Firma digitale: teoria e applicazioni

Prof. ing. Pierluigi Ridolfi

- Richiami di crittografia
- Aspetti tecnici e normativi
- Attività di Certificazione
- Direttiva Europea
- Applicazioni
- Problemi aperti

Università di Bologna, 14 maggio 2001

Decreto del Presidente della Repubblica n. 513, 10/11/'97

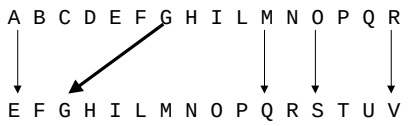
Art. 1, comma 1, sub b)

"**Firma digitale**: il risultato della procedura informatica basata su un ***sistema di chiavi asimmetriche*** a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico …"

Crittografia

- **Codifica simmetrica**
  - un metodo per codificare
  - il metodo inverso per decodificare
  - una sola chiave per la codifica e la decodifica
- **Codifica asimmetrica**
  - chiavi e metodi diversi per codificare e decodificare

Codifica simmetrica: metodo di trasposizione



chiave = 4

ROMA ⇒ VSQE

Codifica simmetrica: metodo di sostituzione

ROMA ⇒ ICPH

Codifica simmetrica: metodo tabellare

A B C D E F G H I L **M** N **O** P Q **R**

a) H T U L M E R O G B P F **C** V N I
b) Q E R T U I O P A S D F G H L **Z**
.....
r) M N B V C Z L H G F **D** S A P O I

chiave = bar
ROMA ⇒ ZCDQ

Codifica simmetrica: Data Encryption Standard

- Il DES è un sistema di codifica basato su una complessa sequenza di trasposizioni e operazioni tabellari, che trasforma un “campo” di 64 bit in un altro di 64 bit, utilizzando una chiave di 56 bit.
- Il procedimento di decodifica è l’inverso di quello di codifica.
- Standard mondiale in vigore da oltre 20 anni.

Basi della sicurezza nella codifica simmetrica

- **Metodo** presunto / noto
- **Cifrario** riservato / noto
- **Chiave** una sola, segreta (nota solo ai corrispondenti)

Punto debole

- C’è sempre una fase in cui la chiave “viaggia” tra i corrispondenti
- In questa fase la chiave può essere intercettata

Alla ricerca di sistemi più sicuri

- Sistemi a due chiavi
- Teorema di Fermat-Eulero
- Sistema RSA
- Principio di funzionamento
- Motivo dell’invulnerabilità

Teorema di Fermat

Se a e n sono due numeri primi, con $a < n$, il resto della divisione tra la potenza a^{n-1} e l'esponente n è sempre **= 1**

Esempi

$a = 2 \quad n = 5 \Rightarrow \quad a^{n-1} = 16$

16 : 5 = 3 con resto **1**

$a = 3 \quad n = 7 \Rightarrow \quad a^{n-1} = 729$

729 : 7 = 104 con resto **1**

Teorema di Eulero

E' una rielaborazione del Teorema di Fermat nel caso che *n* non sia un numero primo ma il prodotto di due numeri primi.

Se a è primo e $n = p \cdot q$ (p e q primi), il resto della divisione della potenza $a^{(p-1)\cdot(q-1)}$ per n è sempre = **1**

Es: $p = 3 \quad q = 5 \quad a = 2$

$a^{(p-1)(q-1)} = 2^8 = 256$

256 : 15 = 17 con resto **1**

Sistema RSA (1)

- Rivest, Shamir, Adleman.
- MIT, 1977.
- Algoritmo basato sul Teorema di Fermat-Eulero.

Sistema RSA (2)

- Le chiavi sono due: una **segreta** (chiave privata), l'altra **non segreta** (chiave pubblica).
- C'è un Ente centrale E che genera le due chiavi.
- *n* sia il prodotto dei due numeri primi *p* e *q*, noti solo a E.

Sistema RSA (3)

- A ogni persona viene assegnata come **chiave pubblica** un numero a caso *h*.
- La corrispondente **chiave privata** *j* viene calcolata in modo che

$$(h \cdot j) : [(p-1) \cdot (q-1)]$$

abbia per resto 1.

Sistema RSA (4)

Se:

m' = resto della divisione di m^h per n

m'' = resto della divisione di m'^j per n

Si dimostra che:

$m'' = m$

Pertanto:

m' = messaggio cifrato
m'' = messaggio decifrato

Esempio

- $p = 3, \quad q = 5 \quad \Rightarrow n = 15$
- $\Rightarrow (p-1)(q-1) = 8$
- $h = 11 \Rightarrow j = 3$
- verifica: $(h \cdot j):8 \Rightarrow$ resto = 1

$m = 2$

$m' \Rightarrow m^{h} = 2^{11} = 2048$

$\Rightarrow : 15 \Rightarrow$ resto = $8 = m'$

$m'' \Rightarrow m'^{j} = 8^{3} = 512$

$\Rightarrow : 15 \Rightarrow$ resto = $2 = m$

Traccia della dimostrazione

- $R[a^{(p-1)(q-1)} : n] = 1$
- $a^{(p-1)(q-1)} = k\,n + 1$
- $R[(h\,j) : [(p-1)(q-1)]] = 1$
- $h\,j - 1 = k\,[(p-1)(q-1)]$
- $m' = R[\,m^{h} : n]$
- $m' = m^{h} - k\,n$
- $m'' = R[\,m'^{j} : n\,]$
- $= R[\,[\,m^{h\,j} + n(\ldots)\,] : n\,]$
- $= R[\,m^{h\,j} : n\,]$
- $= R[\,m\,m^{h\,j-1} : n]$

  $= R[\,m\,m^{k(p-1)(q-1)} : n]$

  $= m$

Sintesi del principio delle due chiavi

- ***j*** è la chiave privata, nota solo all'interessato.
- ***h*** è la chiave pubblica, che tutti possono conoscere.
- ***j*** e ***h*** sono generate simultaneamente, ma non è possibile nota ***h*** ricavare ***j*** (e viceversa).
- Il sistema RSA è praticamente invulnerabile.

Il motivo della invulnerabilità

- E' noto *n*, che si sa essere il prodotto dei due primi *p* e *q*, ma non sono noti né *p* né *q*, né è possibile ricavarli da *n* (si tratta di scomporre in fattori un numero grandissimo, operando per tentativi).
- Non è pertanto possibile calcolare (*p-1*)•(*q*-1).
- Dunque, nota *h*, non è possibile calcolare *j*.

Esempio

- Lunghezza di *n*: 128 bit
- Max $n = 2^{127} \approx 10^{38}$
- Max min (p,q) = $\sqrt{n} \approx 10^{19}$
- N. primi <n = $\Pi(n) \approx n/\log n$
- $\Pi(10^{19}) \approx 10^{17}$
- Calcolatore in grado di fare 10^9 divisioni / secondo
- Occorrono 10^8 secondi ≈ 3 anni

Basi della sicurezza nella codifica asimmetrica

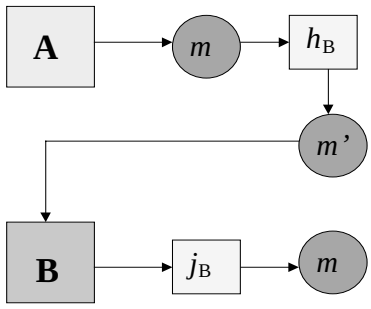
Numero di bit dell'esponente

Segretezza della chiave privata

I tre pilastri della crittografia

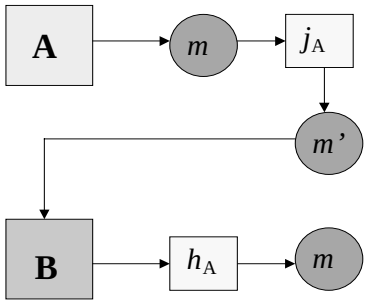
- **Riservatezza**
  ⇒ certezza che il testo può essere letto solo dal destinatario.
- **Autenticità**
  ⇒ certezza del mittente.
- **Integrità**
  ⇒ certezza del messaggio.

Garanzia della riservatezza



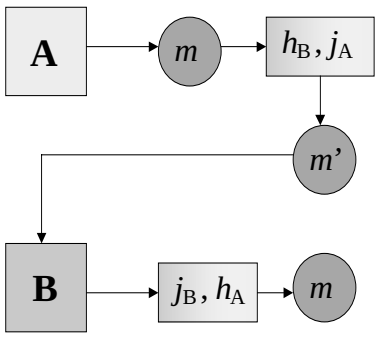
A codifica *m* con la chiave pubblica di B e ottiene *m'* che invia a B; B lo decodifica con la propria chiave privata riottenendo *m.*

Garanzia dell'autenticità



A codifica *m* con la propria chiave privata e ottiene *m'* che invia a B; B lo decodifica con la chiave pubblica di A riottenendo *m.*

Schema del processo di riservatezza e autenticità



Doppia codifica

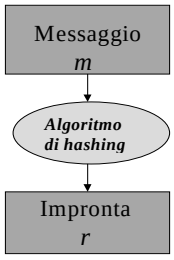
Integrità

- Il processo di autenticità garantisce indirettamente anche l'integrità del messaggio trasmesso, però:

  ⇒ se *m* è lungo la sua codifica può risultare molto onerosa;
  ⇒ solo in pochi casi valgono criteri di riservatezza per i quali occorra codificare *m*.

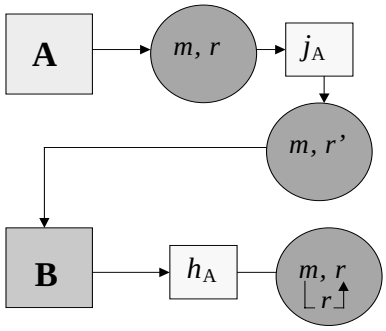
Impronta ("hash")

Campo di lunghezza fissa (in genere 160 bit) ricavato dal messaggio mediante una precisa formula.



La corrispondenza non è biunivoca.
E' praticamente impossibile risalire dall'impronta a un messaggio che generi quell'impronta.

Garanzia dell'integrità



A calcola *r*, lo codifica con la propria chiave privata, ottiene *r'* che invia a B insieme a *m*; B decodifica *r'* con la chiave pubblica di A riottenendo *r*, poi ricalcola l'*r* dell'*m* ricevuto; se le due impronte coincidono significa che *m* non è stato alterato.

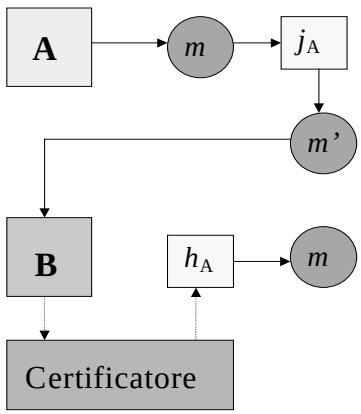
Certificazione

- Garantisce la correttezza formale e sostanziale del mittente.
- Viene ottenuta con particolari procedure informatiche e organizzative.
- Viene assicurata dai Certificatori.

I Certificatori

- Concetto di Comunità.
- I Certificatori:
  - possiedono le chiavi pubbliche di ogni membro della Comunità;
  - le forniscono a richiesta;
  - hanno una struttura tecnica ed etica a prova di frode;
  - sono soggetti a riconoscimento governativa (Elenco dei Certificatori).
- Generazione delle chiavi.

Processo di certificazione



Vantaggi della certificazione

- Non è necessario che B conosca la chiave pubblica di ognuno dei suoi corrispondenti A: basta rivolgersi al Certificatore C.
- Se C risponde fornendo a B la chiave di A, implicitamente garantisce a B che A “esiste”.
- Un uso fraudolento delle chiavi può essere bloccato con una segnalazione a C.

Norme nazionali

- Legge 59/97 (Bassanini), art. 15.
- DPR 513/97: Regolamento in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici.
- ⇒ DPR 445/00 Testo Unico sulla Documentazione Amministrativa
- DPCM 8/2/99: Regole tecniche per l’attuazione del DPR
- Circolare AIPA 26/7/99: elenco dei Certificatori.

Legge n. 59, 15/3/’97

Art. 15, comma 2.

“Gli atti, dati e i documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge; i criteri di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare, entro centottanta giorni dalla data di entrata in vigore della presente legge...”

Definizioni (DPR)

- Documento informatico.
- Firma digitale.
- Dispositivo di firma.
- Certificato.
- Certificatore.

Documento informatico

- Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Cosa completamente diversa è:

- Rappresentazione informatica del contenuto di atti, fatti o dati giuridicamente rilevanti.

Validità

- Il documento informatico è valido a tutti gli effetti di legge, e in particolare soddisfa il requisito legale della forma scritta, se conforme al DPR.
- Corrispondenza ⇒ Mittente.
- Atti di archivio ⇒ Autore.

Firma digitale

Art. 1, comma 1, sub b)

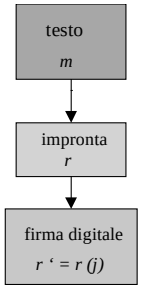
"Il risultato della procedura informatica basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la **provenienza e l'integrità** di un documento informatico …"

Significato della firma digitale

firma digitale

⇓

impronta di un testo codificata con la chiave privata del mittente



Caratteristiche della firma digitale

- La firma digitale dipende dal testo e dal mittente.
- Testi uguali, sottoscritti da soggetti diversi, hanno firme digitali diverse.
- Testi diversi, sottoscritti dallo stesso soggetto, hanno firme digitali diverse.

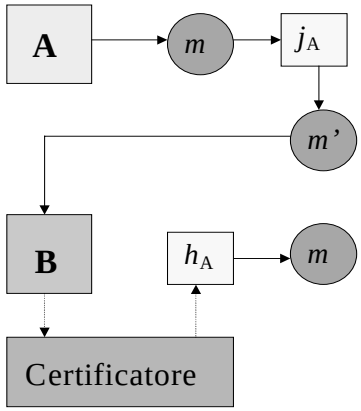
Valore legale della firma digitale

- L'apposizione della firma digitale di un documento informatico equivale alla sottoscrizione di un documento cartaceo.
- Essa integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.
- I contratti stipulati con strumenti informatici ***secondo le disposizioni del DPR*** sono validi a tutti gli effetti di Legge.

Dispositivo di firma

- Formato carta di credito, con chip; va inserito in un apposito lettore collegato a un PC.
- Capace di generare - una volta sola - una coppia di chiavi asimmetriche.
- Dotato di memoria per contenere la chiave privata.
- In grado - tutte le volte che si deve firmare un documento - di generare la firma digitale.

Processo “teorico” di certificazione



Certificato

- Il Certificatore emette un certificato per ogni chiave pubblica di ogni persona nella sua attività di “mittente”.
- Il certificato contiene:
  - l’identificativo del Certificatore;
  - un numero progressivo;
  - l’identificativo del mittente;
  - la chiave pubblica del mittente;
  - eventuali “qualifiche” del mittente;
  - il periodo di validità.
- E’ firmato dal Certificatore.
- E’ in possesso del mittente.
- Va allegato al documento da inviare.

Schema del certificato

Identificativo del Certificatore
N. ordine del certificato
Identificativo dell’Utente
Chiave pubblica dell’Utente
Qualifiche dell’Utente
Periodo di validità
Impronta di tutto quanto sopra
Codifica dell’impronta con la chiave privata del Certificatore
= firma digitale

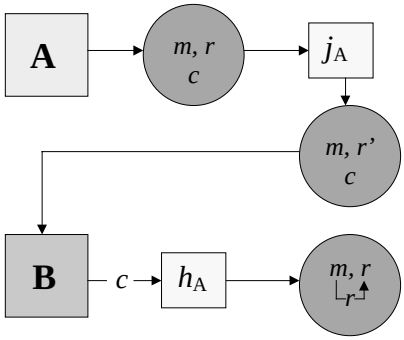
Validità di un certificato

- Elenco dei numeri dei certificati non più validi.
  - *Sospensione*: valore provvisorio.
  - *Revoca*: valore definitivo.
- Sono considerati validi tutti i certificati emessi da un certificatore e non inclusi nell'elenco di quelli sospesi o revocati.
- Responsabilità del Certificatore.

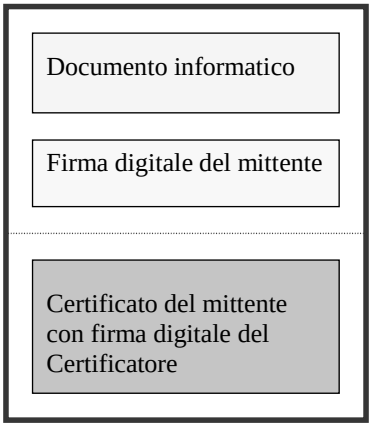
Processo "reale" di certificazione

- Al documento, firmato dal mittente, va allegato il certificato.
- Il destinatario trova direttamente nel certificato la chiave pubblica del mittente.
- Se il destinatario "si fida", procede alla verifica dell'integrità del documento e alla sua lettura.
- Se "non si fida", verifica presso il Certificatore che il certificato non sia incluso nell'elenco di quelli sospesi o revocati.

Schema di uso del certificato



Struttura del messaggio completo



Regole tecniche
(DPCM)

- Decreto previsto dall'art. 3 del DPR relativo a:
  - formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione dei documenti informatici;
  - integrità e riservatezza delle informazioni.
- Pubblicato sulla G.U. del 15/4/99.

Alcuni punti delle regole tecniche

- Algoritmi per la generazione delle chiavi.
- Algoritmi per la generazione dell'impronta.
- Criteri di sicurezza.
- Requisiti dei Certificatori.

Requisiti dei Certificatori

- S.p.A. con capitale non inferiore a quello necessario all'esercizio dell'attività bancaria (6 Ml. Euro).
- Onorabilità dei rappresentanti legali.
- Competenza ed esperienza del personale tecnico.
- Qualità dei processi informatici e dei relativi prodotti.
- Consigliata un'adeguata copertura assicurativa per eventuali danni a terzi.

Profili professionali del personale

a) responsabile della sicurezza;
b) responsabile della generazione e custodia delle chiavi;
c) responsabile della personalizzazione dei dispositivi di firma;
d) responsabile della generazione dei certificati;
e) responsabile della gestione del registro dei certificati;
f) responsabile della registrazione degli utenti;
g) responsabile della sicurezza dei dati;
h) responsabile della crittografia;
i) responsabile dei servizi tecnici;
j) responsabile dell'auditing.

Ruolo dell'AIPA

- Autorità per l'Informatica nella Pubblica Amministrazione.
- Esamina, approva o respinge le domande per esercitare l'attività di Certificatore.
- Tiene l'elenco dei Certificatori.
- E' di fatto responsabile delle regole tecniche.

Elenco Certificatori

- SIA
- SSB
- Finital
- Infocamere
- BNL Multiservizi
- Saritel
- Postecom
- Seceti
- Intesa
- C.T. RUPA
- Enel (in corso)
- Trust Italia (in corso)

Assocertificatori

Modus operandi

- Registrazione
- Attivazione del servizio
- Certificazione

Registrazione dell'Utente

- Operazione periferica
- Responsabilità del Certificatore
- Attribuzione di un codice
- Consegna all'Utente di:
  - dischetto con programma per PC
  - lettore di smart card
  - smart card "vergine" (*dispositivo di firma*) contenuta in busta numerata

Attivazione

- L'Utente installa sul proprio PC il lettore di smart card e il programma ricevuti
- Si collega al Certificatore
- Inserisce il proprio codice
- Inserisce dispositivo di firma "vergine"
- Viene generata all'interno del dispositivo una coppia di chiavi
- La chiave privata resta all'interno del dispositivo
- La chiave pubblica viene inviata al Certificatore
- Il Certificatore genera il certificato e lo invia all'Utente

Gestione

- La firma viene gestita dal programma ricevuto dall'Utente.
- La codifica dell'impronta viene effettuata all'interno del dispositivo di firma: la chiave privata non esce mai.
- Il Certificatore tiene disponibile in linea l'elenco dei certificati, in particolare tiene tempestivamente aggiornato l'elenco di quelli revocati o sospesi.
- Informa tempestivamente l'Utente delle prossime scadenze.

Alternative

Non si applica il DPR:

- se si rinuncia al valore legale della firma digitale

oppure

- se si opera su reti dedicate.

In questi casi si può utilizzare qualunque sistema di firma.

Sistema PGP

- Pretty Good Privacy
  (Philip Zimmerman)
- Tecnologia tipo RSA, molto utilizzata nella posta elettronica.
- Nata per polemica contro restrizioni USA.
- Non ci sono Certificatori.
- Chi attiva una comunicazione manda all'altro anche la propria chiave pubblica.
- Ogni utente mantiene un "portachiavi" personale.

La Direttiva europea

- Pubblicata il 19 gennaio 2000.
- 28 “considerando” e 14 articoli.
- L’impostazione concettuale è diversa da quella italiana.
- L’enfasi non è sulla P.A. ma sul commercio elettronico.
- Criteri di liberalizzazione.

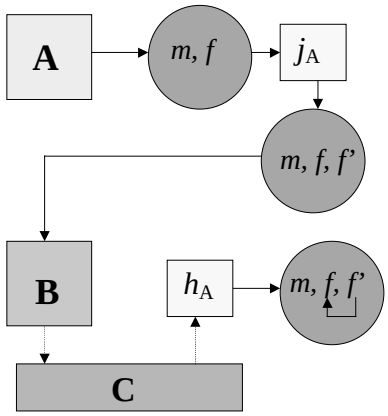
Nuovi concetti

- Firma elettronica
- Dispositivo sicuro.
- Certificatore qualificato.
- Comitato tecnico.
- Comportamenti uniformi all’interno dell’U.E.

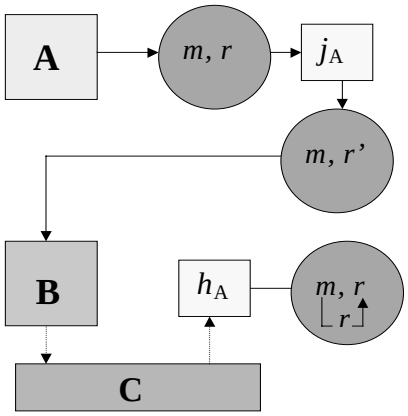
Firma elettronica

- **Firma elettronica** invece di **firma digitale**: nessun riferimento a specifiche tecnologie.
- Distinzione tra “firma elettronica” e “firma elettronica avanzata”.
- “Firma elettronica” garantisce la provenienza (*firma debole*).
- “Firma elettronica avanzata” garantisce anche il contenuto (*firma forte*).

Firma debole



Firma forte



Tipi di firma

- **Firma digitalizzata**:
  ⇒ immagine digitale della firma autografa.
- **Firma digitale**:
  ⇒ impronta di un testo codificata con la chiave privata del mittente.
- **Firma elettronica**:
  ⇒ concetto astratto, di tipo generale: garantisce la provenienza.
- **Firma elettronica avanzata**:
  ⇒ assomiglia ma non coincide con la "nostra" firma digitale
- **Firma elettronica avanzata realizzata con un dispositivo per la creazione di una firma sicura e certificata da un certificatore qualificato:**
  ⇒sinonimo di firma digitale.

Direttiva: punti chiave

- L’attività di certificazione è libera: non occorrono né autorizzazioni né qualificazioni.
- I certificatori possono anche essere dei singoli privati.
- Servizi di certificazione.
- Forme di controllo previste solo quando è coinvolta la P.A.

La direttiva europea e le norme italiane

- Direttiva europea andrà recepita.
- Elenco dei Certificatori solo per la P.A.
- Firma elettronica avanzata obbligatoria per la P.A.; resta valido il DPR.
- Valore legale della firma elettronica “non avanzata”?

Effetti giuridici

- Articolo 5, comma 2

  “Gli Stati membri provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è in forma elettronica, … o non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato ....”

Applicazioni

- Sicurezza delle transazioni nei sistemi di codifica simmetrici e asimmetrici.
- Sistemi a doppia codifica.
- Commercio elettronico.
- Atti notarili.
- Fisco telematico
- Processo telematico
- Problemi aperti.

Sistemi di codifica

- **Sistemi simmetrici**
  - una sola chiave
  - codifica semplice
  - possibilità di intercettazione
- **Sistemi asimmetrici**
  - due chiavi
  - codifica complessa
  - sicurezza elevatissima

Standard

- **Sistemi simmetrici**
  - DES (Data Encryption System)
  - Metodo di traslazione e sostituzione
  - Chiave di 64 bit (utilizzati 56)
- **Sistemi asimmetrici**
  - RSA (Rivest, Shamir, Adleman)
  - Teorema di Fermat-Eulero
  - Chiavi di 128 - 2048 bit

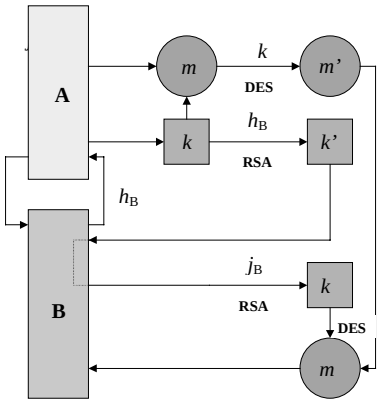
Sicurezza delle transazioni

- I **sistemi a due chiavi** offrono le maggiori garanzie, ma richiedono elaborazioni complesse: è difficile applicarli se il messaggio è lungo.
- I **sistemi a una chiave** offrono minori garanzie, ma richiedono elaborazioni semplici: la lunghezza del messaggio è in pratica ininfluente.
- L'utilizzo combinato di entrambi i sistemi ("**doppia codifica**") offre il massimo della sicurezza insieme a una relativa semplicità di elaborazione, qualunque sia la lunghezza del messaggio.

Sistemi a doppia codifica

- A deve inviare a B un messaggio *m*, non breve, che descrive una "transazione".
- A sceglie a caso una chiave *k*, di 64 bit.
- A codifica (con il DES) *m* mediante la chiave $k \Rightarrow m'$.
- A codifica *k* con $h_B \Rightarrow k'$
- A invia a B *m'* e *k'*
- B decodifica *k'* con $j_B \Rightarrow k$
- B decodifica (con il DES) *m'* con $k \Rightarrow m$

Schema della doppia codifica



e-commerce

- A: acquirente, con accesso a Internet.
- B: venditore, con catalogo elettronico in Internet.
- A consulta il catalogo di B, sceglie la merce da acquistare e attiva la transazione.
- B fornisce ad A la propria chiave pubblica.
- Il PC di A automaticamente:
  - prepara l'ordine elettronico *m*;
  - genera una chiave *k* con cui codifica $m \Rightarrow m'$;
  - codifica *k* con la chiave pubblica di B $\Rightarrow k'$;
  - invia *m'* e *k'* a B.
- Il computer di B automaticamente:
  - decodifica *k'* con la chiave privata di B;
  - con *k* decodifica *m'* e ottiene l'ordine.
- B spedisce la merce.

problema del pagamento

Pagamento con carta di credito (schema teorico)

- CC indichi la Società della Carta di credito.
- A consulta il catalogo di B, sceglie la merce da acquistare, fornisce i dati della propria Carta di credito e attiva la transazione.
- Il PC di A compie automaticamente due operazioni:
  - prepara l'ordine elettronico senza i dati della Carta di credito [la codifica è opzionale] e lo invia a B;
  - prepara la nota di debito con i dati della Carta di credito e con riferimento a B; codifica questa nota con un sistema di doppia codifica e la invia a CC.
- CC decodifica la nota di debito, effettua i controlli rituali, contabilizza l'addebito su A e l'accredito su B, comunica a B il buon fine contabile dell'operazione.
- B riceve il messaggio da CC ed evade l'ordine.
- Sistema sicuro ma informaticamente complesso (2 collegamenti indipendenti).

Pagamento con carta di credito (schema reale 1)

Protocollo SSL

Secure Socket Layer

- Sviluppato da Netscape e utilizzato anche da Microsoft.
- *m* contiene sia i codici della merce sia le coordinate della carta di credito.
- *m* viene cifrato da A con un sistema a doppia codifica.
- L'inoltro delle coordinate della carta di credito a CC è a cura del venditore B.

Osservazioni sulla sicurezza

Pro

- *k* viene generata presso il mittente A, cambia ad ogni transazione e non esce dal PC di A.
- A è sicuro di ordinare merce da un fornitore B affidabile, la cui garanzia è fornita indirettamente da CC.
- B è sicuro di ricevere tramite CC il corrispettivo della merce spedita.

Contro

- B viene a conoscere le coordinate della carta di credito di A: la sicurezza del sistema pertanto è anche in funzione dell'etica di B, non valutabile a priori.

Pagamento con carta di credito (schema reale 2)

Protocollo SET

Secure Electronic Transaction

- Sviluppato su iniziativa di Visa e Mastercard (CC).
- Le coordinate della carta di credito sono prima codificate con la chiave pubblica di CC poi affiancate ai codici della merce: il tutto forma il messaggio *m*, che viene codificato con h_B .
- B al ricevimento di *m'* estrae le coordinate della carta di credito - che sono cifrate - e le invia a CC.
- CC le decodifica e autorizza B a spedire la merce.

Osservazioni sulla sicurezza

Pro

- A è sicuro di ordinare merce da un fornitore B affidabile, la cui garanzia è fornita indirettamente da CC.
- B è sicuro di ricevere il corrispettivo della merce spedita.
- B non viene a conoscere le coordinate della carta di credito di A: la sicurezza del sistema pertanto dipende solo dell'etica di CC, che si presume altissima.

Contro

- Sistema nuovo, molto complesso, in corso di diffusione.

Aspetti innovativi dell'e-commerce

- Mercato vasto quanto il mondo.
- Spese di marketing centralizzate sul sito Internet.
- Spese di distribuzione centralizzate sulla spedizione: efficienza del sistema di consegna.
- Fiducia nel processo.
- Banche come "garanti".

Tipi di e-commerce

- Business to Business
  - aziende comprano tra loro
  - ricerca di prodotti via Internet
  - pubblicità: sito Internet efficace
  - inviti a gare
  - effettuazione di gare
- Business to Customer
  - acquisti al dettaglio
  - pubblicità: occorre arrivare al sito ⇒ banner e/o pubblicità tradizionale verso il sito

Atti notarili

- **Notartel**: rete informatica che collega i 5 mila studi notarili italiani.
- Rete privata che offre particolari garanzie.
- Collegamento con altre Reti:
  - Catasto
  - Conservatorie
  - Cancellerie
  - Camere di Commercio
- Ricevimento e trasmissione di atti per via telematica, sottoscritti con firma digitale.

Fisco telematico

- Soggetti abilitati a inviare dichiarazioni per via telematica.
- Requisiti di ogni soggetto (A):
  - PC con modem;
  - abilitazione Ministeriale;
  - programmi per la gestione delle procedure.
- Ministero assegna le chiavi e svolge la funzione di Certificatore.
- Più dichiarazioni $\Rightarrow$ file.
- File + impronta codificata con $h_A \Rightarrow$ Ministero per via telematica.
- Ministero decodifica con j_A, verifica e rilascia ricevuta elettronica.

Processo telematico

- G.U. 17/4/2001: “Uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo innanzi alla Corte dei Conti”
- Applicazione integrale della norma sull Firma digitale
- Definizione “errata” di Documento informatico

Problemi aperti

- Pluralità di chiavi e di dispositivi di firma.
- Coesistenza di più standard.
- Interoperabilità fra Certificatori
- Area privata e area pubblica.
- P.A. centrale e periferica.
- Coesistenza e compatibilità con la carta di identità elettronica.
- Garanzia di quello che si firma.

Documentazione

www.interlex.it