ostale

- definiran postupak koji određuje koji se algoritmi koriste

Formiranje poruka prema standardu S/MIME

- poruke su kombinacija tijela prema standardu MIME i tipova podataka prema CMS-u
  - jedan format za enveloped-only
  - nekoliko formata za signed-only
  - nekoliko formata za signed i enveloped

Certifikati

- korisnici moraju nabaviti certifikate prije upotrebe
- sukladno standardu X.509, v3
  - hibrid hijerarhije X.509 i PGP-a (web of trust)
- praksa:
  - različiti parovi ključeva za potpisivanje i šifriranje
  - moguće šifirati bez da korisnik ima svoj certifikat (par ključeva)
    - klijenti koji podržavaju S/MIME traže da korisnik instalira svoj certifikat prije nego što šifrira poštu drugima
- osnovni osobni certifikat (class 1) dokazuje da je pošta došla s adrese navedene u polju From:, no ne dokazuje identitet korisnika
- certifikat od CA (class 2) – identificira i verificira korisnika
- postoje i više klase

S/MIME u praksi

- svi klijenti ne upravljaju dobro poštom (attachement smime.p7s)
- problemi s čitanjem pošte preko weba (webmail)
- S/MIME šifrira s kraja na kraj
  - ako je u pošti malware, on će proći neprimijećen - rješenja?
- traži certificiranje
  - nije svima prihvatljivo ili praktično
- nije moguće indeksiranje šifrirane elektroničke pošte
- mogući napadi:
  - prijava pod tuđim imenom, class 1
  - korišenje jednog certifikata, potpisivanje drugog korisnika
  - krivotvorenje zaglavlja poruke

Povjerljivost komunikacije

OpenPGP

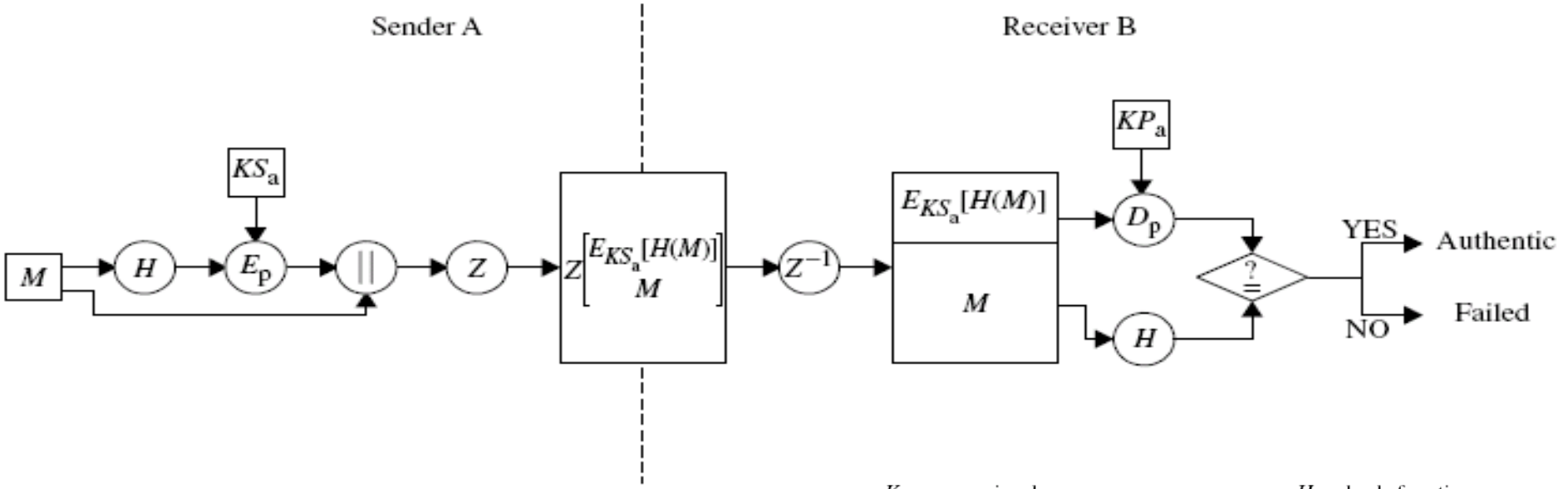
Pretty Good Privacy

- PGP ima svoju opsežnu povijest
  - Free Software Foundation: GnuPG (GPG)
- trenutačno RFC 4880
- dostupan kao plugin u mnogim alatima

Usluge PGP-a

- pet osnovnih usluga
  - autentifikacija (potpis/verifikacija)
  - povjerljivost (šifriranje/dešifriranje)
  - sažimanje (kompresija)
    - dobro i za šifriranje!
  - kompatibilnost s infrastrukturom elektroničke pošte
  - segmentacija i ponovno slaganje poruke
- posebno: upravljanje ključevima
- posljednje tri korisnicima su transparentne

Digitalni potpis

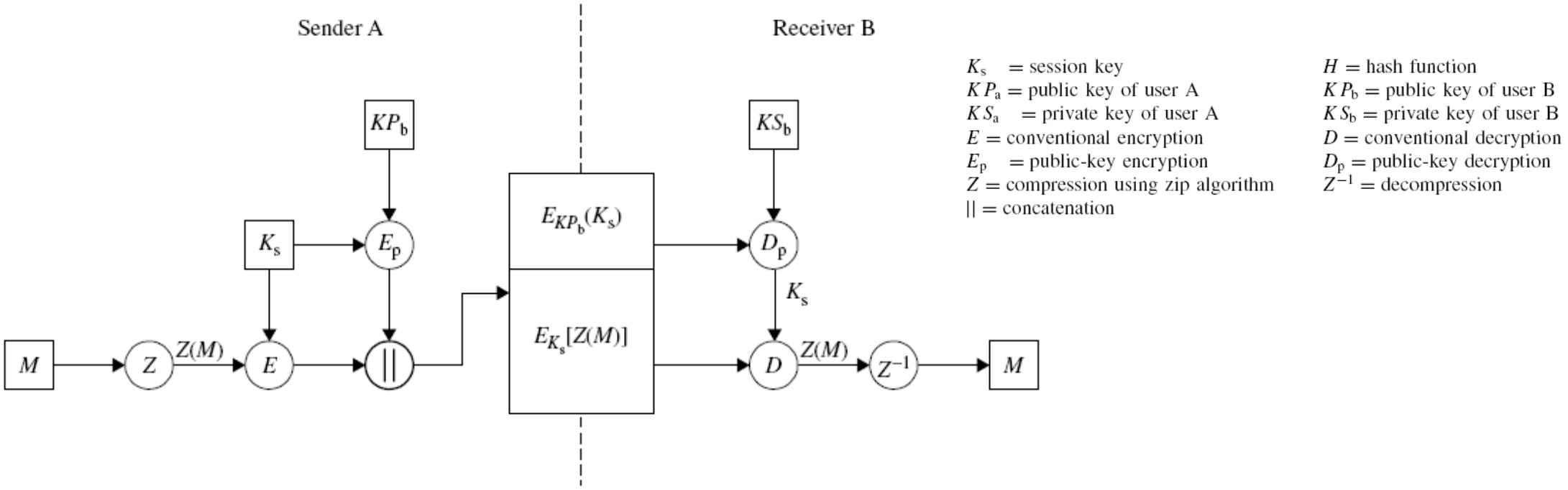


K_s = session key
KP_a = public key of user A
KS_a = private key of user A
E = conventional encryption
E_p = public-key encryption
Z = compression using zip algorithm
|| = concatenation

H = hash function
KP_b = public key of user B
KS_b = private key of user B
D = conventional decryption
D_p = public-key decryption
Z^{-1} = decompression

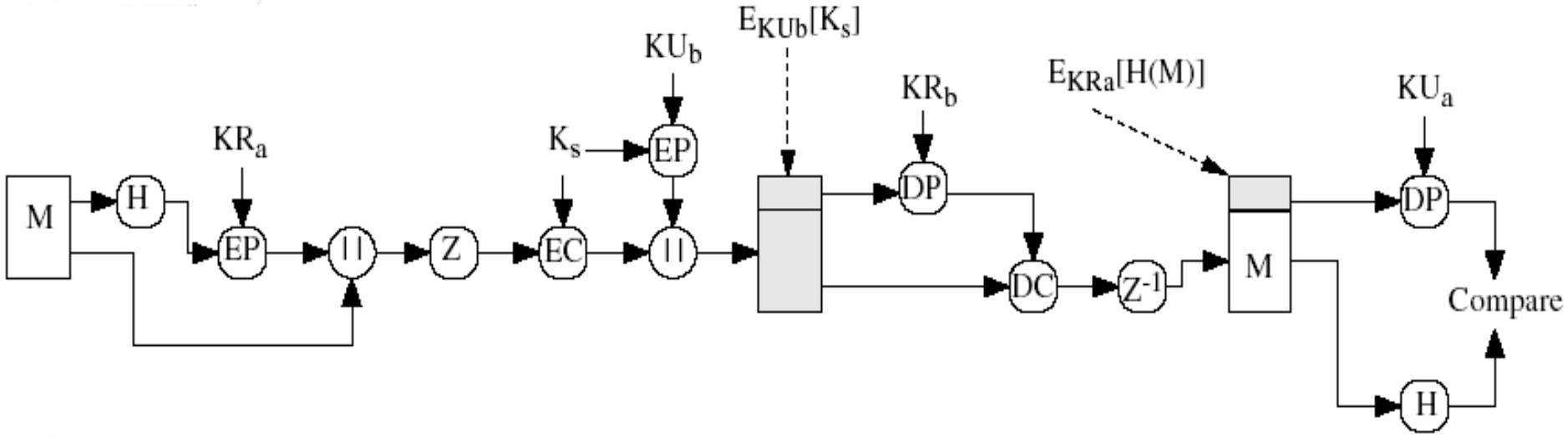
Šifriranje

- primatelj ne može znati identitet pošiljatelja (nema autentifikacije)!
- pošiljatelj zna da samo primatelj može čitati poruku



Šifriranje i digitalni potpis

- poruka se može potpisati i šifrirati
  - autentificirana povjerljivost



Sažimanje

- sažimanje se događa nakon digitalnog potpisa
  - lakše kasnije verificirati ako se pohrani poruka
  - moglo bi se dinamički sažimati prije verifikacije, ali
    - sve implementacije bi morale koristiti isti algoritam sažimanja
    - ali, različite implementacije koriste različite algoritme
- obavlja se prije šifriranja
  - sažimanje smanjuje redundantnost i otežava kriptoanalizu
  - manje korištenje prijenosnih resursa
  - korisno kad se napadi temelje na frekvenciji pojave slova
- podržan: ZIP

Kompatibilnost

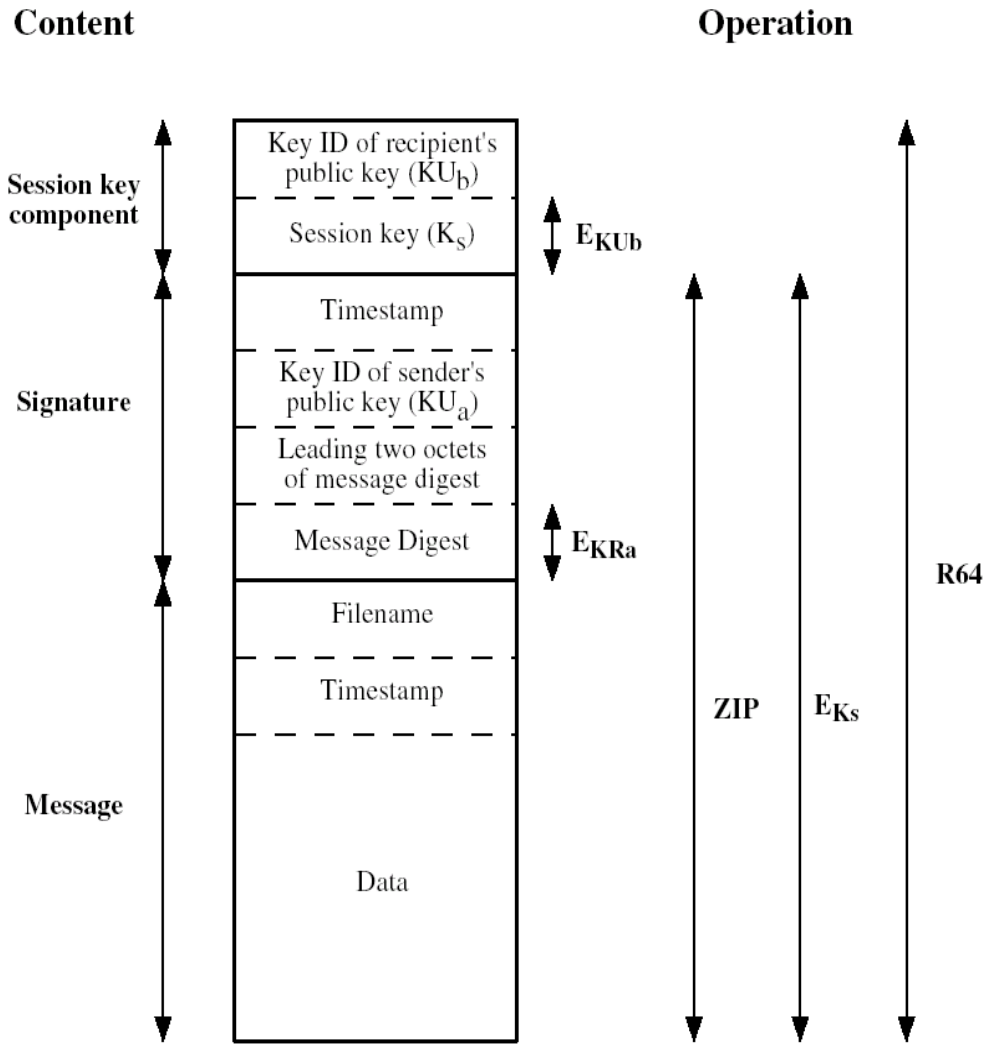
- kompatibilnost s infrastrukturom
- nema nikakve doticaje s privicima
  - jednako radi i u jednostavnim i u složenim sustavima
    - dakako, mora postojati plugin/alat koji zna šifrirati i dešifrirati
  - šifrirani i sažeti sadržaj pretvara se u niz ASCII znakova
    - Radix-64 / base64
    - posljedica: datoteke veće 33%

Algoritmi

- digitalni potpis
  - DSS/SHA ili RSA/SHA
- šifriranje
  - AES, 3DES, IDEA ili CAST (simetrično)
  - Diffie-Hellman ili RSA (asimetrično)
- sažimanje
  - ZIP
- kompatibilnost
  - Radix-64

- identifikacija ključa?

Format poruke



Ključevi

- PGP podržava više parova ključeva po svakom pošiljatelju ili primatelju
- ključevi se pohranjuju lokalno na “privjesku” - *PGP Key Ring*
  - baza podataka
- privatni ključevi čuvaju se šifrirani
  - ID ključa: zadnja 64 bita javnog ključa
- ključ za dešifriranje poruke određuje se temeljem tzv. *passphrase*
  - javni ključevi služe za šifriranje jednokratih simetričnih ključeva i verifikaciju potpisa
  - privatni ključevi služe za dešifriranje simetričnih ključeva i potpisivanje
- odakle ključevi i kako im se može vjerovati?

Upravljanje ključevima

- modeli povjerenja
  - izravno povjerenje
  - hijerarhija povjerenja
  - *“web of trust”*
- nema središnjeg autoriteta
- pojedinci jedni drugima “potpisuju” ključeve
  - takvi “certifikati” pohranjuju se s ključevima na “privjesku”
- PGP izračunava razinu povjerenja za svaki ključ na “privjesku”
  - ovise o broju potpisa na javnom ključu
  - razini povjerenja u svaki od “ovjeravajućih” potpisa
  - povremeno se preračunavaju
- korisnici sami interpretiraju razine povjerenja

Web of

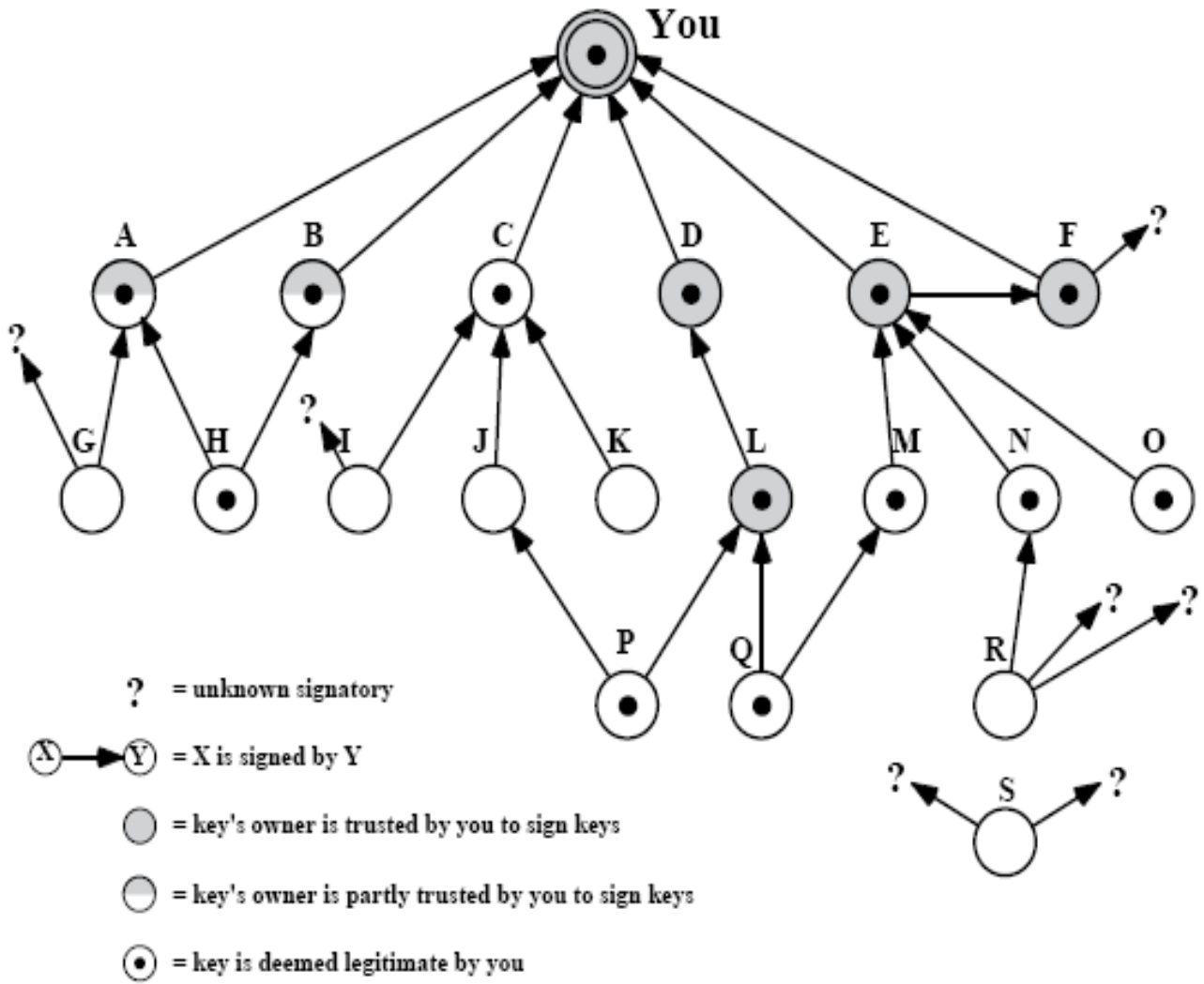


Figure 5.7 PGP Trust Model Example

PGP i X.509

- izvorna namjera bila je da korisnici doprinose mreži povjerenja (web of trust)
  - u stvarnosti, to nije tako
- korisnici uglavnom ne razumiju o čemu se radi i ne mogu interpretirati razine sigurnosti
- kasnije verzije PGP-a podržavaju certifikate prema standardu X.509

Novije metode zaštite na razini poslužitelja:

SPF, DKIM, DMARC

PGP i S/MIME - problemi

- PGP i S/MIME štite ”s kraja na kraj”
  - Problem kod detekcije zlućudnog koda / phishinga (IDS, AV) zbog šifriranja
  - Složeno za većinu korisnika?
- Novija rješenja namijenjena zaštiti elektroničke pošte između mail poslužitelja
  - dakle ne klijenata!
- SPF: *Sender Policy Framework*
- DKIM: *DomainKeys Identified Mail*
- DMARC: *Domain-based Message Authentication, Reporting, & Conformance*

SPF: *Sender Policy Framework*

- Kako potvrditi identitet pošiljatelja?
- U DNS se dodaju IP adrese mail poslužitelja koji smiju slati elektroničku poštu u ime određene domene

```
TXT @ "v=spf1 a include:_spf.google.com ~all"
```

Components	Description
TXT	The DNS zone record type; SPF records are written as TXT records
@	In a DNS file, the "@" symbol is a placeholder used to represent "the current domain"
v=spf1	Identifies the TXT record as an SPF record, utilizing SPF Version 1
a	Authorizes the host(s) identified in the domain's A record(s) to send e-mail
include:	Authorizes mail to be sent on behalf of the domain from google.com
~all	Denotes that this list is all inclusive, and no other servers are allowed to send e-mail

https://www.digitalocean.com/community/tutorials/how-to-use-an-spf-record-to-prevent-spoofing-improve-e-mail-reliability

- Primateljev mail poslužitelj provjerava DNS SPF zapise i prima poštu samo ako zapis postoji!

DKIM: *DomainKeys Identified Mail*

- Kako potvrditi identitet pošiljatelja?
- Digitalno potpisivanje
  - Privatni ključ (mail poslužitelja – ne korisnika!) za potpisivanje FROM: polja
  - Javni ključ mail poslužitelja dostupan putem DNS zapisa
    - Primatelj (poslužitelj) verificira potpis – ispravnost FROM: polja
- Obavezno potpisivanje FROM: polja, ostalo opcionalno

```
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed; d=researchgatemail.net; h=
message-id:date:subject:from:to:mime-version:content-type
:list-unsubscribe; s=rg; bh=pmIGvLojNdgEx4i3O6QNUqgcQYM=; b=Btp6
0Owjik2ucc7Fbtq7FJtO/5gb18Y6pgj6jFuXiaGluHsguXM3FTHOXwJ5CeQJh17S
EnlA5TqmW7xPzFn49h1Co7bawsYpv3rSh58vc+VCEFkGIHqu7yaWacTzStkbN3xX
7QaAuiUvBGwe4QjRArfIf2RctH/EimleSmNWan8=
```

DMARC: *Domain-based Message Authentication, Reporting, & Conformance*

- Odgovara na pitanje: što raditi s porukom koja ne prolazi SPF/DKIM?
- Opcije
  - *none* – ignoriraj poruku
  - *quarantine* – šalje npr. u spam folder
  - *reject* – javlja pošiljatelju (mail poslužitelju) da ne prolazi provjeru
- Koristi SPF ili DKIM za autentifikaciju/verifikaciju pošiljatelja
- Dobar za analizu i reporting!
  - Tko šalje mail u moje ime?
  - Otkrivanje phishing kampanja

Primjer…

```
Authentication-Results: spf=pass (sender IP is 209.15.249.184)
 smtp.mailfrom=bounce.researchgate.net; fer.hr; dkim=pass (signature was
 verified) header.d=researchgatemail.net;fer.hr; dmarc=pass action=none
 header.from=researchgatemail.net;compauth=pass reason=100
Received-SPF: Pass (protection.outlook.com: domain of bounce.researchgate.net
 designates 209.15.249.184 as permitted sender)
 receiver=protection.outlook.com; client-ip=209.15.249.184;
 helo=mr93.researchgate.net;
Received: from mr93.researchgate.net (209.15.249.184) by
 HE1EUR02FT024.mail.protection.outlook.com (10.152.10.181) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.2495.18 via Frontend Transport; Wed, 4 Dec 2019 07:59:20 +0000
Received: from mr93.researchgate.net (localhost [127.0.0.1])
by mr93.researchgate.net (Postfix) with ESMTP id C63363CB9
for <marin.vukovic@fer.hr>; Wed,  4 Dec 2019 07:59:18 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed; d=researchgatemail.net; h=
message-id:date:subject:from:to:mime-version:content-type
:list-unsubscribe; s=rg; bh=pmIGvLojNdgEx4i3O6QNUqgcQYM=; b=Btp6
0Owjik2ucc7Fbtq7FJtO/5gb18Y6pgj6jFuXiaGluHsguXM3FTHOXwJ5CeQJh17S
EnlA5TqmW7xPzFn49h1Co7bawsYpv3rSh58vc+VCEFkGIHqu7yaWacTzStkbN3xX
7QaAuiUvBGwe4QjRArfIf2RctH/EimleSmNWan8=
DomainKey-Signature: a=rsa-sha1; c=nofws; d=researchgatemail.net; h=
message-id:date:subject:from:to:mime-version:content-type
:list-unsubscribe; q=dns; s=rg; b=E3dmXocXyHBcXUTJOMQOg8F8tRtviC
BxObu9oKXWo1f7Nka8FvM0arkG1vUDUXqc+Qk47jaqcAN/dx69O4m1aHEkh/QsNd
Rly+Hh7A2WX1GsOYdPfe1lfkn63YqNuresaQ7/XgZXdCjfvMp3CAZCpM9YdwXN7b
8VazfMQtd9BHA=
```

https://www.socketlabs.com/blog/the-complete-guide-to-email-authentication-part-6/

Primjer…

https://www.learndmarc.com

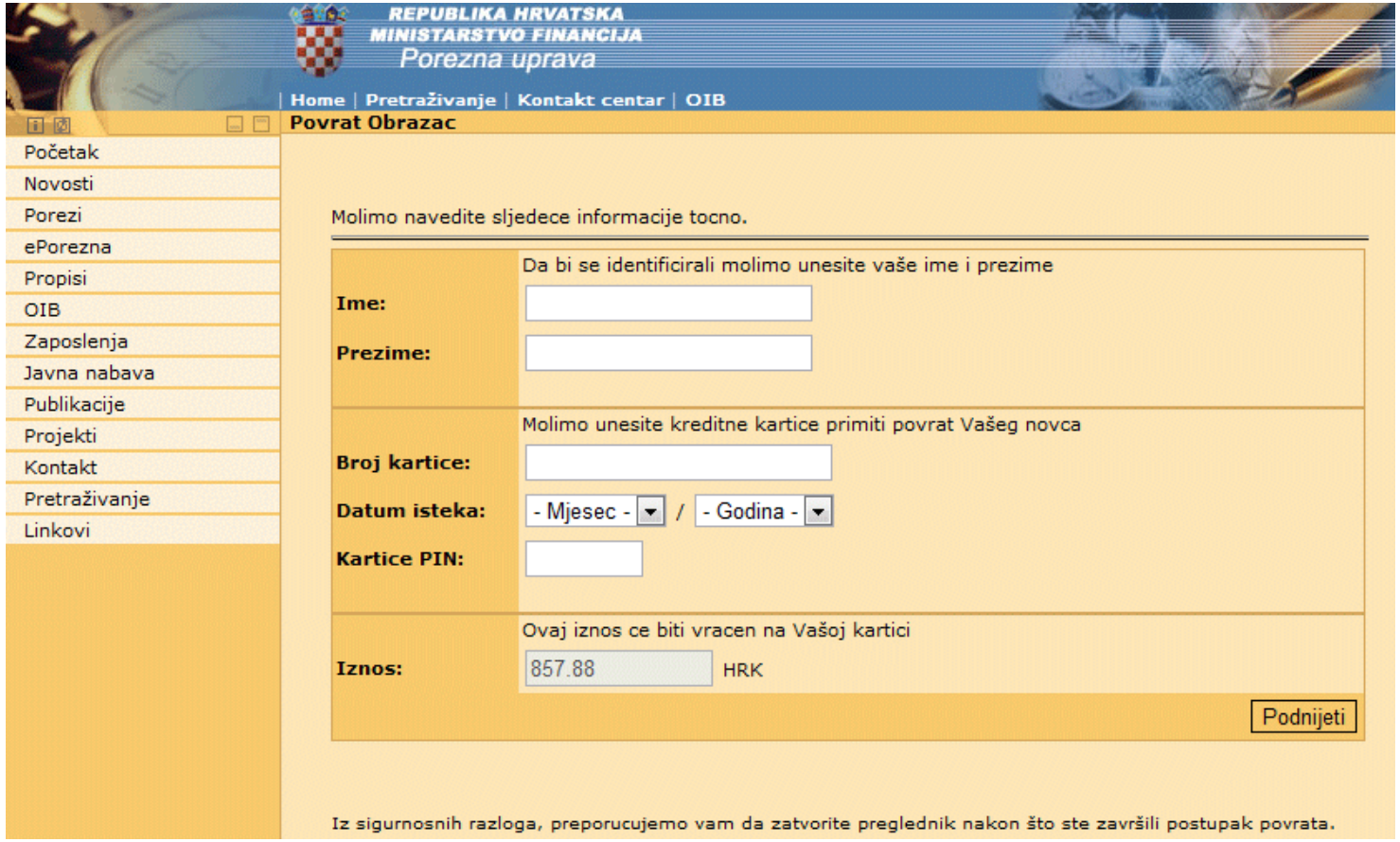
Top 10 e-mail prevara

1. obitelj *Nigerian scam* prevara
2. odobreni krediti na karticama – naplaćuje se "samo" učlanjenje
3. dobitak na lotu
4. *phishing*
5. javljanje na oglas i ponuda veće cijene
6. provizija na bankovne transakcije (slično *Nigerian scamu*)
7. dobrotvorni prilozi
8. *last minute* ponude sa skrivenim troškovima
9. ulančana pisma za zaradu novaca
10. "iznajmljivanje" računala *spammer*ima

http://netforbeginners.about.com/od/scamsandidentitytheft/ss/top10inetscams_10.htm

Primjeri iz Hrvatske…

- *phishing* – porezna uprava



Primjeri iz Hrvatske…

-----Original Message-----
From: PRAVO_IME <Aaron256Smith@yahoo.jp>
Subject: Your password is PRAVI_PW
Date: 3 Oct 2018 05:31:01 CEST
To: PRAVI_PW <PRAVI_PRIMATELJ>
Reply-To: PRAVO_IME <Aaron256Smith@yahoo.jp>

I do know PRAVI_PW is your passphrase. Lets get right to point. You may not know me and you're most likely wondering why you are getting this e mail? Not a single person has compensated me to investigate about you.

Let me tell you, I actually setup a software on the adult video clips (pornographic material) website and do you know what, you visited this website to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a Remote control Desktop with a keylogger which provided me access to your display screen and also web camera. Right after that, my software collected every one of your contacts from your Messenger, FB, as well as email account. And then I made a double-screen video. First part shows the video you were watching (you have a good taste omg), and second part displays the view of your cam, and it is u.

You have only 2 options. Lets look at these types of possibilities in aspects:

First option is to neglect this email message. In this case, I am going to send out your video to just about all of your contacts and then think about about the disgrace you can get. Furthermore in case you are in a loving relationship, just how it can affect?

Number 2 alternative will be to pay me $1000. Let us name it as a donation. In this case, I will quickly eliminate your video recording. You will carry on your life like this never took place and you will never hear back again from me.

You'll make the payment via Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address: 1NuZv1BedveeZr4nwZXh7cwaTwSemkJYMG
[CASE-sensitive, copy & paste it]

If you have been looking at going to the law enforcement, well, this email message cannot be traced back to me. I have covered my moves. I am also not looking to ask you for very much, I would like to be rewarded.

You have one day to make the payment. I've a unique pixel within this message, and at this moment I know that you have read this e-mail. If I do not receive the BitCoins, I will definately send out your video recording to all of your contacts including friends and family, coworkers, and many others. Nonetheless, if I do get paid, I'll erase the video immediately. If you need proof, reply with Yea! then I will send your video recording to your 12 friends. This is a nonnegotiable offer and so please don't waste mine time & yours by replying to this message.
-----Original Message-----

Literatura

- svi navedeni RFC-ovi
- www.tcpipguide.com
- www.gnupg.com
- www.openpgp.com