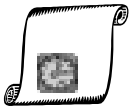
Marcatura Temporale di Documenti Digitali



- Il notaio digitale
- Quando è stato creato il documento **D** ?

Digital Timestamp

La ***marca temporale*** di un documento è qualcosa aggiunto ad esso che prova che il documento è stato "prodotto" **prima**, **dopo** oppure **ad** un fissato momento

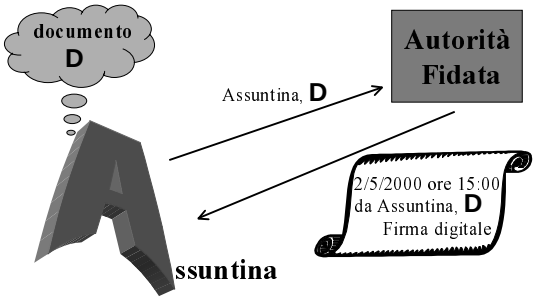
Alcune idee

- Depositare il documento presso un notaio
- Inviare il documento a se stesso, tramite il servizio postale
- Brevetto (se brevettabile…)
- Pubblicare il documento su di un giornale
- Uso di un registro di protocollo
- Foto con un quotidiano (se è un sequestro…)

Facile e Difficile

- È in genere ***facile*** provare che un documento è stato prodotto ***dopo*** una data fissata
- È in genere ***difficile*** provare che un documento è stato prodotto prima di una data fissata

Una soluzione naive



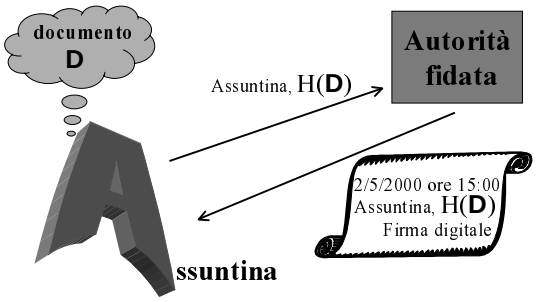
Problemi con la soluzione naive

- Dimensioni del documento **D**
  - per la comunicazione
  - per la memorizzazione dell'Autorità Fidata
- Privatezza del contenuto di **D**
- Quanto è fidata l'Autorità Fidata?

Idea: Funzioni Hash

- Dimensioni del documento **D**
  - per la comunicazione
  - per la memorizzazione dell'Autorità Fidata
- Privatezza del contenuto di **D**
- Quanto è fidata l'Autorità Fidata?

Soluzione naive migliorata



Problema

Sed quis custodiet ipsos custodes?
Giovenale, *Satire*, VI, 100 A.C.

Possibili Soluzioni

Due famiglie di protocolli

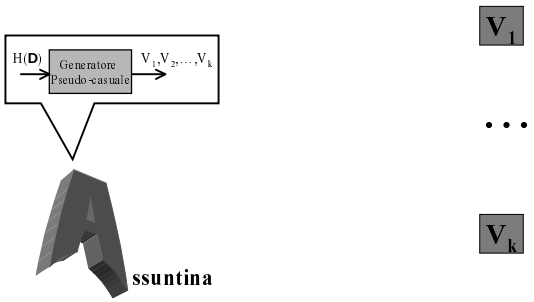
Protocolli distribuiti (senza Autorità Fidata)

Avere più "testimonianze" del tempo

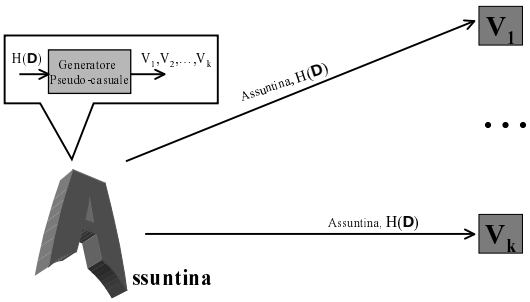
Protocolli con "link" (con Autorità Fidata)

Collegare tra loro le marche dei documenti

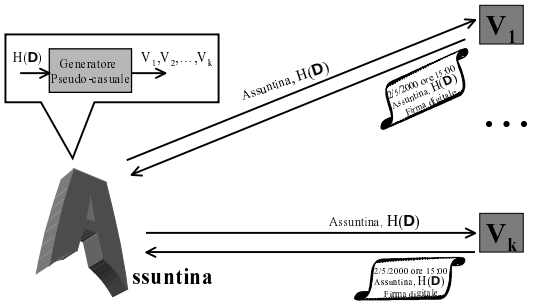
Un protocollo distribuito



Un protocollo distribuito



Un protocollo distribuito



Protocollo Distribuito: Sicurezza

- k grande ⇒ difficile per Assuntina corrompere k persone
- La scelta delle persone da contattare è
  - casuale
  - dipendente dal documento

Protocollo Distribuito: Problemi

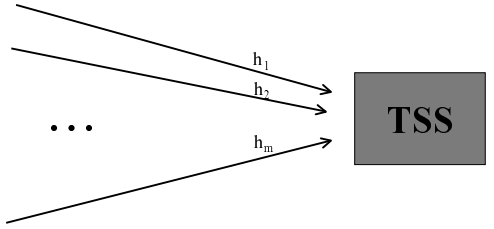
- Ci vogliono molte persone in grado di rispondere immediatamente ad Assuntina
- Durata (vita) delle firme digitali:
  - La firma potrebbe non essere più valida al tempo della verifica della marca temporale:
    - La chiave privata è stata compromessa
    - Lo schema di firme è stato rotto

Protocollo con "link"

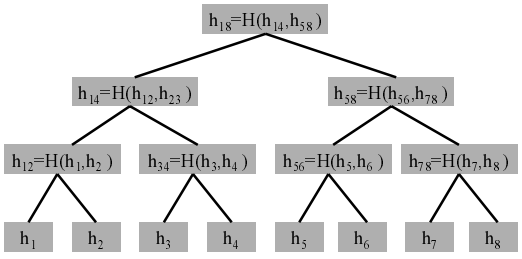
Time Stamping Service (Autorità fidata, … ma non troppo)

- Riceve tutte le richieste in intervalli prefissati
- Le collega tra loro
- Invia ad ognuno una marca temporale
- Vincola se stesso a "non poter predatare"

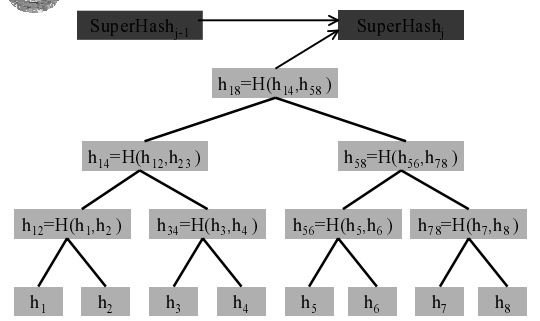
Ricezione richieste
in un prefissato intervallo di tempo



Costruzione albero di hash



Collegamento tra intervalli successivi

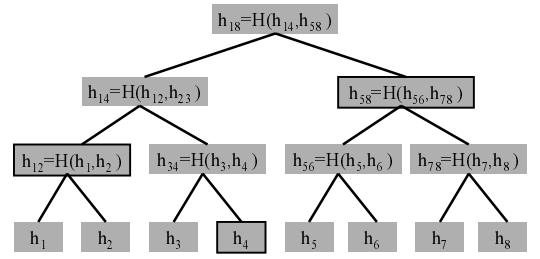


Marca temporale

Inviata per ogni richiesta ricevuta nell'unità di tempo

- ID utente della richiesta
- h_i
- data ed ora
- h_{1m} (valore hash della radice dell'albero)
- info necessarie per verificare che h_i è stato utilizzato per costruire l'albero con radice h_{1m}
- SuperHash$_{j-1}$ e SuperHash$_j$
- Firma del TSS

Info per verifica di "h_3 in albero con radice h_{18}"



Sicurezza del Sistema

Fissato il valore hash della radice, non è possibile

- inserire un nuovo valore nell'albero di hash
- cambiare anche un solo valore nell'albero di hash

…altrimenti si determinerebbe una collisione per la funzione hash

Sicurezza del Sistema

- Si potrebbe rompere lo schema colludendo solo con il TSS e creando una insieme di alberi collegati lunghi "a sufficienza"

- Una possibile soluzione:

pubblicizzare il SuperHash ad intervalli regolari

- ogni giorno su Internet, su quotidiani,…
- distribuzione mediante e-mail, CD,…

Estendere la "vita" di firme digitali

- La firma *F* di un documento digitale **D** potrebbe essere non più valida se la chiave è andata perduta o il sistema di firme è stato "rotto"
- Apponendo una marca temporale su (*F*, **D**), siamo sicuri della validità della firma così come lo eravamo quando la firma è stata fatta la prima volta
- Si confronta la marca temporale di un documento firmato con la data della eventuale revoca della chiave di firma

PGP Digital Timestamping Service

http://www.itconsult.co.uk/stamper.html

- Il TSS firma ogni documento che riceve
- Ogni firma ha un numero seriale
- Il TSS memorizza tutte le firme che genera
- Tutte le marche (Serial Number, Time, Date) emesse possono essere esaminate
- Ogni giorno pubblica due file
  - Numero seriale dell'ultima firma effettuata
  - Tutte le marche emesse quel giorno

Digital Notary

http://www.surety.com

- Il cliente usa del software venduto dalla Surety
- Funzione hash con un digest di 288 bit (MD5+SHA)
- Il sistema usa una struttura ad albero
- L'unità di tempo corrisponde ad un secondo
- Un numero seriale è inserito nel documento
- Il SuperHash è pubblicato in posti accessibili via rete, su un CD-ROM, ed ogni settimana sul Sunday New-York Times

Cifratura Timed-release

Inviare informazioni nel futuro

Obiettivo: cifrare un messaggio che non può essere decifrato da nessuno prima di un prefissato tempo

Crittografia Timed-release

Assuntina vuole che M sia pubblicato al tempo t

- Cifra M con chiave K $M' \leftarrow E_K[M]$
- Pubblica M' e la cifratura della chiave K con una chiave pubblica e_t
- Un TTS al tempo t pubblica la chiave privata d_t corrispondente a e_t