Key Signing Party

Cos'è, a cosa serve e come funziona

Giovanni Mascellani

Gruppo Utenti Linux – Pisa

sabato 22 ottobre 2011 – Linux Day 2011

Gli scopi

Crittografia Alterare un documento in modo che solo determinate persone siano in grado di leggerlo.

Firma digitale Aggiungere ad un documento alcuni dati che certificano con certezza chi è il suo autore e garantiscono che il documento stesso non è stato alterato durante il trasporto.

Oggi esistono tecnologie, ritenute sufficientemente sicure, che permettono di raggiungere questi due obiettivi.

Gli scopi

Crittografia Alterare un documento in modo che solo determinate persone siano in grado di leggerlo.

Firma digitale Aggiungere ad un documento alcuni dati che certificano con certezza chi è il suo autore e garantiscono che il documento stesso non è stato alterato durante il trasporto.

Oggi esistono tecnologie, ritenute sufficientemente sicure, che permettono di raggiungere questi due obiettivi.

Una catena è resistente quanto il suo anello più debole

Con la tecnologia di oggi gli anelli deboli non sono quelli centrali, ma gli estremi, ossia gli utenti che utilizzano impropriamente le tecnologie.

Le chiavi

Una chiave di un meccanismo di crittografia a chiave pubblica è composta da due parti.

Chiave pubblica Permette la cifratura di un documento e la verifica di una firma digitale. Può essere liberamente divulgata, in quanto si ritiene che non sia computazionalmente possibile ottenere la chiave privata a partire da quella pubblica.

Chiave privata Permette la decifratura di un documento e la creazione di una firma digitale. Deve essere mantenuta rigorosamente segreta. Ottenere la chiave pubblica da quella privata è molto semplice.

Le chiavi

Una chiave di un meccanismo di crittografia a chiave pubblica è composta da due parti.

Chiave pubblica Permette la cifratura di un documento e la verifica di una firma digitale. Può essere liberamente divulgata, in quanto si ritiene che non sia computazionalmente possibile ottenere la chiave privata a partire da quella pubblica.

Chiave privata Permette la decifratura di un documento e la creazione di una firma digitale. Deve essere mantenuta rigorosamente segreta. Ottenere la chiave pubblica da quella privata è molto semplice.

Problema di sicurezza

Chiunque può creare una chiave con un qualsiasi nome scritto sopra. Dunque è necessario verificare che il nome scritto su una chiave sia quello giusto prima di utilizzarla.

Come risolvere il problema?

Per scrivere un messaggio segreto a Tizio devo verificare che la chiave con scritto Tizio sia veramente di Tizio.

Idea!

Posso incontrare Tizio di persona e controllare se la copia della chiave che ho io è giusta. Da quel punto in poi potrò scrivere messaggi segreti a Tizio ogni volta che voglio.

Come risolvere il problema?

Per scrivere un messaggio segreto a Tizio devo verificare che la chiave con scritto Tizio sia veramente di Tizio.

Idea?!?? (ma è fattibile? Se Tizio sta in Australia?)

Posso incontrare Tizio di persona e controllare se la copia della chiave che ho io è giusta. Da quel punto in poi potrò scrivere messaggi segreti a Tizio ogni volta che voglio.

Come risolvere il problema?

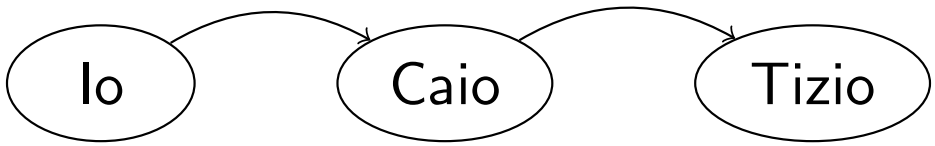
Per scrivere un messaggio segreto a Tizio devo verificare che la chiave con scritto Tizio sia veramente di Tizio.

Idea?!?? (ma è fattibile? Se Tizio sta in Australia?)

Posso incontrare Tizio di persona e controllare se la copia della chiave che ho io è giusta. Da quel punto in poi potrò scrivere messaggi segreti a Tizio ogni volta che voglio.

Ideona!

Se un amico comune (Caio, del quale mi fido) verifica la chiave di Tizio e la firma digitalmente, e io verifico la chiave di Caio, allora so anche che la chiave di Tizio è quella giusta.



Come risolvere il problema?

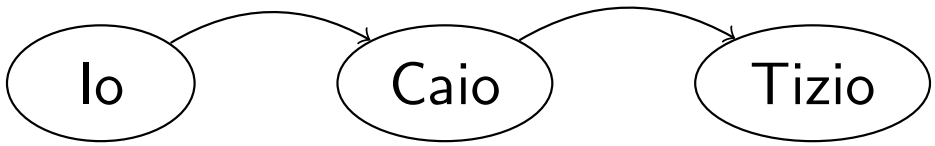
Per scrivere un messaggio segreto a Tizio devo verificare che la chiave con scritto Tizio sia veramente di Tizio.

Idea?!?? (ma è fattibile? Se Tizio sta in Australia?)

Posso incontrare Tizio di persona e controllare se la copia della chiave che ho io è giusta. Da quel punto in poi potrò scrivere messaggi segreti a Tizio ogni volta che voglio.

Ideona!

Se un amico comune (Caio, del quale mi fido) verifica la chiave di Tizio e la firma digitalmente, e io verifico la chiave di Caio, allora so anche che la chiave di Tizio è quella giusta.



Come risolvere il problema?

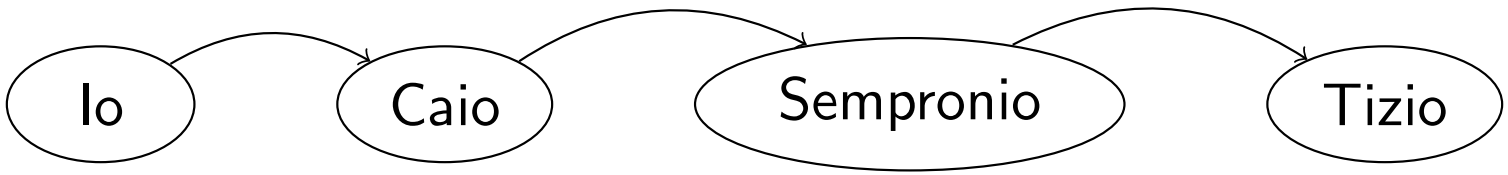
Per scrivere un messaggio segreto a Tizio devo verificare che la chiave con scritto Tizio sia veramente di Tizio.

Idea?!?? (ma è fattibile? Se Tizio sta in Australia?)

Posso incontrare Tizio di persona e controllare se la copia della chiave che ho io è giusta. Da quel punto in poi potrò scrivere messaggi segreti a Tizio ogni volta che voglio.

Ideona!

Se un amico comune (Caio, del quale mi fido) verifica la chiave di Tizio e la firma digitalmente, e io verifico la chiave di Caio, allora so anche che la chiave di Tizio è quella giusta.



Come risolvere il problema?

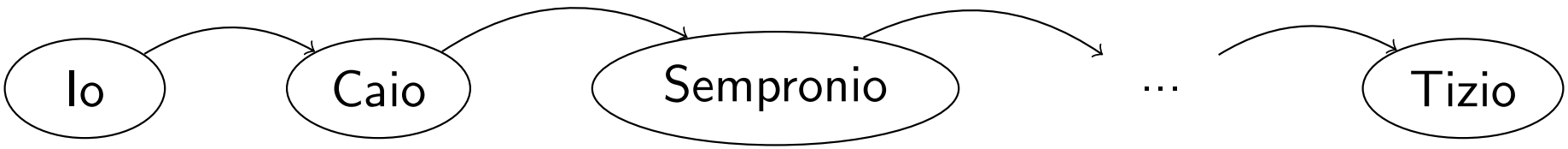
Per scrivere un messaggio segreto a Tizio devo verificare che la chiave con scritto Tizio sia veramente di Tizio.

Idea?!?? (ma è fattibile? Se Tizio sta in Australia?)

Posso incontrare Tizio di persona e controllare se la copia della chiave che ho io è giusta. Da quel punto in poi potrò scrivere messaggi segreti a Tizio ogni volta che voglio.

Ideona!

Se un amico comune (Caio, del quale mi fido) verifica la chiave di Tizio e la firma digitalmente, e io verifico la chiave di Caio, allora so anche che la chiave di Tizio è quella giusta.



Il Web of Trust

Se ognuno firma digitalmente le chiavi che controllare essere corrette si forma una rete di fiducia, il Web of Trust. Chi firma una chiave asserisce di avere verificato che il nome scritto su di essa è corretto. **È quello che faremo anche noi tra poco.**

Il Web of Trust

Se ognuno firma digitalmente le chiavi che controllare essere corrette si forma una rete di fiducia, il Web of Trust. Chi firma una chiave asserisce di avere verificato che il nome scritto su di essa è corretto. **È quello che faremo anche noi tra poco.**

Validità e fiducia

Una chiave può essere:

valida *"Sono sicuro che il proprietario dichiarato è corretto"* (o perché l'ho verificato di persona o perché mi fido di una firma sulla chiave)

invalida *"Non ho garanzia che il proprietario dichiarato sia corretto"*

Se la chiave è valida posso decidere di:

fidarmi *"Considero degne di fiducia le firme fatte con questa chiave"*

non fidarmi *"Non do fiducia alle firme di questa chiave, perché ritengo che il proprietario sia inaffidabile"*

Verificare una chiave

Ad ogni chiave è associato un fingerprint ("impronta digitale"): se due chiavi hanno lo stesso fingerprint, allora sono (quasi) sicuramente uguali.

```
$ gpg --fingerprint D9AB457E
pub   4096R/D9AB457E 2010-02-24 [expires: 2012-04-22]
      Key fingerprint = 82D1 19A8 40C6 EFCA 6F5A  F945 9EDC C991 D9AB 457E
uid                  Giovanni Mascellani <mascellani@poisson.phc.unipi.it>
[...]
```

Verificare una chiave

Ad ogni chiave è associato un fingerprint ("impronta digitale"): se due chiavi hanno lo stesso fingerprint, allora sono (quasi) sicuramente uguali.

```
$ gpg --fingerprint D9AB457E
pub   4096R/D9AB457E 2010-02-24 [expires: 2012-04-22]
      Key fingerprint = 82D1 19A8 40C6 EFCA 6F5A  F945 9EDC C991 D9AB 457E
uid                  Giovanni Mascellani <mascellani@poisson.phc.unipi.it>
[...]
```

Chi vuole verificare questa chiave deve:

- Controllare che il mio vero nome sia Giovanni Mascellani (o perché mi conosce o vedendo un mio documento di identità);
- Controllare che l'email `mascellani@poisson.phc.unipi.it` sia mia (lo stesso controllo va fatto anche per le altre email);
- Controllare che il fingerprint della mia chiave conincida con quello che ha lui.

Fatte queste verifiche può firmare la mia chiave.