ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

La firma digitale tra crittografia e diritto

Maurizio Blancuzzi

Introduzione

La disciplina normativa della firma digitale rappresenta con molta probabilità il punto più elevato di intersezione tra il mondo giuridico e quello delle scienze informatiche e matematiche.
Secondo la definizione tratta dal Decreto Presidente Repubblica 28 dicembre 2000 n.445 la "firma digitale é un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare 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 o di un insieme di documenti informatici".
Il legislatore, pertanto, ha impiegato il concetto di chiave nell'accezione propria della scienza crittografica, la cui conoscenza si rivela di fondamentale importanza per approfondire l'argomento trattato.

La crittografia

Tramite la *crittografia* è possibile scambiarsi informazioni confidenziali in formato elettronico in modo sicuro, rendendo quindi difficilmente accessibili tali informazioni a utenti non autorizzati. In particolare, con il processo di *cifratura* il dato in chiaro viene codificato in una sequenza comprensibile solamente al destinatario; mentre dal testo cifrato si può risalire al testo in chiaro tramite il procedimento inverso, vale a dire la *decifratura*. Tali processi fanno uso di chiavi e la procedura di decifratura di un testo può avvenire solo conoscendo la chiave apposita. Senza entrare troppo nel dettaglio si può affermare che la "forza" della moderna crittografia si basa proprio sulla segretezza delle chiavi piuttosto che su quella degli algoritmi. La principale suddivisione può essere fatta tra sistemi *simmetrici* e sistemi *asimmetrici*.
I primi (esempio DES, IDEA, AES ecc.) utilizzano un'**unica chiave** per codificare e decodificare le informazioni. Tali algoritmi sono più veloci e di più facile realizzazione rispetto quelli asimmetrici ma presentano una debolezza intrinseca: sia il mittente che il destinatario devono essere a conoscenza della chiave. Infatti, se per poter scambiare messaggi riservati entrambi gli interlocutori devono essere a conoscenza di un segreto, allora aumenta la probabilità che tale chiave possa essere scoperta (si pensi al problema della distribuzione delle chiavi).
Per superare questo problema sono stati adottati algoritmi che utilizzano una **coppia di chiavi**, legate tra loro in maniera univoca mediante precise relazioni matematiche. In questo caso le chiavi sono dette, una *privata* (segreta) e l'altra *pubblica*: ciò che viene cifrato con una chiave viene decifrato con l'altra. La chiave privata viene mantenuta segreta dal mittente, mentre quella pubblica viene diffusa a terzi. La validità di un sistema di questo tipo consiste nella difficoltà di ricostruire la chiave privata a partire da quella pubblica ("rottura del cifrario", attività che richiede un tempo esponenziale all'aumentare della lunghezza delle chiavi).
Esistono molti algoritmi a chiavi asimmetriche: il primo risale al 1976 con l'algoritmo Diffie-Helman, ma il più diffuso è senza dubbio RSA, svi-

luppato nel 1977, che prende il nome dalle iniziali dei suoi tre ideatori (Rivest, Shamir e Adleman). La normativa italiana, parlando di firme digitali, indica esplicitamente l'algoritmo RSA e la lunghezza delle chiavi deve essere di almeno 1024 bit.

Nel processo di generazione della firma digitale rivestono particolare importanza gli algoritmi di *hash*, che servono per calcolare l'*impronta* di un documento informatico (file), in altre parole per ridurne la dimensione ad un valore ben preciso (esempio 160 bit secondo la legge italiana). Esistono molti algoritmi di hash; quelli ufficialmente identificati per la firma digitale sono SHA-1 (*Secure Hash Algorithm*) e RIPEMD-160. Questi algoritmi sono tali che:

- è impossibile risalire al documento originale partendo dalla sua impronta;
- è (praticamente) impossibile ottenere la stessa impronta partendo da due documenti differenti.

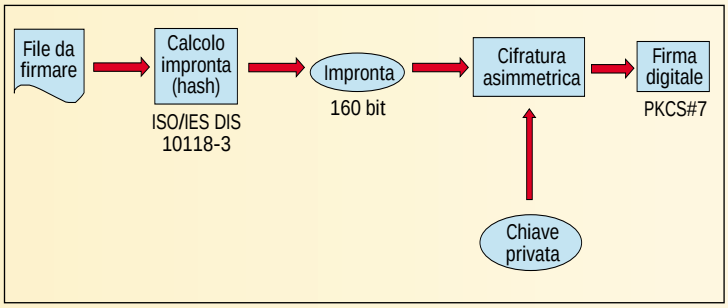

FIGURA 1
Generazione della firma digitale

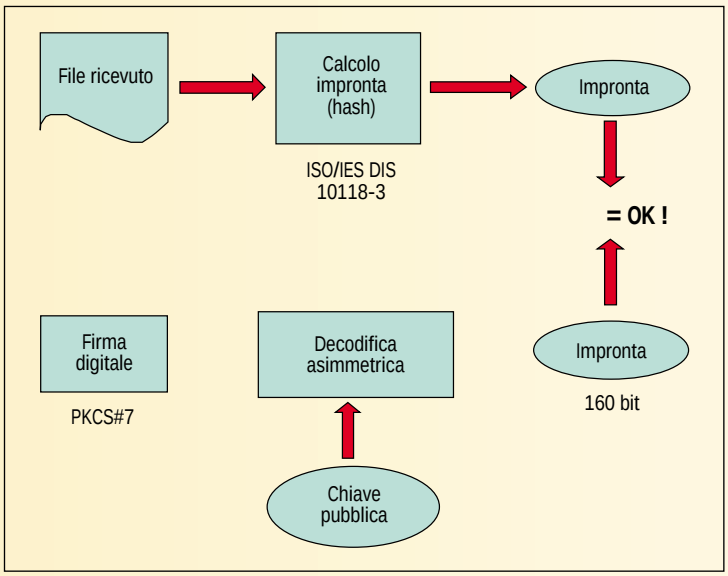

FIGURA 2
Verifica di una firma digitale

Solo l'impronta (e non l'intero documento) viene cifrata utilizzando la chiave privata; questo velocizza molto l'operazione di firma (cifratura) che di per sé è un'operazione complessa e pesante in termini di elaborazione.

Generazione e verifica

Per apporre una firma digitale a un documento informatico (non necessariamente testuale) è, quindi, necessario disporre di una coppia di chiavi digitali asimmetriche: la chiave privata, disponibile solo per il titolare, è utilizzata per sottoscrivere, mentre quella pubblica è invece utilizzata per verificare l'autenticità della firma.

Generazione della firma digitale

1. Dal file originario viene calcolata l'impronta di 160 bit usando un algoritmo di hashing che assicura la corrispondenza univoca tra l'impronta e il file.
2. L'impronta viene cifrata usando la chiave privata. Per fare questo viene utilizzata la smart card, contenente la coppia di chiavi e il certificato digitale, previa digitazione di un P.I.N.; il risultato di tale operazione, generata all'interno della smart card, è la *firma digitale*.
3. Viene quindi costruito un file in formato crittografico standard PKCS#7 costituito da: file originale, impronta cifrata e certificato digitale, con la chiave pubblica, del firmatario (Figura 1).

Verifica della firma digitale

1. L'impronta cifrata viene decifrata tramite la chiave pubblica del firmatario.
2. Viene calcolata nuovamente l'impronta applicando l'algoritmo di hash al file originale.
3. Si confrontano l'impronta estratta dalla firma con quella ricalcolata: se coincidono il messaggio è autentico (Figura 2).

Per l'apposizione o la verifica di una firma digitale vengono utilizzati opportuni programmi software che con semplici interventi dell'utente effettuano tutte le operazioni (hashing, cifratura, decodifica, confronto) in maniera completamente automatica[1].

[1] Sul sito www.cnipa.gov.it sono gratuitamente disponibili vari applicativi software per la generazione/verifica della firma digitale conformi alla circolare n. AIPA/CR/24 del 19 giugno 2000 sull'interoperabilità.

La certificazione

Gli obiettivi da raggiungere con la sottoscrizione digitale sono:
- *integrità*: intesa come la sicurezza che il documento informatico non sia stato modificato dopo la sua sottoscrizione;
- *autenticazione*: la certezza dell'identità del sottoscrittore di un documento;
- *non ripudio*: colui che firma un messaggio non può disconoscerne la paternità.

Tali caratteristiche si possono considerare realizzate solamente se vi è la sicurezza che la chiave pubblica del firmatario sia realmente associata al firmatario stesso. A tal fine è necessaria un'attività di *certificazione* il cui scopo principale è proprio quello di realizzare la corrispondenza biunivoca tra il titolare e la sua coppia di chiavi (pubblica e privata). Tale corrispondenza si realizza previa identificazione diretta del titolare, o indirettamente tramite una *Local Registration Authority* (LRA).
L'attività di certificazione viene svolta da una terza parte fidata, il *Certificatore* che svolge quindi una funzione di *certification authority*. L'attività principale di un Certificatore è l'emissione di certificati digitali che garantiscono l'identità del titolare della coppia di chiavi. Un certificato è quindi l'associazione tra i dati identificativi del titolare e la propria chiave pubblica. Inoltre tale certificato è pubblicamente accessibile e consultabile al fine della verifica dell'identità del firmatario; ogni certificato digitale è a sua volta sottoscritto digitalmente dal Certificatore mediante un'opportuna chiave di "certificazione".
Tra le varie attività "istituzionali" svolte dal Certificatore vi è anche la pubblicazione delle liste di revoca e di sospensione dei certificati (*Certication Revocation List* o CRL e *Certication Suspension List* o CSL).
Le informazioni tipicamente contenute in un certificato in standard ITU X.509 sono:

Versione	esempio V3
Numero di serie	
Algoritmo di firma	esempio sha1With RSAEncryption
Periodo di validità	solitamente da uno a tre anni
Titolare della chiave pubblica	
Valore della chiave pubblica	
Utilizzo del certificato	esempio Nonrepudiation
Impronta del certificato	

La competenza per la tenuta dell'elenco pubblico dei certificatori spetta al Centro Nazionale per l'Informatica nella Pubblica Amministrazione. Tale elenco è reso disponibile telematicamente tramite il sito web www.cnipa.gov.it. e contiene per ogni certificatore abilitato, le seguenti informazioni:
- Ragione o denominazione sociale
- Sede legale
- Rappresentante legale
- Nome X.500
- Indirizzo Internet
- Lista dei certificati delle chiavi di certificazione
- Manuale operativo
- Data di accreditamento volontario
- Data di cessazione e certificatore sostitutivo

Firma digitale e firma autografa

La firma digitale è il risultato di un procedura (cifratura) effettuata su un documento (file) specifico ed è quindi unica e caratteristica per ogni file elaborato. Non è quindi riproducibile ne è possibile apporre una determinata firma digitale ad un documento diverso da quello cui si riferisce.
La firma digitale fornisce un livello di garanzia dell'autenticità del documento anche superiore a quello offerto dalla firma autografa, purché si disponga di strumenti di sottoscrizione sufficientemente sicuri (*crypto-card*) e di un sistema di gestione dei certificati (*Public Key Infrastructure*) efficiente e affidabile. La differenza tra firma autografa e firma digitale è che la prima è legata alla grafia, caratteristica fisica del firmatario, mentre la seconda al possesso di uno strumento informatico (il token di firma) e alla conoscenza di una password.
Inoltre la firma digitale, essendo univocamente connessa al documento sul quale viene calcolata, cambia da un documento all'altro circostanza che ne rende impensabile la falsificazione o l'imitazione come può avvenire per la sottoscrizione vergata di pugno su un foglio di carta.
La firma digitale, infine, non può essere apposta su un documento "in bianco" in quanto l'assenza di un documento comporta l'impossibilità di ricavare l'impronta mediante l'algoritmo di hash (Tabella 1).

Firma autografa	È sempre uguale a sé stessa	Non garantisce l'integrità del testo	Non garantisce l'autenticità	Può essere apposta in bianco
Firma digitale	Varia in relazione al documento	Garantisce l'integrità del testo	Garantisce l'autenticità	Non può essere apposta in bianco

TABELLA 1
Differenze tra firma autografa e digitale

Aspetti giuridici

La firma digitale in Italia è un meccanismo tecnico-normativo in continua evoluzione, sia perché la diffusione delle tecnologie e il conseguente sviluppo della società dell'informazione sono processi inarrestabili, sia per la difficoltà di riconoscere il giusto valore legale ai documenti informatici; la smaterializzazione degli atti giuridici rende necessario predisporre nuove regole del diritto che affianchino quelle tradizionali.
Va riconosciuto al nostro paese il merito di essere stato il primo in Europa ad affrontare questo problema e, a partire dall'art. 15 comma 2 Legge 59/97, ad attribuire ai documenti informatici piena validità e rilevanza a tutti gli effetti di legge.
Il legislatore italiano, peraltro, ha dovuto ben presto fare i conti prima con esigenze di coordinamento che hanno portato all'approvazione del Decreto del Presidente della Repubblica n. 445/2000; poi con l'obbligo di recepimento della direttiva 1999/93/CE che è stata attuata mediante il Decreto Legislativo 23 gennaio 2002, n.10.
Nell'attuale quadro normativo, pertanto, al concetto di firma digitale si è aggiunto quello di firma *elettronica*, suddivisa in varie categorie in relazione al livello di sicurezza richiesto.
Le diverse definizioni ai sensi dell'art. 2 del D.lgs.10/02 sono:

- ***firma elettronica***: *l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autentificazione informatica.*

Di fatto si tratta di una definizione generica (e omnicomprensiva) che identifica dati utilizzati per autenticare altri dati elettronici. Si può definire firma elettronica ogni sistema che può funzionare come chiave per accedere a un dato informatico (per es. una password, un P.I.N., un sistema a chiavi asimmetriche). Informalmente è definita anche come firma "debole" per differenziarla dalla firma digitale.

- ***firma elettronica avanzata***: *la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.*

Come per la firma elettronica "generica" non conta la tecnologia utilizzata, ma è importante che la sottoscrizione avanzata identifichi il firmatario, al quale deve essere ricondotta in maniera univoca; inoltre, deve garantire che l'atto non sia stato modificato.
Ha la stessa validità della firma elettronica generica, ma con il vantaggio che è più sicura: aumenta quindi la possibilità di utilizzarla come prova.

- ***firma elettronica qualificata***: *la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma.*

Si tratta di un ambito ancora più ristretto che richiede un certificato qualificato e deve essere creata mediante un dispositivo sicuro. Le firme elettroniche qualificate costituiscono prova, fino a querela di falso, della volontà del sottoscrittore del documento. È detta anche "firma forte" e corrisponde alla firma digitale con cifratura a doppia chiave asimmetrica, il metodo attualmente più sicuro per trasmettere documenti con la sicurezza dell'integrità, della riservatezza e del non ripudio. Ha quindi lo stesso valore della sottoscrizione tradizionale.
Per poter utilizzare queste differenti tipologie di firme elettroniche serve un nuovo tipo di certificatore: a quelli accreditati si affiancano, quindi, i certificatori di base o notificati. Di conseguenza l'attività che il soggetto certificatore deve compiere viene dimensionata in base al tipo di certificati che intende rilasciare. Queste nuove figure potranno emettere certificati di firma con standard di sicurezza che possono non corrispondere ai criteri fissati dalla legge, come invece dev'essere per i certificatori accreditati. Per questi ultimi i certificati emessi hanno i più elevati requisiti di sicurezza e qualità e su di essi il controllo sarà molto più rigido.

Le firme "forti" possono essere associate a certificati emessi solo da certificatori accreditati, mentre quelle "deboli" da tutti gli altri certificatori.
Il documento sottoscritto con la firma elettronica soddisfa comunque il requisito legale della forma scritta ed è valutabile come prova. In ogni caso non può essergli a priori negata rilevanza giuridica né ammissibilità come mezzo di prova. Quindi il documento sottoscritto elettronicamente è comunque assimilabile a quello cartaceo ed è utilizzabile come prova, seppure dietro valutazione del grado di affidabilità della firma adottata.

Conclusioni

L'interesse per le firme elettroniche appare elevato, come dimostra anche il numero di certificatori accreditati attivi, nonostante gli investimenti economici necessari per esercitare tale attività siano notevoli e non sia previsto un ritorno economico in tempi brevi.
Per quanto riguarda la certificazione, il recepimento delle disposizioni europee porta sì dei vantaggi in un'ottica di liberalizzazione e razionalizzazione, ma introduce anche delle complicazioni e contraddizioni rispetto al precedente sistema che prevedeva solamente certificatori accreditati.
Al di là di problemi tecnici ancora da risolvere e di alcune controverse interpretazioni normative, per poter dare avvio alla "rivoluzione" della firma digitale sembra di fondamentale importanza lo sviluppo dei servizi applicativi che ne sfruttino a pieno la reale natura di sistema abilitante, soprattutto nella gestione in via telematica del rapporto tra il cittadino e la Pubblica Amministrazione (per esempio pratiche e documenti amministrativi *on line*) su cui si basa il concetto di *e-government*.
Proprio in riferimento agli enti pubblici, è stato recentemente approvato un nuovo decreto legislativo intitolato "Codice dell'amministrazione digitale" che, entrando in vigore il 1° gennaio 2006, dovrebbe risolvere le attuali incertezze interpretative sull'efficacia delle firma elettronica e sugli aspetti probatori del documento informatico.

Bibliografia

[1] Cammarata M., Maccarone E.: *La firma digitale sicura*. Giuffrè, 2003.

[2] Finocchiaro G.: *Firma digitale e firme elettroniche*. Giuffrè, 2003.

[3] Rognetta G.: *La firma digitale e il documento informatico*. Ed. Simone, 1999.

[4] Ziccardi G.: *Crittografia e diritto*. Giappichelli, 2003.

[5] IN RETE: *Bollettino informativo del Centro Tecnico*. Presidenza Consiglio dei Ministri.

[6] www.cnipa.gov.it: Centro Nazionale per l'Informatica nella Pubblica Amministrazione.

[7] Il Sole-24 Ore: Guida agli Enti Locali.

[8] Il Sole-24 Ore: Norme e Tributi.

Antonio Piva laureato in Scienze dell'Informazione, Presidente, per il Friuli - Venezia Giulia, dell'ALSI (*Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica*) e direttore responsabile della Rivista di Informatica Giuridica.
Docente a contratto di Informatica giuridica all'Università di Udine.
Consulente sistemi informatici, valutatore di sistemi di qualità ISO9000 e ispettore AICA per ECDL base e advanced.
antonio_piva@libero.it

David D'Agostini avvocato, ha conseguito il master in informatica giuridica e diritto delle nuove tecnologie, fornisce consulenza e assistenza giudiziale e stragiudiziale in materia di *software, privacy* e sicurezza, contratti informatici, *e-commerce*, nomi a dominio, computer crime, firma digitale. Ha rapporti di partnership con società del settore ITC nel Triveneto.
Collabora all'attività di ricerca scientifica dell'Università di Udine e di associazioni culturali.
david.dagostini@adriacom.it

Maurizio Blancuzzi, laureato in Scienze dell'Informazione.
Responsabile settore ICT ed e-government nella PA locale. Membro della commissione informatica giuridica dell'ALSI (*Associazione Nazionale Laureati in Scienze dell'Informazione e Informatica*).
Ha svolto anche attività didattica e di consulenza in materia di ICT ed informatica giuridica.
maublanc@katamail.com