



# LOLUG

*Gruppo Utenti Linux Lodi*

## Certificati digitali con CAcert

*Un'autorità di certificazione no-profit*

**Davide Cerri**

Associazione di Promozione Sociale LOLUG – Gruppo Utenti Linux Lodi

davide@lolug.net

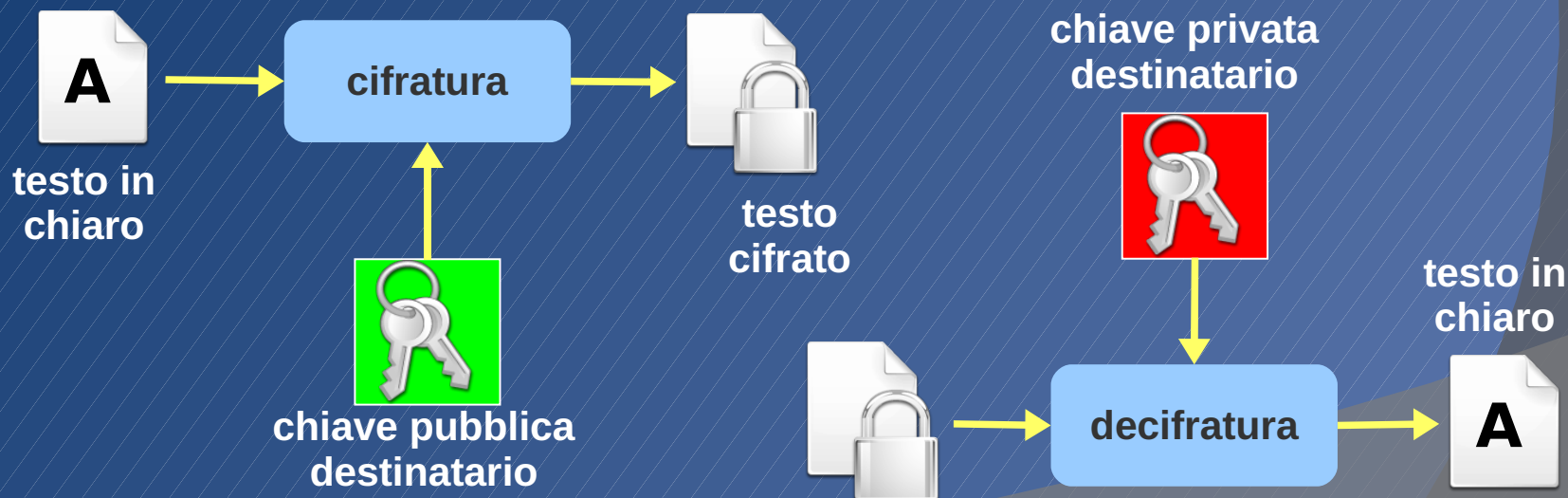
# Crittografia asimmetrica: scopi



- Con la crittografia asimmetrica possiamo:
  - **cifrare** un messaggio
    - si garantisce la **riservatezza**: il contenuto del messaggio non può essere intercettato da terzi
  - **firmare** un messaggio
    - si garantisce l'**autenticazione**: l'interlocutore è davvero chi dice di essere
    - si garantisce l'**integrità**: il contenuto del messaggio non può essere modificato da terzi
- Naturalmente possiamo fare entrambe le cose insieme, cioè firmare e cifrare un messaggio garantendo così tutte e tre le proprietà

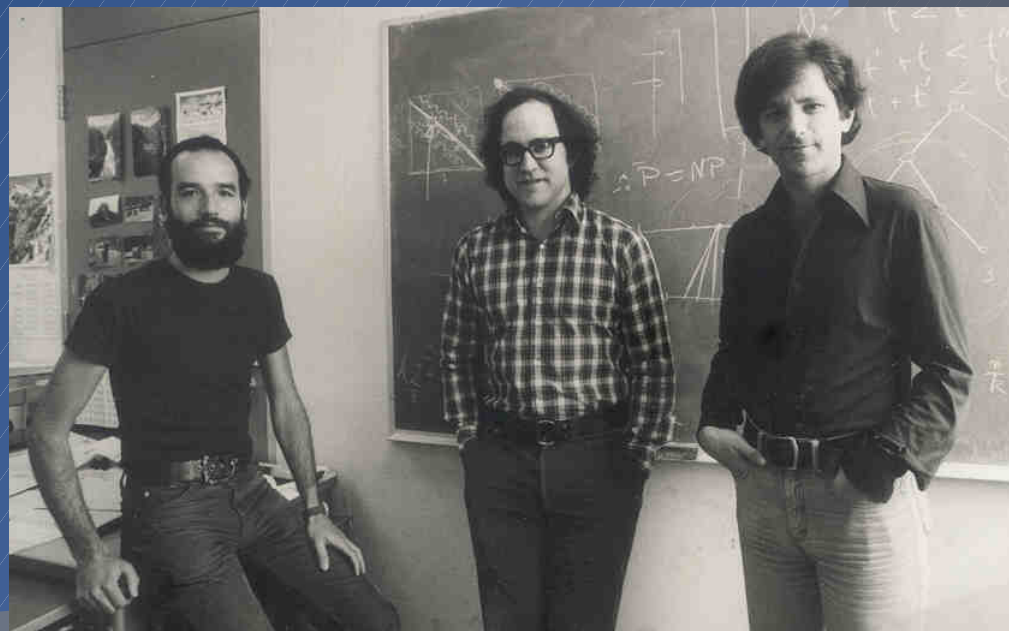
# Crittografia asimmetrica: chiavi

- Con la 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**



# Crittografia asimmetrica: firma

- Con la crittografia asimmetrica è inoltre possibile realizzare la **firma digitale**
  - Il mittente appone una “firma” utilizzando la propria chiave privata, il destinatario verifica la firma utilizzando la chiave pubblica del mittente
- Alcuni algoritmi crittografici asimmetrici:
  - RSA (cifratura e firma)
  - DSA (solo firma)



*Adi Shamir  
Ronald Rivest  
Leonard Adleman*

# Crittografia asimmetrica: riepilogo



- **Per la firma servono le chiavi del mittente**
  - Per poter firmare un'e-mail che mando, devo avere una mia coppia di chiavi
  - Perché la mia firma possa essere verificata, il destinatario deve avere la mia chiave pubblica
- **Per la cifratura servono le chiavi del destinatario**
  - Per poter cifrare un'e-mail che mando, il destinatario deve avere una propria coppia di chiavi, e io devo avere la sua chiave pubblica

# Distribuzione delle chiavi pubbliche



- Resta un problema: come **distribuire le chiavi pubbliche**?
- Non è un problema di riservatezza (la chiave pubblica non è segreta) ma di **autenticazione** ...
- ...come posso ottenere la chiave pubblica di Mario Rossi ed essere sicuro che non si tratti di un impostore?
  - Se le due persone si conoscono possono scambiarsi le chiavi direttamente, ma in generale è difficile...
  - La soluzione è data dai **certificati digitali**

# Certificati digitali e PKI



- Un certificato digitale attesta la **relazione tra un soggetto**, identificato tramite un insieme appropriato di dati, **e una chiave pubblica**
- È un oggetto **pubblico**, potenzialmente 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** (o meglio PKIX)

# Esempio certificato

Certificato:"ID di Davide Cerri a Root CA"

Generale | Dettagli

Questo certificato è stato verificato per i seguenti utilizzi:

- Certificato client SSL
- Certificato server SSL
- Certificato firmatario e-mail
- Certificato e-mail destinatario

**Rilasciato a**

Nome Comune (CN)	Davide Cerri
Organizzazione (O)	<non incluso nel certificato>
Unità Organizzativa (OU)	<non incluso nel certificato>
Numero seriale	05:D4:E7

**Rilasciato da**

Nome Comune (CN)	CA Cert Signing Authority
Organizzazione (O)	Root CA
Unità Organizzativa (OU)	http://www.cacert.org

**Validità**

Rilasciato il	02/10/2008
Scade il	02/10/2010

**Impronte digitali**

Impronta digitale SH1	FC:F1:5F:FE:56:39:91:7B:4D:05:AF:50:17:7A:A6:9D:23:E6:02:13
Impronta digitale MD5	65:73:71:E4:D8:F2:6C:34:6F:AF:07:14:42:8D:D5:B7

Chiudi

Certificato:"ID di Davide Cerri a Root CA"

Generale | Dettagli

**Gerarchia certificato**

- CA Cert Signing Authority  
Davide Cerri

**Campi certificato**

- ID di Davide Cerri a Root CA
  - Certificato
    - Versione
    - Numero seriale
    - Algoritmo firma certificato
    - Emittente
    - Validità
      - Soggetto
      - Info chiave pubblica soggetto
        - Algoritmo chiave pubblica soggetto
        - Chiave pubblica del soggetto

**Valore campo**

Modulo (2048 bit):

```
d0 12 10 da 2e 4c e8 09 5a f8 8e 84 c0 9f d4 ab
10 29 9f 63 7f 1c b3 f1 37 61 f1 5b 7d 42 c2 e4
40 b2 1e 79 43 66 ac 46 4c 7b b8 b3 66 ec da 25
da a0 ae 76 a7 5f 46 9f bc 28 e4 2a 7a ef 6a 17
52 10 5d d2 33 c5 03 87 9e b8 08 f7 16 a7 66 22
f9 29 59 a0 bf cc f3 6e 1c d1 e9 c0 89 2b f7 ff
e8 9b 71 f8 00 3b 38 2e bb 1c 56 04 1b 6a 8c 9d
df 44 42 d7 2d ef 9c 75 f8 35 32 43 fc af 8b a6
```

Esporta

Chiudi

# Richiesta certificato



- L'utente **genera la propria coppia di chiavi** asimmetriche (pubblica – privata)
- L'utente **genera una richiesta di certificato** (CSR – Certificate Signing Request) inserendo la propria chiave pubblica e i propri dati (per esempio nome, cognome, indirizzo e-mail – oppure nome di dominio per un certificato server) **e la invia alla CA**
- La CA verifica la correttezza dei dati, **genera il certificato** e lo restituisce all'utente

# Certificati: utilizzo

- Bob invia ad Alice il proprio **certificato**, firmato dalla CA
- Alice **verifica la firma della CA** sul certificato di Bob, e se è corretta estrae la chiave pubblica di Bob dal certificato
  - Alice deve già avere il **certificato della CA**, per poterne verificare la firma
  - Il certificato della CA (root) è **autofirmato**
- A questo punto Alice ha ottenuto la chiave pubblica di Bob, la cui identità è garantita dalla CA

# Certificati: utilizzo e problemi



- È comunque necessario ottenere in qualche modo sicuro il **certificato della CA**: il problema della distribuzione delle chiavi pubbliche rimane, ma **su scala molto più ridotta**
- Un certificato può essere **revocato**, ad esempio se il proprietario si accorge del furto della chiave privata corrispondente
  - la CA pubblica una **lista dei certificati revocati** (CRL), da essa firmata, che andrebbe controllata per accertarsi della validità di un certificato
- Il sistema implica una **fiducia nella CA**, ma... chi lo garantisce?

# Certificati: utilizzo (in pratica)



- In pratica, i certificati digitali X.509 vengono usati principalmente per due cose:
  - per l'**autenticazione delle connessioni TLS/SSL**
    - in particolare il famoso “**lucchetto del browser**”, o HTTPS (soprattutto per l'autenticazione del server, poco comune per l'autenticazione del client)
  - per la **firma e cifrature delle e-mail** (S/MIME)
- I certificati root delle CA sono **preinstallati** nel sistema operativo o nell'applicazione (per esempio il browser)
  - La scelta di quali CA inserire dipende dal fornitore del software
  - L'utente può ovviamente modificare la lista

# Chi sono le CA?

- Le autorità di certificazione sono generalmente **società private**
  - Qualche nome: VeriSign, Thawte, Postecom
- Un certificato digitale ha un costo che va di solito da qualche decina di euro (persone) a qualche centinaio (server), e una durata di solito compresa tra uno e tre anni
  - Per uso personale, Thawte rilascia anche certificati gratuiti con un meccanismo analogo a CAcert
- Il **costo non trascurabile** dei certificati ne limita molto il loro utilizzo e diffusione

- CAcert è un'**autorità di certificazione no-profit**, nata per favorire un'ampia diffusione dei certificati digitali
- Nata in Australia nel 2002, è **gestita da volontari**
- I certificati sono **gratuiti**, sia per l'uso come client/e-mail che per l'uso server



<http://www.cacert.org/>

# CAcert: servizi forniti



- CAcert fornisce i **seguenti servizi**:
  - emissione certificati X.509 “client” (e-mail, autenticazione client TLS/SSL)
  - emissione certificati “server” (autenticazione server TLS/SSL)
  - firma certificato OpenPGP
- Tutti i servizi sono forniti in maniera **automatizzata e gratuita** tramite il sito web
- La titolarità di un indirizzo e-mail viene verificata con un messaggio di “ping”
- La titolarità di un dominio viene verificata tramite indirizzi e-mail autoritativi del dominio

# CAcert: verifica dell'identità



- La **verifica dell'identità** (nome e cognome) è un po' più complicata, e non automatizzabile
- Se la propria identità non è verificata, si possono ottenere certificati con il solo indirizzo e-mail e durata ridotta (6 mesi)
- La verifica dell'identità viene effettuata tramite la rete degli **Accertatori** (Assurer)
- Una volta che la propria identità è stata verificata, è possibile ottenere tutti i certificati che si vogliono tramite il sito web di CAcert
  - Verifica dell'identità ed emissione dei certificati sono processi separati in CAcert

# CAcert: verifica dell'identità



- La verifica dell'identità si basa su un **sistema a punti** e sul cosiddetto “web of trust”
  - Il nome in realtà non è molto corretto...
- Incontrando **di persona** un **Accertatore CAcert** e mostrandogli dei **documenti d'identità** si possono ottenere fino a 35 punti
- Con almeno 50 punti la propria identità è **verificata**, e si possono avere certificati nominativi e con durata di 2 anni
- Per diventare Accertatori bisogna avere ottenuto almeno 100 punti e superare un test

# Il WoT di CAcert e PGP



- Il “web of trust” di CAcert, può ricordare per certi versi **PGP**
- In realtà è un sistema molto diverso:
  - **CAcert è una CA**, per cui i certificati sono firmati da CAcert, e non dagli Accertatori
  - Ci sono **policy** precise a cui gli Accertatori in particolare si devono attenere, e un processo di risoluzione controversie
  - Il sistema è, da un punto di vista logico, centralizzato: come per le normali CA commerciali **la fiducia risiede nella CA**
    - La CA è però gestita in modo collaborativo

# CAcert: qualche numero

Utenti	128.145
Indirizzi e-mail verificati	167.165
Domini verificati	88.184
Certificati emessi	392.889
Attestazioni di identità effettuate	96.767
Utenti con 1-49 punti	4.280
Utenti con 50-99 punti	3.378
Utenti con 100 punti e oltre	10.093
Accertatori	1.199
Punti assegnati	1.744.467

Statistiche al 7/11/2008  
<http://www.cacert.org/stats.php>

# CAcert: problemi



- Il certificato root di CAcert **non è per ora incluso nei browser** e client di posta più diffusi
  - Questo significa che **è necessario installarlo manualmente**, altrimenti si ottiene un avviso di certificato non verificabile
  - CAcert sta seguendo un percorso di **auditing per l'inclusione in Firefox**
- Il **numero di Accertatori è ancora basso**, per cui può essere difficile ottenere la verifica della propria identità
  - Possiamo provare a farlo crescere...