Francesco Gennai

La firma digitale *

Introduzione

Internet, oltre ad un potente mezzo di comunicazione, rappresenta oggi una preziosa fonte di informazioni in continua evoluzione, e, per questo, è ormai diventato uno strumento di studio e di lavoro indispensabile. D'altra parte bisogna considerare che Internet comporta rischi di sicurezza per i sistemi connessi e per i dati che viaggiano nella rete.

L'utilizzo della rete Internet nell'ambito delle attività di Document Delivery svolte dalle biblioteche, ha portato notevoli benefici: la diminuizione dei tempi di evasione delle richieste, il miglioramento della qualità del servizio, e al tempo stesso la diminuzione dei costi di trasmissione, rispetto all'utilizzo di strumenti classici come il fax e la posta di superficie [1].

E' importante notare che:

- La rete internet agevola la trasmissione di documenti in forma elettronica.
- La rete internet è un mezzo di comunicazione non sicuro.

Data la natura delicata delle operazioni di fornitura elettronica che spesso coinvolgono documenti soggetti a copyright un aspetto fondamentale è legato alla certificazione delle transazioni elettroniche in termini di:

- certificazione dei corrispondenti (mittente, destinatario);
- certificazione della azione (trasmissione);
- garanzia della correttezza dei dati trasmessi (che non siano stati modificati durante il transito);
- confidenzialità dei dati (solo il destinatario deve avere accesso al contenuto).

Le tecnologie di firma elettronica e di cifratura possono essere applicate a tutte quelle operazioni di trattamento dei dati per le quali sono richieste una o più delle suddette garanzie. Per esempio, utilizzando in modo opportuno la firma digitale è possibile identificare con certezza i soggetti che effettuano l'operazione di richiesta di un articolo. Mi preme far notare come in questo caso il soggetto dell'azione, identificato dalla firma

digitale, sia una persona fisica e non un nodo di rete o un indirizzo di posta elettronica. Vedremo più avanti come possa avvenire l'identificazione (o certificazione) del soggetto che opera mediante la firma digitale.

1.1 Crittografia

Con il termine crittografia vengono indicati algoritmi e funzioni matematiche per la cifratura di dati. La cifratura assicura la confidenzialità del messaggio: il suo contenuto sarà accessibile solo al destinatario finale e perciò se intercettato durante il transito non sarà fruibile (a meno di compromissione delle chiavi o degli algoritmi crittografici). Nell'ambito delle tecnologie di sicurezza possiamo individuare tre componenti fondamentali, che analizzeremo nel seguito:

- Cifratura
- Firma digitale
- Certification Authority

Gli algoritmi di crittografia si dividono in due grandi classi:

1. **A chiave privata o simmetrici**, caratterizzati da due proprietà:

- La chiave usata per la cifratura e la decifratura è la **stessa**.
- La chiave è rigorosamente **segreta**.

Questi algoritmi sono efficienti dal punto di vista computazionale, ma richiedono che ogni utente condivida una chiave segreta con ogni suo interlocutore, e al crescere del numero di utenti diventano problematici la gestione delle chiavi ed il loro trasferimento.

Lo scambio della chiave segreta tra due interlocutori dovrebbe avvenire in modo estremamente sicuro.

2. **A chiave pubblica o asimmetrici**, caratterizzati dalle seguenti proprietà:

- Esistono due chiavi, **equivalenti** ai fini della cifratura, ma **diverse**.
- Quello che una delle due chiavi cifra, l'altra decifra.
- Delle due chiavi una è **segreta** e l'altra è **pubblica**.

Ogni utente ha una coppia di chiavi, quella segreta deve essere custodita con attenzione, l'altra viene distribuita ai propri interlocutori e talvolta è pubblicata su qualche server perchè sia più facilmente reperibile.

Nel caso degli algoritmi a chiave pubblica (asimmetrici) i problemi di reperimento della chiave di un potenziale interlocutore sono ridotti al minimo ed il suo trasferimento non richiede particolari accorgimenti di sicurezza, essendo la stessa di pubblico dominio.

Nel seguito analizzeremo gli algoritmi a chiave pubblica, perchè sono quelli su cui principalmente si basano gli attuali standard di firma digitale.

Prima di descrivere i "meccanismi" con cui si applica la "firma digitale" credo sia importante far notare come gli stessi siano applicabili ad una qualsiasi rappresentazione digitale di un dato; tra questi, la più significativa, è il "file".

Un file può contenere un semplice testo, un documento WORD, un documento PDF, un'immagine GIF, un eseguibile, ma, ancor più, può contenere un intero messaggio di posta elettronica, composto, per esempio, da una parte di testo descrittiva del suo contenuto, e da uno o più allegati (attachment) di vario formato: qualsiasi sia il tipo ed il contenuto del file, esso non è altro che una banale sequenza di bit a cui è possibile applicare in modo semplice la crittografia.

In virtù di questa semplicità applicativa, alcuni degli strumenti che normalmente utilizziamo per l'accesso ai servizi Internet, sono, già da tempo, in grado di effettuare operazioni crittografiche secondo gli standard più diffusi. Tra questi strumenti vi sono la maggioranza dei client di posta elettronica e dei web browser.

Negli esempi che seguono faremo riferimento allo scambio di messaggi di posta elettronica tra due interlocutori. Potete quindi immaginare che i messaggi di posta elettronica, oggetto dell'esempio, contengano una parte testo che descrive il contenuto e uno o più attachment di documenti WORD, PDF, etc.

1.2 Cifratura con chiave pubblica (o asimmetrica)

L'applicazione di un algoritmo di cifratura ad un messaggio offre le seguenti garanzie:

- **riservatezza** o confidenzialità del suo contenuto (analogamente alla busta in un sistema postale convenzionale);
- **integrità** del contenuto trasmesso, cioè la garanzia che il messaggio non sia stato modificato da terzi oppure a causa di errori nella trasmissione in rete;

La figura 1 illustra il procedimento di cifratura dei dati con algoritmo a chiave pubblica o asimmetrica. Il mittente che vuole proteggere il messaggio "blah, blah ...blah... blah..." in modo che possa essere leggibile esclusivamente dal destinatario, utilizza la **chiave pubblica del destinatario** per applicare l'algoritmo di cifratura (operazione attivabile, in modo semplice, sul client di posta elettronica). Il messaggio attraversa Internet e giunge nella casella di destinazione. **Solo il destinatario** che possiede la chiave privata **è in grado di decifrare il messaggio** (operazione attivabile, in modo semplice, sul client di posta elettronica).

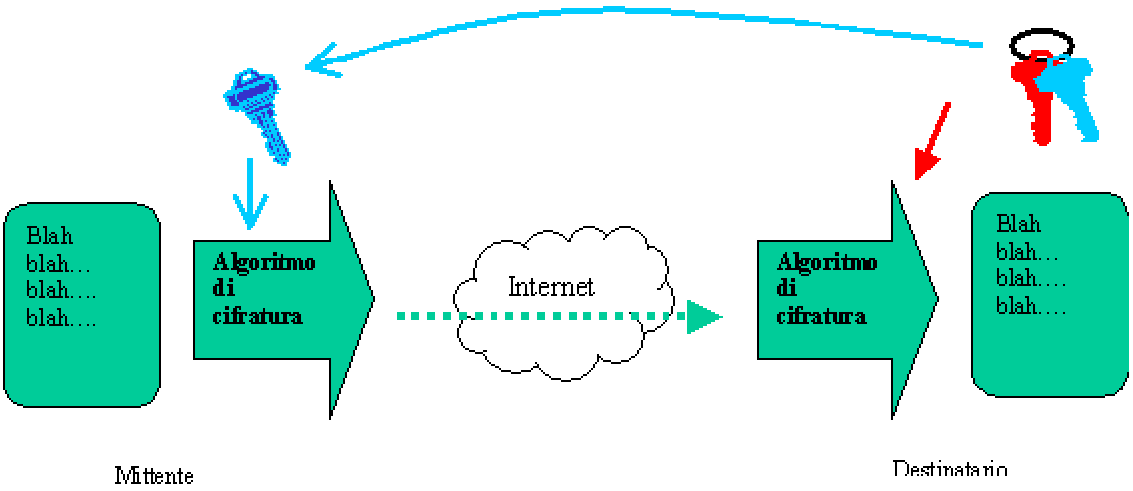

Fig. 1 - Cifratura con chiavi asimmetrica

1.3 Firma digitale

La firma digitale viene generata e associata ad un messaggio dal mittente (per esempio, tramite il proprio client di posta elettronica), la verifica della firma è operata dal destinatario (per esempio, tramite il proprio client di posta elettronica). La firma digitale introduce alcune garanzie fondamentali:

- l'**integrità** del contenuto del documento trasmesso, cioè la garanzia che esso non sia stato modificato da terzi oppure a causa di errori nella trasmissione in rete;
- la effettiva provenienza da colui che si dichiara mittente cioè l'**autenticazione** di chi invia;
- il **non ripudio**: chi trasmette non può negare di avere spedito il messaggio.

L'applicazione della firma digitale comprende i seguenti passi:

- al messaggio viene applicato un algoritmo di hash, cioè una funzione matematica che trasforma il messaggio in una sua rappresentazione univoca composta da un numero fisso e piccolo di bit, detto digest o sommario (è simile ad un impronta digitale), come mostrato in figura 2;
- il digest viene cifrato con la chiave privata del mittente (Fig. 3). Il risultato di questa operazione è una sequenza di bit che rappresenta la firma digitale del messaggio.
- il messaggio originale e la relativa firma digitale vengono inclusi nel messaggio inviato alla casella del destinatario.

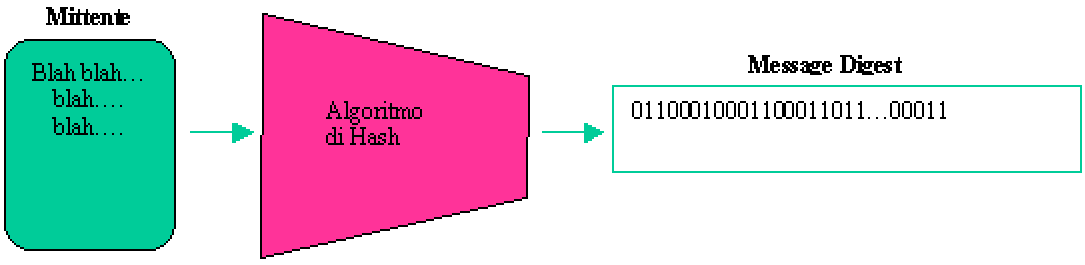

Fig. 2 - Algoritmo di hash

La verifica della firma digitale avviene da parte del destinatario che:

- applica al messaggio ricevuto la stessa funzione di hash che aveva applicato il mittente ottenendo il digest del messaggio;
- prende la chiave pubblica del mittente e la utilizza per decifrare la firma digitale ottenendo il digest del messaggio;
- confronta i due digest. Se sono uguali la verifica è andata a buon fine e questo conferma due importanti condizioni:

1. la firma è stata generata con la chiave privata corrispondente alla chiave pubblica utilizzata al precedente punto 2 (posso quindi identificare il firmatario, possessore della chiave privata);
2. il messaggio ricevuto non ha subito alcuna variazione durante il transito in Internet. (Nel caso di una sua variazione (anche minima) la funzione di hash applicata al punto 1 avrebbe prodotto un diverso digest).

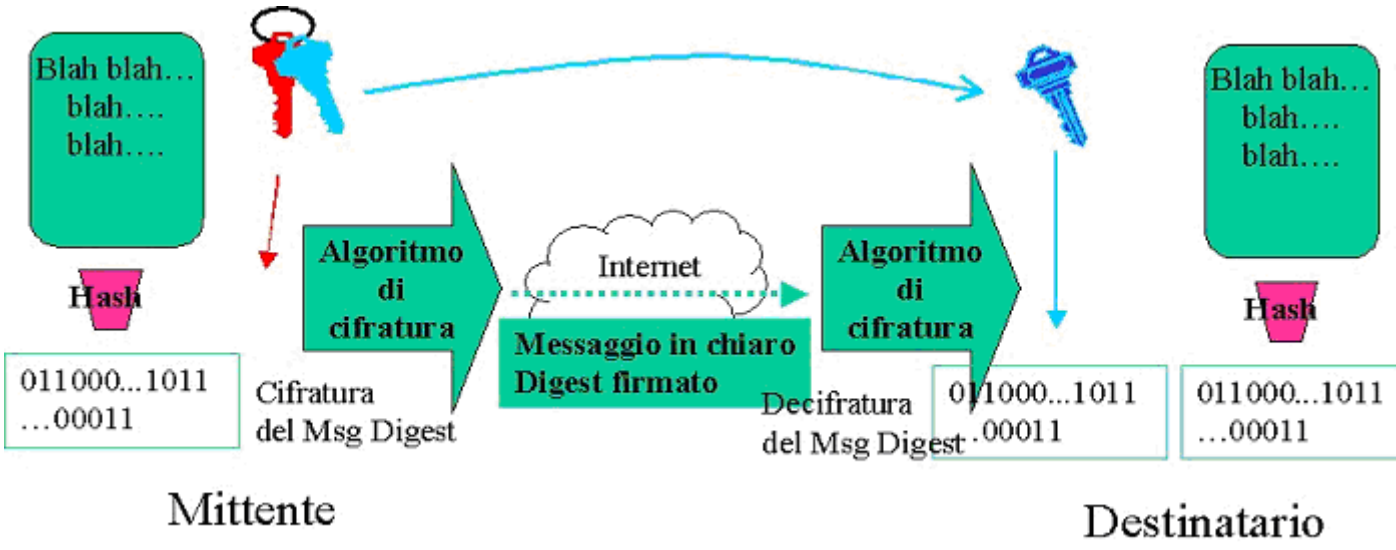

Fig. 3 - Firma digitale

Alcuni aspetti che mi sembra importante notare sono:

La validità di una firma digitale (verifica) viene stabilita solo ed esclusivamente attraverso l'applicazione degli algoritmi di crittografia. In assenza di ciò non esiste alcuna possibilità di stabilire con certezza il soggetto che ha prodotto un determinato documento in formato elettronico. Ad esempio il sistema di posta elettronica non garantisce in alcun modo che il messaggio che abbiamo ricevuto sia stato scritto ed inviato dall'indirizzo che appare nel mittente (campo from).

Il messaggio, composto da una parte testo ed uno o più attachment (word, pdf, gif, tiff, ...), non viene trasformato dall'operazione di firma. Sarà quindi perfettamente leggibile da destinatari, anche non dotati di strumenti per la firma digitale. Ovviamente tali destinatari non saranno in grado di effettuare la "verifica" della firma. E' quindi possibile introdurre l'utilizzo della firma digitale mantenendo la totale compatibilità verso chi ancora non la avesse adottata.

La chiave privata (di fatto una sequenza di bit) può essere memorizzata su un dischetto o, meglio ancora, una smart card di proprietà esclusiva del soggetto identificato. L'accesso alla chiave privata è protetto da password.

1.4 Certification Authority

Dalle precedenti descrizioni si può notare come l'applicazione della firma digitale allo scambio di documenti in rete tra due interlocutori, comporti il possesso della chiave pubblica da parte di un interlocutore, corrispondente a quella privata dell'altro. La chiave pubblica di un soggetto può essere trasmessa all'interessato via e-mail, o trasferita tramite un dischetto o talvolta, scaricata da server Internet.

Qualsiasi sia il meccanismo con cui si viene in possesso di una chiave pubblica, occorre disporre di strumenti che assicurino che essa sia effettivamente quella associata alla chiave privata posseduta dal nostro interlocutore.

Un azione di falsificazione potrebbe infatti generare una coppia di chiavi "false" distribuendo la pubblica a nome di un determinato soggetto. Ogni operazione di firma effettuata con la chiave privata falsa risulterebbe così verificabile con successo con la corrispondente chiave pubblica (falsa) e quindi erroneamente attribuibile al soggetto.

Vi sono almeno un paio di soluzioni a questo problema.

La prima, consiste nello scambio diretto delle chiavi pubbliche tra i potenziali interlocutori. Tale scambio normalmente avviene mediante un incontro tra gli interessati. Ovviamente questa soluzione non è facilmente applicabile a larghe comunità di utenti che potrebbero trovare difficoltà nell'organizzare incontri personali.

La seconda soluzione introduce una terza entità con il compito di "certificare" che una determinata chiave pubblica sia effettivamente quella corrispondente alla chiave privata di un determinato soggetto, indentificato con meccanismi ritenuti sufficienti alla scopo

(esempio: identificazione della persona e della relativa chiave pubblica presso uno sportello di certificazione, etc..).

Questa terza entità prende il nome di "Certification Authority".

La Certification Authority è una organizzazione che garantisce l'appartenenza di una chiave pubblica ad un determinato soggetto, mediante l'emissione di certificati.

Ciascun utente non avrà più bisogno di incontrare il proprio interlocutore per ottenere la rispettiva chiave pubblica, ma potrà ottenerla direttamente dalla Certification Authority di cui entrambi gli interlocutori si fidano.

I dati identificativi di un utente e la rispettiva chiave pubblica (una sequenza di bit) sono memorizzati, in formato standard, in file chiamati "certificati".

Tali certificati, vengono firmati con la chiave privata della Certification Authority ed eventualmente resi pubblici attraverso server.

Gli applicativi (client di posta elettronica, web browser, invio documenti, etc.) possono così estrarre i dati di un soggetto e la relativa chiave pubblica da un certificato la cui validità è garantita dalla firma digitale della Certification Authority.

Tra le regole e i compiti della Certification Authority vi sono:

- stabilire e rendere nota la politica di sicurezza con la quale identifica le persone e gestisce le rispettive chiavi pubbliche, cioè norme, procedure amministrative e tecniche mediante le quali genera un certificato;
- gestire il database dei certificati;
- gestire la Certificate Revocation List (CRL), cioè la lista dei certificati revocati e pertanto non più validi.

2. Scenari per il document delivery elettronico

L'applicazione della firma digitale a tutte quelle operazioni che possono essere svolte mediante i sistemi informatici impone delle considerazioni di carattere normativo-legale che non sono oggetto del presente articolo. Si rimanda perciò alla bibliografia presente nel sito del Ministro per l'Innovazione e le Tecnologie [2].

Giusto per fare un esempio, il riconoscimento della validità da parte di un soggetto (pubblica amministrazione o privato) di un nota di addebito spedita via posta elettronica e digitalmente firmata, in alternativa ad un analogo documento spedito via fax e firmato manualmente, è argomento di tipo prettamente normativo-legale.

Diverse sono però le operazioni che possono essere integrate dall'utilizzo della firma digitale.

Nello svolgimento delle attività di Document Delivery, la firma digitale potrebbe essere utilizzata per migliorare la sicurezza dei servizi offerti via Internet come per esempio la certificazione di un messaggio di posta elettronica richiedente un determinato servizio o la cifratura di un messaggio di posta elettronica che trasporta dati sensibili tra due soggetti (ad esempio, una fattura).

Anche se nella fase iniziale potrebbe non essere applicabile un significato "legale" ad una tale certificazione è fuori dubbio che essa renderebbe il servizio più sicuro e flessibile permettendo di accettare richieste di servizio inviate anche via posta elettronica oltre al tradizionale metodo di richiesta via web con user e password.

Una graduale introduzione sperimentale della firma digitale negli attuali processi di "document delivery elettronico", oltre che rendere gli stessi più sicuri e flessibili e quindi più competitivi, permetterebbe la diffusione di queste tecnologie e conoscenze tra gli operatori del settore.

Come ho già fatto notare, la "firma digitale" è compatibile con gli attuali meccanismi di comunicazione via rete e molti degli strumenti che utilizziamo quotidianamente includono funzioni ed opzioni per la "firma digitale".

Tutto questo significa che è relativamente semplice promuoverne l'adozione in forma sperimentale e ridotta a sottoinsiemi di utenti interessati alla sperimentazione, senza creare alcun problema di interoperabilità tra gli utenti o servizi che utilizzano la firma digitale e quelli che non la utilizzano.

Conclusioni

L'introduzione delle tecnologie di crittografia a chiave pubblica e di firma digitale nelle attività di Document Delivery delle biblioteche consente di certificare le transazioni. Gli utenti inoltre diventono familiari con queste tecnologie che hanno un campo di applicazione più vasto e generale.

Il sistema bibliotecario nazionale potrebbe dotarsi di una propria Certification Authority, finalizzata alla certificazione dei processi di document delivery elettronico tra biblioteche. E' possibile creare l'ambiente crittografico necessario all'utilizzo della tecnologia di firma digitale utilizzando SW di pubblico dominio come quello sviluppato dai Laboratori OpenSSL [3] e dalla organizzazione OpenCA [4].

Francesco Gennai, ISTI - CNR Pisa, e-mail: Francesco.Gennai@isti.cnr.it

Bibliografia e note

* Questo articolo riprende il testo della relazione tenuta in occasione del II Workshop "Document Delivery via Internet e cooperazione inter-bibliotecaria", Bologna, 28 maggio 2003.

[1] Evaluation of an Internet document delivery service. S. Mangiaracina, P. Salamone, M. Buzzi, F. Gennai, L. Abba. 7th Interlending and Document Supply Conference, Ljubljana, 1-5 October 2001, pp. 121-133.

[2] Atti normativi e documenti relativi alla Firma Elettronica. Ministro per l'innovazione e le Tecnologie. <http://www.innovazione.gov.it/ita/intervento/normativa/normativa_firmadigitale.shtml>.

[3] OpenSSL, <http://www.ssl.org/>.

[4] OpenCA, Research and development Labs, <http://www.openca.org/>.