



Consorzio per la formazione e la ricerca in Ingegneria dell'Informazione
Politecnico di Milano

Protezione della posta elettronica mediante crittografia

Davide Cerri

CEFRIEL - Area e-Service Technologies

cerri@cefriel.it

<http://www.cefriel.it/~cerri/>



- La **posta elettronica** è una delle applicazioni più usate su Internet...
- Ma quali sono i problemi di sicurezza?
 - ▶ **riservatezza**: non c'è garanzia che solo il destinatario possa leggere il messaggio;
 - ▶ **autenticazione**: non c'è garanzia sull'identità del mittente;
 - ▶ **integrità**: non c'è garanzia che il messaggio non sia stato alterato.



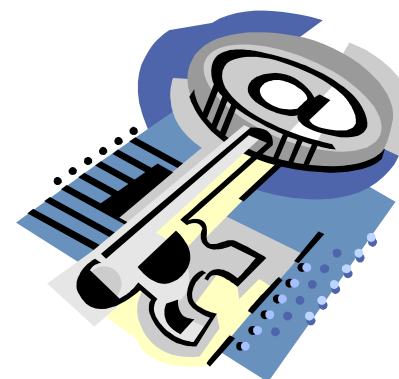


```
Return-Path: Mittente
Received: from Nome_server1 (Nome_server1 [IP_server1]) by
  Nome_server2 (Postfix) with ESMTP id 409524426 for
  Destinatario; Tue, 26 Mar 2002 13:30:03 +0100 (CET)
Received: from there (localhost [127.0.0.1]) by
  Nome_server1 (Postfix) with SMTP id CB87E5FFB for
  Destinatario; Tue, 26 Mar 2002 13:27:42 +0100 (CET)
From: Mittente
To: Destinatario
Subject: Messaggio di prova
Date: Tue, 26 Mar 2002 13:27:42 +0100
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-8859-15"
Content-Transfer-Encoding: 8bit
Message-Id: <20020326122742.CB87E5FFB@Server1>
```

Questo è il corpo del messaggio.

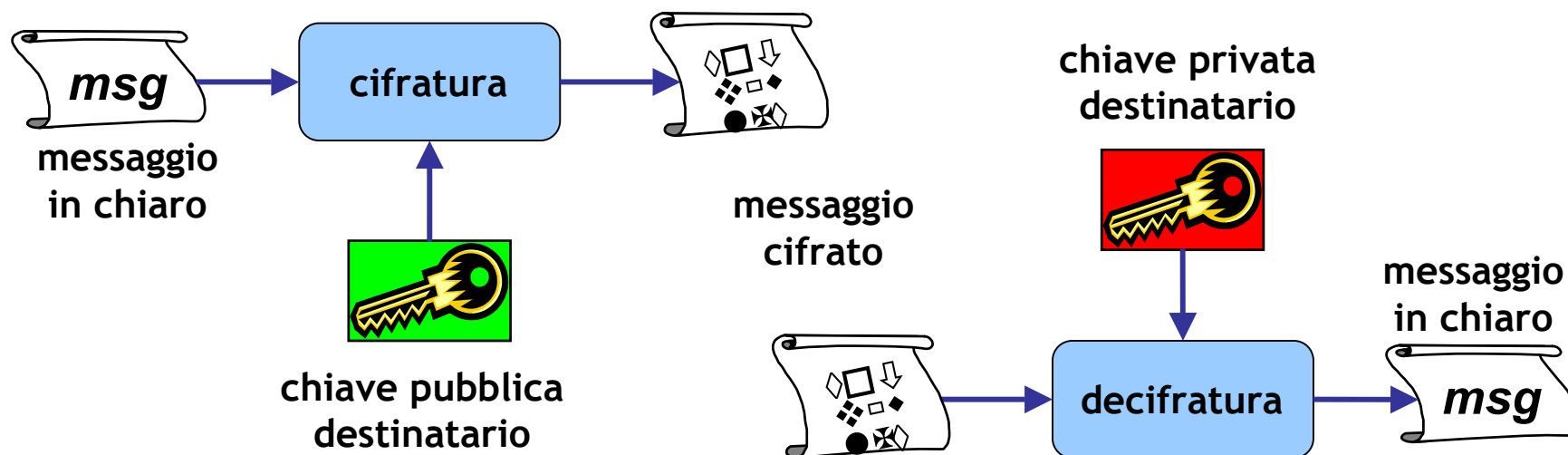


- Per proteggere la posta elettronica, e in generale le comunicazioni su Internet, si utilizza la **crittografia**.
- La crittografia è la scienza che si occupa di **proteggere le informazioni** rendendole sicure, in modo che un utente non autorizzato che ne entri in possesso **non sia in grado di comprenderle**.
- In particolare, si utilizza la **crittografia a chiave pubblica**:
 - ▶ ogni utente ha una **coppia di chiavi** (chiave pubblica e chiave privata).



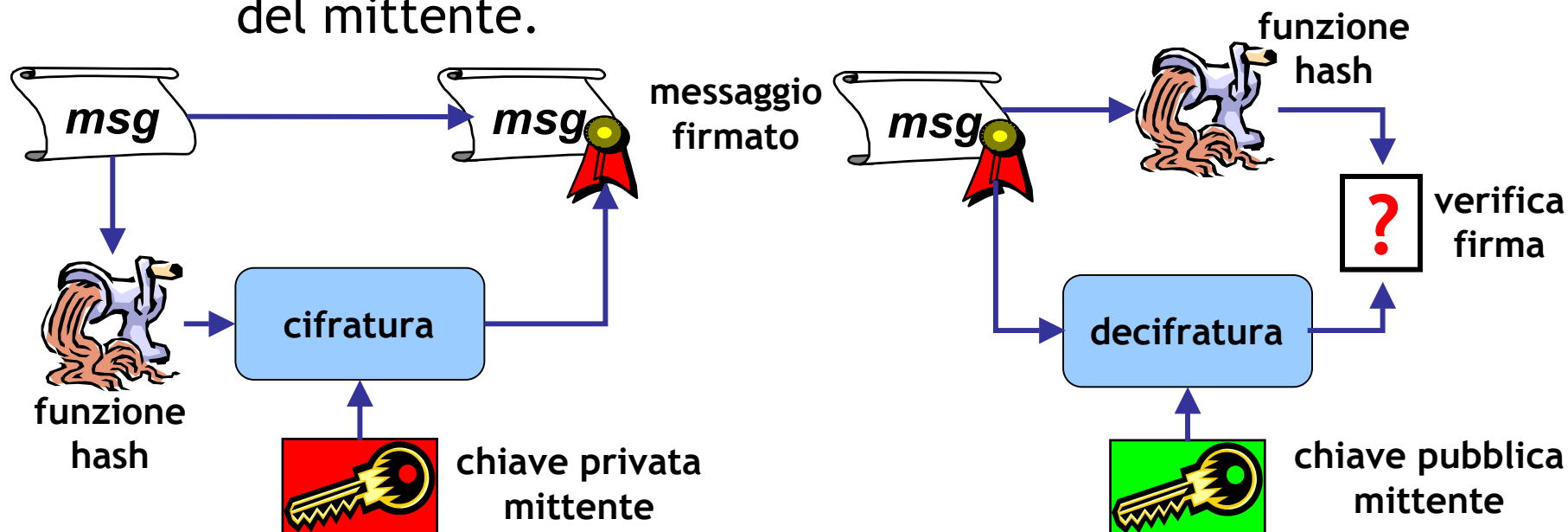


- Nella crittografia asimmetrica ogni utente ha una **coppia di chiavi**, costituita da una **chiave pubblica** e una **chiave privata**.
- Il messaggio viene cifrato con la chiave **pubblica** del **destinatario**, che potrà decifrarlo con la propria chiave **privata**.



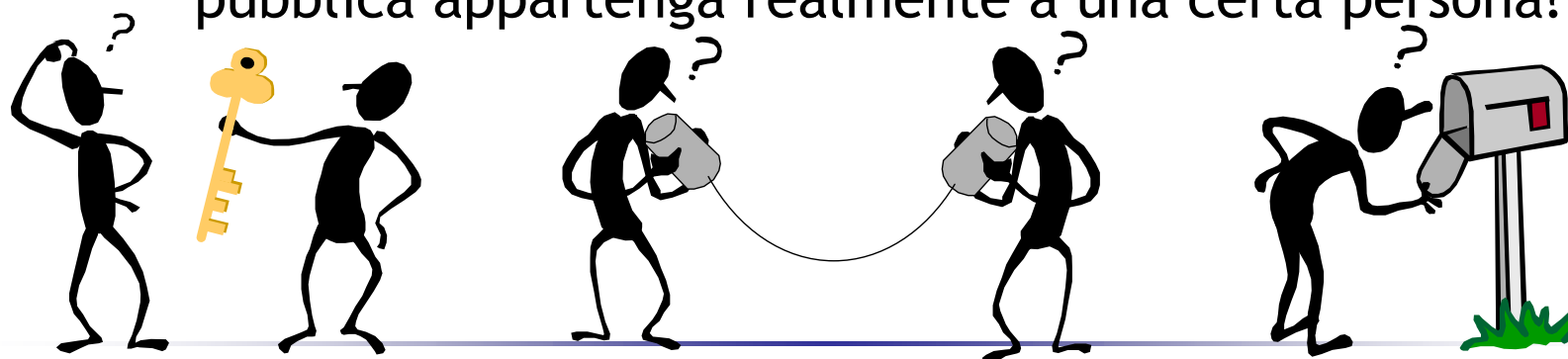


- Con alcuni algoritmi si può anche cifrare con la chiave privata e poi decifrare con quella pubblica.
 - ▶ Questo permette di realizzare la **firma digitale!**
 - ▶ Il mittente firma con la propria chiave **privata**, il destinatario verifica la firma con la chiave **pubblica** del mittente.





- La crittografia a chiave pubblica permette di avere:
 - ▶ riservatezza (**cifrando** il messaggio),
 - ▶ autenticazione e integrità (**firmando** il messaggio).
- Ma c'è il problema della **distribuzione delle chiavi pubbliche**:
 - ▶ come si può ottenere la chiave pubblica di una persona?
 - ▶ come si può essere sicuri che una certa chiave pubblica appartenga realmente a una certa persona?





- Un certificato digitale attesta la **relazione tra un soggetto** (individuo o altra entità) identificato tramite un insieme appropriato di dati (nome, cognome, eccetera) **e una chiave pubblica**.
- È un oggetto **pubblico**, accessibile da chiunque.
- È emesso da un'**autorità di certificazione** (CA), che lo firma con la **propria chiave privata**.
- L'infrastruttura di gestione prende il nome di **Public Key Infrastructure** (PKI).
- Lo standard utilizzato per la gestione dei certificati digitali è **X.509**.



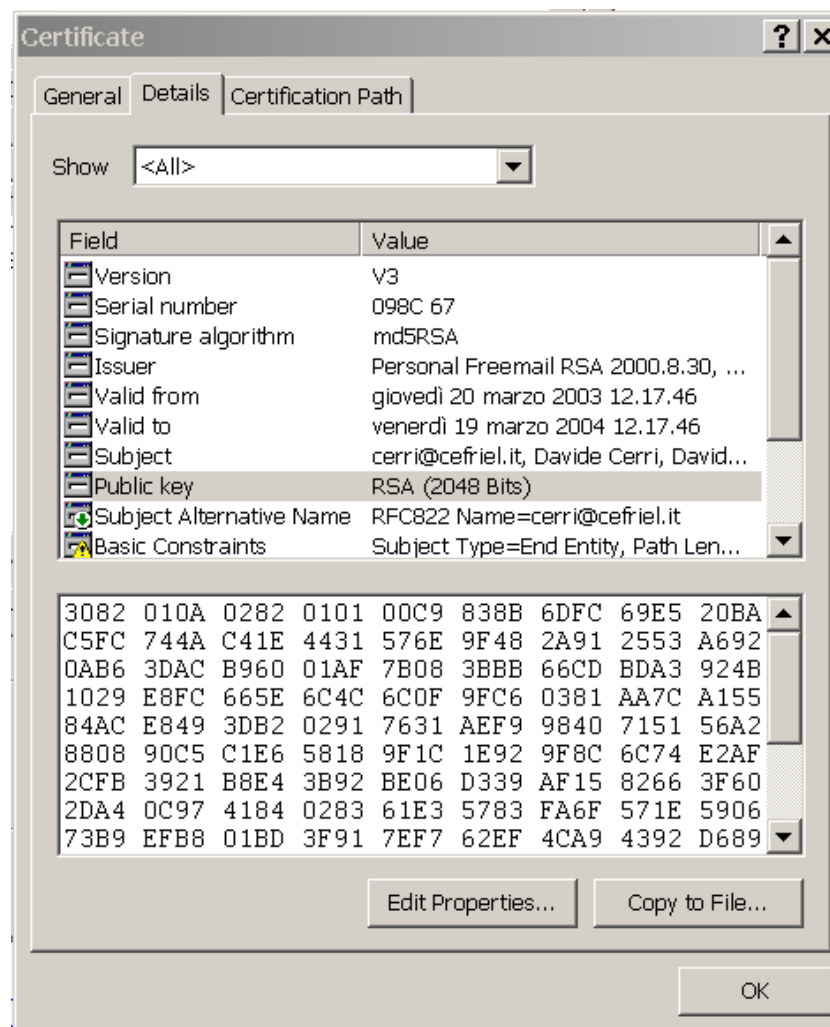
Certificati X.509

- Un **certificato X.509** contiene varie informazioni, tra cui:
 - ▶ numero seriale
 - ▶ nome della CA emittitrice
 - ▶ periodo di validità
 - ▶ nome del soggetto
 - ▶ chiave pubblica del soggetto
 - ▶ firma della CA





Certificati X.509: esempio da browser





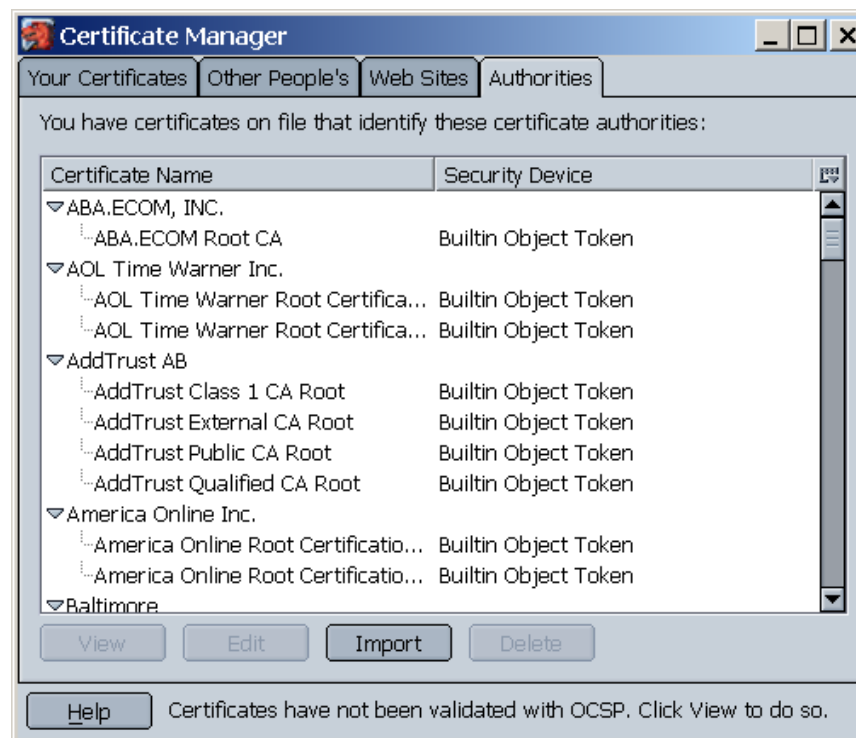
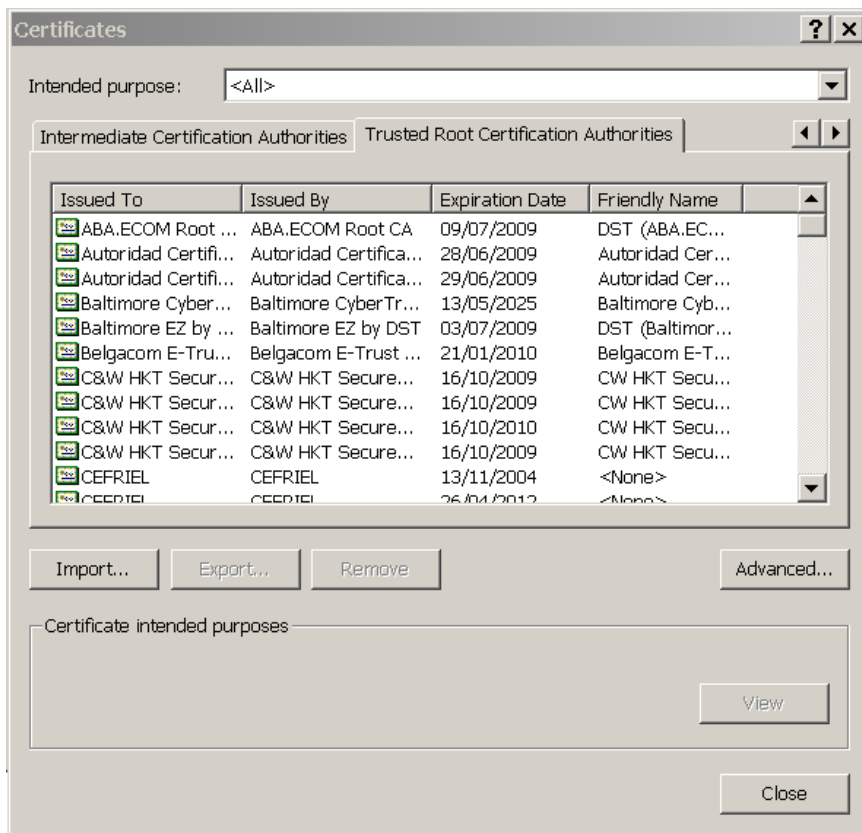
- Con un certificato si ha la garanzia che una data chiave pubblica appartenga ad un dato utente.
 - ▶ Tale garanzia è **fornita dall'autorità di certificazione**.
- Ma per controllare l'autenticità del certificato dell'utente è **necessario avere la chiave pubblica** (quindi il certificato) **della CA**.
 - ▶ I certificati delle CA sono **autofirmati**.
 - ▶ È necessario **ottenerli con un meccanismo ad hoc** (ad esempio preinstallati nel sistema operativo o nell'applicazione).



Certificati X.509: gestione da browser

MS Internet Explorer:

Tools -> Internet Options ->
-> Content -> Certificates



Mozilla/Netscape:

Edit -> Preferences -> Privacy & Security ->
-> Certificates -> Manage Certificates



- Un utente ha bisogno di una coppia di chiavi pubblica/privata, ma...
 - ▶ come la **genera**?
 - ▶ come **custodisce** la chiave privata, in modo che nessuno se ne impossessi?
 - ▶ come **trasporta** la chiave privata, in modo da poterla utilizzare in qualunque luogo?
- Potrebbe tenere la chiave privata su un dischetto, ma non sarebbe molto sicuro...
- Per maggiore sicurezza, si utilizzano le **smart-card**.
 - ▶ Le operazioni crittografiche vengono svolte **all'interno della carta**.





- Esistono due standard IETF per la protezione della posta elettronica:
 - ▶ **S/MIME**,
 - ▶ **OpenPGP**.
- Con entrambi è possibile garantire:
 - ▶ riservatezza dei messaggi,
 - ▶ integrità dei messaggi,
 - ▶ autenticazione del mittente.





S/MIME

- **S/MIME** (Secure/Multipurpose Internet Mail Extensions) è un'estensione di MIME che introduce **funzionalità di sicurezza**.
- Introduce nuovi tipi di contenuto per i messaggi di posta elettronica, che possono essere utilizzati per **inserire firme, certificati, blocchi di dati cifrati**.
- Utilizza i **certificati X.509** per l'autenticazione.
- È **implementato nativamente in molti client di posta** (MS Outlook, MS Outlook Express, Mozilla/Netscape...) senza bisogno di programmi aggiuntivi.



S/MIME: esempio su MS Outlook

Digital Signature: Valid

Message: Messaggio cifrato e firmato

This message is digitally signed

██████████ CN=Davide Cerri; G=Davide; SN=Cerri

✓ Signature: Valid

- ✓ Contents not altered after message was signed
- ✓ Certificate not revoked
- ✓ Certificate not expired
- ✓ Certificate trusted

Always warn me about errors

View Certificate

View Certificate

General Details Certification Path Trust

Certificate Information

This certificate is intended to:

- Protects e-mail messages

Issued to: Davide Cerri

Issued by: Personal Freemail RSA 2000.8.30

Valid from 19/04/2002 to 19/04/2003

Issuer Statement

OK

Messaggio cifrato e firmato - Message (Plain Text) ...

File Edit View Insert Format PGP Tools Actions Help

Reply Reply to All Forward

From: Davide Cerri Sent: martedì 30/04/2002 16.45

To: ██████████

Cc: Davide Cerri

Subject: Messaggio cifrato e firmato

Security: Signed & encrypted

Messaggio cifrato e firmato.

Encrypted Message

Encryption Algorithm: 3DES

Encryption Certificate... OK



S/MIME: esempio su Mozilla

The screenshot illustrates the S/MIME process in Mozilla Mail. It shows three windows:

- Message Security:** A window titled "Message Security" with two sections:
 - Message Is Signed:** "This message includes a valid digital signature. The message has not been altered since it was sent." It lists: Signed by: Davide Cerri, Email address: davide.cerri@cefriel.it, Certificate issued by: Personal Freemail RSA 2000.8.30. A button "View Signature Certificate" is present.
 - Message Is Encrypted:** "This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network." Buttons "OK" and "Help" are at the bottom.
- Certificate Viewer:** A window titled "Certificate Viewer: 'Davide Cerri'" with "General" and "Details" tabs. The "General" tab shows:
 - This certificate has been verified for the following uses:** Email Signer Certificate, Email Recipient Certificate.
 - Issued To:** Common Name (CN) Davide Cerri, Organization (O) <Not Part Of Certificate>, Organizational Unit (OU) <Not Part Of Certificate>, Serial Number 07:31:85.
 - Issued By:** Common Name (CN) Personal Freemail RSA 2000.8.30, Organization (O) Thawte, Organizational Unit (OU) Certificate Services.
 - Validity:** Issued On 10/04/2002, Expires On 10/04/2003.
 - Fingerprints:** SHA1 Fingerprint 2D:24:E7:18:EF:37:F1:F6:65:44:93:01:A9:07:BA:AC:D2:56:13:39; MD5 Fingerprint 32:D6:57:9A:DC:1F:50:F7:8F:E3:E1:57:83:D7:42:35.
- Compose:** A window titled "Compose: Re: Prova mail cifrata e firmata." with a "Security" menu open. The menu options are:
 - No Encryption
 - Require Encryption
 - Digitally Sign (checked)
 - Message SecurityThe "To:" field contains "Davide Cerri <da...>". The "Subject:" field contains "Re: Prova mail cifrata e firmata." The body text reads: "Davide Cerri wrote: > Prova mail cifrata e firmata."



OpenPGP

- **PGP** (Pretty Good Privacy) nasce dal lavoro di Philip Zimmermann.
- Si tratta di un **programma crittografico** (più tardi divenuto uno standard - OpenPGP), usato **principalmente per la posta elettronica**.
- Esistono un'implementazione proprietaria (PGP) e una libera (GnuPG - Gnu Privacy Guard), disponibili per diverse piattaforme (<http://www.pgpi.org/>).
- Necessita solitamente di **plugin per i client di posta**.



*Philip
Zimmermann*



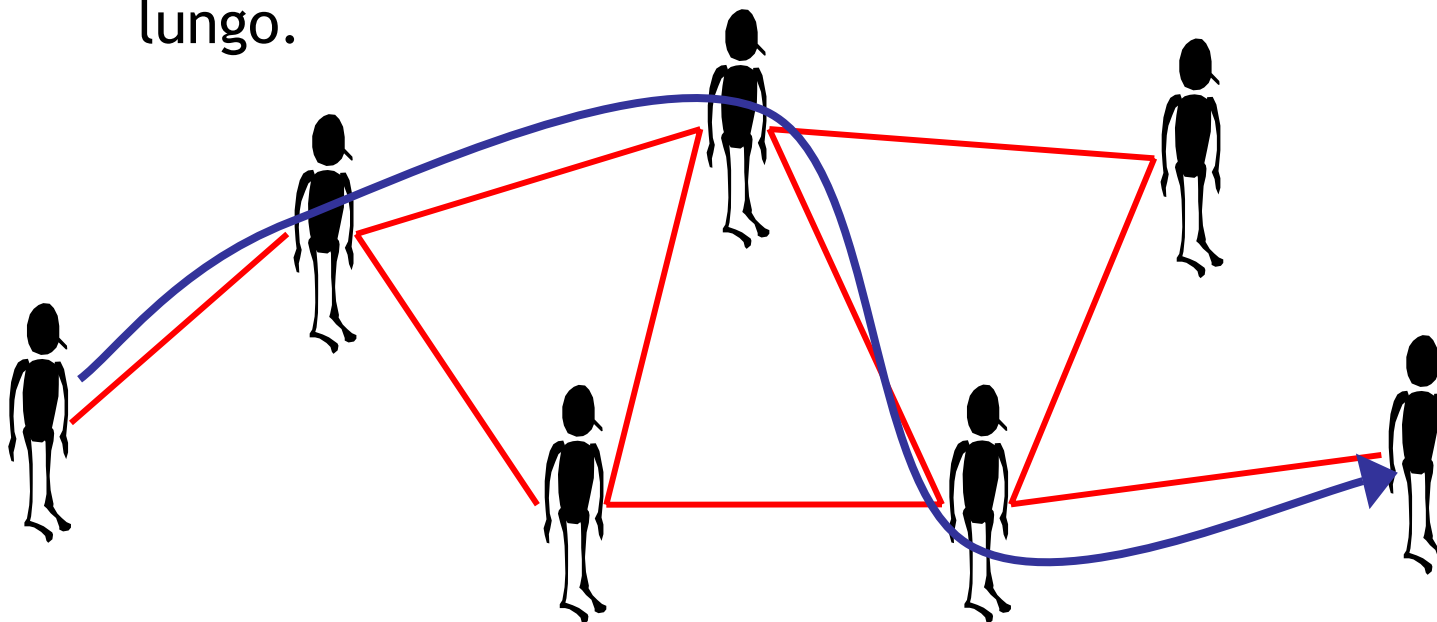
OpenPGP: web of trust (1)

- OpenPGP non utilizza i certificati X.509 e le autorità di certificazione, ma ha un proprio modello detto “**web of trust**”.
- Il web of trust **non ha autorità centrali**: sono gli stessi utenti a certificare gli altri utenti.
 - ▶ Un certificato OpenPGP può contenere **molte firme**, mentre un certificato X.509 contiene solo la firma dell'autorità che lo ha emesso.
- La decisione sulla validità di una chiave si basa sulla **fiducia** che si ha negli utenti che hanno firmato (cioè certificato) quella chiave.



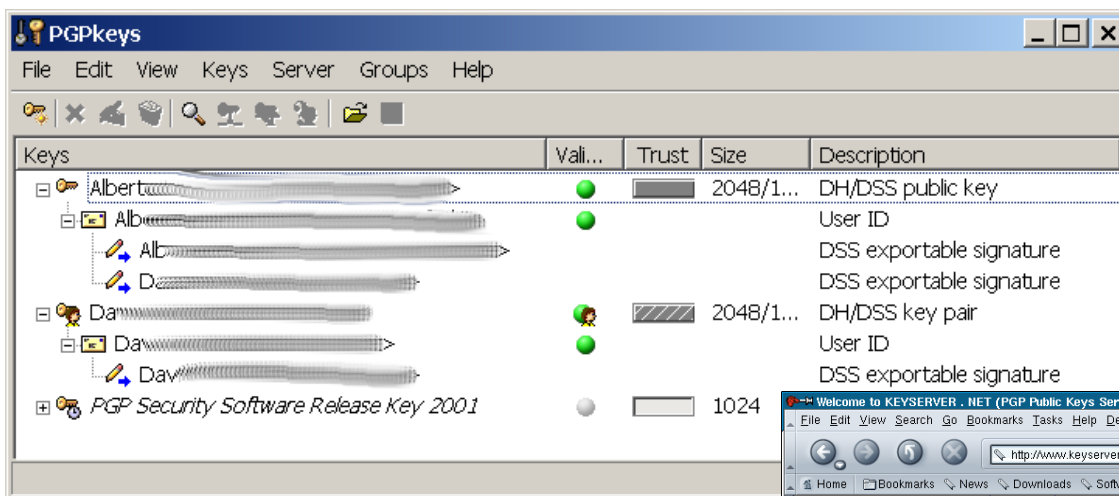
OpenPGP: web of trust (2)

- L'idea su cui si basa il web of trust ricorda il "principio dei sei gradi di separazione".
 - ▶ Anche se due utenti non si "conoscono" direttamente si possono collegare attraverso il grafo delle "conoscenze" con un percorso in genere non troppo lungo.

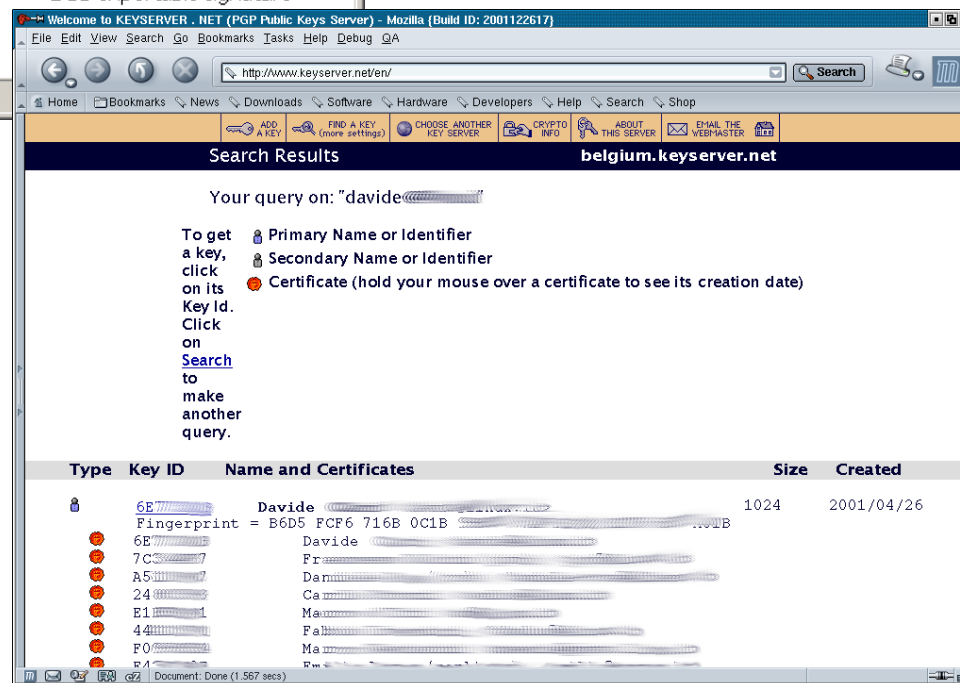




PGP: screenshot



<http://www.keyserver.net/>





Grazie dell'attenzione

cefriel
Politecnico di Milano

Domande?

cerri@cefriel.it
<http://www.cefriel.it/~cerri/>

