Firma digitale
aspetti tecnologici

Gianni Bianchini
Firenze Linux User Group
giannibi@firenze.linux.it

Convegno E-Privacy 2003
Firenze, Palazzo Vecchio, 14 Giugno 2003

Sommario

- Obiettivi
- Public Key Infrastructure
- Algoritmi crittografici per la firma
- Autorità di certificazione
- Processo di firma
- Attacchi alla firma digitale
- Soluzioni hardware e software

Firma digitale: obiettivi

La *firma digitale* è un'informazione aggiunta ad un insieme di dati con lo scopo di garantire

- *Autenticazione*
  - Garanzia dell'identità dell'ente originante
- *Integrità*
  - Protezione dall'alterazione da parte di enti non autorizzati
- *Non ripudiabilità*
  - Protezione dallo stesso ente originante, che potrebbe negare di essere la fonte dei dati

La *cifratura* dei dati completa il quadro garantendo la *riservatezza*

Firma digitale: obiettivi

- Applicazioni
  - Integrità e provenienza di documenti informatici
  - Integrità di dati contenuti in memoria di massa (es. intrusion detection)
  - Autenticazione ed integrità del traffico in reti sicure
- Firma digitale vs. firma autografa
  - Intrinsecamente (anche se non fisicamente) legata al singolo testo
  - Non trasferibile da un testo ad un altro
  - Non direttamente riconducibile all'identità del soggetto che la appone
  - Soluzione: *autorità di certificazione* (stabilisce, garantisce e pubblica l'associazione firma-soggetto)

Public Key Infrastructure (PKI)

- Fondamento: schemi crittografici asimmetrici o a chiave pubblica
- Funzioni di hash
- Algoritmi di cifratura e generazione/verifica firme
- Autorità di certificazione
- Servizi di directory
- Sistemi di gestione delle chiavi

Schemi crittografici a chiave pubblica

- Chiavi diverse per le operazioni di cifratura (K_c) e decifratura (K_d)
- Cifratura del messaggio M

$$X = \mathrm{cifra}(K_c, M)$$

- Decifratura

$$M = \mathrm{decifra}(K_d, X)$$

- Assunto: le due chiavi non possono essere calcolate l'una dall'altra in tempo ragionevole
- Comunicazione riservata: $K_c = K_p$ è *pubblica*, $K_d = K_s$ è *privata*
- Firma: $K_d = K_p$ è pubblica, $K_c = K_s$ è privata

Comunicazione riservata

A vuole comunicare in modo riservato il messaggio M a B attraverso un canale non sicuro

- A conosce la chiave pubblica K_p^B di B, con essa produce il cifrato X di M e lo comunica a B

$$X = \text{cifra}(K_p^B, M)$$

- A comunica il cifrato X a B
- B rivela il messaggio dal cifrato mediante la propria chiave privata K_s^B

$$M = \text{decifra}(K_s^B, X)$$

- Solo B è in grado di decifrare correttamente il messaggio poiché è l'unico a possedere la chiave privata K_s^B corrispondente a K_p^B

Comunicazione autenticata

A vuole comunicare il messaggio M con garanzia di autenticità e integrità

- A produce il cifrato X di M mediante la propria chiave privata K_s^A (chiave di firma)

$$X = \text{cifra}(K_s^A, M)$$

- A comunica M e X (nessuna esigenza di riservatezza!)
- Il destinatario decifra X con la chiave pubblica K_p^A di A e confronta il risultato con M
- Se $M == \text{decifra}(K_p^A, X)$, allora
  - ⋆ il messaggio M non è stato alterato
  - ⋆ il messaggio M proviene dal possessore della chiave privata K_s^A

Funzioni di hash (digest)

La generazione e l'invio del cifrato dell'intero messaggio sono dispendiosi

Una *funzione di hash* riduce un input di lunghezza variabile M ad un output di lunghezza fissa H

$$H = \mathrm{hash}(M)$$

con le seguenti proprietà:

- Impossibilità di dedurre l'input M dall'output H
- Impossibilità di generare un dato output
- Impossibilità di determinare due input che producono lo stesso output
- Verifica di integrità: $H == \mathrm{hash}(M)$
  - ⋆ Non garantisce l'autenticità (un intruso può facilmente sostituire M e ricalcolare H)
- MD5 (1992), SHA$-x$ (1995), RIPEMD

Message authentication codes (MAC)

- Funzione hash del messaggio M e della chiave di firma K_s^A

$$AH = \mathrm{hash}(K_s^A, \mathrm{hash}(K_s^A, M))$$

- Garantiscono integrità e autenticazione
  - ⋆ Non è possibile ricostruire un MAC coerente di un messaggio modificato in assenza della chiave di firma
- HMAC-MD5, HMAC-SHA

Algoritmi per la firma digitale

In generale

$$\text{Firma} = \text{Funzione hash} + \text{cifratura asimmetrica}$$

- Generazione della firma F dal messaggio M

$$H = \text{hash}(M)$$
$$F = \text{cifra}(K_s^A, H)$$

- Trasmissione di M e F
- Condizione di integrità e autenticità

$$\text{hash}(M) == \text{decifra}(K_p^A, F)$$

Algoritmi per la firma digitale

- RSA (1978)
  - Identico al corrispondente di cifratura
  - Chiavi pubblica e privata interscambiabili
- ElGamal di firma (1985)
- Schnorr (1990)
- Digital Signature Standard (DSS) (NIST, 1994)
  - Definisce l'algoritmo di firma DSA
  - Adotta SHA come algoritmo di hash
  - Specifiche per la generazione dei parametri dell'algoritmo

L’autorità di certficazione

Risponde al problema dell’associazione tra chiavi ed identità fisica del possessore

- Accerta l’identità del possessore di un insieme di chiavi private e la corrispondenza con le rispettive chiavi pubbliche
- Garantisce l’identità del possessore delle chiavi private (a meno della compromissione della segretezza di queste)
- Garantisce la non ripudiabilità dei messaggi verificabili con una data chiave pubblica, certificando il detentore della corrispondente chiave privata

Il processo di firma

- Azioni preliminari
  - ⋆ Registrazione dell'utente A presso un'autorità di certificazione (CA)
  - ⋆ Generazione di una coppia di chiavi pubblica-privata (K_p^A, K_s^A)
  - ⋆ Certificazione della chiave pubblica presso la CA
  - ⋆ Registrazione e pubblicazione della chiave pubblica
- Successivamente, l'utente può firmare documenti usando la propria chiave privata, fino alla scadenza della certificazione sulla chiave pubblica
- La validità della chiave pubblica può essere revocata in ogni momento, a seguito di (sospetta) compromissione della chiave privata

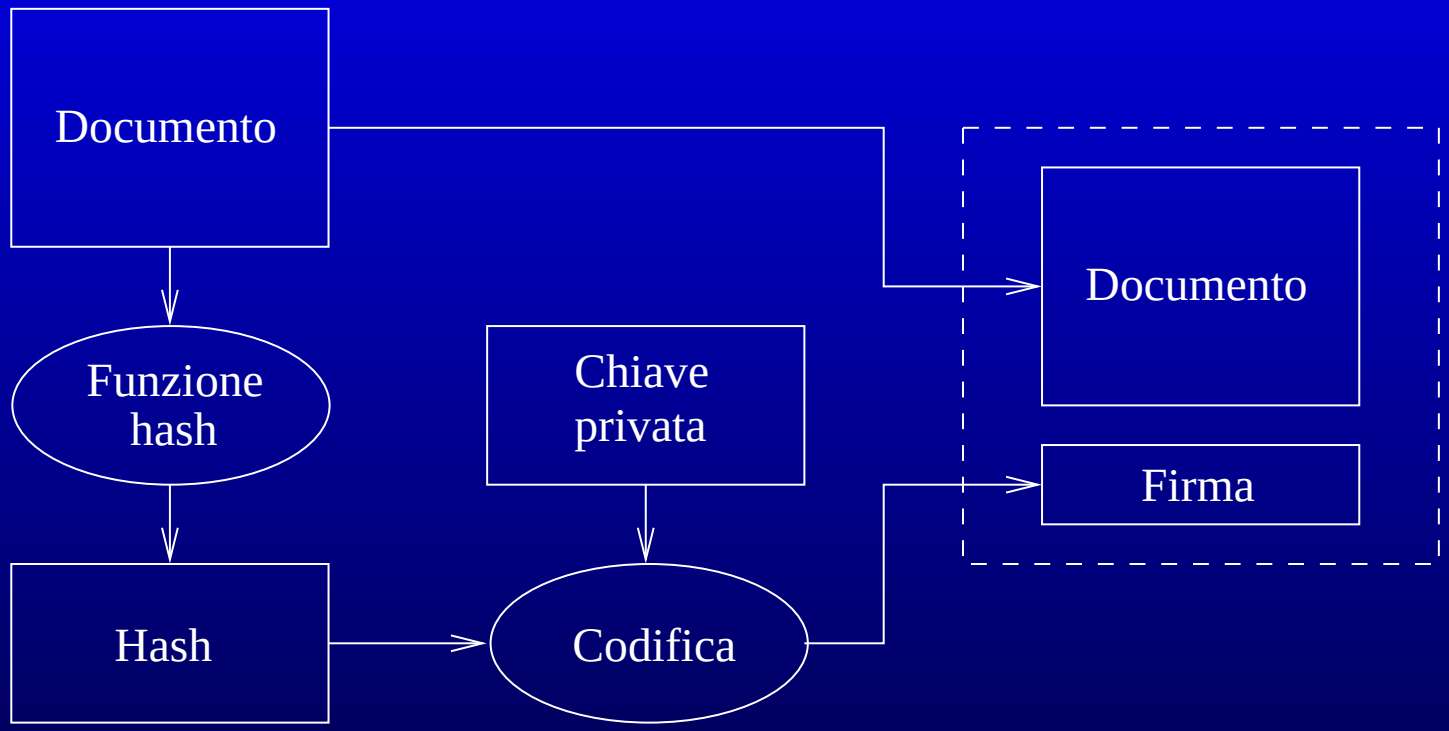
Registrazione dell'utente presso la CA

- L'utente richiede alla CA la registrazione fornendo la documentazione richiesta per accertare l'identità
- La CA attribuisce all'utente un identificatore di cui essa garantisce l'univocità
- La CA inserisce l'utente con l'identificatore attribuitogli nei cataloghi di utenti registrati che essa gestisce
- La CA fornisce attraverso un canale sicuro una chiave crittografica K_a che l'utente dovrà utilizzare per le richieste di certificazione delle chiavi

Certificazione e registrazione delle chiavi

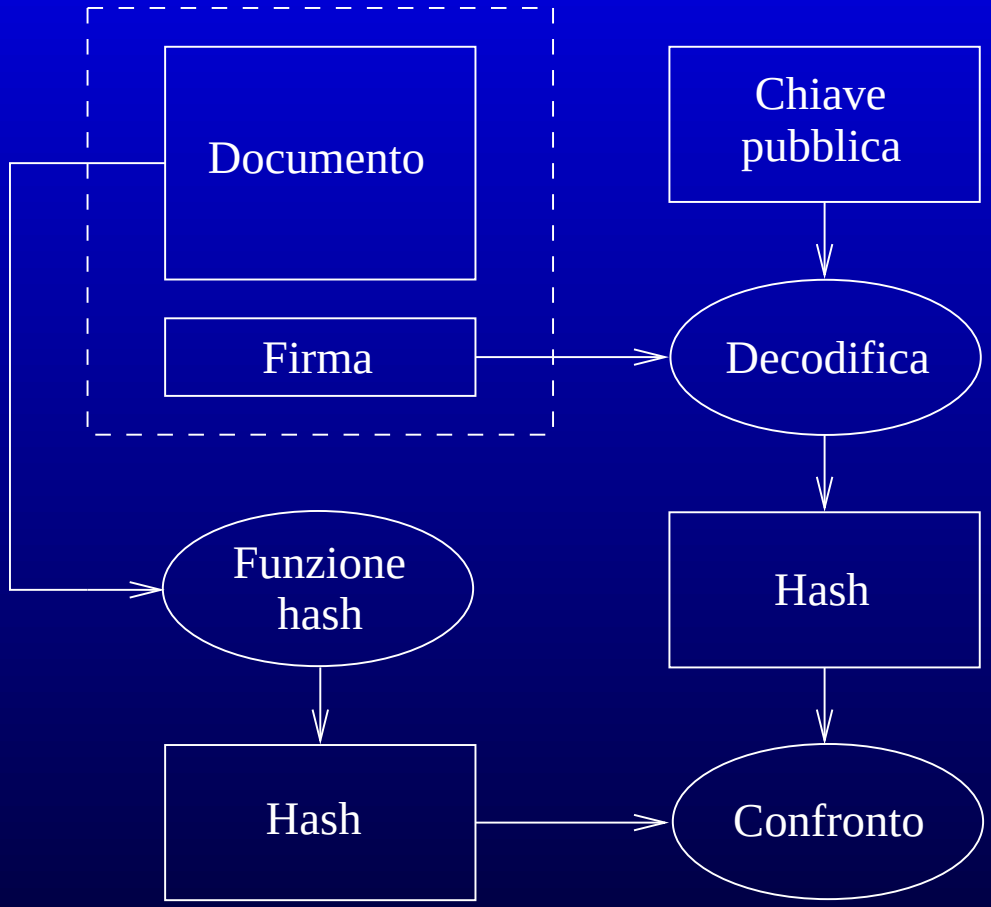
- L'utente invia alla CA la richiesta di certificazione per la chiave K_p^A, autenticandola con la chiave K_a ricevuta dalla CA all registrazione
- La CA genera a partire da K_p^A una chiave pubblica certificata, firmata con la propria chiave privata per garantirne la provenienza, che potrà essere accertata da chiunque utilizzando la chiave pubblica della CA
- Il certificato può essere reso disponibile in cataloghi ai quali può accedere chiunque abbia bisogno di accertare la validità di una firma
- L'ente certificatore stesso può provvedere alla generazione delle chiavi (es. fornitura dispositivi di firma hardware)

Generazione della firma



- Generazione di una “busta” (PKCS#7)
- È possibile (ma non necessario) allegare il certificato del mittente
- Specifiche di formato: S/MIME, PGP

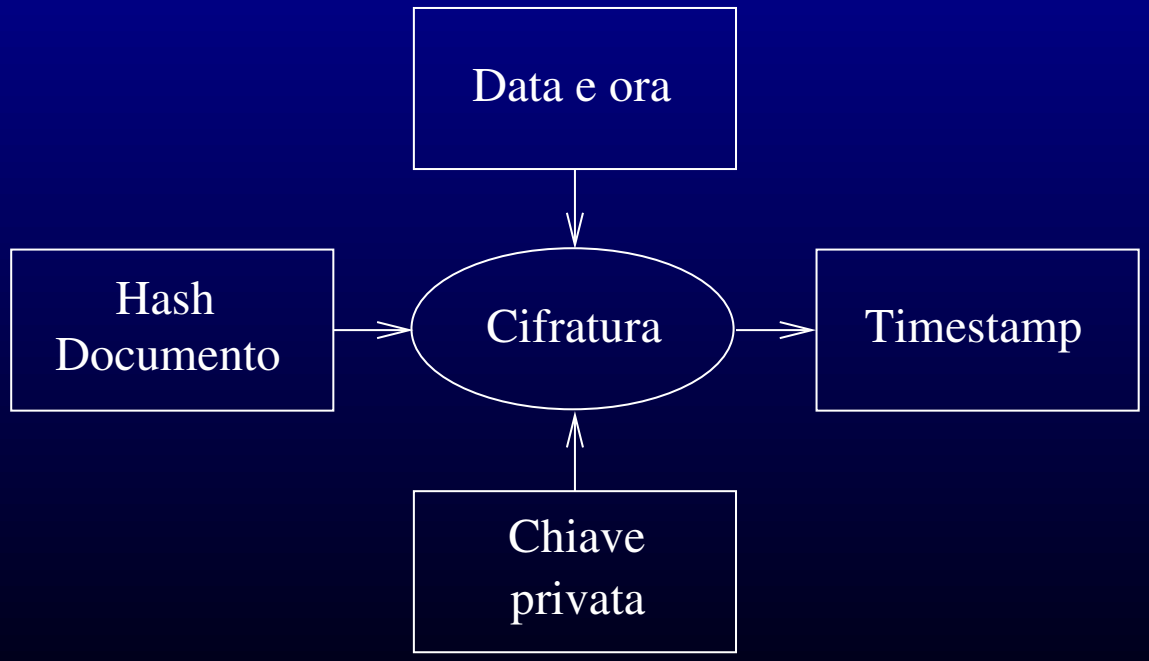
Verifica della firma



- Presuppone la verifica dell'identità del mittente mediante la chiave pubblica della CA

Timestamp

- Risponde all'esigenza di certificare data e ora di redazione/pubblicazione
- Viene effettuata da un'autorità di certificazione (TSA)
- Data e ora (tempo certificato) più hash del documento cifrati con la chiave privata della TSA



Punti deboli e possibilità di attacco

- Tutti gli attacchi ad un sistema a chiave pubblica
  - ⋆ Attacchi agli algoritmi crittografici (fattorizzazione (RSA), logaritmo discreto (DSA), ecc.)
  - ⋆ Inferenza di informazioni sulla chiave privata dalle firme
- Macro nei documenti oggetto di firma
- Falsificazione identità del titolare (CA)
- Debolezza dell procedure della CA e fattore umano
- Compromissione del software di firma
- Memorizzazione ed uso delle chiavi private

Problemi con la gestione della chiave privata

- La chiave privata è memorizzata su un supporto fisico e protetta da una passphrase (PKCS#8, PKCS#12)
  - ⋆ Attacco a forza bruta
- Vulnerabilità del supporto di memorizzazione
- Attacchi alla memoria del software di firma
- Attacchi di tipo generico ai sistemi
  - ⋆ Network-based
  - ⋆ Accesso fisico
  - ⋆ Key logging
  - ⋆ ...

Dispositivi di firma

- Smart cards
  - ⋆ Low-end: dispositivi di memoria (schede telefoniche)
  - ⋆ High-end: microprocessore + memoria + firmware (SIM, JavaCards)
- Token crittografici

- Memorizzazione delle chiavi
- Implementazione degli algoritmi di firma
  - ⋆ La chiave privata non lascia mai il dispositivo

Attacchi

- Attacchi non invasivi
  - Modifica condizioni ambientali (induzione comportamenti anomali)
  - Misura potenza assorbita in diverse situazioni operative
- Attacchi invasivi
  - Bombardamento elettronico
  - Analisi della struttura e dello stato interno
- Compromissione del sistema ospite di firma
  - Il sistema ospite può indurre il dispositivo di firma a firmare qualcosa che non si intende firmare
- Compromissione del sistema di verifica e attacchi alle chiavi pubbliche
  - Falsificazione della CA e dei root certificates

La solita regola d’oro

Ogni catena è resistente quanto il suo anello più debole

Grazie per l’attenzione!

/giannibi

Riferimenti

- P. Gutmann, *Encryption and security tutorial*, http://www.cs.auckland.ac.nz/ pgut001/tutorial.
- M. Terranova, *Firma digitale: tecnologie e standard*, http://www.privacy.it/firma.html.
- E. Zimuel, *Introduzione alla crittografia ed alla crittoanalisi*, Italian Cyberspace Law Conference, Bologna 2001.
- B. Schneier, *Applied cryptography*, 2nd edition, John Wiley & Sons, 1996.
- M. Bellare, R. Canetti, H. Krawczyk, *Keyed Hash Functions for Message Authentication*, Advances in Cryptology – CRYPTO 96 Proceedings, Lecture Notes in Computer Science, Springer-Verlag Vol. 1109, N. Koblitz, ed, 1996, pp. 1-15.

Riferimenti

- National Institute of Standards and Technology, *Digital Signature Standard*, http://www.itl.nist.gov/fipspubs/fip186.htm.
- R. L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, in ”Communications of the ACM”, vol. 21 (1978), n. 2, pp. 120-126.
- C. Schnorr, *Efficient signature generation by smart cards*, in ”Journal of Cryptology”, n. 4 (1991), pp. 161-174.
- Public Key Cryptography Standards (PKCS) http://www.rsasecurity.com/rsalabs/pkcs.
- C. Ellison, B. Schneier, *Ten risks of PKI: what you’re not being told about public key infrastructure*, Computer Security Journal, vol. 16, n. 1, 2000, pp. 1-7, http://www.counterpane.com/pki-risks.html.