

## NOTE SULLA FIRMA DIGITALE

a cura di  
*Palmino Sacco*

La **firma digitale** è un'informazione che viene aggiunta ad un documento informatico al fine di garantirne integrità e provenienza. Sebbene l'uso per la sottoscrizione dei documenti formati su supporti informatici sia quello più naturale, la firma digitale può essere utilizzata per autenticare una qualunque sequenza di simboli binari, indipendentemente dal loro significato. Un esempio sempre più comune di questo uso generalizzato è l'aggiunta di firme digitali ai file contenuti nella memoria di massa di un sistema di elaborazione onde contrastare gli attacchi dei virus e degli hackers. La principale differenza tra firma autografa e firma digitale sta nel fatto che la prima è direttamente riconducibile all'identità di colui che la appone, poiché la calligrafia è un elemento identificativo della persona, mentre la seconda non possiede questa proprietà. Per coprire questa deficienza si ricorre all'autorità di certificazione (vedi paragrafo precedente), il cui compito è quello di stabilire, garantire e pubblicare l'associazione tra firma digitale e soggetto che l'ha apposta. Per contro, mentre l'associazione tra il testo di un documento e la firma autografa è ottenuta esclusivamente attraverso il supporto cartaceo, la firma digitale è intrinsecamente legata al testo a cui è apposta, tanto che i due oggetti possono essere fisicamente separati senza che per questo venga meno il legame esistente tra loro. Conseguenza di ciò è l'unicità della firma digitale, nel senso che a testi diversi corrispondono firme diverse e quindi, nonostante la sua perfetta replicabilità, è impossibile trasferirla da un testo ad un altro. I meccanismi di firma digitale poggiano essenzialmente su algoritmi crittografici a chiavi pubbliche, che sono detti anche a chiavi asimmetriche poiché utilizzano chiavi diverse per le operazioni di cifratura e decifratura. Un calcolo statistico ha dimostrato che è 600 milioni di volte più difficile contraffare la firma elettronica rispetto alla tradizionale firma autografa.

### La firma digitale in dettaglio:

Tecnicamente la firma digitale è basata su una funzione di hash non invertibile ed uno schema di cifratura a chiave pubblica. La funzione di hash non invertibile (detta anche valore di controllo o checksum) verifica l'eventuale modifica dei dati durante la trasmissione, accodando al messaggio un valore di controllo ottenuto effettuando alcune operazioni sui dati protetti. Scopo di tale funzione è quello di fornire al destinatario del messaggio un mezzo per individuare le eventuali alterazioni dei dati trasmessi. La funzione hash produce una sorta di impronta digitale del messaggio, di dimensioni molto più piccole del messaggio stesso.

Il processo di firma digitale richiede che l'utente effettui una serie di azioni preliminari, necessarie alla predisposizione delle chiavi utilizzate dal sistema di crittografia su cui il meccanismo di firma si basa; in particolare occorre:

1. la registrazione dell'utente presso una Autorità di Certificazione (AC),
2. la generazione di una coppia di chiavi  $K_s$  e  $K_p$ ,
3. la certificazione della chiave pubblica  $K_p$ ,
4. la registrazione della chiave pubblica  $K_p$ .

Una volta espletate tali operazioni l'utente è in grado di firmare elettronicamente un numero qualunque di documenti, sfruttando la sua chiave segreta  $K_s$ , durante il periodo di validità della certificazione della corrispondente chiave pubblica. Tale periodo può essere interrotto prima del suo naturale termine dalla revoca della certificazione della chiave pubblica, che di norma viene effettuata su richiesta del proprietario nel caso in cui questi ritenga che la segretezza della sua chiave privata sia stata compromessa.

La firma viene apposta mediante una sequenza di tre operazioni:

1. generazione dell'impronta del documento da firmare,
2. generazione della firma mediante cifratura dell'impronta,
3. apposizione della firma al documento.

### Registrazione dell'utente

La registrazione dell'utente presso una autorità di certificazione ha il duplice scopo di rendere questa certa della sua identità ed instaurare con esso un canale di comunicazione sicuro attraverso il quale verranno fatte viaggiare le chiavi pubbliche di cui viene richiesta la certificazione. All'atto della registrazione l'autorità di certificazione attribuisce all'utente un identificatore, di cui viene garantita l'univocità, attraverso il quale sarà possibile a chiunque reperire in modo diretto e sicuro i certificati rilasciati al soggetto corrispondente all'interno dei cataloghi pubblici in cui questi sono registrati.

La registrazione avviene attraverso la seguente procedura:

1. L'utente richiede alla AC la registrazione fornendo la documentazione richiesta da questa per accertare l'identità del richiedente.
2. Verificata la validità della richiesta, la AC attribuisce all'utente un identificatore di cui essa garantisce l'univocità.

3. La AC inserisce l'utente con l'identificatore attribuitogli nei cataloghi di utenti registrati che essa gestisce.
4. La AC fornisce attraverso un canale sicuro la chiave crittografica che l'utente dovrà utilizzare per le richieste di certificazione delle chiavi.

La necessità di utilizzare un canale sicuro asserita al punto 4 nasce dal fatto che, sebbene le richieste di certificazione contengono chiavi pubbliche per le quali non è richiesta una protezione ai fini della riservatezza, la AC deve essere certa che ciascuna richiesta provenga effettivamente dell'utente in essa indicato e non da un altro soggetto che lo sta impersonando. La segretezza della chiave, che di norma è una chiave pubblica e pertanto non dovrebbe essere protetta, viene qui utilizzata come strumento di autenticazione dell'origine.

#### *Generazione della coppia di chiavi*

L'utente, mediante un programma adatto al sistema crittografico adottato, genera una coppia di chiavi da utilizzare una per la generazione della firma, che verrà mantenuta segreta e corrisponde perciò a  $K_s$ , e l'altra, destinata alla verifica, che verrà resa pubblica ed assume perciò il ruolo di  $K_p$ .

#### *Certificazione della chiave pubblica*

La certificazione della chiave pubblica ha lo scopo di assicurare chiunque riceva un documento correttamente firmato circa l'identità del soggetto che ha apposto la firma. L'operazione avviene attraverso tre passi:

1. L'utente invia alla AC la richiesta di certificazione per la chiave  $K_p$  generata nella fase precedente, autenticandola mediante la chiave ricevuta dalla AC durante il processo di registrazione. L'autenticazione può avvenire sia mediante cifratura del messaggio di richiesta, ovvero mediante la sua sottoscrizione digitale. Poiché lo scambio di messaggi implicato nella certificazione è bilaterale, in questa fase si possono utilizzare algoritmi di crittografia simmetrici.
2. La AC genera il certificato e lo sottoscrive per garantirne la provenienza che potrà essere accertata da chiunque utilizzando la chiave pubblica della AC.
3. Il certificato viene inviato al richiedente.

#### *Registrazione della chiave pubblica*

Una volta emesso, il certificato può essere reso disponibile in uno o più cataloghi ai quali può accedere chiunque abbia bisogno di accertare la validità di una sottoscrizione digitale. Questa operazione viene di norma effettuata, almeno per i cataloghi di sua competenza, dalla AC contestualmente all'emissione.

#### *Generazione dell'impronta*

Al testo da firmare viene applicata una funzione di hash appositamente studiata che produce una stringa binaria di lunghezza costante e piccola, normalmente 128 o 160 bit. La funzione di hash assicura l'unicità di tale stringa, nel senso che a due testi diversi non corrisponde la medesima impronta. Sono disponibili diversi algoritmi di generazione, quali, ad esempio, MD2, MD4 [RIVE90] e MD5 [RIVE92], originariamente progettati per operare in combinazione con lo RSA ma utilizzabili con qualsiasi cifrario. Sono disponibili anche algoritmi di hash per i quali è in corso la standardizzazione ufficiale da parte organismi internazionali, ne sono un esempio il RIPEMD a 128 e 160 bit ed il Secure Hash Algorithm (SHA-1) [JTC196]. L'utilità dell'uso dell'impronta è duplice, in primo luogo consente di evitare che per la generazione della firma sia necessario applicare l'algoritmo di cifratura, che è intrinsecamente inefficiente, all'intero testo che può essere molto lungo. Inoltre consente l'autenticazione, da parte di una terza parte fidata, della sottoscrizione di un documento senza che questa venga a conoscenza del suo contenuto. Una tipica situazione in cui si sfruttano tali caratteristiche dell'impronta è la marcatura temporale.

#### *Generazione della firma*

La generazione della firma consiste semplicemente nella cifratura, con la chiave segreta  $K_s$ , dell'impronta digitale generata in precedenza.

#### *Apposizione della firma*

La firma digitale generata al passo precedente viene aggiunta in una posizione predefinita, normalmente alla fine, al testo del documento. Normalmente, insieme con la firma vera e propria, viene allegato al documento anche il valore dell'impronta digitale ed eventualmente anche il certificato da cui è possibile recuperare il valore della chiave pubblica.

#### *Verifica della firma digitale*

L'operazione di verifica della firma digitale viene effettuata ricollocando, con la medesima funzione di hash usata nella fase di sottoscrizione, il valore dell'impronta e controllando che il valore così ottenuto coincida con quello generato per decodifica della firma digitale stessa. La disponibilità del valore dell'impronta all'interno del messaggio semplifica l'operazione.

In linea di principio non sarebbe necessario allegare alla firma digitale il certificato rilasciato dalla AC, poiché il destinatario può comunque reperirlo nei cataloghi, tuttavia la sua presenza semplifica l'operazione di verifica, che può così utilizzare l'identificatore assoluto del certificato stesso, che rende più efficiente l'accesso ai cataloghi, limitando la ricerca alle liste dei certificati revocati e sospesi.

## **Il D. Lgs. n. 10/2002: la firma elettronica “debole” o “forte”**

Il Decreto Legislativo n. 10/2002 ha introdotto in Italia la cosiddetta firma elettronica debole. Questa consiste in ogni mezzo elettronico di identificazione e si affianca alla firma elettronica forte il cui esempio principale è rappresentato dalla firma digitale propriamente detta, che rimane pienamente efficace. Le principali differenze tra le due firme riguardano principalmente il grado di sicurezza relativo alla possibilità di accertare la provenienza e l'autenticità del documento elettronico collegato, altissimo nel caso della firma digitale, e le conseguenze nel campo delle prove processuali.

Questi nuovi aspetti hanno comportato delle inevitabili modifiche di alcuni articoli del T.U. n. 445/2000.

**Efficacia probatoria.**

L'art. 10 del T.U. è stato completamente sostituito dal nuovo D.Lgs. n. 10/2002.

Nel nuovo testo, rimane invariata l'equiparazione tra documento informatico ed atto scritto al fine di soddisfare il requisito della forma scritta richiesto dalle disposizioni del codice civile e delle leggi speciali. La differenza tra firma elettronica 'debole' e firma elettronica avanzata porterà come conseguenza una diversa rilevanza ed efficacia probatoria. Il documento informatico provvisto di firma elettronica "debole", pur essendo considerato dall'ordinamento giuridico come documento scritto, verrà liberamente valutato dal giudice ai fini processuali, mentre, nel caso di documento munito di firma elettronica avanzata, il documento informatico assumerà l'efficacia probatoria della scrittura privata ex art. 2702 del c.c. La scrittura o il contratto informatico farà quindi piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto se colui contro cui la scrittura è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata riconosciuta.

**Riconoscimento della firma digitale**

Appare quindi modificato l'art. 24 del T.U. (ex art.16 del D.P.R. 513/97) il quale, prescrive che si ha per riconosciuta la firma digitale, la cui apposizione sia autenticata da notaio o da altro pubblico ufficiale.

In questo caso il notaio attesta:

- che la firma digitale è stata apposta in sua presenza dal titolare, previamente identificato;
- che il documento sottoscritto risponde alla volontà della parte;
- non è in contrasto con l'ordinamento giuridico;
- attesta la validità della cosiddetta "chiave utilizzata".

Il notaio a sua volta apporrà la firma digitale sostitutiva di sigilli, timbri ed altro di simile.

Il D.Lgs. n. 10/2002 ha stravolto il sistema delle certificazioni che erano affidate a società specializzate incluse in un apposito elenco predisposto e tenuto a cura dell'A.I.P.A., d'intesa con un alto funzionario dello Stato delegato dal Presidente del Consiglio dei Ministri in qualità di Autorità nazionale per la sicurezza.

Un'altra importante applicazione della firma digitale nel garantire l'integrità dei dati è rappresentata dalla **marcatuta temporale**.

Qualora sia necessario attribuire ad un documento certezza circa il momento in cui questo è stato redatto ed è divenuto valido, si ricorre alla sua marcatura temporale. Questa consiste nella generazione da parte di una terza parte fidata, normalmente una Autorità Certificatrice, di una ulteriore firma digitale per il documento marcato.

L'operazione avviene secondo la seguente procedura:

1. L'impronta del documento viene inviata al servizio di marcatura temporale, l'impronta costituisce un riferimento certo al testo originale ma non ne consente la ricostruzione, pertanto la marcatura può essere effettuata da una terza parte senza compromettere la confidenzialità del testo marcato.
2. Il servizio di marcatura aggiunge all'impronta ricevuta **la data e l'ora**, ottenendo una "impronta marcata".
3. L'impronta marcata viene cifrata con la chiave segreta del servizio, ottenendo la marca temporale da cui è possibile recuperare, mediante la chiave pubblica del servizio, l'impronta del documento e la data e l'ora della sua generazione.
4. La marca temporale viene inviata al richiedente, che la allega al documento.

La marcatura temporale è per certi versi analoga all'autenticazione di un documento e può essere usata per garantire che questo non venga in un secondo tempo sostituito con uno diverso da parte del medesimo soggetto che lo ha emesso.