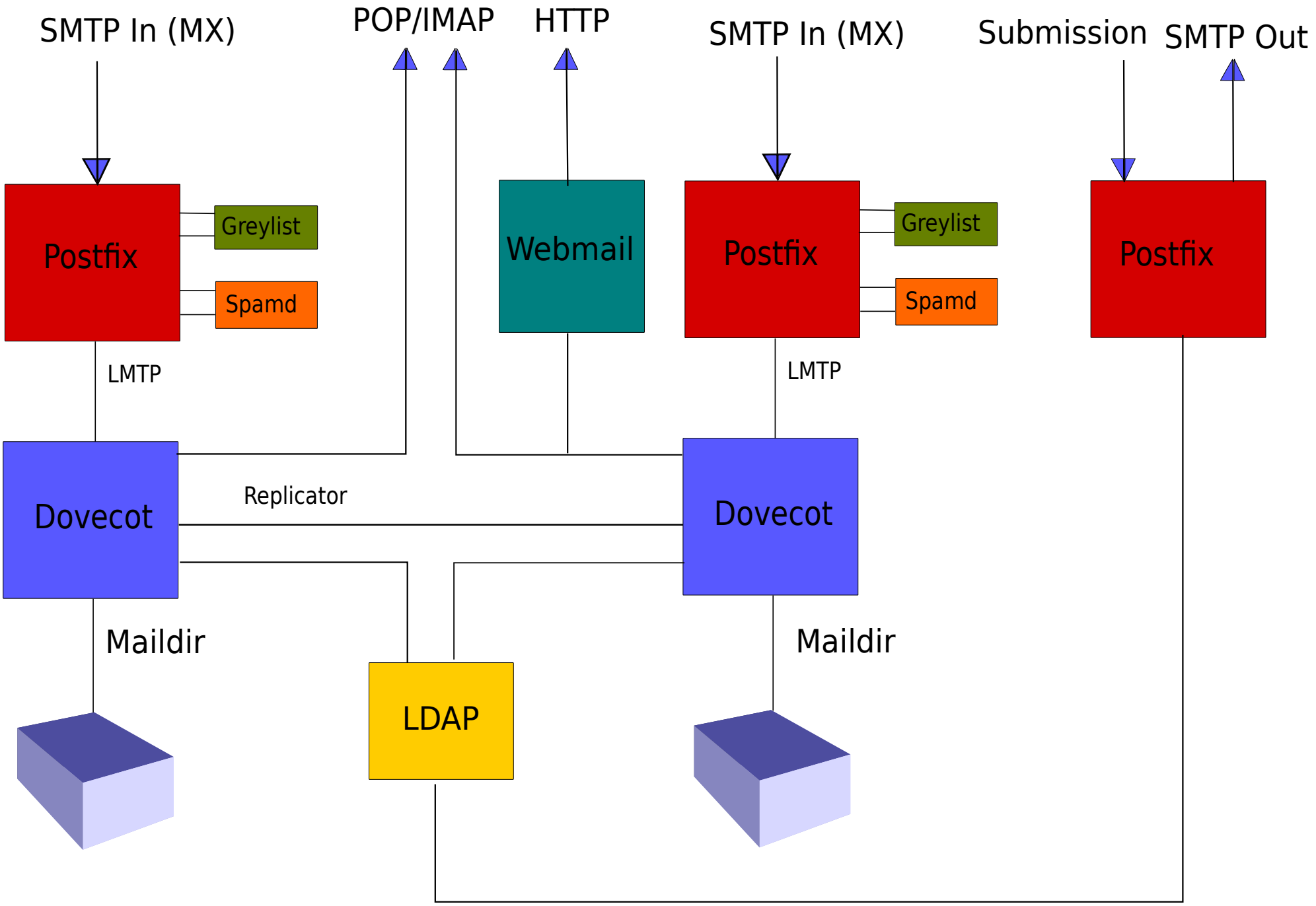
EHLO posta.inaf.it

C. Giorgieri (INAF centrale) - F. Bedosti (INAF IRA)

Migrazione verso un sistema di posta distribuito per 2 kiloutenti


SMTP In (MX)
POP/IMAP
HTTP
SMTP In (MX)
Submission
SMTP Out
Postfix
Greylist
Spamd
Webmail
Postfix
Greylist
Spamd
Postfix
LMTP
LMTP
Dovecot
Replicator
Dovecot
Maildir
LDAP
Maildir

Spam!

L’aspetto piu complesso nella gestione di un sistema di posta oggi.

Le tecniche antispam basate sulla “sender autentication” sono ormai necessarie.

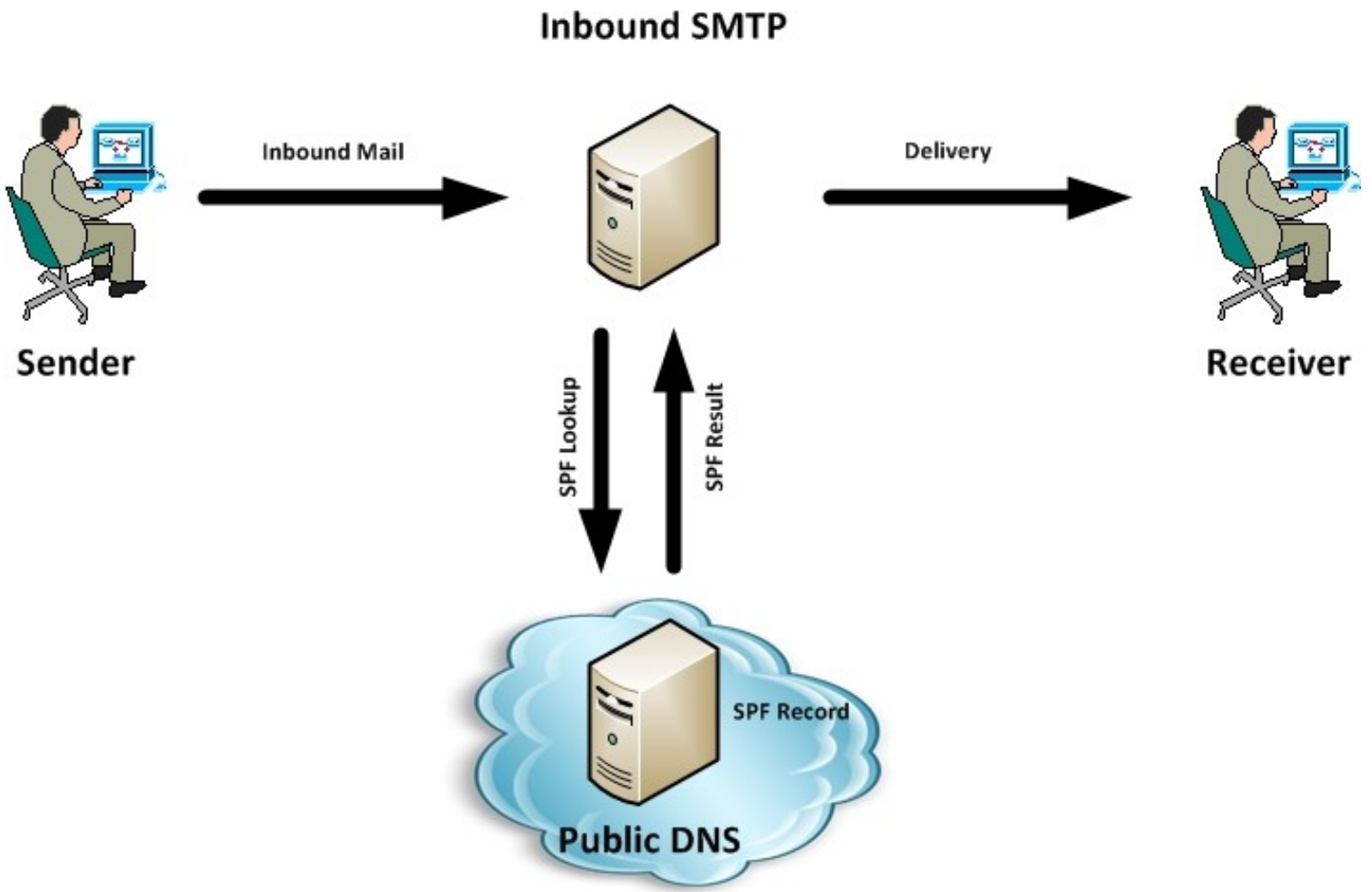
Molti grossi gestori di posta non accettano posta su ipv6 se non firmata con SPF o DKIM.

Sono piu problematiche in scenari complessi.

Sender Policy Framework (SPF)

- Combatte l’email spoofing
- Il sender pubblica via DNS una lista degli MX autorizzati ad inviare messaggi da quel dominio.
- Il 30% della posta legittima lo usa
- Pro:
  - Semplice
  - economico
- Contro
  - Non forwardabile (mailing lists…)
  - Non permette identità di invio diverse

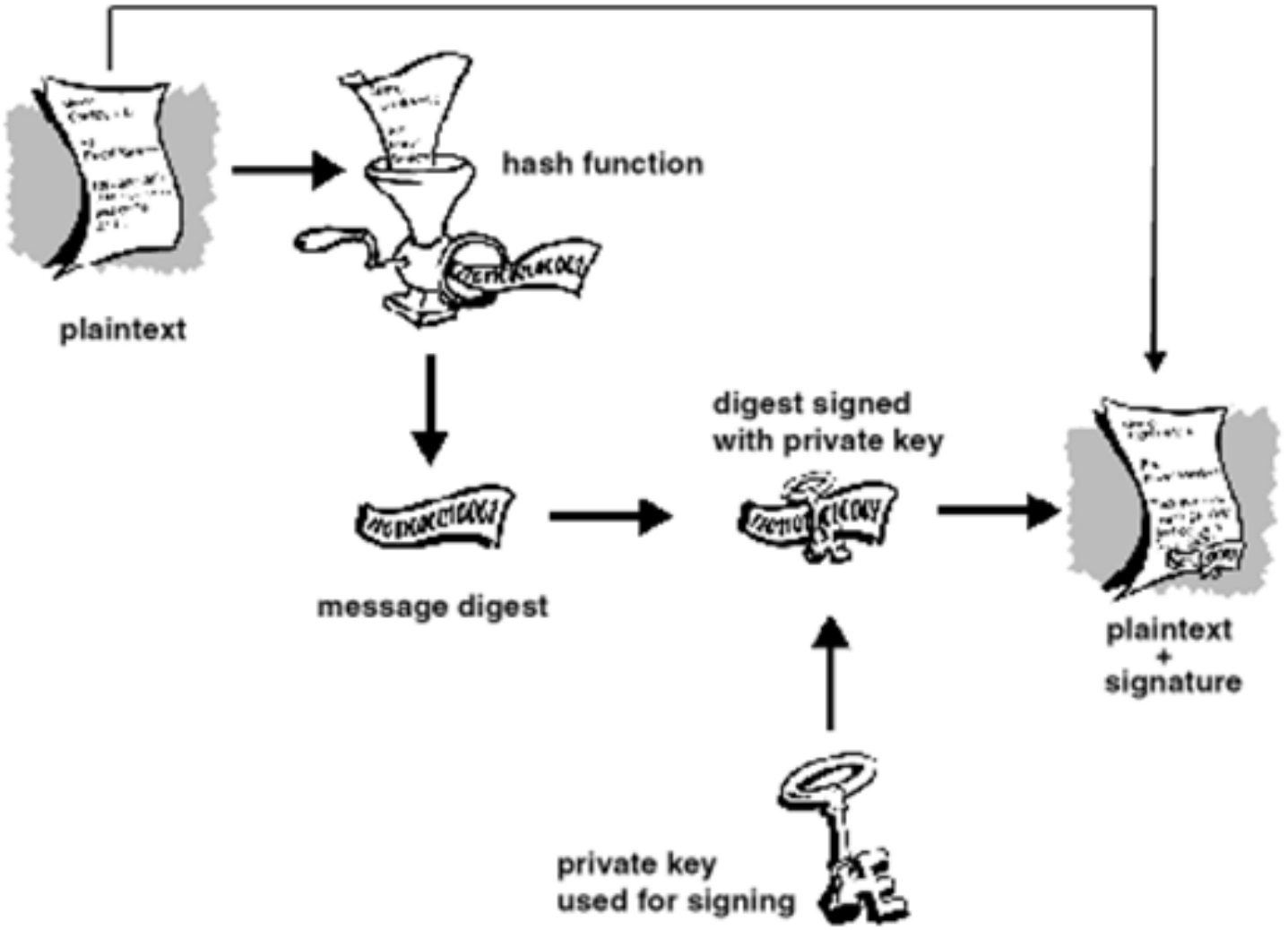
- posta.inaf.it. TXT"v=spf1 ip4:192.167.165.15 ip4:193.205.246.2 ip6:2001:760:2a14::15 -all"



DomainKeys Identified Mail (DKIM)

- Combatte l’email spoofing
- Il sender firma parte dell’header e il body con una chiave la cui controparte pubblica è accessibile via DNS.
- Pro:
  - Flessibile
  - Forwardabile
- Contro:
  - Non tollera modifiche del contenuto o di alcune parti dell’header (footer di mailing lists…)
  - Non permette identità di invio diverse

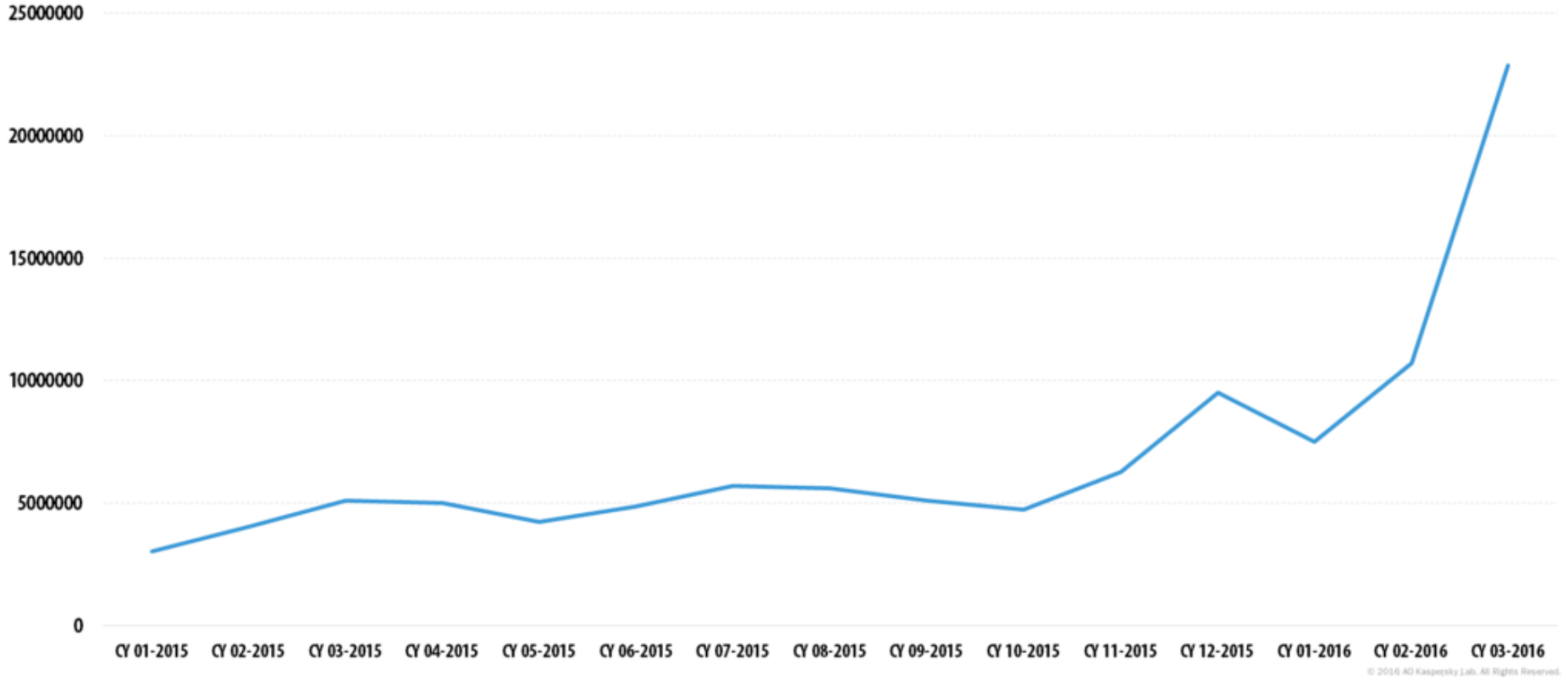
- default._domainkey.posta.inaf.it. 86400 IN TXT "v=DKIM1; k=rsa; p=MIG[...]AQAB"



Greylisting

- Respinge i messaggi al primo tentativo, memorizzando la tripla (mittente, destinatario, ip)
- Se il sender effettua un secondo tentativo con la stessa tripla dopo N secondi, allora accetta il messaggio.
- Pro:
  - economico
  - Efficace, blocca il 75% dei messaggi
- Con:
  - introduce un ritardo
  - Modello pensato per uno scenatio 1MX:1MX
    - Il ritardo aumenta se il sender ha grandi pool di MX di uscita
    - Se ci sono piu MX di ricezione, questi devono coordinarsi

Tornano i virus



Disponibilità

Per garantire una certa affidabilità del sistema occorre replicare:

- I dati
- Le rubriche, pubbliche e private
- Lo stato dei filtri anti-spam
- Lo stato dei filtri server-side
- La sessione della webmail

Autenticazione

- Ldap.inaf.it (round robin)
  - Usato da
    - Rubriche pubbliche
    - Autenticazione POP/IMAP
    - Autenticazione SMTP outbound
    - Inbound & mapping Alias
  - Campi:
    - uid: francesco.bedosti
    - mail: f.bedosti@ira.inaf.it
    - ou: IRA Bologna

Migrazione/1

La situazione attuale

~ 20 domini di posta, ~ 1900 utenti

- Differenti sistemi di autenticazione
- Differenti formati di mailbox
- Complessi strati di alias, gestiti in maniera eterogenea
- Un alias @inaf.it per tutti, definito da ldap
- Utenti esclusivamente locali, effimeri, robot...
- Mailing Lists

Migrazione/2

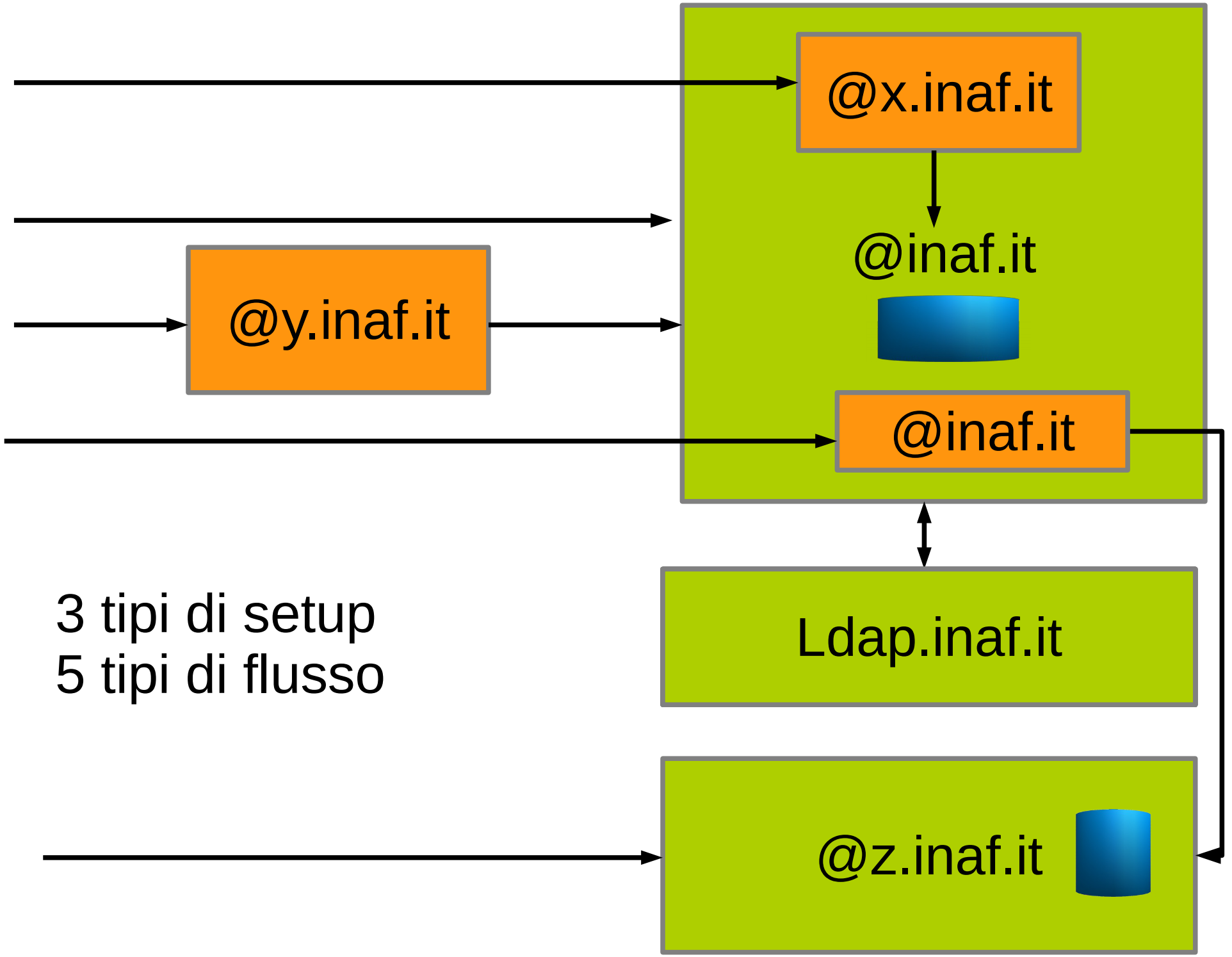
problematiche

- Graduale e parziale
  - Non tutti gli istituti portano la propria posta a @inaf.it
  - Non nello stesso momento
- Il dominio @inaf.it e' gia usato da
  - Alias
  - Utenti (INAF centrale)
- Ogni istituto deve poter amministrare i propri alias e utenti locali
  - Dai sysadmin?
  - Dagli utenti?
- Il sistema di posta è strettamente connesso ad altre infrastrutture locali (allarmi, liste…)
  - Mynetworks sweet mynetworks...
  - Appliances che pretendono di inviare senza autenticarsi
  - Problemi con i sistemi di sender authentication
- Gli alias che puntano ad indirizzi inesistenti generano grandi quantità di bounces

Migrazione/3

procedure

- Periodo di transizione, durante il quale:
  - configurare i client e verificare che tutto funzioni
  - trasferire i dati
    - Convertire maildir?
    - O copiare via IMAP?
  - trasferire le definizioni degli alias


@x.inaf.it
@inaf.it
@y.inaf.it
@inaf.it
3 tipi di setup
5 tipi di flusso
Ldap.inaf.it
@z.inaf.it

Grazie