La firma elettronica: aspetti tecnici, legali e opportunità di utilizzo

Silvano Marioni,
CISSP, responsabile CAS Sicurezza Informatica SUPSI

Riccardo Schuhmacher,
avvocato

Prefazione

La firma elettronica non è una firma nel senso classico del termine ma piuttosto il risultato un procedimento matematico, che utilizzando un'opportuna infrastruttura tecnica, permette di garantire da un lato l'autenticità di un documento elettronico e dall'altro l'identità del mittente.

Nonostante la tecnologia sia presente ed utilizzata da numerosi anni, solo recentemente è diventata di attualità anche nel campo giuridico, per il fatto che a determinate condizioni, può essere equiparata alla firma autografa.

Per comprendere il valore legale della firma elettronica è importante esaminare gli aspetti tecnici del suo funzionamento a partire dal suo rapporto con la crittografia, e in particolare con la tecnica della crittografia a chiave pubblica. Questo aspetto verrà affrontato nella prima parte dell'articolo che presenterà in seguito la direttiva europea e la regolamentazione legale svizzera sulla firma elettronica. In conclusione saranno esaminate le opportunità di utilizzo nello studio legale con esempi di applicazioni pratiche già oggi possibili.

La crittografia a chiave pubblica

Un sistema crittografico permette la trasmissione sicura di un messaggio tra due interlocutori che utilizzano una chiave di cifratura comune e segreta. Con questa chiave il mittente cifra il messaggio e può trasmetterlo in modo sicuro al destinatario che, utilizzando la medesima chiave, decifra il testo e lo riottiene leggibile. Condizione fondamentale per la cifratura sicura è che lo scambio e la condivisione di questa chiave deve avvenire solo tra gli interlocutori, senza che terze persone riescano ad intercettarla. Ciò è facilmente realizzabile finché si tratta di comunicare tra due persone ma il problema diventa più complesso quando aumenta il numero degli interlocutori: cresce infatti il rischio che se uno solo degli interlocutori perde il controllo della sua chiave segreta, tutto il sistema risulta compromesso con la perdita di segretezza di tutti i messaggi.

Il problema della distribuzione delle chiavi di cifratura ebbe una soluzione negli anni '70 quando, grazie all'avvento dell'informatica, gli studiosi di crittografia trovarono nuove soluzioni che avrebbero creato una vera e propria rivoluzione.

In quegli anni tre ricercatori del MIT, Ronald Rivest, Adi Shamir e Leonard Adleman intuirono la possibilità di un sistema di crittografia asimmetrico, in cui per cifrare e decifrare venivano utilizzati sistemi di calcolo e chiavi differenti.

L'algoritmo, che si chiamò RSA dalle iniziali dei suoi inventori, fu un cambiamento radicale rispetto agli strumenti di cifratura esistenti, perché non richiedeva più lo scambio di una chiave segreta. Il suo funzionamento è basato su una coppia di chiavi complementari: una chiave, utilizzata per cifrare, che deve essere obbligatoriamente resa pubblica – da qui il nome crittografia a chiave pubblica – e una chiave utilizzata per decifrare, che deve essere mantenuta segreta.

Per la trasmissione sicura di un messaggio al destinatario, il mittente deve ottenere la sua chiave pubblica e utilizzarla per cifrare, con la certezza che il destinatario sarà in grado di decifrarlo con la sua chiave privata.

Il sistema ha rivoluzionato i dogmi della crittografia fino ad allora conosciuta, garantendo una comunicazione riservata dei dati senza nessuno scambio anticipato di chiavi segrete e semplificando la comunicazione con un numero infinito di interlocutori. Tutto questo ha permesso lo sviluppo della rete Internet, dei sistemi di comunicazione sicura e del commercio elettronico; sarebbe stato infatti impensabile utilizzare un sistema di crittografia a chiave simmetrica a causa degli enormi problemi logistici per lo scambio delle chiavi degli attori coinvolti.

La firma digitale

Ma un nuovo vantaggio che questo algoritmo asimmetrico ha rispetto ai tradizionali algoritmi simmetrici è una funzionalità che in precedenza non era neanche possibile immaginare: la possibilità di garantire che il messaggio è stato inviato da una persona definita e, contemporaneamente, che non è stato modificato.

In questo caso le chiavi sono utilizzate in modo inverso; il mittente cifra con la sua chiave privata e invia il documento al destinatario che se riesce a decifrarlo con la chiave pubblica del mittente ha la certezza della provenienza e dell'integrità del messaggio, senza nessuno scambio preventivo di chiavi segrete. Queste sono le caratteristiche tipiche di un documento cartaceo a cui è stata apposta una firma autografa; da qui il nome firma digitale.

In definitiva la firma digitale non è semplicemente una forma elettronica della firma autografa; essa garantisce l'autenticazione del mittente attribuendo il messaggio al firmatario, l'integrità del documento prevenendo ogni modifica al messaggio firmato.

A titolo di precisazione va detto che l'algoritmo RSA si basa sulla matematica dei grandi numeri e richiede una grande potenza di calcolo. Per un documento di una certa dimensione i tempi di cifratura, trascurabili su un supercomputer accademico, possono diventare inaccettabili su un moderno personal computer. Per motivi di semplicità tralasciamo di presentare le soluzioni tecniche a questo problema, e rimandiamo eventuali approfondimenti alle referenze.

Da quanto visto finora si deduce che, sia nel caso della crittografia che della firma digitale, la chiave pubblica è molto importante per l'identificazione della controparte. Nel primo caso essa garantisce l'invio di un messaggio protetto ad una persona definita, nel secondo caso permette di avere la certezza che il messaggio proviene da una persona definita.

La certezza che la chiave pubblica appartenga veramente al titolare, che la dichiara come sua, diventa quindi il cardine di tutto il sistema ed è il requisito fondamentale per evitare che un impostore possa farne un uso fraudolento.

A questo scopo è necessario che qualcuno si assuma il compito tecnico, ed entro certi limiti legale, di certificare che una particolare chiave pubblica appartenga veramente ad un soggetto definito: questo ente è l'autorità di certificazione.

L'autorità di certificazione è un organismo che – analogamente a un notaio – garantisce l'associazione tra un titolare e la sua chiave pubblica, tramite l'emissione di un certificato digitale che contiene queste informazioni.

La validità del certificato digitale è dato dal fatto che l'autorità di certificazione firma in modo digitale il certificato garantendo la sua integrità e si assume quindi la responsabilità della validità dei dati in esso contenuti.

L'autorità di certificazione deve svolgere una serie di compiti quali l'identificazione dei soggetti, la generazione delle chiavi, la loro distribuzione, la messa a disposizione dei Certificati Digitali, il loro rinnovo alla scadenza, l'eventuale revoca in caso di perdita o di furto.

Oggi esistono numerose autorità di certificazione commerciali che, pur non avendo un riconoscimento delle loro funzionalità di firma da parte delle differenti legislazioni nazionali, sono comunque indispensabili per lo svolgimento delle attività di commercio elettronico su Internet, garantendo la cifratura a chiave pubblica e la firma digitale delle transazioni elettroniche.

Aspetti legali della firma elettronica: la direttiva europea

Parallelamente all'evoluzione della tecnica relativa alla firma digitale, durante la seconda metà degli anni novanta è sorta sempre di più l'esigenza di inquadrarla anche dal punto di vista legislativo. È apparso subito evidente che l'efficacia e la validità della soluzioni sarebbero state direttamente proporzionali al livello di interoperabilità dei sistemi nelle diverse realtà giuridiche nazionali. È in questo contesto che ha acquistato un particolare importanza il modello legislativo europeo sulla firma elettronica, con la direttiva 1999/93/CE del 13 dicembre 1999. Questo documento ha definito i concetti base che sono stati poi recepiti nella diverse legislazione dei paesi europei e anche in quella svizzera.

Nei primi esempi di legislazione sull'argomento si parlava di firma digitale ma con il documento dell'Unione Europea compare il termine firma elettronica. Volendo fare una precisazione tecnico-linguistica si deve dire che una firma digitale è un tipo particolare di firma elettronica come avremo modo di vedere in seguito.

La normativa europea liberalizza l'emissione dei certificati introducendo diversi livelli di firma con diversi gradi probatori. Nella direttiva si parla infatti di firma elettronica semplice, firma elettronica avanzata e firma elettronica qualificata.

La firma elettronica semplice riguarda dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di identificazione.

La firma elettronica semplice può includere l'immagine digitalizzata di una firma autografa o un semplice nome (ad esempio Aldo Bianchi) alla fine di un documento elettronico. Non è basata su un certificato e non dà nessuna indicazione sulla provenienza o l'autenticità della firma, limitando notevolmente il suo valore probatorio.

La firma elettronica avanzata è una firma elettronica che deve essere connessa in maniera unica e essere idonea ad identificare il firmatario. Deve essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo e essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica dei dati

La firma digitale, così come ne abbiamo discusso finora, è un tipo di firma elettronica avanzata con un grado di robustezza tecnica che permette di identificare il firmatario e di garantire l'integrità del documento sulla base di un algoritmo matematico a tutt'oggi impossibile da falsificare. La firma elettronica qualificata è una firma elettronica avanzata basata su un certificato qualificato e creata mediante un dispositivo per la creazione di una firma sicura. Nella maggior parte delle legislazioni dei paesi europei viene considerata giuridicamente equivalenti alle firma autografa.

Il certificato qualificato è un certificato digitale conforme ai requisiti dell'allegato I della direttiva 1999/93/CE per quanto riguarda le informazioni che deve riportare.

Per quanto riguarda le modalità di emissione esso deve essere fornito da un prestatore di servizi di certificazione (autorità di certificazione) che soddisfa i requisiti dell'allegato II della medesima direttiva. Vediamo nel dettaglio come queste esigenze sono state recepite nella legislazione svizzera.

La regolamentazione sulla firma elettronica in Svizzera

In Svizzera il Consiglio federale si è occupato dello sviluppo di un'adeguata strategia sin dal 1998. Il 1. maggio 2000 è entrata in vigore la prima normativa "a carattere sperimentale" come si definiva la stessa Ordinanza sui servizi di certificazione elettronica (OSCert) del 12 aprile 2000.

L'Ordinanza aveva per scopo di definire le condizioni per il riconoscimento dei prestatori di servizi di certificazione e, in senso lato, di promuovere la fornitura della firma elettronica e quindi l'utilizzo della stessa. Essa ha dunque creato le prime basi, che sono state concretizzate solo nel settembre 2001, quando il Consiglio federale ha emanato le disposizioni d'esecuzione tecniche che definivano in modo più concreto le condizioni tecniche e organizzative che i prestatori di servizi avrebbero dovuto adempiere per il riconoscimento.

Proprio per favorire la diffusione dell'utilizzo della firma elettronica, e ben comprendendo che la sola istituzione delle autorità di certificazione non era sufficiente a tale scopo, il Consiglio federale ha ben presto creato le basi per il riconoscimento della firma elettronica nei rapporti di diritto privato.

Il 6 luglio 2001 è così stato licenziato il messaggio relativo alla Legge federale sui servizi di certificazione nel campo della firma elettronica, che doveva sostituire l'Ordinanza sperimentale del 1. maggio 2000 e che di fatto ha posto le basi per il quadro normativo che attualmente è in vigore e che ha creato le migliori premesse per il riconoscimento delle autorità di certificazione, per l'utilizzo della firma elettronica nei rapporti di diritto privato e per l'utilizzo della firma elettronica nei rapporti con le autorità.

Per quanto concerne il riconoscimento delle autorità di certificazione, il 1. gennaio 2005 è entrata in vigore la Legge federale sui servizi di certificazione nel campo della firma elettronica (Legge federale sulla firma elettronica, FiEle) del 19 dicembre 2003.

Essa ha sostanzialmente ripreso il contenuto dell'Ordinanza sperimentale sui servizi di certificazione elettronica entrata in vigore il 1. maggio 2000, definendo le condizioni necessarie per essere riconosciuti prestatori di servizi di certificazione (art. 3 e segg. FiEle) la generazione e l'utilizzo di chiavi per la creazione la verifica della firma (art. 6 FiEle) le informazioni che devono essere contenute in un certificato qualificato (art. 7 FiEle) e i doveri delle autorità di certificazione, rispettivamente dell'autorità di vigilanza. La legge federale ha inoltre disciplinato la responsabilità dei prestatori di servizi di certificazione e degli organismi di riconoscimento (art. 16 e 17 FiEle) e ha creato le basi per la modifica di diverse norme di diritto privato.

Dal 1. gennaio 2005 sono dunque stati modificati e inseriti diversi articoli nel Codice delle obbligazioni, fra cui, proprio in tema di responsabilità, l'art. 59a CO che prevede che il titolare di una chiave per la creazione della firma è responsabile verso terzi per l'utilizzo abusivo della stessa, sempre che non renda verosimile di aver adottato le misure di sicurezza necessarie.

È inoltre naturalmente stato introdotto l'art. 14 cpv. 2bis CO che prevede che la firma elettronica qualificata è equiparata alla firma autografa.

Sulla base della Legge federale sulla firma elettronica sono inoltre state adottate norme di e-government, al fine di rendere possibile le comunicazioni elettroniche fra utente e amministrazione in tema di marchi (art. 40 Legge federale sulla protezione dei marchi) design (art. 26a Legge federale sul design) brevetti (art. 65a Legge federale sui brevetti) oltre a norme relative alla tenuta informatizzata del registro di commercio e del registro fondiario e lo scambio di informazioni con le relative auto-

rità (art. 929a CO, risp. art. 942 cpv. 3 e 4, 949a, 970 e 970a CCS).

La Legge federale sulla firma elettronica ha dunque posto in primo luogo le basi affinché venissero nuovamente create autorità di certificazione riconosciute. Infatti, proprio a causa del mancato riconoscimento della firma elettronica sia nei rapporti di diritto privato che nel rapporto con le autorità, il 31 dicembre 2001 l'unica autorità di certificazione svizzera riconosciuta sulla base dell'ordinanza sperimentale del 1. maggio 2000 – Swisskey - aveva dovuto chiudere i battenti.

Con l'entrata in vigore della Legge federale e con il riconoscimento della firma digitale, è rinato un chiaro interesse relativo all'ottenimento del riconoscimento quale prestatore di servizio di certificazione. Oggi vi sono quattro autorità riconosciute: Swisscom Solution AG, QuoVadis Trustlink Schweiz AG, SwissSign AG e l'Ufficio federale dell'informativa e della telecomunicazione.

La Legge federale ha in secondo luogo sicuramente dato un deciso input allo sviluppo delle infrastrutture necessarie per permettere all'utente di comunicare con le autorità in via elettronica.

Questo sviluppo ha portato in pochissimi anni risultati che possono essere definiti eclatanti. Uno di questi concerne i rapporti con il Tribunale federale. Come è noto il 1. gennaio 2007 è entrata in vigore la Legge federale sul Tribunale federale del 17 giugno 2005 (LTF). All'art. 42 cpv. 4 essa definisce esplicitamente che gli atti scritti potranno essere trasmessi al Tribunale federale per via elettronica, a condizione che la parte o il patrocinatore vi apponga una firma elettronica riconosciuta. Allo stesso modo il Tribunale federale potrà notificare la sentenza alle parti per via elettronica (art. 60 cpv. 3 LPT). Il Tribunale federale ha adottato uno specifico regolamento al riguardo (Regolamento del Tribunale federale sulla comunicazione elettronica con le parti e le autorità inferiori (RCETF) del 5 dicembre 2006) in cui ha definito che la trasmissione degli atti deve avvenire attraverso una specifica piattaforma di distribuzione, basata sulla tecnologia IncaMail, sviluppata dalla Posta svizzera. Si tratta di una piattaforma informatica, denominata juslink (www.juslink.ch) da utilizzare in combinazione con la propria firma digitale riconosciuta. La piattaforma funge da vero e proprio ufficio postale elettronico. Essa assiste l'utente nella compilazione dei messaggi e gli mette a disposizione proprie caselle postali, rilasciando ricevute in merito alle trasmissioni eseguite. La piattaforma tiene inoltre un registro degli utilizzatori.

Sempre in tema di egovernment è stato annunciato pochi giorni orsono che il 1. gennaio 2008 entrerà in vigore l'Ordinanza concernente la comunicazione per via elettronica nell'ambito di una procedura amministrativa che concretizza la Legge federale sulla procedura amministrativa, che già prevedeva l'invio di atti e la notifica di sentenza in forma elettronica (cfr. art. 11b cpv. 2, 21a cpv. 1 e 34 cpv. 1bis PA).

Anche le autorità giudiziarie si stanno dunque dotando delle regole per la trasmissione elettronica degli atti, che in determinati campi dell'amministrazione esiste da tempo. Si pensi che l'Amministrazione federale delle contribuzioni accetta dal 2002 la trasmissione elettronica di dati per l'IVA, sulla base dell'Ordinanza del DFF concernente la trasmissione elettronica di dati e di informazioni (OeIDI) del 30 gennaio 2002. Tale Ordinanza era sin troppo precoce rispetto alla situazione di mercato esistente. Considerato infatti che in quegli anni non vi erano autorità di certificazione svizzere, per promuovere il servizio di egovernment l'amministrazione aveva deciso di accettare firme digitali rilasciate da un'autorità di certificazione germanica.

Le applicazioni pratiche oggi e domani nello studio legale

Le applicazioni pratiche della firma digitale nello studio legale sono già oggi molteplici.

Esse concernono innanzitutto proprio la comunicazione con le autorità amministrative e giudiziarie.

La firma elettronica e le normative che sono state e che verranno emanate nei prossimi anni, sicuramente anche a livello cantonale, creano le condizioni per potersi validamente rivolgere alle autorità in forma elettronica, con la comodità e il risparmio di costi per il mandante che ciò comporta.

Il limite consiste oggi non tanto nella procedura necessaria per poter ottenere il certificato elettronico qualificato. Questo è ottenibile facilmente presso le società riconosciute, compilando il formulario che viene messo a disposizione online e recandosi personalmente presso l'autorità di certificazione con un valido documento d'identità e la copia della patente d'avvocato, qualora si voglia far registrare anche il titolo. Il limite consiste piuttosto nel fatto che la comunicazione con le autorità avviene attraverso una piattaforma specifica, che è completamente estranea agli usuali strumenti informatici che utilizza il legale nell'ambito della sua attività. Si deve installare un nuovo programma e utilizzare una nuova interfaccia, mentre sarebbe stato più semplice potere gestire la comunicazione attraverso gli usuali programmi di posta elettronica, come ad esempio Outlook. Il tempo permetterà di capire se i legali si abitueranno alla nuova piattaforma o se le autorità dovranno fare un ulteriore passo verso l'utente.

Le applicazioni pratiche concernono poi già oggi le comunicazioni per via elettronica con i clienti e con i colleghi. L'e-mail viene comunemente usato per trasmettere comunicazioni in modo pratico e veloce. Un tale messaggio deve però essere equiparato a una cartolina scritta a matita: tutti ne possono leggere il contenuto, che può essere oltretutto modificato durante l'invio. Il destinatario non ha alcuna certezza in merito all'identità del mittente e in merito all'integrità messaggio.

La situazione è completamente diversa se il messaggio è munito di firma elettronica generata con un certificato qualificato. Utilizzando la firma elettronica, il mittente adempie i criteri oggi vigenti in materia di sicurezza informatica, fornendo al destinatario solide garanzie in merito all'integrità del messaggio e all'identità del mittente. Il legale che utilizza la firma elettronica, si mette dunque al riparo da critiche e contestazioni da parte dei suoi interlocutori. E al contrario, il legale può confidare nei messaggi di posta elettronica, da lui ricevuti sia sotto il profilo dell'integrità dei dati in essi contenuti, sia sotto il profilo dell'autenticità. Ciò costituisce un evidente vantaggio e permette ad esempio – in teoria già oggi, in pratica quando vi sarà una più ampia diffusione dell'identità elettronica – di concludere via posta elettronica contratti debitamente firmati da tutte le parti. Questo sarà la realtà sia nei rapporti di diritto privato, che in quelli con le autorità, quando queste avranno concretamente implementato ciò per cui già oggi esiste la base legale. A titolo esemplificativo l'avvocato potrà inviare mediante posta elettronica al proprio cliente un'istanza indirizzata all'ufficio registri o una bozza di fideiussione. Quest'ultimo la potrà comodamente firmare elettronicamente e validamente trasmettere via e-mail al proprio interlocutore, il quale potrà procedere nelle sue incombenze.

Le applicazioni pratiche per lo studio legale concernono poi servizi di cui possono usufruire già oggi tutti gli utenti dell'amministrazione cantonale e federale. Il legale può dunque già oggi inviare la propria dichiarazione IVA per via elettronica. Mediante l'utilizzo della firma elettronica, il legale può inoltre già oggi archiviare elettronicamente i libri, i documenti con-

tabili e la corrispondenza d'affari, conformemente all'art. 957 CO e all'Ordinanza federale sulla tenuta e la conservazione dei libri di commercio (OLC) del 24 aprile 2002. L'archiviazione elettronica, mediante l'utilizzo di una firma elettronica che garantisca la sicurezza dei dati, potrà d'altronde essere adottata anche per gli incarti, ad eccezione di eventuali documenti originali che si dovessero trovare nei dossiers archiviati e che dovranno forzatamente essere archiviati fisicamente o eventualmente restituiti al cliente.

In sostanza la firma elettronica offrirà allo studio legale ulteriore comodità e rapidità nella comunicazione con i propri interlocutori, siano essi clienti, controparti o autorità giudiziarie o amministrative. La firma elettronica garantirà l'affidabilità e – laddove la legge impone una determinata forma – la validità degli scambi di informazioni. Sorgeranno certamente nuovi problemi. Rimane ad esempio irrisolto il problema probatorio dell'invio, rispettivamente della ricevuta del messaggio. Emergeranno inoltre sicuramente nuovi abusi, ai quali la giurisprudenza dovrà dare risposte chiare al fine di non far sorgere incertezze in merito all'utilizzo della firma elettronica.

Tutto ciò avverrà però solo quando la firma elettronica sarà sufficientemente diffusa, affinché se ne possa offrire sistematicamente l'utilizzo nelle comunicazioni.

Postfazione

A causa della nostra dipendenza dagli strumenti informatici, esistono alcuni casi in cui la firma elettronica - anche se limitatamente alla firma elettronica avanzata - è comunque la sola tecnologia che può e deve essere utilizzata. Citeremo due esempi. Il primo caso è quello delle indagini informatiche dove le prove esistono solo in formato elettronico. Detto in altri termini se si vogliono preservare le informazioni contenute su un disco di un PC per poterle presentare come prova, è assolutamente necessario firmare tutto il contenuto del disco per dare la garanzia alle parti e al giudice che le informazioni non siano state manomesse in seguito.

Un'altra funzione tecnica con interessanti risvolti legali è la marcatura temporale. Si tratta di una seconda firma digitale, aggiunta rispetto a quella del documento, che viene rilasciata da una terza parte fidata e che contiene le informazioni relative alla data e all'ora e che deve essere inviata al richiedente. Questi potrà apporla al documento per garantire in questo modo l'istante in cui esso è stato creato. Risulta così possibile dare una certezza temporale anche ai documenti che esistono solo in formato elettronico, sia che vengano trasmessi con strumenti informatici o archiviati in modo elettronico su supporti di archiviazione riscrivibili.

Referenze

Singh Simon
Codici e Segreti, Rizzoli, Milano 1999

Guida crittografia e PGP
http://sicurezza.html.it/guide/leggi/85/
guida-crittografia-e-pgp/

Direttiva 1999/93/CE del Parlamento europeo
e del Consiglio del 13 dicembre 1999
http://www.interlex.it/testi/99_93ce.htm

Legge federale sui servizi di certificazione
nel campo della firma elettronica (FiEle)
http://www.admin.ch/ch/i/rs/c943_03.html

Ordinanza del sui servizi di certificazione
nel campo della firma elettronica (OFiEle)
http://www.admin.ch/ch/i/rs/c943_032.html