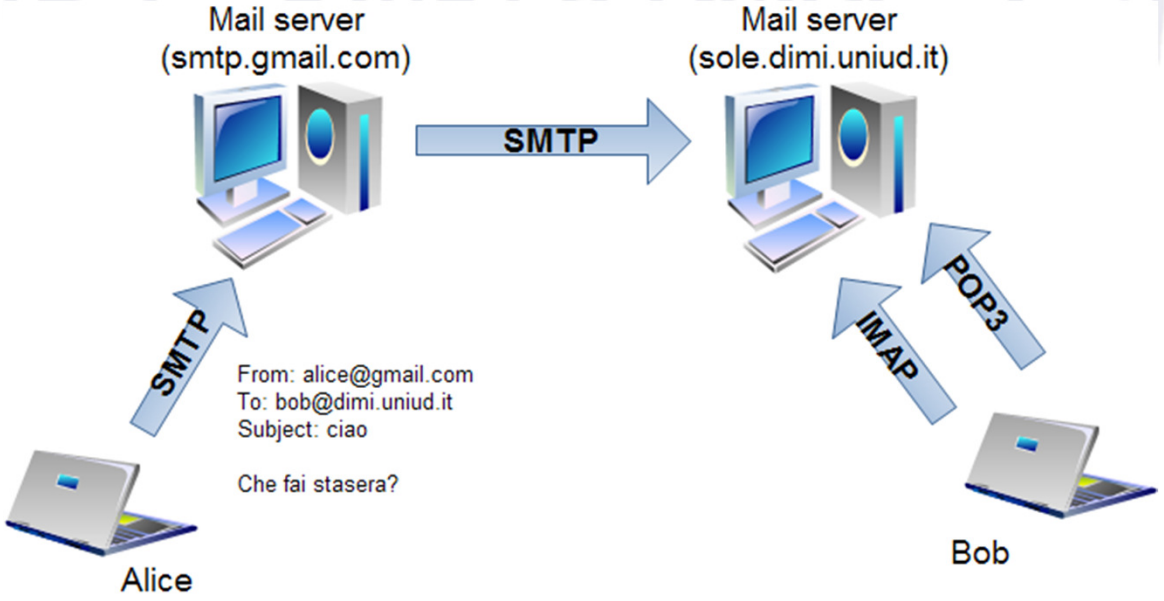
Posta elettronica e sicurezza

Protocolli per la posta elettronica

- Distinguiamo tra due tipi di protocolli per la gestione della posta elettronica:
  - Protocolli per l'invio della posta (SMTP)
  - Protocolli per l'accesso alla posta memorizzata su un server (POP3, IMAP)



Protocolli per la posta elettronica

- I protocolli SMTP, POP3, IMAP sono stati studiati senza considerare le implicazioni relative alla sicurezza
- Il traffico viene trasmesso in chiaro, SMTP non ha alcun meccanismo di autenticazione

- I protocolli standard per l'invio e la ricezione della posta elettronica sono insicuri!

SMTP

- I server SMTP accettano connessioni sulla porta 25
- Il protocollo si basa sullo scambio di semplici comandi formati da righe di testo in chiaro
- Esistono versioni più sicure del protocollo (ESMTP), ma il protocollo SMTP standard è ancora molto diffuso

S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: Alice Example <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye

Sicurezza di SMTP

- Il protocollo SMTP non offre alcuna garanzia di riservatezza (il testo viene trasmesso in chiaro)…
- …né autenticazione: è possibile spedire mail con un mittente falsificato, il tutto rispettando il protocollo SMTP

E-mail spoofing

- Usare il comando telnet per collegarsi alla porta 25 di un server SMTP
- Usare i seguenti comandi SMTP
  - `HELO nome.di.dominio`
  - `MAIL FROM: indirizzo@del.mittente`
  - `RCPT TO: indirizzo@del.destinatario`
  - `DATA`

HELO specifica il nome della macchina da cui proviene il messaggio
MAIL FROM: specifica l'indirizzo del mittente
RCPT TO: specifica l'indirizzo del destinatario
DATA: indica che le righe successive fanno parte del corpo della mail

E-mail spoofing / 2

- Dopo il comando **`DATA`** si scrive la mail vera e propria, composta da un gruppo di header e un body, separati da una linea vuota.

- La mail viene conclusa da una linea contenente esclusivamente un punto

- La connessione viene chiusa dal comando QUIT

E-mail spoofing - esempio

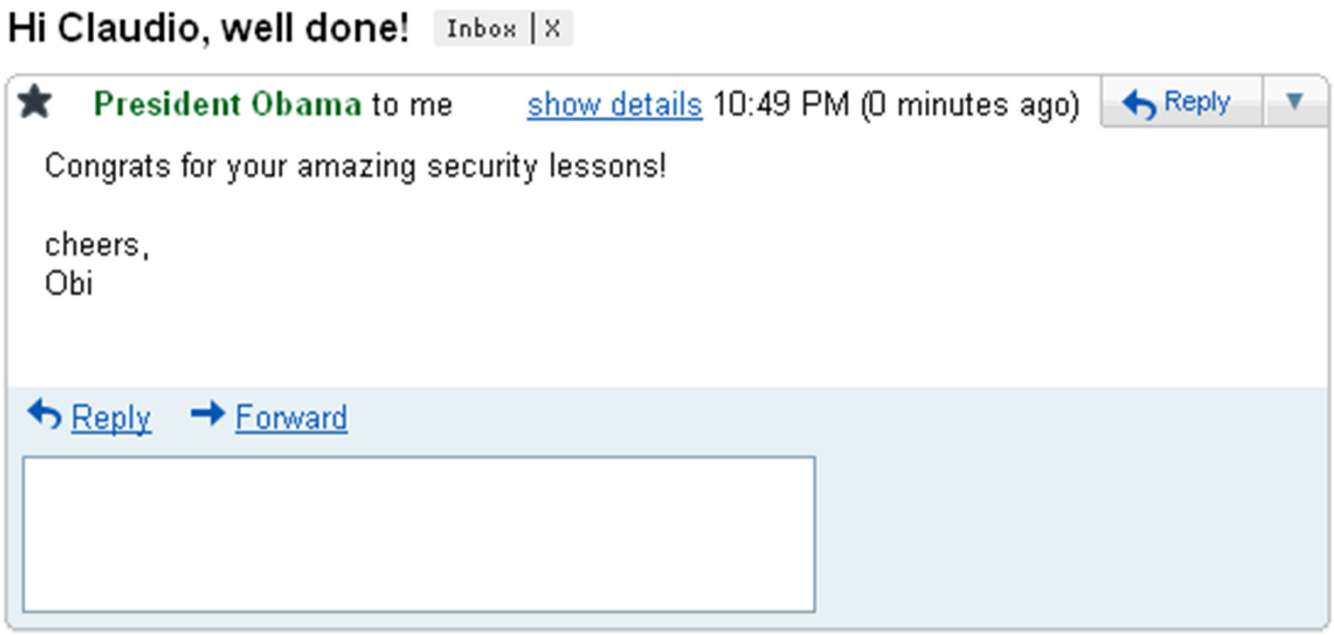
```
avires:/etc/postfix# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
220 avires.dimi.uniud.it ESMTP Postfix (Debian/GNU)
HELO whitehouse.gov
250 avires.dimi.uniud.it
MAIL FROM: president@whitehouse.gov
250 2.1.0 Ok
RCPT TO: [redacted]@gmail.com
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: President Obama <president@whitehouse.gov>
To: Claudio Piciarelli <[redacted]@gmail.com>
Subject: Hi Claudio, well done!

Congrats for your amazing security lessons!

cheers,
Obi
.
250 2.0.0 Ok: queued as 57A50186
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
avires:/etc/postfix#
```

E-mail spoofing – esempio / 2

- La mail giunge a destinazione con il mittente falsificato…



E-mail spoofing – esempio / 3

```
Delivered-To: [redacted]@gmail.com
Received: by 10.216.182.81 with SMTP id n59cs96531wem;
        Sun, 21 Mar 2010 14:25:34 -0700 (PDT)
Received: by 10.87.73.40 with SMTP id a40mr7308707fgl.41.1269206734021;
        Sun, 21 Mar 2010 14:25:34 -0700 (PDT)
Return-Path: <president@whitehouse.gov>
Received: from quasar.dimi.uniud.it (quasar.dimi.uniud.it [158.110.144.24])
        by mx.google.com with ESMTP id 25si430710fxm.29.2010.03.21.14.25.33;
        Sun, 21 Mar 2010 14:25:33 -0700 (PDT)
Received-SPF: neutral (google.com: 158.110.144.24 is neither permitted nor denied by best guess r
Authentication-Results: mx.google.com; spf=neutral (google.com: 158.110.144.24 is neither permitt
Received: from localhost (localhost [127.0.0.1])
        by quasar.dimi.uniud.it (Postfix) with ESMTP id 51A471BDF97
        for <[redacted]@gmail.com>; Sun, 21 Mar 2010 22:25:33 +0100 (CET)
Received: from quasar.dimi.uniud.it ([127.0.0.1])
 by localhost (quasar.dimi.uniud.it [127.0.0.1]) (amavisd-maia, port 10024)
 with ESMTP id 15596-04 for <[redacted]@gmail.com>;
 Sun, 21 Mar 2010 22:25:30 +0100 (CET)
Received: from sole.dimi.uniud.it (sole.dimi.uniud.it [158.110.144.29])
        by quasar.dimi.uniud.it (Postfix) with ESMTP id F3B451BDF54
        for <[redacted]@gmail.com>; Sun, 21 Mar 2010 22:25:29 +0100 (CET)
Received: from avires.dimi.uniud.it (primergy.dimi.uniud.it [158.110.144.168])
        by sole.dimi.uniud.it (Postfix) with ESMTP id 413CB3FC141
        for <[redacted]@gmail.com>; Sun, 21 Mar 2010 22:25:30 +0100 (CET)
Received: from whitehouse.gov (localhost.localdomain [127.0.0.1])
        by avires.dimi.uniud.it (Postfix) with SMTP id 57A50186
        for <[redacted]@gmail.com>; Sun, 21 Mar 2010 22:49:36 +0100 (CET)
From: President Obama <president@whitehouse.gov>
To: Claudio Piciarelli <[redacted]@gmail.com>
Subject: Hi Claudio, well done!
Message-Id: <20100321214944.57A50186@avires.dimi.uniud.it>
Date: Sun, 21 Mar 2010 22:49:36 +0100 (CET)
X-Virus-Scanned: Maia Mailguard 1.0.2

Congrats for your amazing security lessons!

cheers,
Obi
```

Unico indizio della frode: l'indirizzo IP della macchina sorgente

Rendere sicura la posta elettronica

- Possibili approcci:
  - Usare una variante sicura del protocollo che garantisca autenticazione e riservatezza (SASL + TLS) (prossima lezione)
  - Spostare la gestione della sicurezza a livello di applicazione, e continuare a trasmettere i dati (autenticati e cifrati) su un canale insicuro

Un software per la posta sicura (e non solo): PGP

- PGP (Pretty Good Privacy) è un software per la gestione di documenti cifrati/autenticati basato su un approccio ibrido (crittografia asimmetrica + simmetrica)
- Inizialmente sviluppato da Phil Zimmermann nel 1991
- Nascita travagliata, dovuta a problemi di brevetti (algoritmo RSA) e alla legge USA sull'esportazione di materiale bellico
- Una volta messo su internet, fu impossibile fermarne la diffusione

Lo standard OpenPGP e le alternative

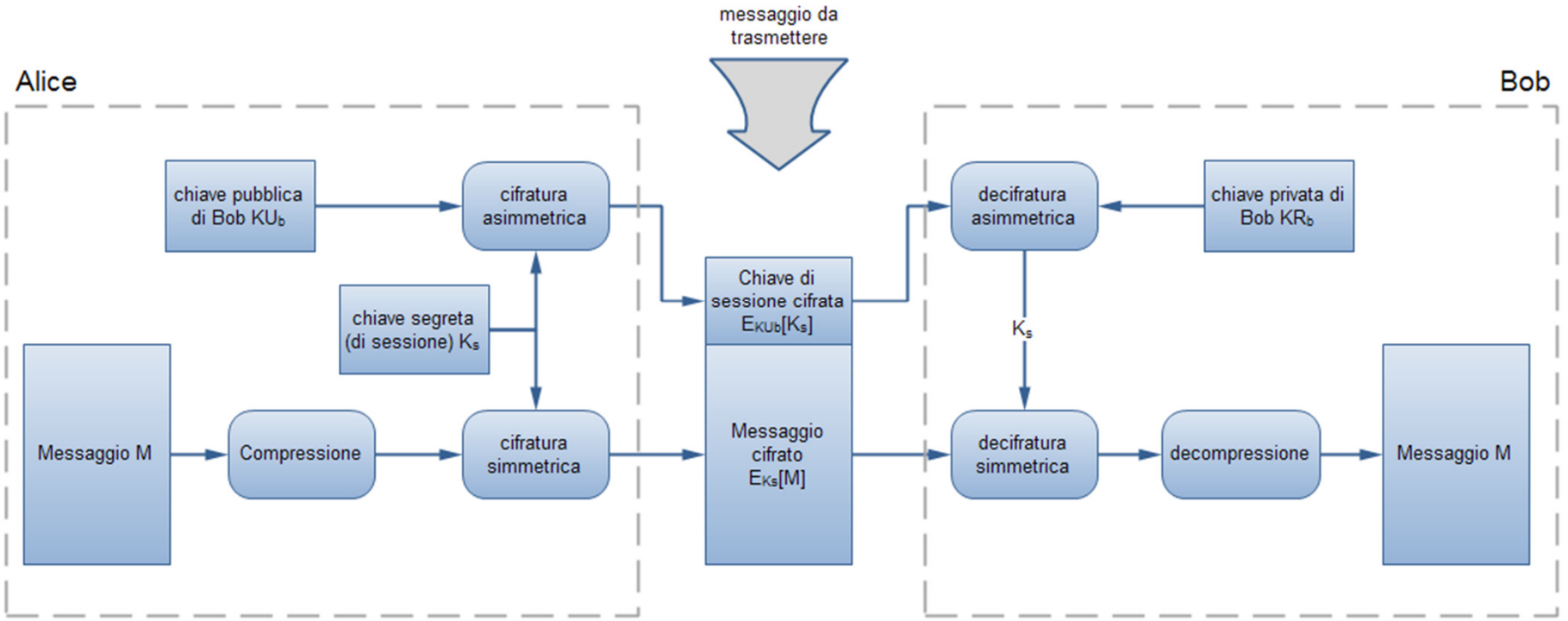
- Oggi PGP è diventato un prodotto commerciale (http://www.pgp.com)
- Tuttavia il formato dei messaggi è stato standardizzato (OpenPGP), per cui è stato possibile sviluppare alternative free compatibili con PGP
- La versione free più usata attualmente: GPG (GNU Privacy Guard) http://www.gnupg.org

Segretezza in PGP

- Approccio ibrido
- Cifratura simmetrica a blocchi 64 bit CFB (cipher feedback). Algoritmi usati: IDEA, 3DES, CAST-128, Blowfish, Twofish, AES
- Cifratura a chiave pubblica per la trasmissione delle chiavi segrete simmetriche. Algoritmi usati: RSA, ElGamal

- La chiave usata per la cifratura simmetrica (detta *chiave di sessione*) è una chiave casuale e monouso (la dimensione della chiave dipende dall'algoritmo usato. Tipicamente: 128 bit).

Segretezza in PGP / 2



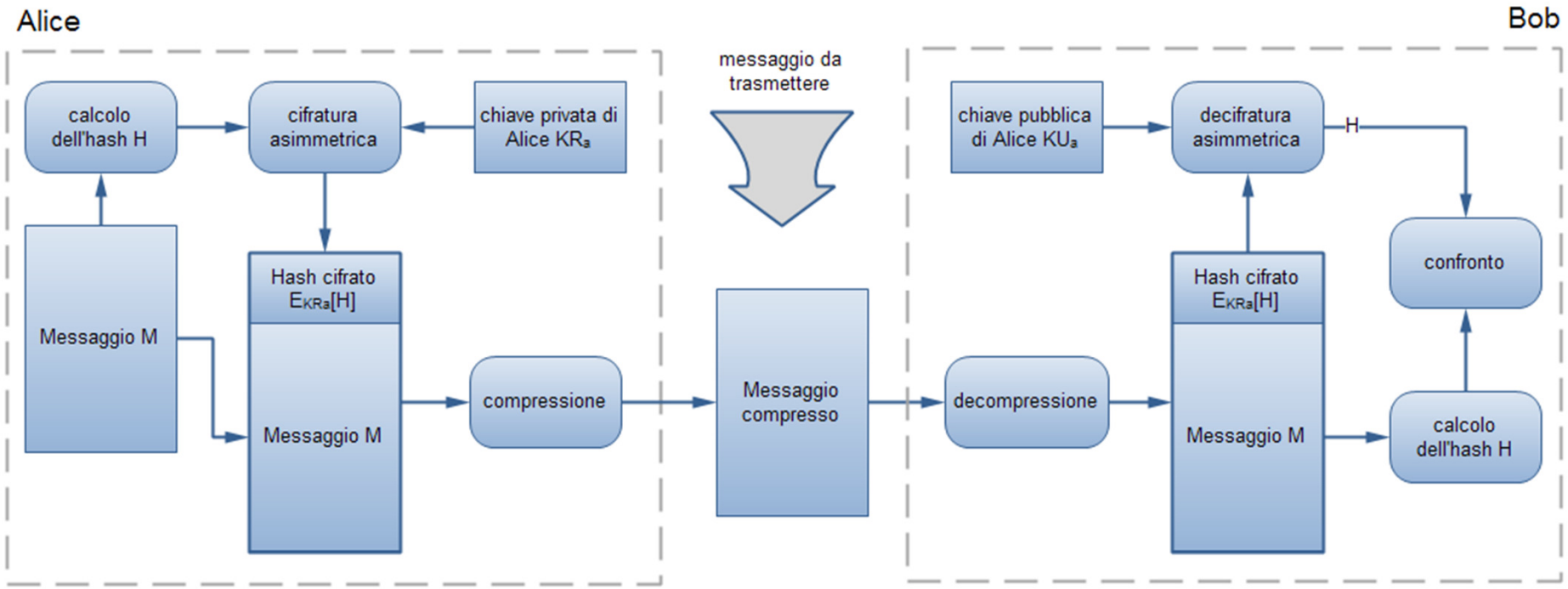
Autenticazione in PGP

- Generazione di un hash del messaggio. Algoritmi: MD5 (deprecato), SHA-1, SHA-2

- Firma digitale dell'hash, usando gli algoritmi di cifratura a chiave pubblica o un algoritmo apposito per la firma digitale (DSA)

(garantisce autenticazione, integrità, non ripudiabilità)

Autenticazione in PGP / 2



Segretezza e autenticazione

- Segretezza e autenticazione possono essere garantite applicando entrambi gli schemi

- Prima il messaggio viene firmato digitalmente e poi cifrato

Compatibilità con la posta elettronica

- Gli standard di posta elettronica non sono studiati per trasmettere byte arbitrari, ma solo testo
- I file creati da PGP vengono trasformati in file di testo mediante la codifica Radix-64 (procedura di *armoring*)
- Gruppi di 3 byte vengono suddivisi in 4 elementi di 6 bit ciascuno. Ogni elemento è codificato secondo la seguente tabella:

Binary	ASCII	Binary	ASCII	Binary	ASCII	Binary	ASCII
000000	A	010000	Q	100000	g	110000	w
000001	B	010001	R	100001	h	110001	x
000010	C	010010	S	100010	i	110010	y
000011	D	010011	T	100011	j	110011	z
000100	E	010100	U	100100	k	110100	0
000101	F	010101	V	100101	l	110101	1
000110	G	010110	W	100110	m	110110	2
000111	H	010111	X	100111	n	110111	3
001000	I	011000	Y	101000	o	111000	4
001001	J	011001	Z	101001	p	111001	5
001010	K	011010	a	101010	q	111010	6
001011	L	011011	b	101011	r	111011	7
001100	M	011100	c	101100	s	111100	8
001101	N	011101	d	101101	t	111101	9
001110	O	011110	e	101110	u	111110	+
001111	P	011111	f	101111	v	111111	/

I key ring

- Le chiavi pubbliche e private di un utente sono contenute nei cosiddetti key ring (portachiavi)
- In un keyring, ogni chiave è contraddistinta da un ID univoco, composto dai 64 bit meno significativi della chiave pubblica
- Ad ogni chiave sono associate una o più identità (tipicamente gli indirizzi e-mail di un utente)
- Le identità permettono di selezionare automaticamente la chiave di cifratura corretta quando si spedisce un messaggio cifrato
- Ad ogni chiave è associato anche un hash (chiamato *fingerprint*), che permette di verificarne rapidamente l'integrità

Metodi di diffusione della chiave pubblica

- Consegna della chiave su canale sicuro
- Verifica della chiave mediante hash
- Uso di certification authorities esterne

- *Web of trust* (tecnica adottata per la prima volta proprio da PGP!): sistema decentralizzato in cui ogni utente può fungere da garante per le chiavi altrui, firmando digitalmente un certificato che ne garantisce l'autenticità

Web of trust di PGP

- Nel web of trust di PGP, è possibile specificare diversi livelli di “trust” per ogni utente
- Se A si fida pienamente di B, e B certifica la validità della chiave di C, allora A considera valida la chiave di C
- Se A si fida marginalmente di X, Y e Z, e tutti loro certificano la validità della chiave di C, allora A considera valida la chiave di C

- In altre parole, più basso è il livello di trust, più conferme sono necessarie prima di considerare valida una chiave.

S/MIME

- S/MIME è un altro standard per la gestione della posta elettronica cifrata e autenticata
- Concettualmente molto simile a PGP, ma usa esclusivamente certificati garantiti da certification autorities esterne

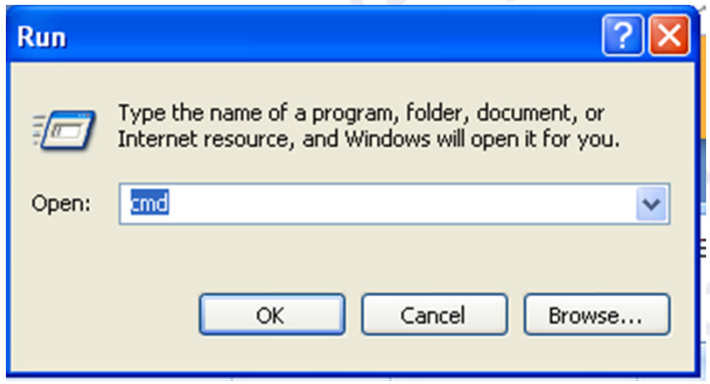
S/MIME e PGP a confronto:

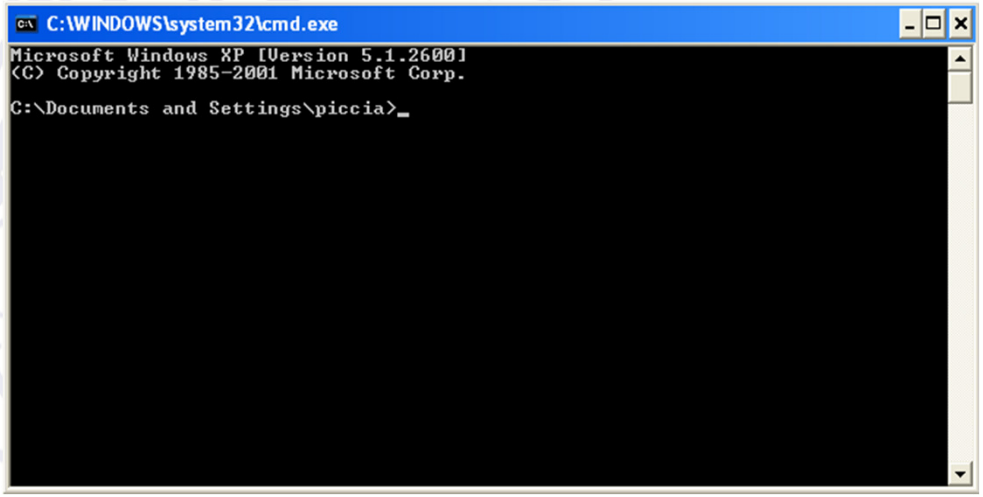
S/MIME: meglio integrato con gli strumenti e gli standard per la gestione della posta elettronica. Richiede una CA esterna.

PGP: più generico, non è limitato al solo utilizzo nella posta elettronica. Può essere usato anche per cifrare/autenticare file. Non richiede una CA esterna.

Uso di GPG

- Scaricabile dall'indirizzo: http://www.gnupg.org/
- Se non potete installarlo, è sufficiente l'eseguibile gpg.exe, scaricabile dal sito del docente
- Gpg è un programma a *linea di comando!* Per eseguirlo, dovete aprire una *shell dei comandi*
- dal menù start, selezionare "run" ed eseguire il programma "cmd"





Uso di GPG – creare le chiavi

- Creare una coppia di chiavi:

  `gpg --gen-key`

- Dovrete scegliere l'algoritmo da usare, la dimensione delle chiavi, l'identità dell'utente…
- La chiave segreta verrà protetta da una password

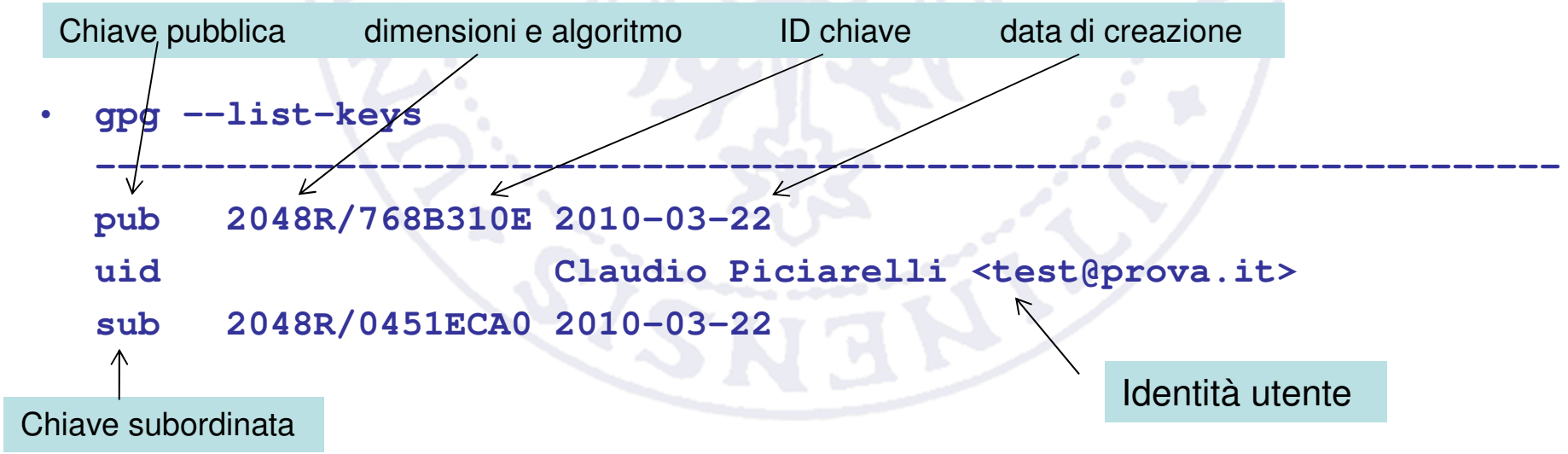
- Le chiavi vengono memorizzate in `c:\documents and settings\<nome utente>\Application data\gnupg`

- Per vedere la chiave pubblica appena generata:

  `gpg --list-keys`

Uso di GPG – visualizzare le chiavi

- In realtà GPG crea due coppie di chiavi: una usata solo per la cifratura, e una per le firme digitali. Una delle due è la chiave principale, l'altra è una chiave subordinata.
- Per l'utente finale, si comportano a tutti gli effetti come se fossero una chiave sola



Uso di GPG – esportare le chiavi

- Esportare la propria chiave pubblica per condividerla con altri…

```
gpg -a -o chiave.asc --export <identità utente>
```

- -a indica di creare un file di testo ASCII (e non un file binario)
- -o specifica il nome del file in cui salvare la chiave
- --export indica l'identità dell'utente o l'ID della chiave da esportare

Uso di GPG – importare le chiavi

- Scaricare la chiave PGP del docente dalla sua home page e importarla nel proprio keyring

```
gpg --import file_contenente_la_chiave_pubblica
gpg --edit-key piciarelli
 trust
 …
 quit
```

- Con l'opzione "edit key" possiamo cambiare il livello di trust per una determinata chiave

Uso di GPG – cifrare e decifrare un messaggio

```
gpg -a -o segreto.txt -r piciarelli -e
chiaro.txt
```

- -a (armor) indica di creare un file di testo anziché binario
- -o (output) indica il nome del file cifrato da creare
- -e (encrypt) indica il nome del file in chiaro da cifrare
- -r (recipient) indica il destinatario (identificato dall'ID della chiave o da una parte univoca dell'identificativo utente)

```
gpg -o messaggio.txt -d segreto.txt
```

- -d: decifra il messaggio

Uso di GPG – firmare e verificare un messaggio

- Per firmare si usa –s (sign) o --clearsign. Il secondo lascia visibile il messaggio originale.
- La validità di una firma può essere verificata con il comando --verify

```
gpg -o firmato.txt --clearsign
messaggio.txt
```

```
gpg --verify firmato.txt
```

Uso di GPG – concatenazione comandi

- Un messaggio può essere firmato e cifrato contemporaneamente. E' possibile scrivere i comandi in forma compatta (-sear=Sign, Encrypt, Armor, Recipient)

```
gpg -o segreto.txt -sear piciarelli chiaro.txt
```

- La decifratura di un messaggio cifrato e firmato comporta automaticamente la verifica della firma

```
gpg -o chiaro.txt -d segreto.txt
```

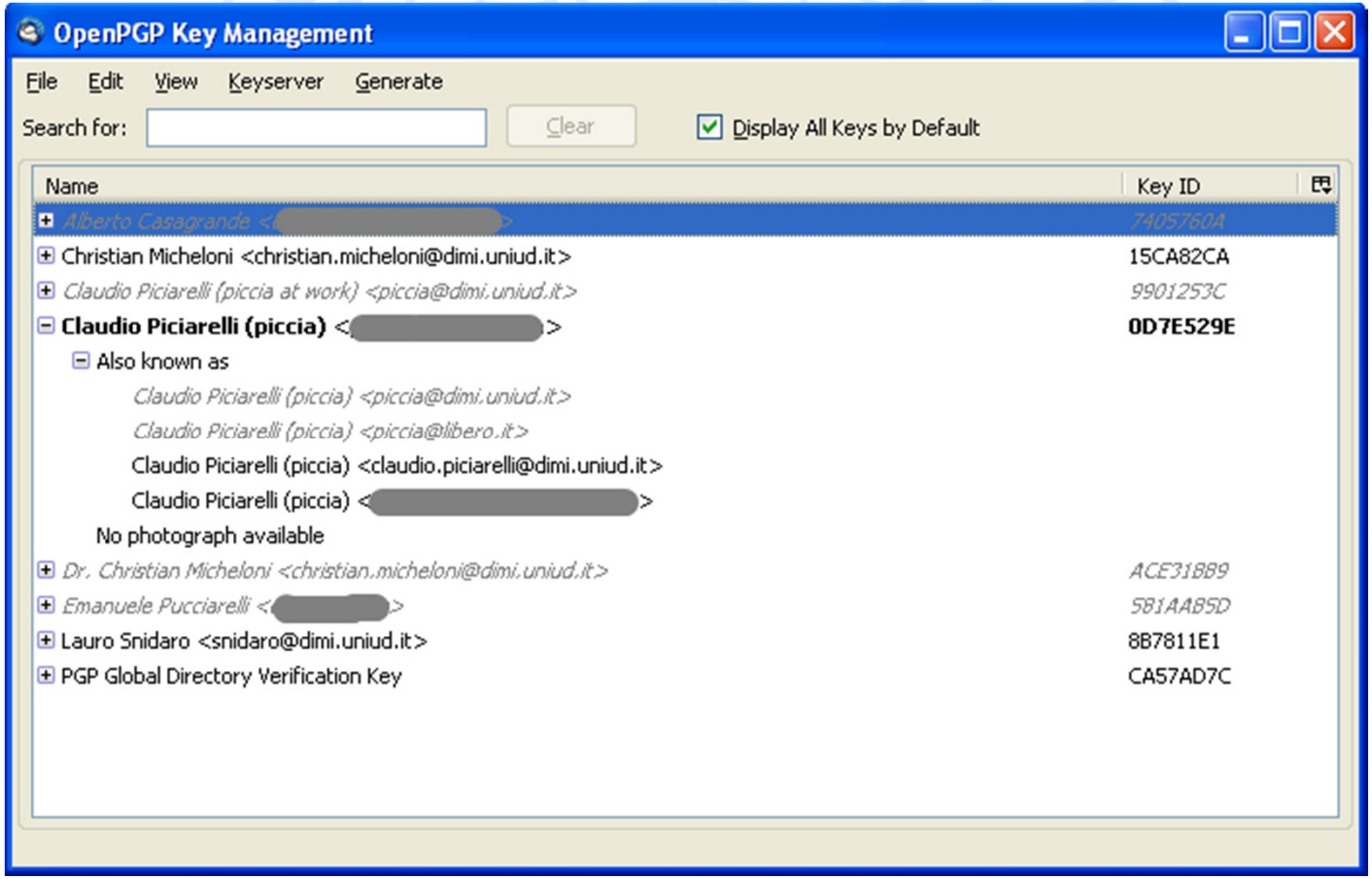
Considerazioni sull'uso di PGP e S/MIME

- Sia PGP che S/MIME sono studiati per essere integrati nei client di posta (es. per thunderbird: il plugin **Enigmail**)

- Oggigiorno sta prendendo sempre più piede l'utilizzo della webmail, che tuttavia non si integra bene con l'utilizzo di strumenti di cifratura e autenticazione (in quanto è necessario accedere ai keyring memorizzati localmente sulla macchina dell'utente).

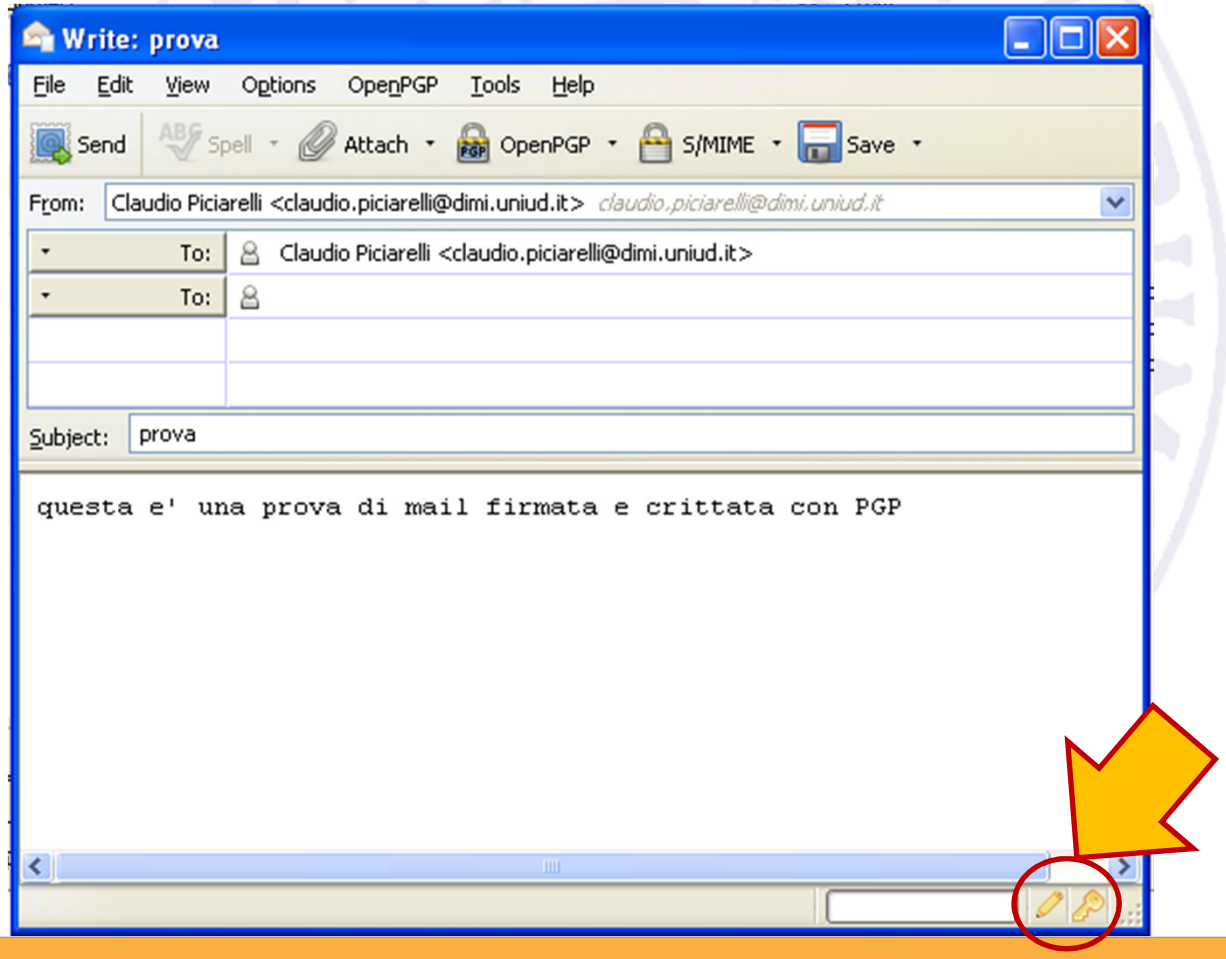
Thunderbird + Enigmail

- Key ring pubblico



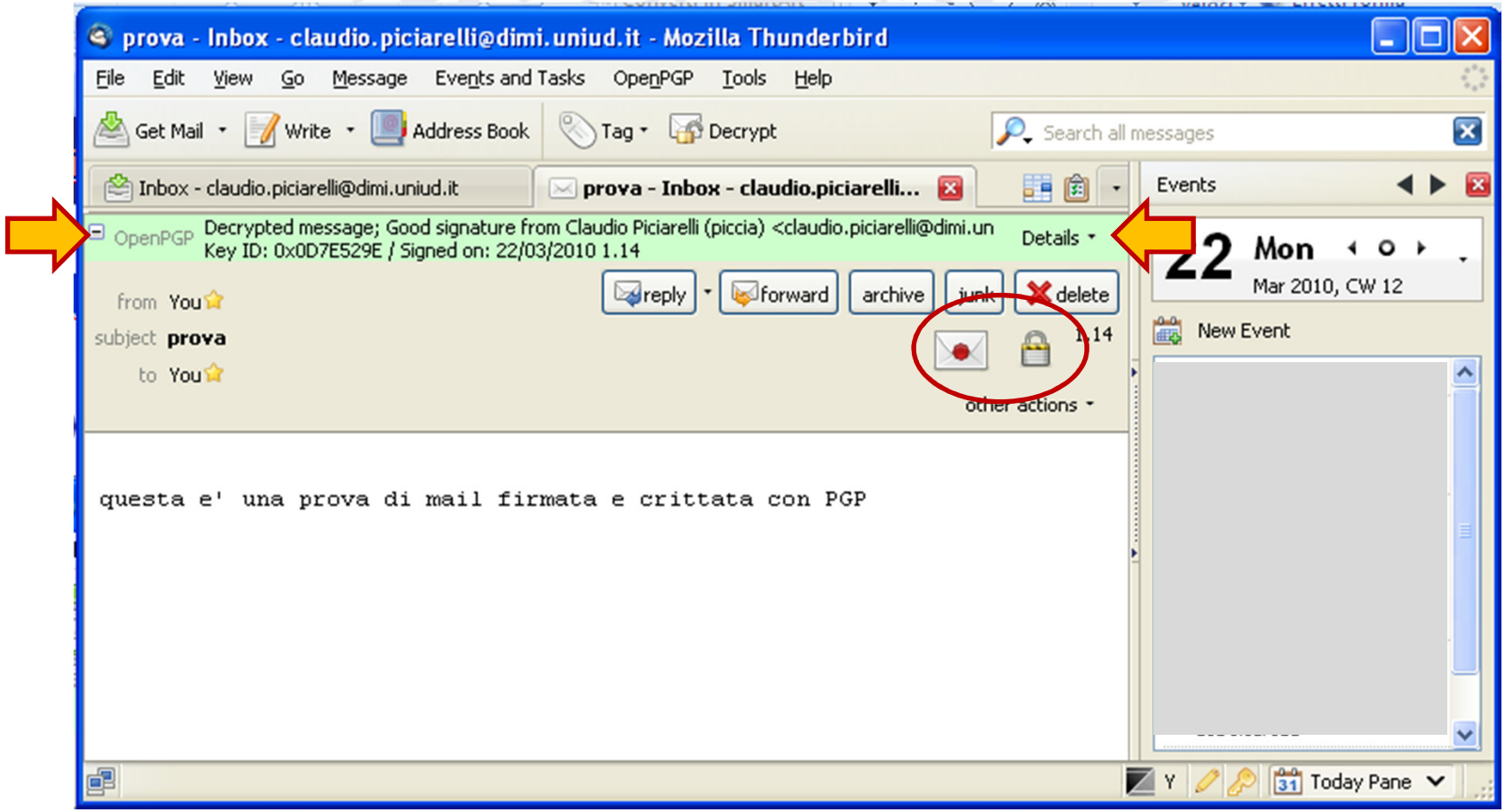
Thunderbird + Enigmail

- Invio di una mail firmata e cifrata



Thunderbird + Enigmail

- Decifratura e verifica



Posta Elettronica Certificata (PEC)

- Vantaggi della posta elettronica cifrata/firmata con PGP o S/MIME rispetto alla e-mail tradizionale:
  - Riservatezza
  - Autenticazione
  - Integrità
  - Non ripudiabilità
- Problemi non affrontati:
  - Mancanza di ricevute di spedizione
  - Nessuna notifica di avvenuta consegna
- Per questo la semplice mail cifrata/firmata non ha valore legale (come l'avrebbe ad esempio una raccomandata A/R)

PEC

- La Posta Elettronica Certificata è uno strumento per sopperire a queste lacune, affinché l'e-mail abbia valore legale.

- Attualmente utilizzata dalla PA, studi professionali (commercialisti, avvocati…), imprese. In questi settori l'uso della PEC sta diventando obbligatorio

I gestori del servizio

- Il funzionamento della PEC si basa sull'ipotesi che i gestori del servizio siano fidati. Per questo devono essere accreditati presso un ente centrale, il CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione)

- Il CNIPA attesta l'identità del gestore e certifica il suo rispetto degli standard di interoperabilità della PEC

Gli utenti

- I gestori del servizio a loro volta certificano l'identità dell'utente finale
- Il funzionamento della PEC si basa quindi sui rapporti di fiducia tra gli utenti e i gestori del servizio, i quali garantiscono per l'identità degli utenti stessi

- L'utente A si fida dell'identità dell'utente B perché certificata dal gestore G
- L'utente A si fida di G in quanto è accreditato dal CNIPA

Servizi principali della PEC

- Dare una ricevuta al mittente che attesti l'invio della mail
- Dare una conferma al mittente che il messaggio è stato recapitato correttamente (analogia raccomandata A/R)

- Attenzione: la PEC certifica che il messaggio è stato consegnato al destinatario, ma non certifica in alcun modo l'effettiva lettura del messaggio

Servizi principali della PEC / 2

- Garantire la riservatezza dei dati, ricorrendo a protocolli sicuri

- Garantire l'autenticità e integrità dei dati mediante firme digitali da parte del gestore.

Vantaggi della PEC

- Semplicità: dal punto di vista dell'utente, non c'è differenza rispetto all'utilizzo della e-mail tradizionale (in particolare, le operazioni di firma digitale sono delegate al gestore)
- Tracciabilità delle comunicazioni: i gestori sono obbligati a conservare i log di ogni transazione per 30 mesi
- Economicità, rapidità e comodità in confronto alla posta raccomandata tradizionale

Svantaggi della PEC

- La firma digitale viene applicata dal gestore, per cui non accompagna il messaggio in tutto il suo percorso dal mittente al destinatario

- E' uno standard esclusivamente italiano (mancanza di interoperabilità con Paesi stranieri)

Aspetti tecnici

- 3 tipi di messaggi
  - Ricevute: attestano che una determinata fase di trasmissione della mail è andata a buon fine
  - Avvisi: avvisano l'utente di eventuali problemi
  - Buste: contengono i messaggi veri e propri

Ricevute

- **Accettazione:** attesta che il gestore ha preso in consegna la mail dell'utente. Dimostra che una determinata mail è stata spedita. *(da: gestore mittente, a: mittente)*

- **Presa in carico**: attesta il passaggio di responsabilità al gestore del destinatario *(da: gestore destinatario, a: gestore mittente)*

- **Consegna:** attesta che il messaggio è stato depositato correttamente nella casella di posta elettronica del destinatario (non garantisce che sia stata letta!) *(da: gestore destinatario, a: mittente)*

Avvisi

- **Non accettazione:** errori formali nel messaggio inviato, ad es. la presenza di destinatari nascosti – vietati dalla PEC
- **Mancata consegna**: ad es. per guasti all'infrastruttura che causano il superamento del tempo massimo di consegna
- **Virus:** rilevazione di virus nel messaggio (il gestore del destinatario è obbligato ad effettuare questo tipo di controllo)

Buste

- Una busta contiene il messaggio di posta elettronica vero e proprio. Due tipi:

- **Busta di trasporto**: contiene il messaggio originale ed è firmata dal gestore

- **Busta anomalia**: usata per il trasporto di messaggi errati o provenienti da indirizzi non PEC. Firmata dal gestore

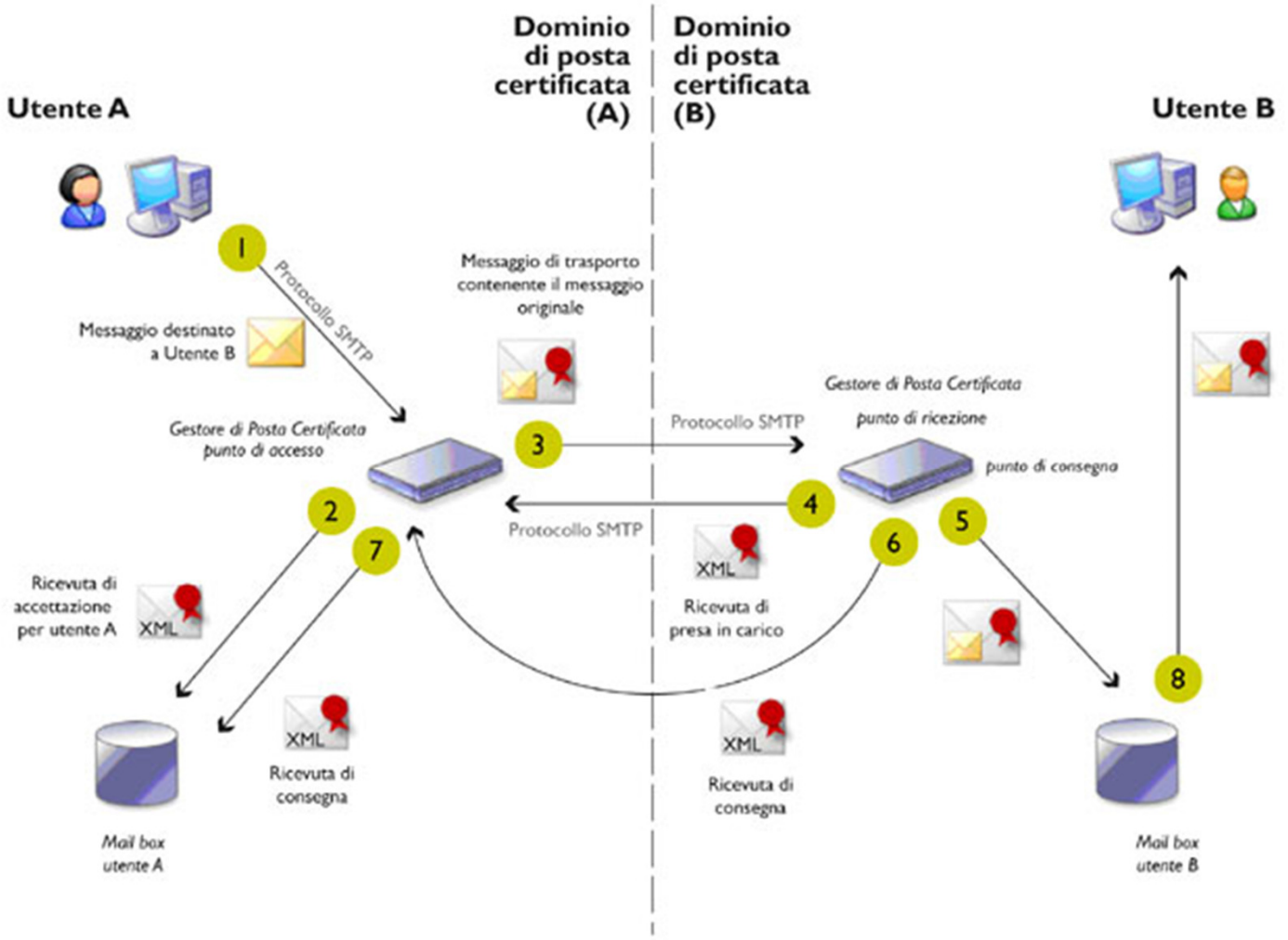
Esempio di trasmissione di un messaggio

Supponiamo che Alice debba inviare una mail PEC a Bob:

- Alice invia il messaggio al gestore mittente, il quale verifica l'identità di Alice (password, smart card, ecc.)
- Il gestore mittente verifica la validità del messaggio e consegna ad Alice una ricevuta di accettazione
- Il gestore mittente inserisce il messaggio in una busta di trasporto, la firma digitalmente e la invia al gestore destinatario
- Il gestore destinatario verifica la validità del messaggio, si assicura dell'assenza di virus e invia al gestore mittente una ricevuta di presa in carico
- Il gestore destinatario deposita il messaggio nella casella di posta di Bob ed invia ad Alice una ricevuta di avvenuta consegna.

Tutte le ricevute e la busta di trasporto sono firmate digitalmente dai rispettivi gestori

Esempio di trasmissione di un messaggio /2



(Immagine tratta da: http://www.flynetitalia.it/data/servclienti/pec.php)

Interazioni con messaggi non-PEC

- Una casella PEC può inviare messaggi ad una casella non PEC. In questo caso tuttavia riceverà solo le ricevute di accettazione

- Una casella non PEC può inviare messaggi ad una casella PEC, ma verranno inseriti in una busta anomalia per segnalare all'utente la provenienza da un indirizzo non certificato

Un esempio di gestore PEC

- Poste italiane: http://postecert.poste.it/pec/index.shtml
- 100 MB, max 200 invii/giorno, € 5.50 + IVA / anno

Un altro esempio

- https://www.postacertificata.gov.it
- Gratuita, ma solo per la comunicazione con le PA