

*Corso di Informatica Medica*



# Email, sicurezza e posta elettronica certificata

*Lucio Marinelli*

# Email



- “Electronic mail”
- Prima email inviata in ARPANET nel 1971
- Nata insieme alla stessa internet
- Sistema “store-and-forward”
- Codificata utilizzando algoritmo “MIME”
- Invia messaggi di testo ma anche file come allegati

# Struttura email



- Intestazione (“header”)
  - From: mittente
  - To: destinatario
  - CC: destinatario in copia
  - BCC/CCN: destinatario in copia nascosta
  - Subject: oggetto
- Corpo (“body”)
- Allegati (“attachment”)

Invia

Salva adesso

Ignora

Autosave disabled


**Da:** [luciomarinelli@gmail.com](mailto:luciomarinelli@gmail.com) [cambia](#)

**A:** |

**Cc:**

**Ccn:**

**Oggetto:**

 [Allega un file](#)

[Formattazione speciale »](#)

\* 

[Controlla ortografia ▼](#)

—  
Lucio Marinelli

Invia

Salva adesso

Ignora

Autosave disabled

Completato



# Indirizzo email



nome\_utente@host.dominio

## Esempi:

marcorossi@alice.it

paoloverdi@libero.it

giuliobianchi@gmail.com

- mai spazi
- sempre minuscolo (maiuscole=minuscole)
- elemento @ caratterizza l'indirizzo email

# Password



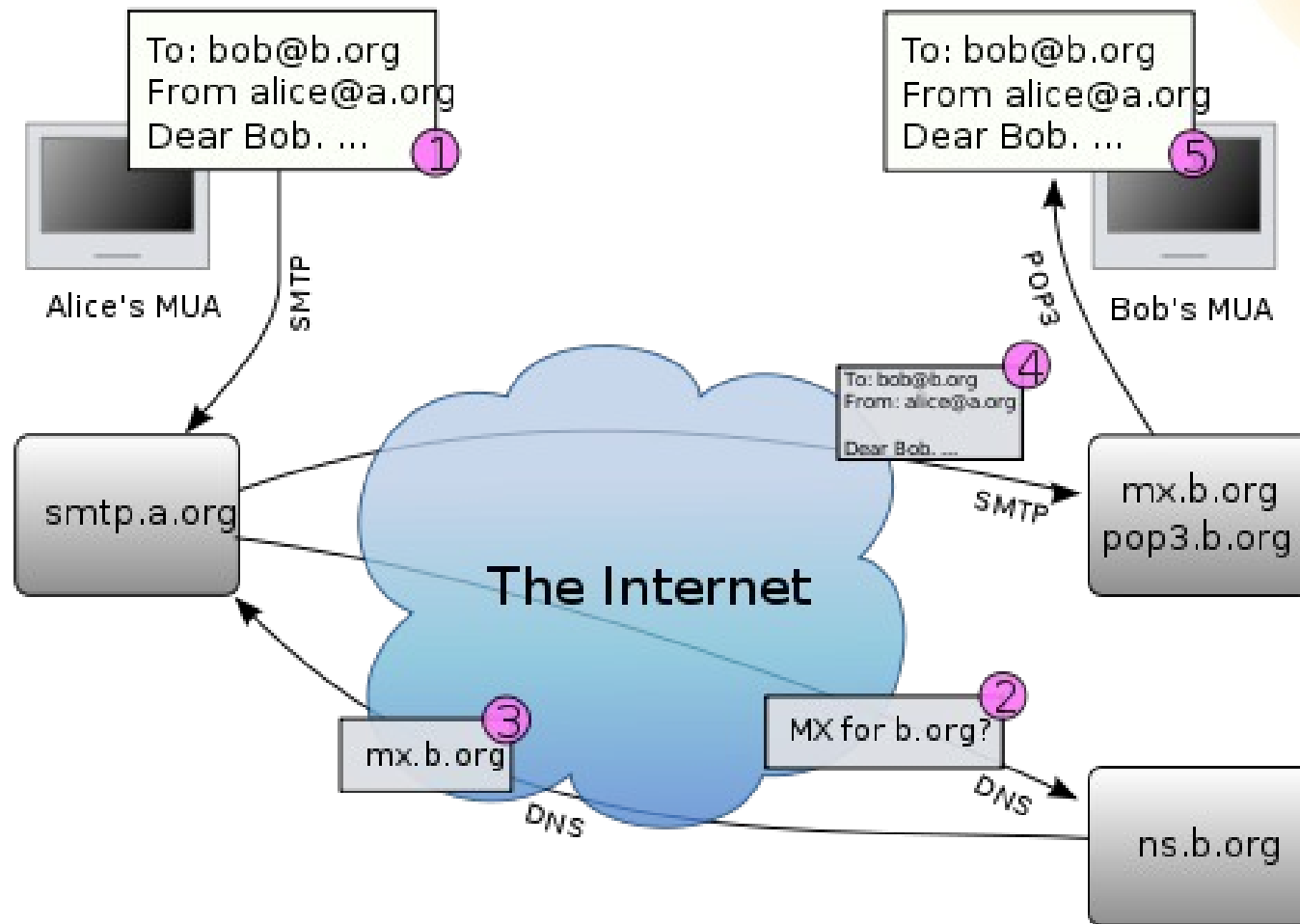
- Si associa ad ogni indirizzo email
- Utilizzata in generale in informatica ogni volta che si vuole limitare l'accesso ad una risorsa
- Tentativi di uso illecito utilizzano algoritmi che cercano di “indovinare” la password, per cui:
  - Meglio lunga
  - Contenente anche numeri o simboli (es. &-\_)
  - Evitare proprio nome e data di nascita o comunque informazioni facilmente ottenibili
  - Non utilizzare la stessa password per tutti i servizi

# Cosa serve?



- Tramite browser internet
  - Necessario essere collegati (online)
  - Si utilizza l'interfaccia del proprio provider email
  - Tutti i messaggi disponibili da qualsiasi PC
  - Spazio limitato
- Tramite programma di posta
  - Utilizzabile anche non collegati (offline)
  - Necessario configurare il programma di posta
  - I messaggi restano sul proprio PC
  - Spazio virtualmente illimitato

# Percorso del messaggio email





# Email e sicurezza

- Crittografia permette di limitare accesso a dati
- Email viaggiano non crittografate
- Possibilità di intercettazione
- Identità mittente non sicura
- Consegna del messaggio non garantita
- Difficile filtrare email non desiderate
- Rischio virus



# Email sicura

- Algoritmo S/MIME invece che MIME
- Firma sicura del messaggio
- Crittografia del contenuto
- Sistema di crittografia a chiave pubblica
- Anello di autorità certificatrici internazionali
- Interoperabilità da/verso estero



# Crittografia asimmetrica

*Whitfield Diffie and Martin Hellman, 1975*

- E' possibile creare una coppia di chiavi “speculari” e uniche (pubblica e privata)
- La chiave pubblica viene data a tutti
- La chiave privata resta riservata
- Ciò che viene criptato con una chiave pubblica può essere decriptato solo con la corrispondente chiave privata
- Ciò che viene firmato con una chiave privata può essere verificato solo con la corrispondente chiave pubblica

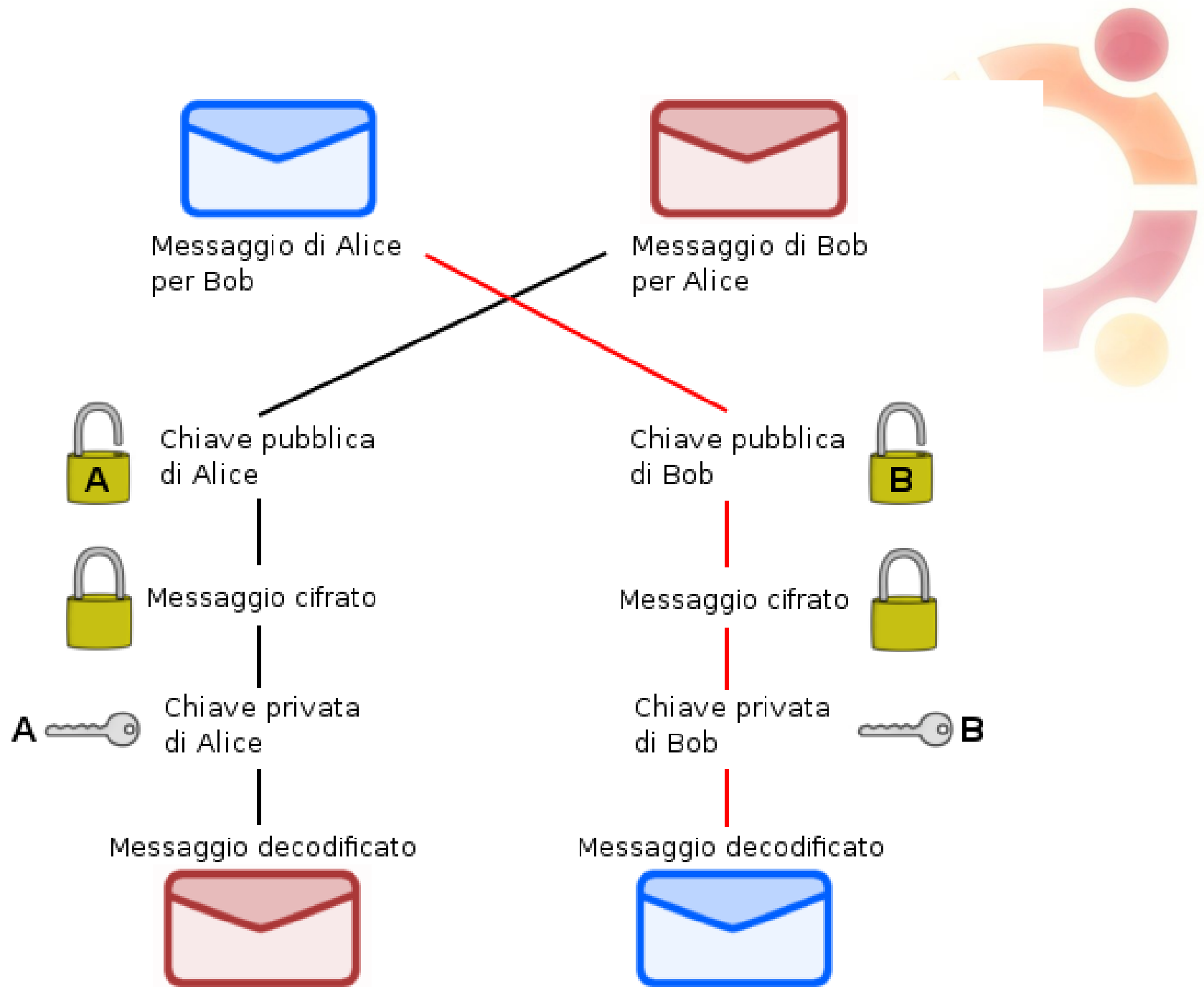


Il *lucchetto* corrisponde alla  
chiave pubblica



La *chiave* corrisponde alla  
chiave privata





# Legge 20 Gennaio 2009

conversione del D.L. 185/2008

articolo 16

6) Le imprese costituite in forma societaria sono tenute a indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali. Entro tre anni dalla data di entrata in vigore del presente decreto tutte le imprese, già costituite in forma societaria alla medesima data di entrata in vigore, comunicano al registro delle imprese l'indirizzo di posta elettronica certificata. L'iscrizione dell'indirizzo di posta elettronica certificata nel registro delle imprese e le sue successive eventuali variazioni sono esenti dall'imposta di bollo e dai diritti di segreteria

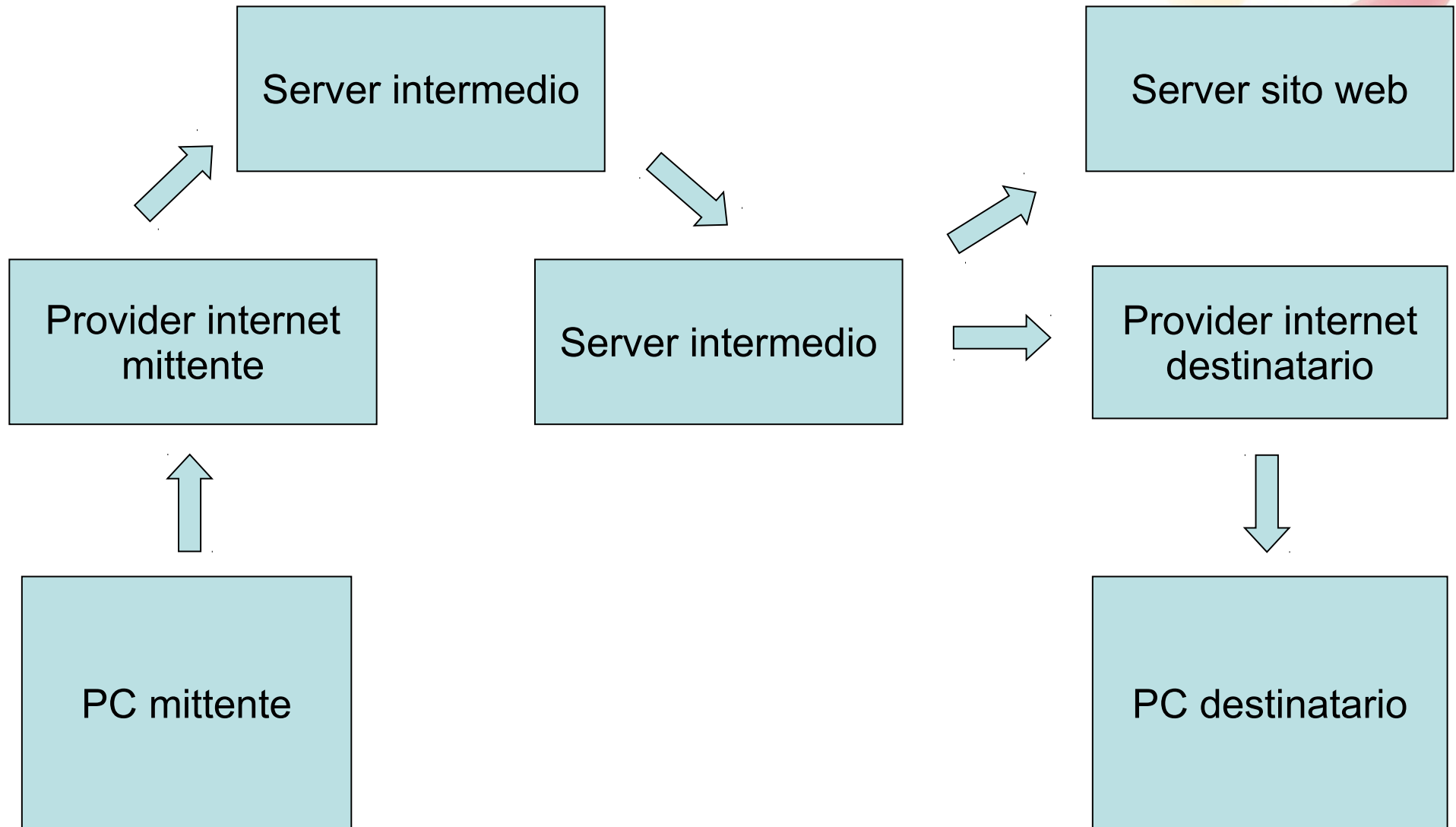
7) I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata o analogo indirizzo di posta elettronica di cui al comma 6 entro un anno dalla data di entrata in vigore del presente decreto. Gli ordini e i collegi pubblicano in un elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni, i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata.

# Sistemi di garanzia



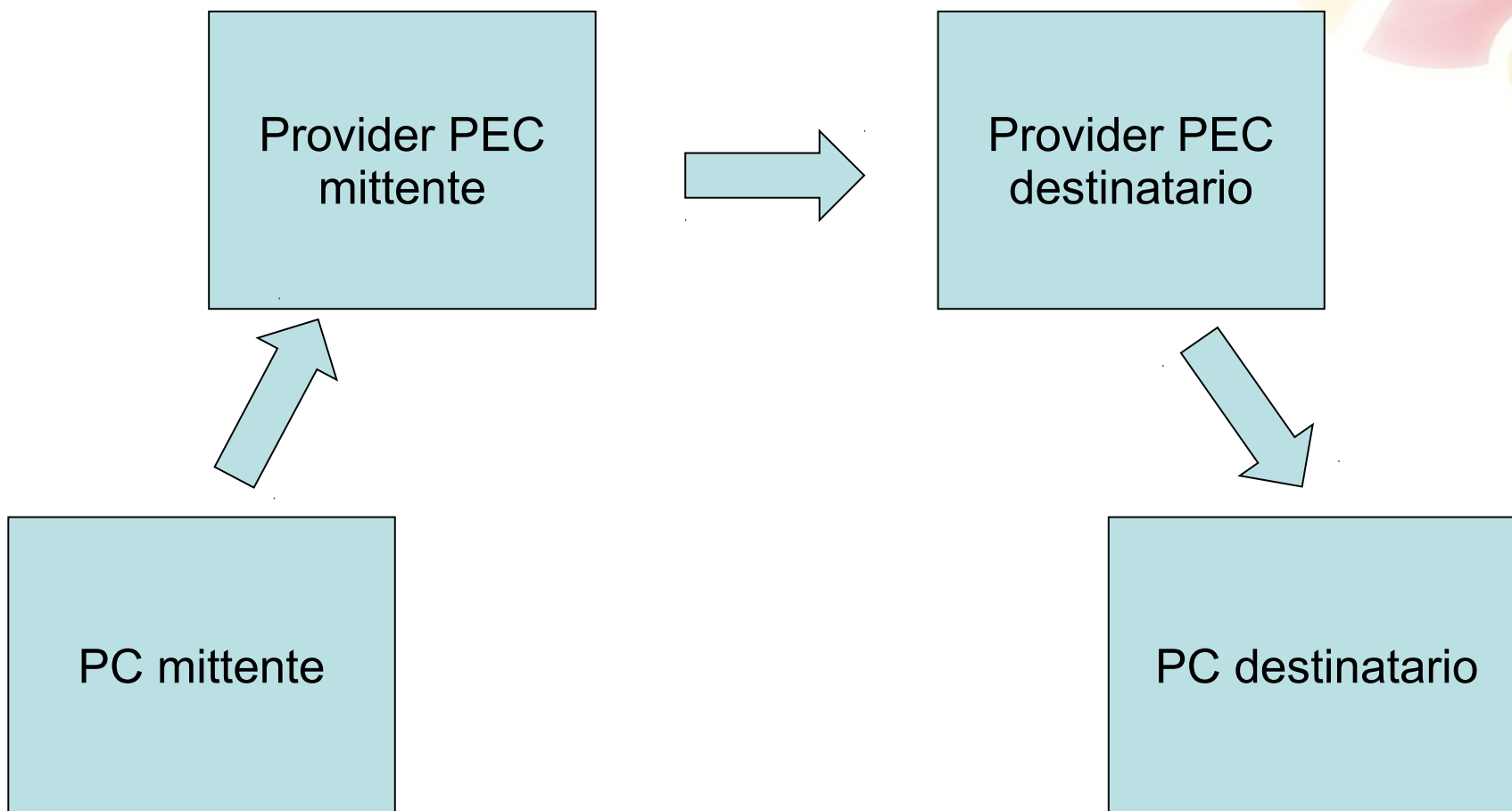
- Posta elettronica certificata (PEC)
- Certificati di posta elettronica S/MIME (CPE)
- [crittografia a chiave pubblica non certificata, es. open PGP, GnuPG]

# Come viaggiano le informazioni su internet





# Come viaggia la PEC



# Posta elettronica certificata

- E' chi fornisce il servizio (provider) a “chiudere la busta” e certificarla
- Ricevute di consegna generate dal provider
- Necessario usare indirizzo email del provider
- Funziona solo in Italia
- Il contenuto della mail non è crittografato



# PEC: punti oscuri



- La data e ora di invio è certificata solo dalla PEC e non dai certificati S/MIME
- Solo i certificati S/MIME permettono l'interoperabilità con i sistemi internazionali
- L'obbligo di dotarsi di PEC non è sanzionato
- Non è chiaro se l'indirizzo di PEC possa essere usato solo per scopi professionali

# Newsletter



- Servizio basato su email
- Lista di iscritti sottoforma di indirizzi email
- Il gestore invia a tutti una email con contenuti informativi, aggiornamento, ecc
- Di solito comunicazioni periodiche
- Gli iscritti ricevono passivamente
- Possibilità di rimuovere o iscrivere il proprio indirizzo email

# Mailing list

- Gruppo di iscritti sottoforma di indirizzi email
- Ciascuno può inviare un messaggio alla lista
- Ciascuno può rispondere ad un messaggio
- Ogni messaggio inviato viene ritrasmesso automaticamente a tutti
- Ruolo attivo degli iscritti
- Possibilità di rimuovere o iscrivere il proprio indirizzo email



# Spam

- Email indesiderate a contenuto pubblicitario
- “Mercato” di indirizzi email validi
- Visitando il link nel messaggio oppure rispondendo si “valida” la propria email
- Filtri anti-spam



# Scam

- Scam = atto fraudolento
- Molto spesso email che prospetta un guadagno gratis
  - Offerte di denaro
  - Vincita alla lotteria
  - Proposte sentimentali
  - **Phishing**



# Phishing

- “a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly”
- Email apparentemente provenienti dalla propria banca
- Richiedono inserimento di password e dati personali
- I dati vengono raccolti e utilizzati da pirati





# Esempio di phishing

Avviso di segnalazione...

Da: Grupo Banca Popolare <agenzia@bpb.it>...Aggiungi alla Rubrica

Abbiamo identificato da poco tempo che diversi computer si sono stati collegati al Suo conto Online Banking e sono stati presenti molteplici errori di parola prima del collegamento. Adesso e' necessario che Lei ci riconfermi le informazioni del Suo presente conto.

Se non riceviamo le informazioni entro il 11 Giovedì, 2010, saremo costretti a sospendere il Suo conto per un periodo indefinito, come se fosse stato usato in scopi fraudolenti. La ringraziamo per la Sua cooperazione in questo problema.

Per confermare i dati del Suo conto Online Banking cliccare sul seguente link:

<https://hbnet.cedacri.it/HBNET/login.nsf/05424?readform>

La ringraziamo per la Sua pazienza riguardando questo inconveniente.

© 2010 Banca Popolare di Bari, Società cooperativa per Azioni - Sede sociale e Direzione Generale  
Corso Cavour 19 - 70122 Bari Cod. fisc. e Partita iva n. 00254030729 - Iscr. reg. impr. di Bari n.  
00254030729 - Albo az. cred. n. 4616 / REA n. 105047 - ABI 05424 - Capitale Sociale Euro  
298.911.190,00 i.v. xhtml - credits

# Email spoofing



- Modificata l'intestazione della email in modo da modificare il campo “From”
- Messaggio apparentemente proveniente da una persona nota
- Tecnica spesso utilizzata in associazione alle precedenti (spam, scam...)
- Se associata a virus è possibile che venga utilizzata la lista degli indirizzi dei propri conoscenti

# Virus



- Piccolo programma in grado di replicarsi e diffondere da un computer a un altro
- Può determinare o meno danno dei dati presenti sul computer o alterarne il funzionamento
- Possono essere nascosti all'interno di software funzionante (trojan)
- Possono propagarsi direttamente su internet o tramite email o tramite dispositivi removibili (es. chiavette USB)

# Spyware



- Piccolo programma che infetta un computer e alterarne il funzionamento
- Non ha capacità autoreplicante
- Può determinare l'acquisizione automatica di altro spyware tramite internet
- Può rallentare il computer
- Può acquisire dati personali o riguardanti la navigazione
- Non sempre rimosso dagli antivirus

# Come difendersi?



- In Windows avere sempre un antivirus attivo e aggiornato
- Attivare il firewall
- Mantenere il computer aggiornato (correzione di vulnerabilità del sistema operativo)
- Non installare software proveniente da fonti non sicure
- Non eseguire allegati email sospetti
- Non rispondere a email di origine sospetta



I contenuti sono resi disponibili sotto licenza CreativeCommons:

“Attribuzione - Non commerciale

- Condividi allo stesso modo 2.5 (ITALIA)”

<http://creativecommons.org/licenses/by-sa/2.5/it/>

