Internet e architetture di rete

Antonio Prado
https://www.prado.it

Ciclo di seminari - Calendario

Internet: Sistemi autonomi e Governance

07 aprile 2016

Addio IPv4, Benvenuto IPv6

14 aprile 2016

Architetture di instradamento a Internet: il BGP

21 aprile 2016

Numeri e Nomi: il DNS

28 aprile 2016

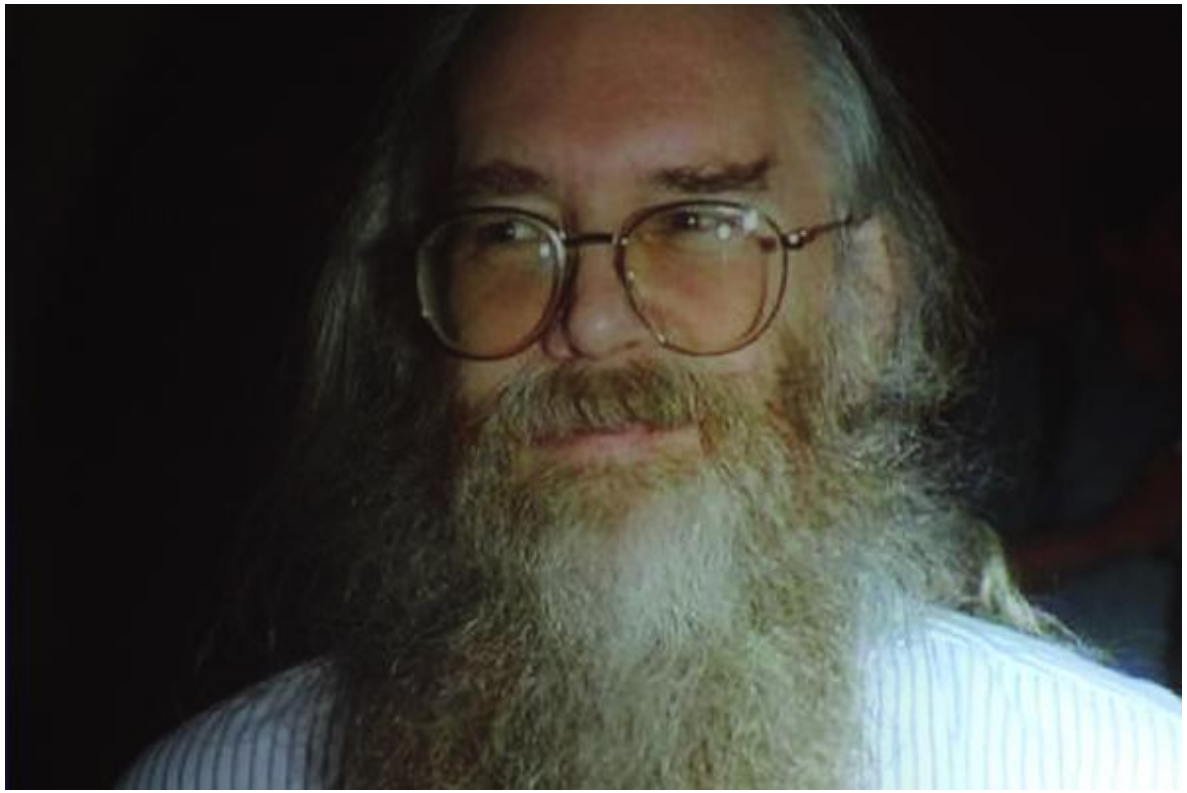
34 anni di e-mail: SMTP

05 maggio 2016

34 anni di e-mail: SMTP

TCP ~~/UDP~~ 25

[Jon_Postel]



Jon Postel, Internet pioneer (1943-1998)

Il cinque maggio

Ei fu. Siccome immobile,

dato il mortal sospiro,

stette la spoglia immemore

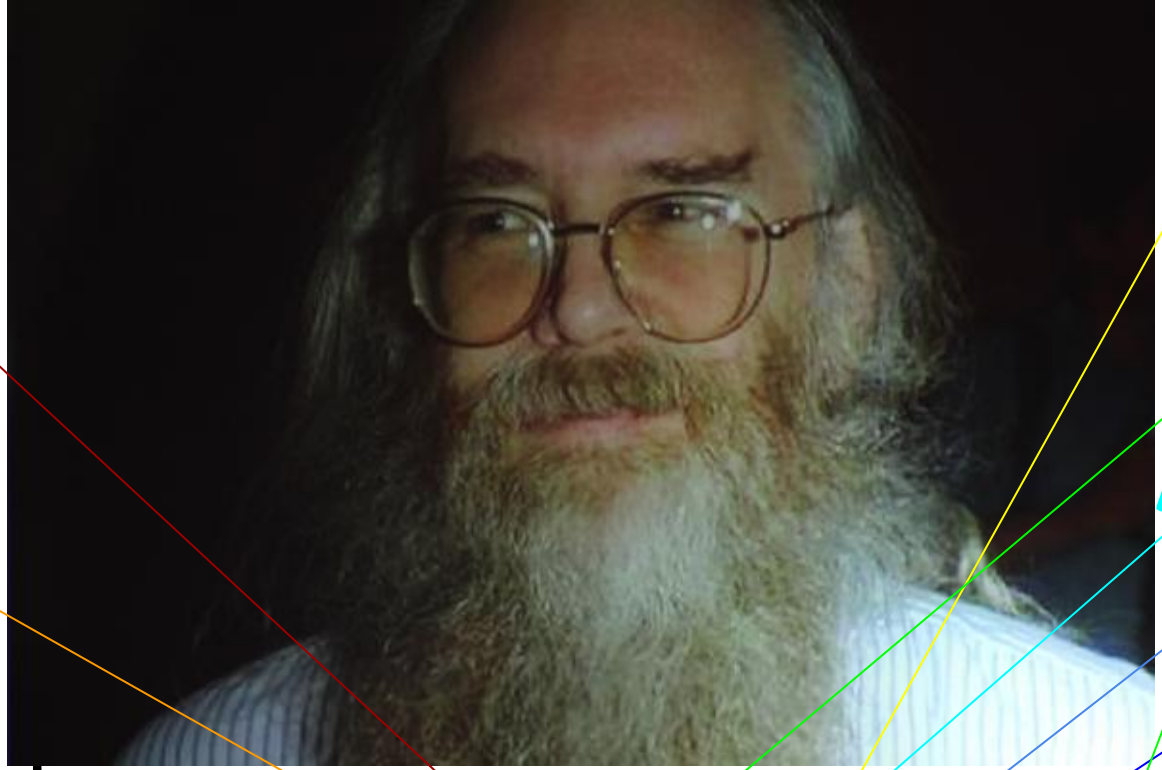
orba di tanto spiro,

così percossa, attonita

la terra al nunzio sta

[...]

ODE di Alessandro Manzoni, 1821



spam

UDP

hostnames

telnet

SMTP

IP

ICMP

TCP

Jon Postel, Internet pioneer (1943-1998)

[RFC 77, 127, 128, 139, 145, 158, 165, 204, 229, 236, 268, 295, 317, 318, 322, 324, 328, 346, 347, 348, 349, 429, 433, 489, 516, 580, 587, 604, 640, 659, 661, 678, 690, 694, 706, 717, 718, 719, 730, 750, 753, 754, 755, 759, 760, 761, 762, 764, 765, 766, 767, 768, 769, 770, 774, 776, 777, **788**, 790, 791, 792, 793, 795, 796, **821**,]

agosto 1982

Simple Mail Transfer Protocol

[RFC 821]

RFC 821
RFC 2821
RFC 5321

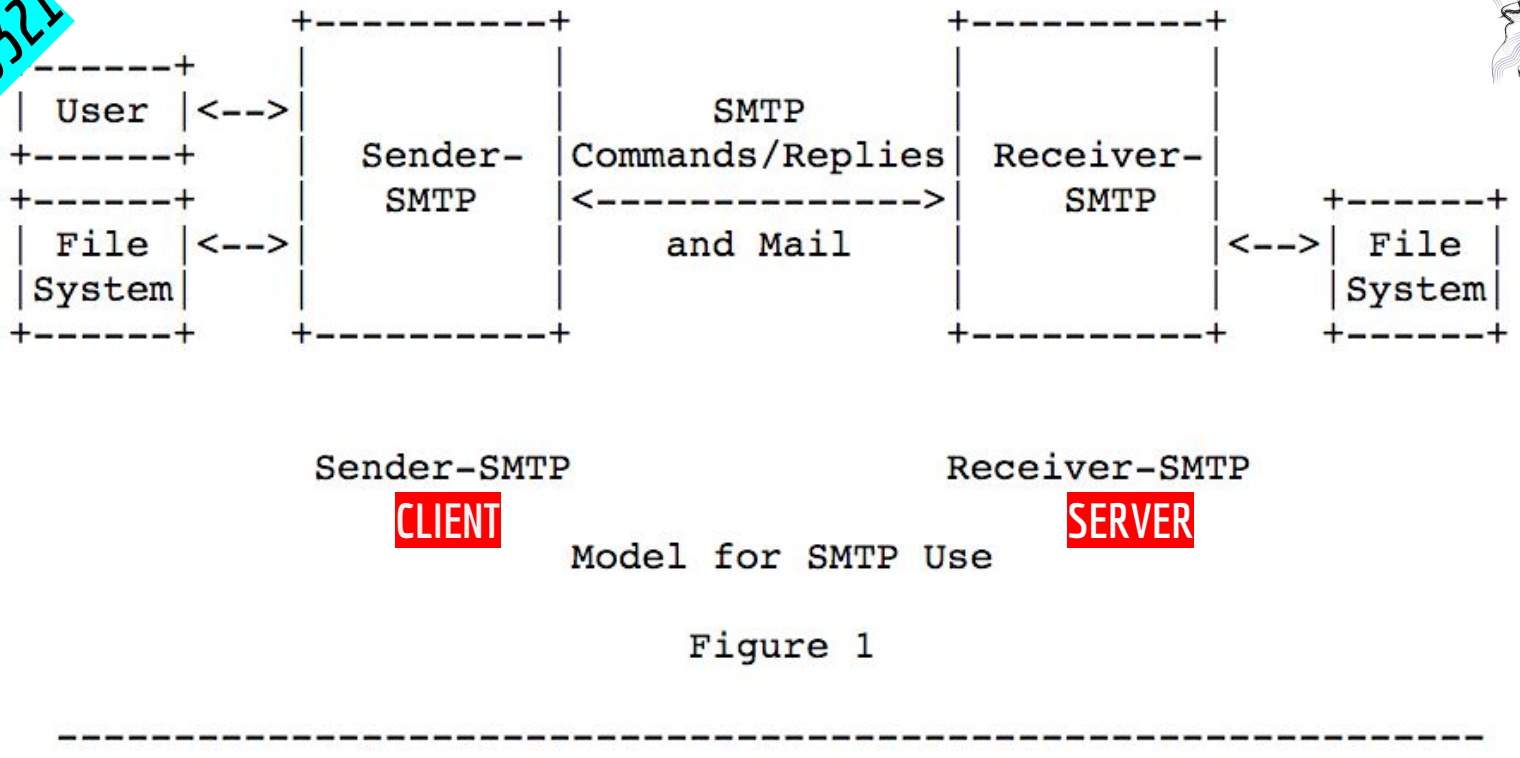


Figure 1

Simple Mail Transfer Protocol (edito nel 1982, aggiornato nel 2001 e nel 2008): il modello

SMTP dialog, lock-step, one-at-a-time

Mail transaction in 3 passaggi

MAIL FROM: ‹John.Smith@USC-ISI.ARPA›

1

250 OK

RCPT TO: ‹Mario.Rossi@USC-ISI.ARPA›

2

250 OK / 550 Failure

DATA: testo del messaggio

.

3

250 OK

SMTP, Apertura e chiusura

Hello,
I am usc-isif.arpa

HELO USC-ISIF.ARPA

E' il nome host del mittente, non stringa inventata

250 BBN-UNIX.ARPA

CIAO

QUIT

221 BBN-UNIX.ARPA Service closing transmission channel

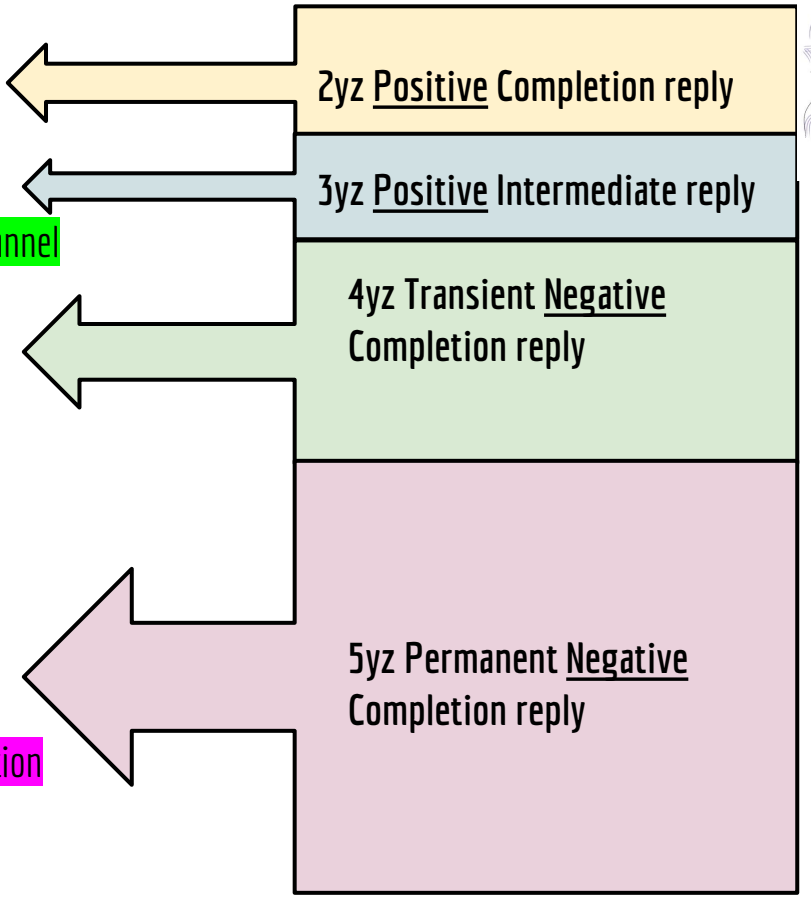
SMTP, impossibile recapitare il messaggio

Example Undeliverable Mail Notification Message

```
S: MAIL FROM:<>
R: 250 ok
S: RCPT TO:<@HOSTX.ARPA:JOE@HOSTW.ARPA>
R: 250 ok
S: DATA
R: 354 send the mail data, end with .
S: Date: 23 Oct 81 11:22:33
S: From: SMTP@HOSTY.ARPA
S: To: JOE@HOSTW.ARPA
S: Subject: Mail System Problem
S:
S:   Sorry JOE, your message to SAM@HOSTZ.ARPA lost.
S:   HOSTZ.ARPA said this:
S:    "550 No Such User"
S: .
R: 250 ok
```

SMTP, codici di risposta

220 ‹domain› Service ready
221 ‹domain› Service closing transmission channel
250 Requested mail action okay, completed
354 Start mail input; end with ‹CRLF›.‹CRLF›
421 ‹domain› Service not available, closing transmission channel
450 Requested mail action not taken: mailbox unavailable
451 Requested action aborted: local error in processing
452 Requested action not taken: insufficient system storage
500 Syntax error, command unrecognized
501 Syntax error in parameters or arguments
502 Command not implemented
503 Bad sequence of commands
504 Command parameter not implemented
550 Requested action not taken: mailbox unavailable
552 Requested mail action aborted: exceeded storage allocation
553 Requested action not taken: mailbox name not allowed
554 Transaction failed



Terminologia

SENDER → RECIPIENT

Client → Server

MUA → MTA → MUA

Mail User Agent — Mail Transfer Agent — Mail User Agent

RELAY

GATEWAY

HOST

DOMAIN

FQDN

Fully Qualified Domain Name

MAILBOX

ADDRESS

ALIAS

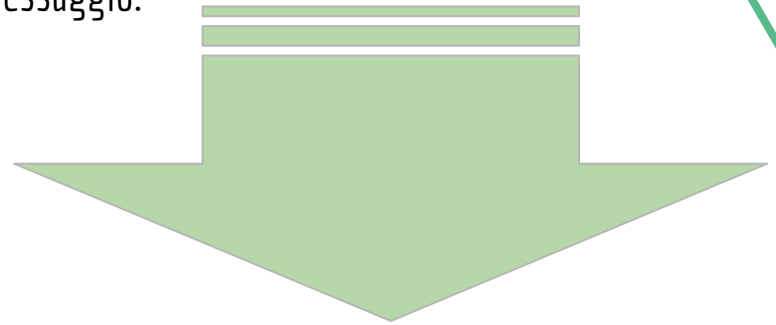
MAILING LIST

Risoluzione del nome

Individuazione del FQDN	mario.rossi@garr.it ⟶ garr.it
RIchiesta al DNS per il RR IN MX	*dig garr.it MX* ⟶ **15 lx1.dir.garr.it** 20 lx5.dir.garr.it
Se MX multipli, scelta su priorità con numero più basso	**lx1.dir.garr.it**
Se manca RR IN MX, usa IN A	

Affidabilità della consegna

Non appena il server SMTP accetta un messaggio restituendo al client una risposta di tipo **250 OK**, sta accettando la **responsabilità** di consegnare quel messaggio.

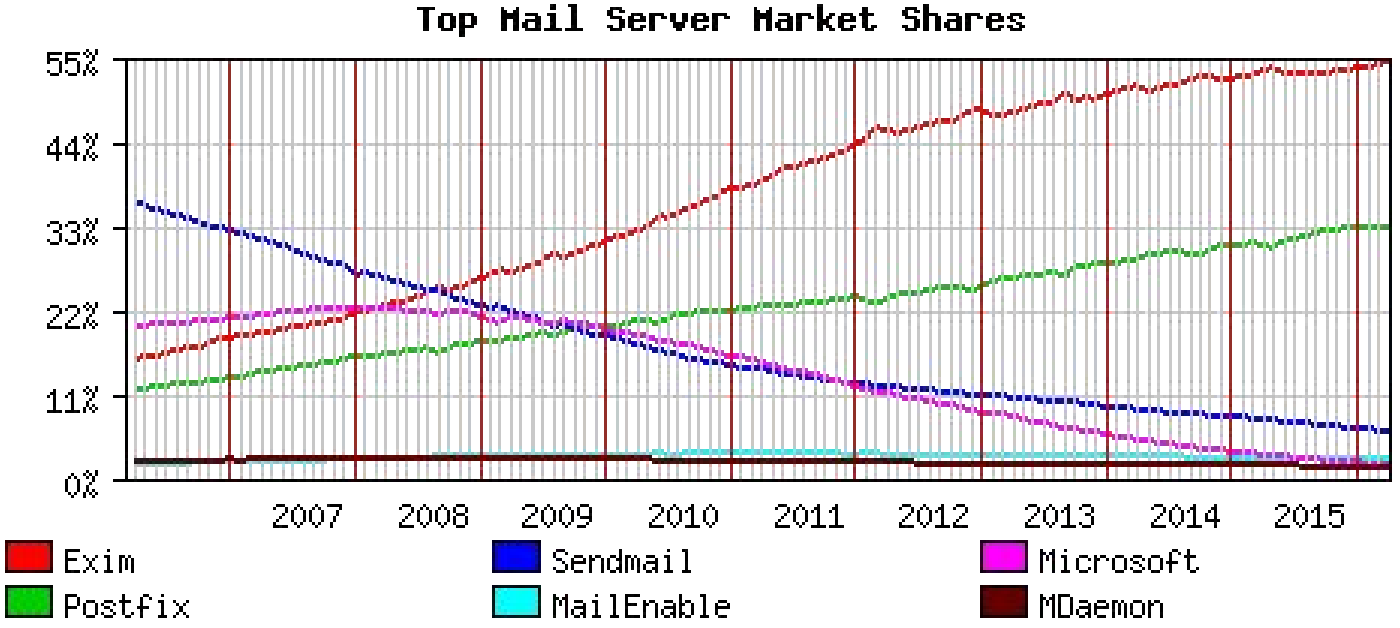


Il server DEVE assumersi **seriamente** questa responsabilità e NON DEVE perdere il messaggio per futili motivi.

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
C: MAIL FROM:‹Smith@bar.com›
S: 250 OK
C: RCPT TO:‹Jones@foo.com›
S: 250 OK
C: DATA
S: 354 Start mail input; end with ‹CRLF›.‹CRLF›
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel

Software per SMTP server (20160401, E-Soft Inc.)

Server Type	Number of Servers	Percent
Exim	604,931	54.29%
Postfix	364,470	32.71%
Sendmail	67,479	6.06%



SMTP, live sessions (recap)

Per prima cosa individuare il server MX:

dig domain.tld MX

Selezionare quello con il valore più basso nel campo priorità (in caso di assenza di RR IN MX, individuare RR IN A)
Connettersi alla porta TCP 25 del server con un terminale virtuale di rete, a esempio un client telnet (RFC 854)

telnet mx.domain.tld 25

Usare i comandi indicati da RFC 2821: EHLO, MAIL, RCPT, DATA, QUIT

SMTP, live sessions

telnet lx1.dir.garr.it 25
Trying 193.206.158.2...
Connected to lx1.dir.garr.it.
Escape character is '^]'.
S: 220 lx1.dir.garr.it ESMTP Sendmail 8.15.2/8.14.4/Debian-4; Sun, 1 May 2016 17:56:55 +0200
C: ehlo mytest.com
S: 250-lx1.dir.garr.it
C: MAIL FROM:‹mario.rossi@mytest.com›
S: 250 2.1.0 ‹mario.rossi@mytest.com›... Sender ok
C: RCPT TO:‹postmaster@garr.it›
S: 250 2.1.5 ‹postmaster@garr.it›... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: MAIL FROM:‹mario.rossi@mytest.com›
C: RCPT TO:‹postmaster@garr.it›
C: SUBJECT: test e-mail
C: Solo un messaggio di testo a scopo didattico
C: .
S: 250 2.0.0 u41Futqt008498 Message accepted for delivery
C: QUIT
S: 221 2.0.0 lx1.dir.garr.it closing connection

novembre 1975

SPAM, nozione proveniente da RFC 706:

J. Postel, *On the Junk Mail Problem*

Misure anti-spam su SMTP di base

Mittente → agenzia-di-spam@servizio-spam.com

Nome a dominio del mittente → servizio-spam.com

FQDN server di provenienza → mta.server-di-spam.net

"Only resolvable, fully-qualified domain names (FQDNs) are permitted when domain names are used in SMTP" [RFC 5321]

IP server di provenienza → 192.0.2.25

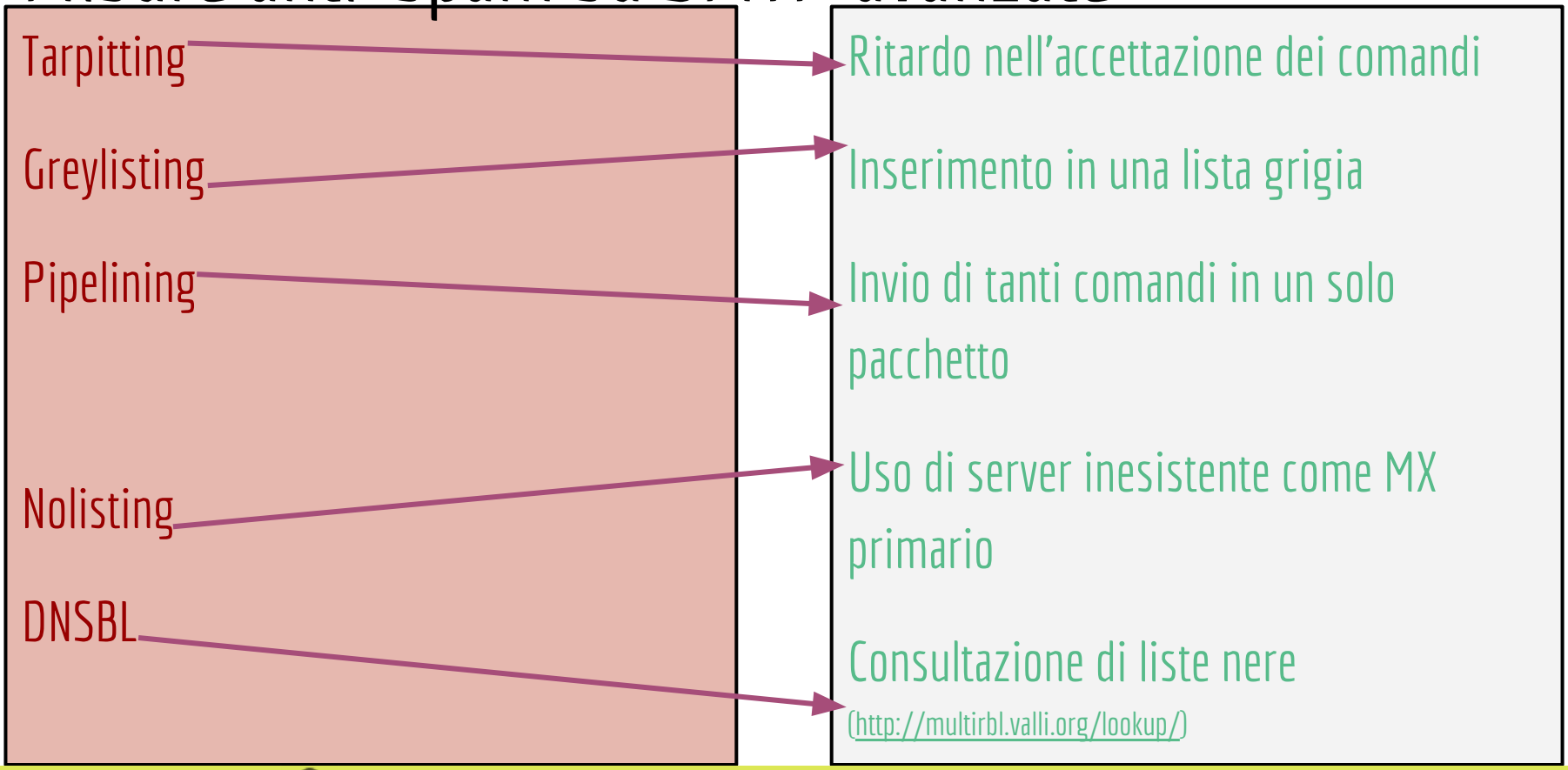
Puntatore IP server di provenienza → 25.2.0.192.in-addr.arpa. IN PTR

"Add the reverse IN-ADDR entry for each host address in the appropriate zone files for each network the host in on" [RFC 1033]
"Make sure your PTR and A records match. For every IP address, there should be a matching PTR record in the in-addr.arpa domain" [RFC 1912].

DIchiarazione in HELO (o EHLO) → EHLO server-di-spam

"The domain name given in the EHLO command MUST be either a primary host name (a domain name that resolves to an address RR) or, if the host has no name, an address literal" [RFC 5321]

Misure anti-spam su SMTP avanzate



Misure anti-spam su SMTP, e-mail authentication

SPF (Sender Policy Framework)	RFC 7208
DKIM (DomainKeys Identified Mail)	RFC 6376
DMARC (Domain-based Message Authentication, Reporting and Conformance)	RFC 7489
ADSP (Author Domain Signing Practices)	RFC 5617

Misure anti-spam su SMTP, SPF

SPF (Sender Policy Framework)

Voglio dichiarare pubblicamente a quali server affido il compito di consegnare i miei messaggi.
La dichiarazione si fa in un RR IN TXT secondo la sintassi indicata in RFC

dig garr.it TXT +short

"v=spf1 ip4:193.206.158.2 ip6:2001:760:0:158::2 ip4:193.206.158.53 ip6:2001:760:0:158::53 ip4:193.206.158.29 ip6:2001:760:0:158::29 ip4:193.206.139.45 ip4:193.206.158.43 ip6:2001:760:0:158::43 ip4:192.84.145.62 ip4:90.147.160.68 ip4:90.147.60.75 -all"

RFC 7208

Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1

Misure anti-spam su SMTP, DKIM

DKIM (DomainKeys Identified Mail)

Firmo tutte le e-mail che invio.

Pubblico la chiave nel DNS (RR IN TXT) così che il mio destinatario possa verificare la corrispondenza quanto riportato nel messaggio e quanto dichiarato nel DNS

dig cyrus._domainkey.garr.it TXT +short

"v=DKIM1\; g=*\; t=y\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC75HKZ8vvRztcuoEjxcijMCu4cTUE6L2cleKd
JVaCp2JayUmauS5XwnuGioVqI2DSim39lA2rxOAvdVVJ6ihnJknQiWdPLIIFn8XCJwhXQ8eVbojJHTg
aKDS4wju4U0oyqJYpNdJsETc8IS1ZIrzsl8pgKOZnmMGbGuuI+ICznBwIDAQAB"

RFC 6376

DomainKeys Identified Mail (DKIM) Signatures

Misure anti-spam su SMTP, DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance)

Una volta impostate le misure SPF e DKIM, è possibile pubblicare nel DNS (RR IN TXT) la policy che il server del destinatario deve osservare:

dig _dmarc.prado.it TXT +short

"v=DMARC1\; p=reject\;"

In questo caso reject, cioè: scartare il messaggio

RFC 7489

Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Misure anti-spam su SMTP, ADSP

ADSP (Author Domain Signing Practices)

Subordinato a DKIM, è uno strumento in mano al mittente di un nome a dominio il quale può far sapere ai destinatari come comportarsi nel caso in cui il messaggio non riporti una firma DKIM valida.

dig _adsp._domainkey.prado.it TXT +short

"dkim=discardable"

In questo caso il messaggio è da scartare.

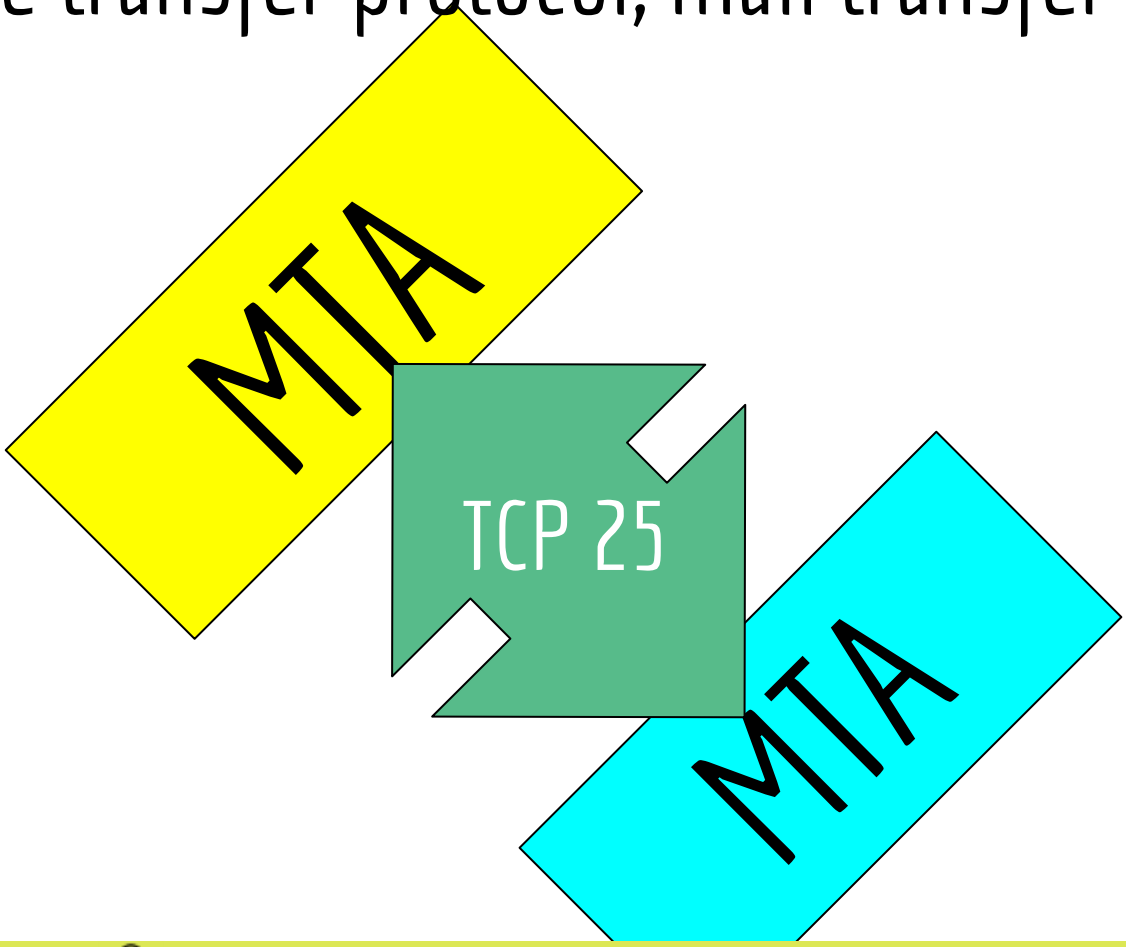
RFC 5617

DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)

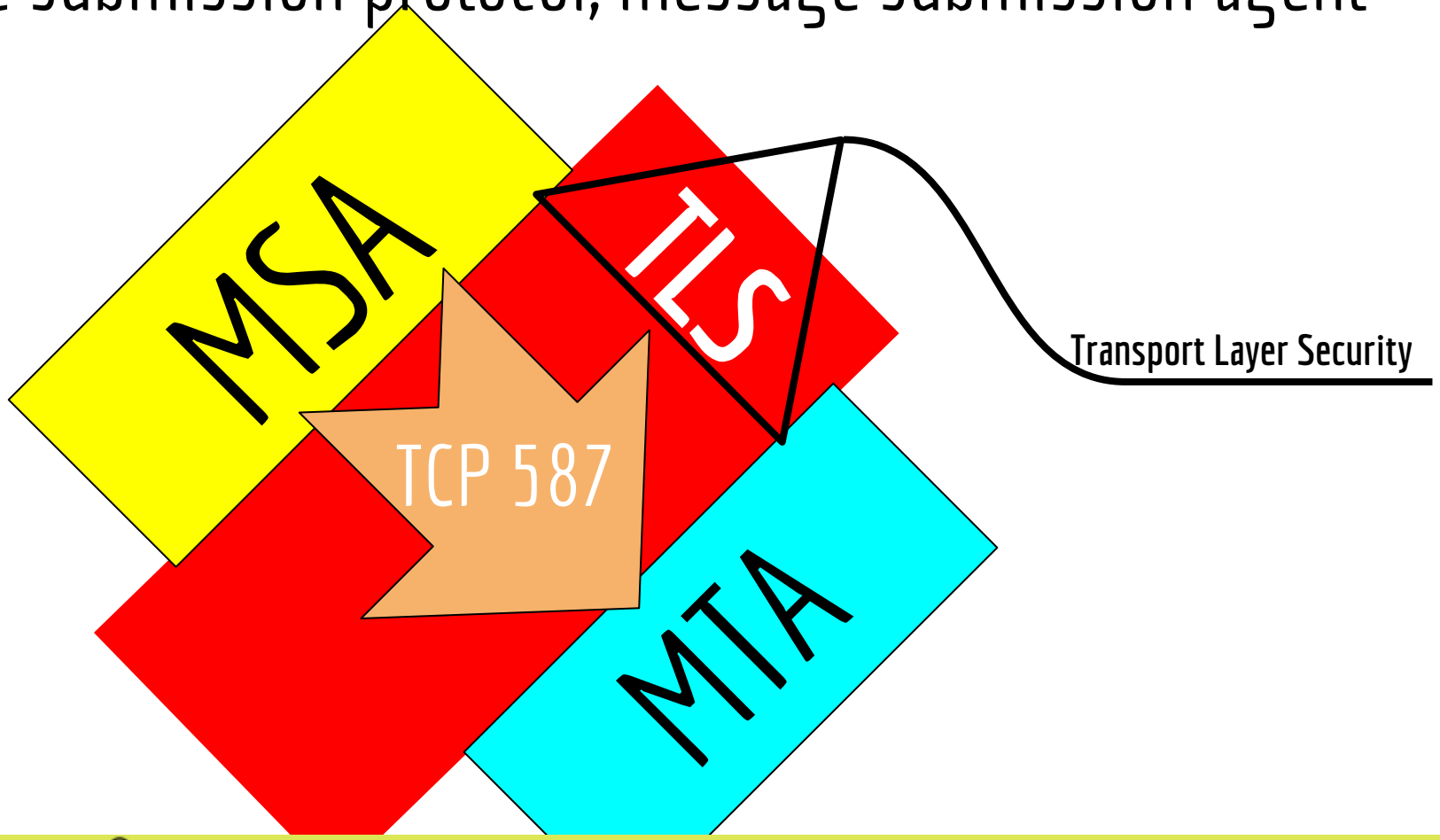
SMTP e crittografia

[RFC 7817, Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols]

Message transfer protocol, mail transfer agent



Message submission protocol, message submission agent



SSL, TLS, STARTTLS

SSL, Secure Socket Layer: protocollo di crittografia superato (SSL 1, 2, 3)

TLS, Transport Layer Security: protocollo di crittografia in auge (TLS 1.2)

Entrambi i protocolli rendono private le comunicazioni tra CLIENT e SERVER attraverso crittografia simmetrica e asimmetrica

STARTTLS è un comando per crittografare (con TLS) una comunicazione non protetta, precedentemente stabilita su canale non protetto, senza necessità di cambiare porta di comunicazione (TCP 465)

Live lab

```
perl -MMIME::Base64 -e 'print encode_base64("\000user\@domain.tld\000password")'
```

openssl s_client -starttls smtp -connect smtp.gmail.com:587 -crlf -ign_eof

```
CONNECTED(00000003)
depth=2 /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
[...]
SSL handshake has read 3492 bytes and written 491 bytes
New, TLSv1/SSLv3, Cipher is AES128-SHA
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : AES128-SHA
    Session-ID: A26BA5EBCABC00A83BAB69B243B81F9D97446B9AA147EACCC982AEF1497298E6
    Session-ID-ctx:
    Master-Key:
E983ECAC1FEE8FDDF8E41BA4BE4B84F3DE4EA13A9DED17F1170D85FD79B9883B36C6067C2B15F6757C68D73789FBE584
    Key-Arg   : None
    Start Time: 1462264156
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
```

CUT

1

```
---
250 SMTPUTF8
EHLO mytest.com
250-smtp.gmail.com at your service, [185.5.200.252]
250-SIZE 35882577
250-8BITMIME
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
AUTH PLAIN AWWWWHxxxxxx5rb2ZpYYYYY5jb20AQZZZZZZ=
235 2.7.0 Accepted
MAIL FROM:<mario.rossi@mytest.com>
250 2.1.0 OK jh2sm2473712wjb.39 - gsmtp
RCPT TO:<someuser@gmail.com>
250 2.1.5 OK jh2sm2473712wjb.39 - gsmtp
DATA
354  Go ahead jh2sm2473712wjb.39 - gsmtp
questo il mio messaggio
.
250 2.0.0 OK 1462264188 jh2sm2473712wjb.39 - gsmtp
QUIT
221 2.0.0 closing connection jh2sm2473712wjb.39 - gsmtp
read:errno=0
```

2

PEC, lo strano caso tutto italiano

[RFC 6109, La Posta Elettronica Certificata - Italian Certified Electronic Mail]

PEC, cos'è e a cosa serve?

È un sistema elettronico per la trasmissione di documenti informatici: al mittente viene rilasciata una documentazione (cioè una ricevuta) elettronica di **INVIO** e **CONSEGNA**.

Serve a superare le debolezze della posta elettronica tradizionale e può essere utilizzata in qualsiasi contesto nel quale sia necessario avere prova dell'**INVIO** e della **CONSEGNA** di una comunicazione.

PEC, chi la gestisce?

Elenco pubblico gestori PEC

- ACI Informatica S.p.A.
- Actalis S.p.A.
- Ancitel S.p.A.
- ARUBA PEC S.p.A.
- Cedacri S.p.A.
- Consiglio Nazionale del Notariato
- Fastweb S.p.A.
- HP ES Italia S.r.l. (già EDS Italia S.r.l.)
- IN.TE.S.A. S.p.A.
- Infocert S.p.A.
- Innova Puglia S.p.A.
- INTRED S.p.A.
- ITnet S.r.l.
- KPNQwest Italia S.p.A.
- Namirial S.p.A.
- Numera Sistemi e Informatica S.p.A.
- Poste Italiane S.p.A.
- Postecom S.p.A.
- Regione Basilicata
- Regione Marche
- Register.it S.p.A.
- Sogei – Società Generale d'Informatica S.p.A.
- Telecom Italia Trust Technologies S.r.l. (già I.T. Telecom S.r.l.)
- TWT S.p.A.
- Università degli studi di Napoli Federico II

Live lab

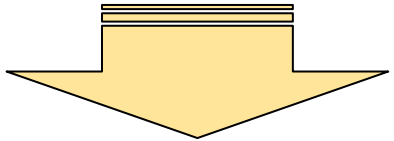
perl -MMIME::Base64 -e 'print encode_base64("\000user\@domain.tld\000password")'

```
openssl s_client -connect smtps.pec.aruba.it:465 -crlf -ign_eof
CONNECTED(00000003)
depth=1 /C=IT/ST=Milano/L=Milano/O=Actalis S.p.A./03358520967/CN=Actalis
Authentication CA G3
verify error:num=20:unable to get local issuer certificate
verify return:0
[...]
```

CUT

```
220 smtps.pec.aruba.it ESMTP Postfix
EHLO mytest.com
250-smtps.pec.aruba.it
250-PIPELINING
250-SIZE 157286400
250-ETRN
250-AUTH LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250 8BITMIME
```

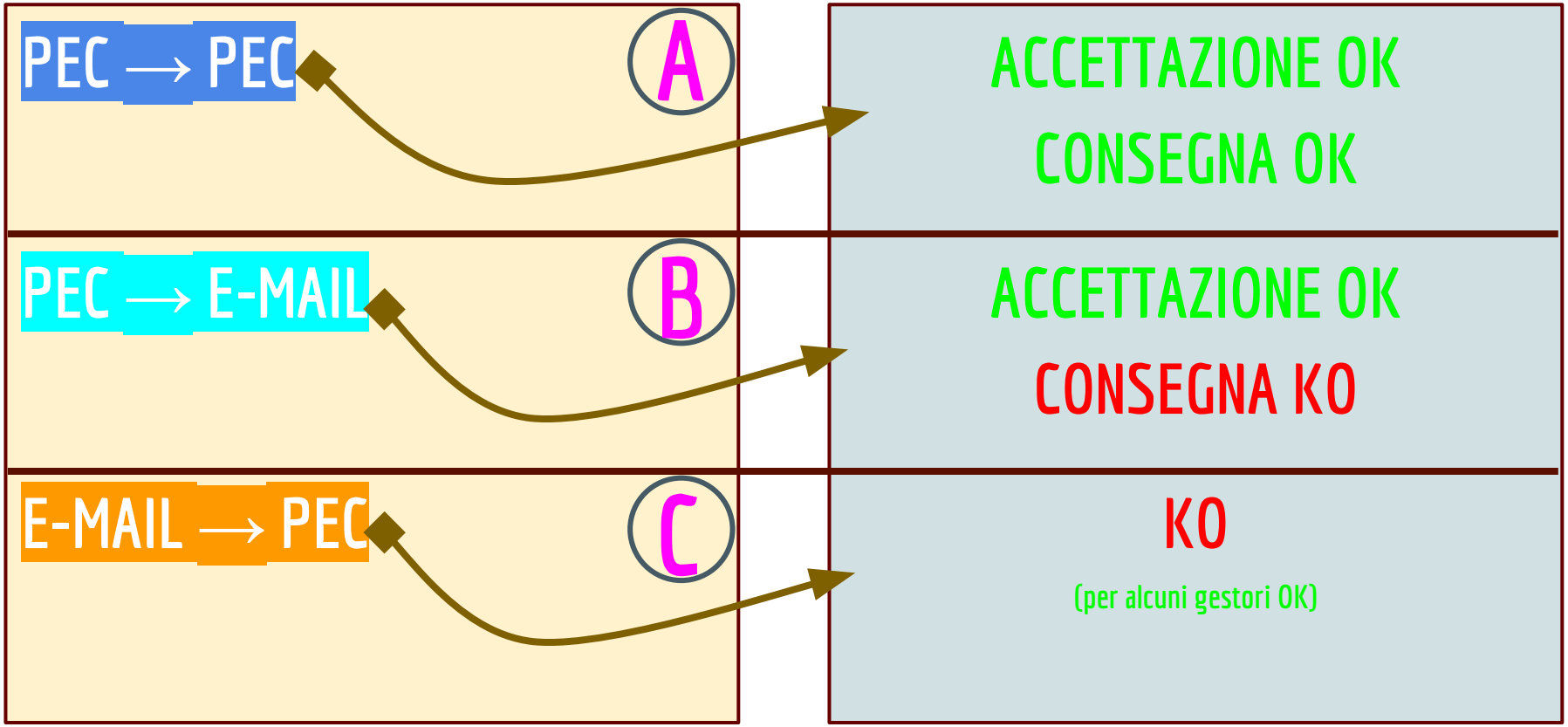
1



```
AUTH PLAIN AGFudG9uaW8ucHJAcGVjLml0AHBpcHBvcGx1dG8=
235 2.7.0 Authentication successful
MAIL FROM:<mario.rossi@pec.it>
250 2.1.0 Ok
RCPT TO:<carlo.bianchi@pec.it>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
mio test di posta elettronica certificata
.
250 2.0.0 Ok: queued as 3qzdRb25SHz2KJFH1
QUIT
221 2.0.0 Bye
```

2

PEC, Interoperabilità



ottobre 2015

SMTP e sicurezza (oltre la crittografia)

[RFC 7672, SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)]

SMTP, debolezze e rimedi: DNSSEC, TLS

SCENARIO A

CLIENT ⟶ MTA ⟶ (DNS) ⟶ SERVER MX (e-mail)

Debolezza:

CLIENT ⟶ MTA ⟶ (DNS) ⟶ FAKE SERVER MX

Rimedio:

CLIENT ⟶ MTA ⟶ (DNSSEC) ⟶ SERVER MX

SCENARIO B

CLIENT ⟶ MTA ⟶ (DNS) ⟶ SERVER MX (e-mail)

Debolezza:

CLIENT ⟶ MTA ⟶ (DNS) ⟶ SERVER MX (e-mail leakage)

Rimedio:

CLIENT ⟶ MTA ⟶ (DNS) ⟶ SERVER MX (e-mail) via TLS

SMTP, debolezze e rimedi: DNSSEC, DANE, TLS

SCENARIO

CLIENT ⟶ MTA ⟶ (DNS) ⟶ SERVER MX (e-mail) via TLS

Debolezza:

CLIENT ⟶ MTA ⟶ (DNS) ⟶ MITM (NO TLS) ⇢ SERVER MX (e-mail) via TLS

Rimedio:

CLIENT ⟶ MTA ⟶ (DNSSEC) ⟶ (DANE) ⟶ SERVER MX (e-mail) via TLS

SMTP e DANE

DANE è un protocollo per legare i certificati TLS all'infrastruttura DNS realizzata con DNSSEC

Il resource record usato nella zona DNS è **TLSA**

```
san-benedetto-del-tronto.gov.it.                    IN MX 10 mail
_587._tcp.mail.san-benedetto-del-tronto.gov.it. IN TLSA 3 1 1 86f34e0f3bf3b4bf33614ad197a8d7a6ecbb4a1df10b3598626e94a7ccd2892b
```

dig _587._tcp.mail.san-benedetto-del-tronto.gov.it. TLSA +dnssec

```
_587._tcp.mail.san-benedetto-del-tronto.gov.it.  86151 IN TLSA 3 1 1 86F34E0F3BF3B4BF33614AD197A8D7A6ECBB4A1DF10B3598626E94A7 CCD2892B


_587._tcp.mail.san-benedetto-del-tronto.gov.it.  86151 IN RRSIG TLSA 8 6 86400 20160510043921 20160502224750 40059 san-benedetto-del-tronto.gov.it.
m3hwqfRwBg986AVucmL2tSqUUoAHvogXTbGBJIK6+F0w08DhPAHR+oMw /VC/sjDujUTr9T4PpOPfv1g2FE6+INHUURktR0wto8E6YIg3n6W4/ca/
t+MApmMFwSBcewYHPHu3rqQuFiwpIII9g2RKYITRrxj8HI3PJ+m1l+E/ gRM=
```

Conclusioni

SMTP è un protocollo che negli ultimi 34 anni ha subìto delle modifiche per meglio adattarsi al crescere dell'industria di Internet su scala planetaria.

Oggi dunque è necessario avvalersi di tutti i miglioramenti e adattamenti proposti dai gruppi di lavoro IETF per far sì che le comunicazioni via e-mail siano le più affidabili e sicure possibile.

Consigli:

Software affidabile e RFC compliant	SPF
FQDN (hostname e EHLO)	DKIM
IP e IPv6	DMARC
PTR corretto	ADSP
TLS	DANE (ove possibile)
DNSSEC (ove possibile)	...?

BONUS

CUTTING EDGE Slides

marzo 2016

[draft-margolis-smtp-sts-00, SMTP Strict Transport Security]


SMTP OTS
YAHOO!
Google
LinkedIn
COMCAST
1&1
Microsoft

SMTP Secure Transport Security, a cosa serve

Con il meccanismo STS i fornitori del servizio di posta elettronica possono dichiarare la loro capacità di instaurare connessioni protette da TLS.

I nomi a dominio dei destinatari pubblicano delle policy per specificare:

- se gli MTA mittenti possono aspettarsi il supporto di TLS
- come gli MTA possono validare il certificato TLS del server esibito al momento della consegna dei messaggi
- cosa fare nel caso in cui TLS non può essere negoziato con successo

SMTP Secure Transport Security, differenze con DANE

- DANE richiede **DNSSEC** per autenticare RR TLSA
- SMTP-STS si basa su un sistema di **Certification Authority** e sul meccanismo **TOFU** (trust on first use)
- SMTP-STS prevede la possibilità di funzionare solo in **modalità report**, così da consentire un progressivo impiego in ambiente di produzione.

SMTP-STS può funzionare con DANE

Conclusioni

SMTP è un protocollo che negli ultimi 34 anni ha subìto delle modifiche per meglio adattarsi al crescere dell'industria di Internet su scala planetaria.

Oggi dunque è necessario avvalersi di tutti i miglioramenti e adattamenti proposti dai gruppi di lavoro IETF per far sì che le comunicazioni via e-mail siano le più affidabili e sicure possibile.

Consigli:

Software affidabile e RFC compliant	SPF
FQDN (hostname e EHLO)	DKIM
IP e IPv6	DMARC
PTR corretto	ADSP
TLS	DANE (ove possibile)
DNSSEC (ove possibile)	*(SMTP-STS)*

Questions?