Il documento informatico
e la firma digitale nelle applicazioni pratiche

La firma digitale
e le sue possibili applicazioni

dott. Enrico Zimuel (enrico@zimuel.it)

Pescara, 15 febbraio 2008

Note sul Copyright:

Questa presentazione è stata creata con OpenOffice 2.0
www.openoffice.org

Sommario

- Che cos'è la crittografia
- La crittografia a chiave pubblica
- Le Certification Authority
- La firma digitale e le funzioni hash
- Differenze tra firma digitale e firma autografa
- La smart card ed il dispositivo di firma
- Esempi d'utilizzo

La crittografia

- La **crittografia** (dal greco *kryptos*, nascosto, e *graphein*, scrivere) è la scienza che si occupa dello studio delle scritture “segrete”.
- E' una disciplina antichissima, le cui origini risalgono alle prime forme di comunicazione dell'uomo, anche se si è sviluppata come scienza vera e propria solo dopo la seconda guerra mondiale .
- Utilizzata ovunque nel quotidiano: bancomat, internet (SSL), cellulari (GSM/UMTS) , trasmissioni satellitari (SECA2).

Gli ambiti d'utilizzo della crittografia

- **Autenticazione**: operazione che consente di assicurare l'identità di un utente in un processo di comunicazione.
- **Riservatezza**: protezione dell'informazione da occhi indiscreti. Ad esempio protezione di un messaggio (email) su di un canale pubblico di comunicazione (internet).
- **Integrità**: operazione che consente di certificare l'originalità di un messaggio o di un documento.
- **Anonimato**: operazione che consente di non rendere rintracciabile una comunicazione, è una delle operazioni più complesse da realizzare.

La crittografia a chiave pubblica

- Ideata nel 1976 da Whitfield Diffie e Martin Hellman per risolvere il problema della "trasmissione della chiave" nei sistemi di cifratura simmetrici
- Utilizza una coppia di chiavi per le operazioni di cifratura (*encryption*) e decifrazione (*decryption*).
- Una chiave detta pubblica (**public key**) viene utilizzata per le operazioni di encryption.
- L'altra chiave, detta privata (**private key**), viene utilizzata per le operazioni di decryption.

Esempio di cifratura di un messaggio

Esempio di autenticazione di un messaggio

Chiave pubblica A

Chiave privata A

Chiave pubblica B

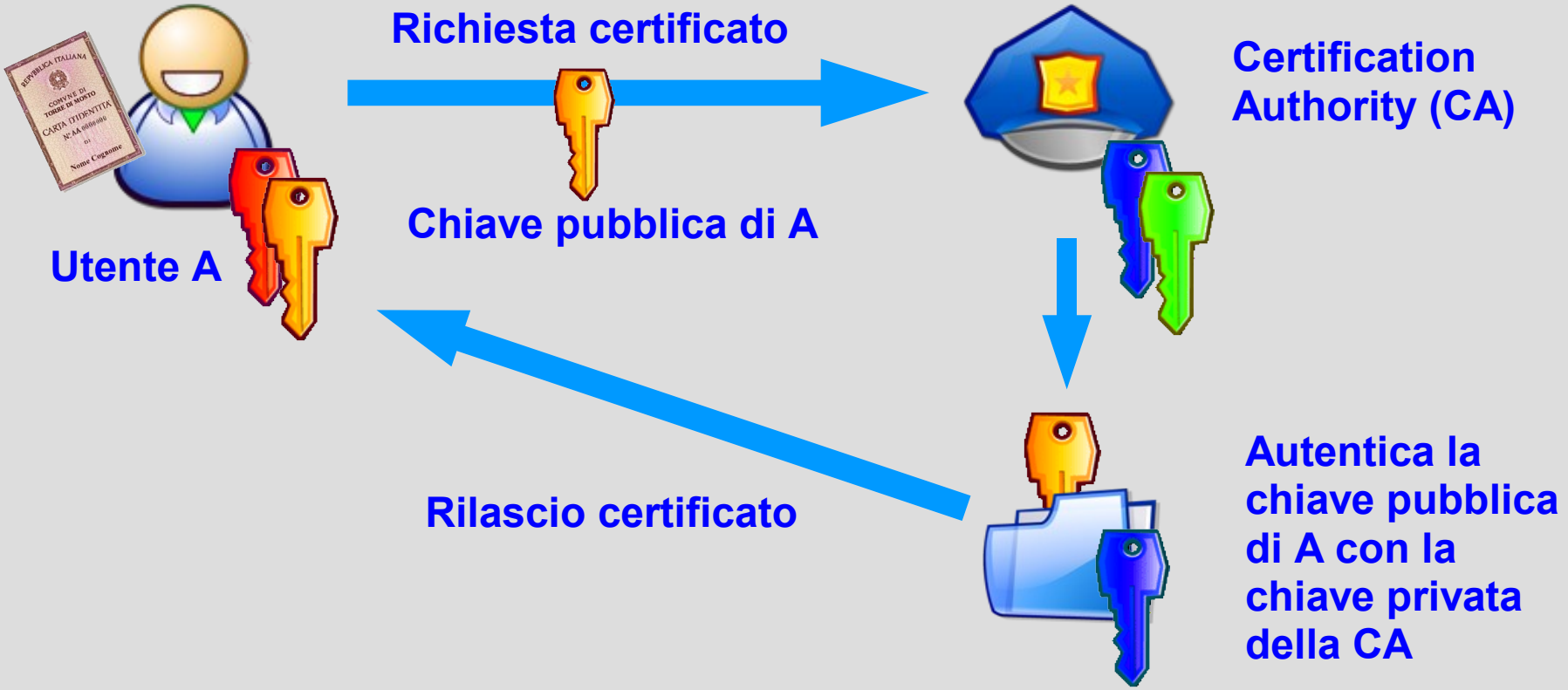
Chiave privata B

Esempio di cifratura ed autenticazione di un messaggio

La nascita delle Certification Authority (CA)

- Chi mi garantisce la corrispondenza delle chiavi pubbliche con i legittimi proprietari?
- Nascita delle Certification Authority (CA).
- "**Certificazione**, il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene... "
  DPR 10 Novembre 1997, n. 513
- Ogni CA deve avere un registro dei certificati e delle revoce consultabile pubblicamente per via telematica

Il processo di certificazione



La smart card rilasciata dall'ente certificatore

- Cosa contiene la smart card rilasciata dall'ente certificatore?
  - la chiave pubblica e privata dell'utente (generata direttamente dall'ente);
  - il certificato digitale (contenente la chiave pubblica dell'utente firmata tramite la chiave privata dell'ente certifcatore).

La firma digitale

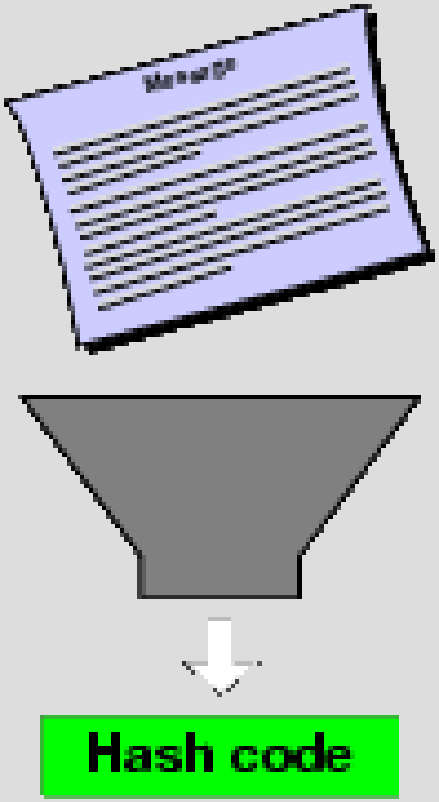
- La firma digitale è l'operazione di autenticazione che consente di legare un documento alla chiave pubblica del firmatario.
- Per effettuare tale operazione è necessario utilizzare la chiave privata del firmatario.
- Chiunque può verificare la firma digitale in un documento utilizzando la chiave pubblica del firmatario.
- Nell'ordinamento giuridico italiano la firma digitale a crittografia asimmetrica è riconosciuta ed equiparata a tutti gli effetti di legge alla firma autografa su carta.

Il processo di firma digitale

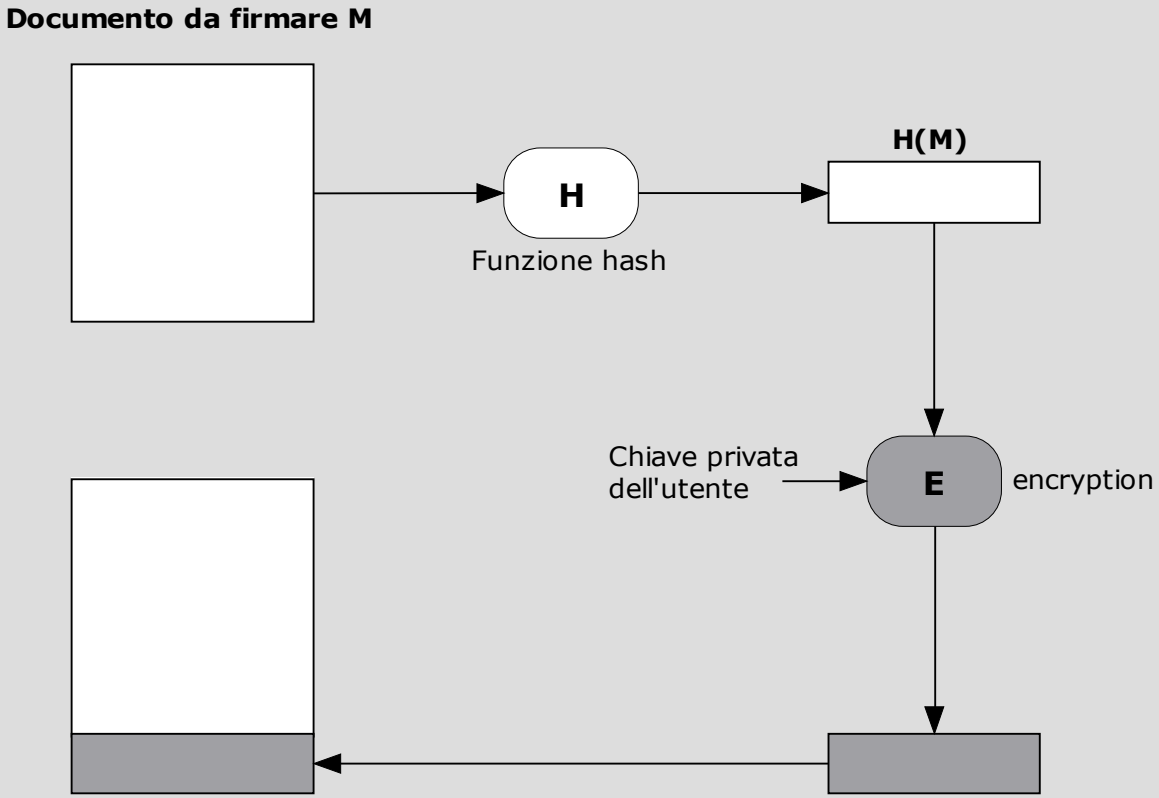
- Per poter firmare un documento è necessario disporre della chiave privata del firmatario.
- Problema: per l'autenticazione di un documento di grandi dimensioni con un algoritmo a chiave pubblica occorre molto tempo.
- Soluzione: il procedimento di “firma” non viene applicato a tutto il documento ma solo ad un suo “riassunto” generato attraverso l'utilizzo di una funzione hash.
- La firma dell'hash del documento corrisponde alla firma digitale del documento.

Le funzioni hash sicure

- Vengono utilizzate per generare un sorta di “riassunto” di un documento informatico (file).
- Una funzione hash accetta in ingresso un messaggio di lunghezza variabile M e produce in uscita un digest di messaggio H(M) di lunghezza fissa.
- Questo digest (impronta digitale, targa, riassunto) è strettamente legato al messaggio M; ogni messaggio M genera un H(M) univoco.
- Anche considerando due messaggi M ed M' differenti solo per un carattere le loro funzioni hash H(M) e H(M') saranno diverse.



Schema di firma di un documento informatico



Documento firmato:
Il ricevente può verificare la firma utilizzando la chiave pubblica dell'utente firmatario e riapplicando la funzione hash

Differenze tra firma digitale e firma convenzionale

	Firma autografa	Firma digitale
Creazione	manuale	mediante algoritmo di creazione
Apposizione	sul documento: la firma è parte integrante del documento	come allegato: il documento firmato è costituito dalla coppia (documento, firma)
Verifica	confronto con una firma autenticata: metodo insicuro	mediante algoritmo di verifica pubblicamente noto: metodo sicuro
Copia	distinguibile	indistinguibile
Validità temporale	illimitata	limitata
Automazione	non possibile	possibile

Esempi d'utilizzo della firma digitale

Bibliografia

- M. Cammarata “Firme elettroniche. Problemi normativi del documento informatico”, Monti & Ambrosini Editore, 2007
- M. Cammarata, E. Maccarone “La firma digitale sicura”, Giuffrè Editore, 2003
- F. Rizzo, “Il documento informatico. «Paternità» e «falsità»”, Edizioni scientifiche italiane, 2005
- F. Sivilli, “La crittografia nella società dell'informazione”, Edizioni Giuridiche Simone, 2006
- C. Giustozzi, A. Monti, E. Zimuel “Segreti, Spie e Codici Cifrati”, Apogeo Editore, 1999