LA FIRMA DIGITALE

Introduzione

Lo straordinario sviluppo dei sistemi informatici, delle reti di comunicazione e dei servizi offerti mediante la tecnologia dell'informazione, può considerarsi, senza ombra di dubbio, come la grande rivoluzione della fine del secolo. La conseguenza del fenomeno ha enormi ripercussioni sul modo in cui gli uomini lavorano, si scambiano informazioni, gestiscono le proprie attività : insomma la qualità stessa della vita è influenzata in modo determinante dalle innovazioni introdotte.

Le implicazioni dovute ai mutamenti dei sistemi di elaborazione e comunicazione risultano indubbiamente positive, se vengono valutate in termini di efficienza e di semplificazione della vita stessa, ma hanno comunque risvolti negativi, quando si considerino le possibili intromissioni nella privacy dell'individuo e se si tenga conto del continuo aggiornamento per restare al passo coi tempi e non risultare tagliati fuori dallo sviluppo della società.

La dipendenza della efficienza del funzionamento dei nuovi sistemi informatici dalla sicurezza con la quale vengono effettuate le operazioni di elaborazione e comunicazione delle informazioni, risulta un fattore determinante affinché il processo a cui assistiamo possa condurre a una società migliore.

La Crittografia si presenta come uno degli strumenti fondamentali per conseguire gli obiettivi di sicurezza richiesti.

Sicurezza dei sistemi informativi

Da un punto di vista generale il termine sicurezza può essere utilizzato per indicare l' insieme delle misure di protezione idonee ad assicurare la lotta contro il verificarsi di eventi che mettano in dubbio la correttezza delle operazioni compiute dal sistema informativo.

Mediante la sicurezza si proteggono le comunicazioni e le operazioni di elaborazione, garantendo le seguenti proprietà dei dati e dei flussi informativi : riservatezza, integrità e autenticazione.

Più in dettaglio :

- garantire l' integrità della informazione, significa impedire che il contenuto dei dati possa essere alterato da chi non sia autorizzato a effettuare modifiche ;

- garantire la riservatezza della informazione, significa essere certi che chi ne abbia diritto possa accedere alle informazioni quando lo ritenga necessario ; anche se qualcuno intercetta il pacchetto non deve poterlo leggere ;

- garantire l' autenticità del mittente significa crittografare il messaggio con la firma digitale .

Le sopra menzionate caratteristiche di sicurezza di un sistema informativo possono essere considerate come "servizi di sicurezza". Infatti esse sono concetti astratti e complessi, che definiscono le caratteristiche che un sistema deve possedere per essere considerato sicuro.

I servizi di sicurezza sono poi realizzati mediante una serie di "meccanismi di sicurezza". E' importante comprendere la sottile differenza che contraddistingue e differenzia i servizi dai meccanismi. I meccanismi di sicurezza sono tutte quelle procedure che consentono di realizzare i servizi nel concreto. Essi sono definiti nei minimi dettagli realizzativi e procedurali, attraverso protocolli, algoritmi, programmi e schemi hardware.

Possiamo dire che i meccanismi di sicurezza sono i pilastri su cui fondare la sicurezza globale di un sistema informativo.

Così come i servizi di sicurezza sono caratterizzati dal fatto di fornire garanzie di riservatezza, autenticità etc., altrettanto può essere specificato per la caratterizzazione dei meccanismi di sicurezza, con una potenziale sovrapposizione di definizioni. Si può parlare anche in questo caso, infatti, di meccanismi per garantire la riservatezza delle informazioni, la loro integrità, e si potrebbe aggiungere l' autenticità, oltre che il non ripudio, etc. Va notato che in questo caso, però, si parla di cose concrete, che devono portare a una realizzazione pratica.

La crittografia

Con il termine crittografia si intende il processo di trasformazione dei dati attraverso algoritmi matematici. I dati dopo tale trattamento risultano illeggibili a chi non disponga di una chiave di decrittazione.

Scopo della crittografia è ricercare una funzione che trasformi il messaggio da trasmettere, detto testo in chiaro, in un testo cifrato, da cui non si possa facilmente risalire al testo originario, senza conoscere a priori l' algoritmo della funzione inversa. Il processo di trasformazione del testo in chiaro (pain text) in un testo cifrato (cipher text) viene chiamato criptazione, il processo inverso decrittazione o decifrazione.

Un modello crittografico viene valutato in funzione della protezione che offre a tre diversi scenari d' attacco

1. Il primo, e più semplice scenario quello in cui l' agente ostile ha a disposizione solo il testo cifrato.
2. Poiché però molto spesso si è in grado di conoscere o prevedere a priori il contenuto di buona parte del messaggio (si pensi a una richiesta d' ordine di cui l' hacker conosce il modello ma ricerca il numero della carta di credito), viene spesso richiesto che il modello crittografico resista anche a fronte della completa conoscenza del testo in chiaro : il sistema viene considerato sicuro solo se la contemporanea conoscenza del testo in chiaro e del testo cifrato non dà la possibilità di ottenere la chiave usata per criptare.
3. Infine un modello crittografico di elevata affidabilità è quello in cui non sia possibile ottenere informazioni circa la chiave usata, anche nel caso in cui sia l' agente ostile stesso a scegliere il testo in chiaro.

In ogni caso è considerato assolutamente insicuro un modello che basi la sua efficacia sull' ipotesi che l' agente ostile non conosca l' algoritmo usato per cifrare.

La crittografia è stata implementata a diversi livelli e viene comunemente utilizzata per garantire la riservatezza nella trasmissione di numeri di carte di credito o di semplici messaggi di e-mail, ma anche nell' ambito dei sistemi di certificazione e di firma digitale.

Esistono diversi sistemi di crittografia allo scopo di proteggere il contenuto delle comunicazioni e/o di autenticare l' identità del mittente di un messaggio. **Nei sistemi a chiave privata o a crittografia simmetrica** è prevista una singola chiave condivisa tra mittente e ricevente, in quelli a chiave pubblica o a crittografia asimmetrica a ciascun utente del sistema sono assegnate due chiavi differenti una pubblica e una privata.

Nei sistemi regolati da un sistema di crittografia a chiave privata il messaggio viene criptato attraverso un unica chiave nota solo al mittente e al destinatario. La scienza della crittografia a chiave privata è molto antica. Un esempio molto semplice di tale cifratura, chiamata anche **crittografia tradizionale**, risale ai tempi di Giulio Cesare quando, per rendere illeggibili i segreti militari, ogni lettera del messaggio cifrato veniva sostituita con quella che la precede o la segue di un numero "x" di posizioni. Tale modello secondo i criteri sopra specificati è molto sicuro, in quanto conoscendo l' algoritmo (scalare di x posizioni) la chiave (x) è facilmente individuabile.

In tempi più recenti alcune macchine per crittografare sono diventate famose, come Enigma, l' apparecchio messo a punto dai nazisti prima della Seconda guerra mondiale per codificare le trasmissioni militari.
I principali problemi generati da un sistema di crittografia a chiave privata sono :

1. da un lato la necessità di scambio preliminare della chiave tra mittente e destinatario attraverso un canale reputato sicuro (se voglio scambiare dati via e-mail devo prima comunicare la chiave al mio interlocutore per telefono o per lettera),
2. dall' altro la necessità di generare un numero molto elevato di chiavi. Infatti come mostrato nella seconda colonna della tabella 1, dato un sistema di n utenti sono necessarie n(n-1)/2 chiavi per permettere il dialogo cifrato bidirezionale tra tutti i soggetti del sistema.

tabella 1

Numero di soggetti	Chiavi necessarie	
	Sistema a chiave privata	Sistema a chiave pubblica

N	n(n-1)/2	2n

Nei sistemi regolati da un metodo di **crittografia a chiave pubblica**, ad ogni utente vengono assegnate due chiavi : una chiave pubblica, appunto, e una chiave privata.

La chiave pubblica viene messa a disposizione di chiunque, all'interno di un apposito archivio ; la chiave privata, invece, deve venire conservata da ciascun utente.

Per spedire un messaggio ad un determinato soggetto, è necessario procurarsi la sua chiave pubblica e criptare il messaggio con essa ; il destinatario, e soltanto lui, potrà decifrare il messaggio con la propria chiave privata. In questo modo viene meno il problema della comunicazione della chiave e il numero di chiavi necessarie diminuisce notevolmente.

Inoltre attraverso tale sistema non è solo possibile mantenere la riservatezza ma anche verificare l'autenticità di un messaggio attraverso la cosiddetta **firma digitale**.

Firma digitale

La firma digitale basata sulla crittografia a chiave pubblica si è ormai affermata come principale strumento in grado, allo stato attuale della tecnologia, di assicurare l'integrità e la provenienza dei documenti informatici, e quindi di svolgere per questi la funzione che nei documenti tradizionali è assolta dalla firma autografa.

L'AIPA (Autorità per l'Informatica nella Pubblica Amministrazione) ha assunto un ruolo trainante nella predisposizione della normativa del settore, svolgendo un'intensa attività che ha portato al regolamento contenuto nel DPR 10 novembre 1997, n. 513.

Tale regolamento ha stabilito quali sono gli scenari di riferimento giuridici, tecnologici ed organizzativi per ottenere quanto necessario ad un efficace utilizzo del documento informatico e della firma digitale.

Un ulteriore provvedimento legislativo, il DPMC 8 febbraio 1999, anch' esso sviluppato e proposto dall'Autorità per l'informatica nella Pubblica Amministrazione, regola gli aspetti tecnici ed organizzativi di chi usufruisce ed opera con i documenti informatici e la firma digitale.

Lo scenario presente e futuro

La pubblicazione della circolare per l'iscrizione all'elenco pubblico dei certificatori costituisce il tassello conclusivo del processo legislativo descritto.

Viene così completato, in tempi estremamente rapidi, rispetto alla complessità della materia, il processo legislativo iniziato con la legge Bassanini n. 59 del 15 marzo 1997 destinata a rivoluzionare il mondo burocratico-amministrativo, rendendo validi ai fini di legge documenti, atti e contratti realizzati e trasmessi tramite mezzi informatici e telematici.

Diventa perciò una realtà per le Pubbliche Amministrazioni, le imprese e i privati scambiare documenti elettronici con la stessa validità dei corrispondenti documenti cartacei.

L'uso legale della firma digitale consentirà grossi benefici sia per il settore pubblico che per il settore privato, migliorando i processi della Pubblica Amministrazione attraverso la razionalizzazione, semplificazione ed accelerazione dei provvedimenti amministrativi, con un significativo impatto sullo scenario sociale, economico e finanziario del Paese.

L'Italia si è posta all'avanguardia essendo il primo paese ad avere attribuito piena validità giuridica ai documenti elettronici.

L'elenco pubblico dei certificatori

Per garantire l'identità dei soggetti che utilizzano la firma digitale e per fornire protezione nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività di certificazione, il DPR n, 513/97 (art. 8) richiede che il soggetto certificatore sia in possesso di particolari requisiti e sia incluso in un elenco pubblico, consultabile telematicamente, predisposto, tenuto ed aggiornato a cura dell'Autorità per l'Informatica nella Pubblica Amministrazione.

Le Pubbliche Amministrazioni possono anch' esse certificare le chiavi osservando le regole tecniche dettate dall'art. 62 del DPMC 8 febbraio 1999.

Autorità di certificazione

L'Autorità di Certificazione svolge una procedura di elaborazione informatica applicata alle chiavi di criptazione assegnate agli utenti ("certificazione delle chiavi).Mediante questa attività essa garantisce pubblicamente l'unicità ed univocità delle chiavi stesse, la loro appartenenza al soggetto o ente indicato, il periodo temporale all'interno del quale le chiavi possono essere validamente e legittimamente utilizzate.

La separazione esistente nel nostro ordinamento tra settore pubblico e settore privato ha suggerito l'opportunità di creare due distinte Autorità di Certificazione :

1. Settore pubblico : l'Autorità Amministrativa di Certificazione, composta da rappresentanti della Pubblica Amministrazione
2. Settore privato : l'Autorità Notarile di Certificazione, composta da notai.

Per garantire l'armonizzazione dell'intero sistema, e per un costruttivo dialogo tra le autorità, fra di loro o con analoghe istituzioni estere, è prevista la creazione di un organismo superiore composto dai medesimi membri di tali autorità riuniti sotto la presidenza del presidente pro tempore dell'A .I.P.A. (Autorità per l'Informatica nella Pubblica Amministrazione).

Autorita' Amministrativa di Certificazione

Tra i compiti principali svolti dall'A.A.C. è possibile menzionare :

- generazione, conservazione, certificazione e pubblicazione delle chiavi di criptazione per tutti gli Organi, Uffici, Dirigenti, Funzionari e Dipendenti della Pubblica Amministrazione ;
- controllo e supervisione delle attività svolte dalle Autorità Intermedie di Certificazione (vedi sotto) ;
- formazione, tenuta e pubblicazione in forma telematica dell'Albo pubblico delle Autorità Intermedie di Certificazione.

Autorità Notarile di Certificazione

Tra i compiti principali svolti dall'A.N.C. è possibile menzionare :

- generazione, conservazione, certificazione e pubblicazione delle chiavi di criptazione per tutti i soggetti che ne facciano richiesta, ad eccezione di quelli per i quali sono competenti il C.S.A.C. (Consiglio Superiore delle Autorità di Certificazione) e l'A.A.C. ;
- controllo e supervisione dell'attività delle Autorità Private di Certificazione (A.P.C.) ;
- formazione, tenuta e pubblicazione in forma telematica dell'Albo pubblico delle A.P.C.

Autorità Private di Certificazione (A.P.C.)

Le A.P.C. sono soggetti di diritto privato costituiti in forma di società di capitale, associazione riconosciuta, consorzio con rappresentanza esterna o società cooperativa aventi adeguati requisiti tecnici e professionali. Esse assumono la rappresentanza dei propri soci innanzi la A.N.C., sempre per il tramite di un notaio, per la generazione, gestione e conservazione delle chiavi di criptazione dei propri rappresentanti.

Consiglio Superiore delle Autorità di Certificazione (C.S.A.C.)

Esso svolge le seguenti principali attività :

- coordinamento della attività della A.A.C. e della A.N.C. ;

- generazione , gestione, certificazione e conservazione in copia delle chiavi di crittografia della A.A.C. e della A.N.C. ;
- generazione, gestione, certificazione e conservazione in copia delle chiavi di crittografia dei seguenti soggetti : Presidente della Repubblica, Presidenti del Senato e della Camera dei Deputati, Ministeri di Stato, Presidente della Corte Costituzionale ;
- certificazione delle chiavi di criptazione attribuite dalla A.A.C. ai rappresentanti istituzionali delle singole Pubbliche Amministrazioni ;
- certificazione delle chiavi di criptazione attribuite dalla A.N.C. ai notai ;
- coordinamento tra le autorità italiane di certificazione ed omologhe istituzioni estere.

Autorità Intermedie di Certificazione

Come è già accaduto in altri Stati, nessun divieto è dato dal nostro ordinamento per la nascita ed organizzazione di Autorità Intermedie o Private di certificazione (esempio di autorità privata è la Associazione delle Banche per il settore bancario). E' da sottolineare tuttavia l'imposizione di limiti richiesti sui requisiti soggettivi e patrimoniali di tali enti al fine di tutelare gli utenti finali e garantire la efficienza del mercato.

Cos'è è la firma digitale e a cosa serve ?

La firma digitale è l' equivalente elettronico di una tradizionale firma apposta su carta. La sua funzione principale è perciò quella di attestare la validità e la veridicità di un documento.

Dal punto di vista tecnico la firma digitale è una codifica crittografica del documento, basata su di un algoritmo di *hashing* e di un altro algoritmo di cifratura asimmetrico.

La firma digitale garantisce, oltre che l' AUTENTICAZIONE del mittente del documento e del messaggio trasmesso, anche l' INTEGRITA' del messaggio permettendo di verificare che non ci siano state modifiche rispetto all' originale. In altre parole, attraverso la firma digitale si evita che il nostro documento venga intercettato e manipolato senza che nessuno se ne accorga.

Algoritmo di Hashing

In generale l' hashing è una tecnica che riduce una stringa di bit di lunghezza variabile in una sequenza di caratteri di lunghezza fissa avente particolari proprietà, detta HASH. Per la firma digitale si utilizzano particolari funzioni di hash, che fanno sì che :

- è impossibile ottenere lo stesso hash a partire da due documenti diversi (non è cioè possibile che eseguendo il 'calcolo' di hashing su due documenti diversi si ottenga il medesimo risultato) ;
- è impossibile ricostruire il testo originale tramite il solo MESSAGE DIGEST (così è detto l' hash prodotto attraverso particolari funzioni di hash unidirezionali).

La firma digitale nella crittografia asimmetrica

I metodi crittografici a chiave pubblica possono essere utilizzati per la costruzione di strumenti per la firma digitale, variamente concepiti. Mentre nella crittografia la chiave pubblica viene usata per la cifratura, ed il destinatario usa quella privata per leggere in chiaro il messaggio, nel sistema della firma digitale il mittente utilizza la funzione di cifratura e la sua chiave privata per generare un' informazione che (associata al messaggio) ne verifica la provenienza, grazie alla segretezza della chiave privata. Chiunque può accertare la provenienza del messaggio adoperando la chiave pubblica.

L' algoritmo RSA, usato per generare firme elettroniche, si basa semplicemente sull' inversione del ruolo delle chiavi rispetto a quello utilizzato per assicurare la riservatezza. Le differenze fra le due applicazioni risiedono essenzialmente nel fatto che per la firma digitale si evita di dover applicare l' operazione di cifratura all' intero testo (con notevole risparmio di tempo).

Il testo da firmare viene compresso in una sorta di riassunto (detto impronta digitale), tramite un' apposita funzione di Hash, costruita in modo da rendere minima la probabilità che da testi diversi si possa ottenere il

medesimo valore della impronta. La dimensione del riassunto è fissa, e molto più piccola di quella del messaggio originale ; sicché la generazione della firma risulta estremamente rapida.

In base ai recenti studi svolti dll' AIPA, sono state individuate determinate attività preliminari necessarie alla predisposizione delle chiavi utilizzate dal sistema di crittografia su cui il meccanismo di firma si basa.
Prima tra queste è la registrazione dell'utente presso un'Autorità di Certificazione con lo scopo duplice di rendere certa la sua identità ed instaurate con essa un canale di comunicazione sicuro attraverso il quale verranno fatte viaggiare le chiavi pubbliche di cui viene richiesta la certificazione. All'atto della registrazione la Autorità di Certificazione attribuirà all' utente un identificatore, di cui viene assicurata l' univocità, attraverso il quale sarà possibile a chiunque reperire in modo diretto e sicuro i certificati rilasciati al soggetto corrispondente all' interno di registri pubblici in cui questi sono registrati.

Mediante un software adatto al sistema crittografico adottato, l' utente genera una coppia di chiavi da utilizzare : una, che verrà mantenuta segreta, per l' apposizione della firma ; l' altra, destinata alla verifica che verrà resa pubblica attraverso i registri della Autorità di Certificazione.

La certificazione della chiave pubblica ha lo scopo di assicurare, a chiunque riceva un documento correttamente firmato, l' identità del soggetto che ha posto la firma. La richiesta di certificazione all' Autorità di Certificazione da parte della utente avviene attraverso l' invio della chiave pubblica, generata autenticandola mediante l' identificatore attribuito all' utente nella precedente registrazione presso l ' autorità stessa. In questo modo, l' utente riceve un certificato che garantisce la provenienza della chiave pubblica attraverso l' intermediazione della Autorità di Certificazione.

Una volta emesso, il certificato viene reso disponibile in uno o più registri, ai quali può accedere chiunque abbia bisogno di verificare la validità di una sottoscrizione digitale.

L' utente dispone, da questo momento, della sua chiave privata con la quale firmerà i messaggi ; della chiave pubblica indicata nei registri o inviabile direttamente al destinatario come allegato del messaggio ; del certificato che attribuisce alla firma validità e provenienza. L' utente è in grado di firmare elettronicamente un numero qualunque di documenti, attraverso la chiave privata, 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, conseguita su richiesta del proprietario (ad esempio, nel caso in cui questi ritenga che la segretezza della sua chiave privata sia stata compromessa).

Passando all' esame del processo di generazione della firma, questa viene apposta mediante una sequenza di tre operazioni.
Inizialmente si ha la generazione della impronta, mediante l' applicazione al testo da firmare di una funzione di Hash appositamente studiata, la quale assicura l' unicità della stringa generata. L'utilità dell'uso della impronta è duplice, in primo luogo consente di evitare che per la generazione della firma sia necessario applicare l' algoritmo di cifratura all' intero testo che può essere molto lungo. Inoltre permette la autenticazione, da parte di una terza parte fidata (l'Autorità di Certificazione), della sottoscrizione di un documento senza che questa venga a conoscenza del suo contenuto.

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

La firma digitale viene apposta al testo del messaggio in una posizione predefinita (per solito, alla fine). Assieme alla firma vera e propria è allegato "il valore" della impronta digitale ed eventualmente anche il certificato da cui è possibile recuperare il valore della chiave pubblica.

L ' operazione di verifica della firma digitale viene effettuata ricollocando, con la medesima funzione di Hash usata nella fase di sottoscrizione, il valore della impronta e controllando che il valore così ottenuto coincida con quello generato per decodifica della firma digitale stessa.

Qualora sia necessario attribuire a 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 della Autorità di Certificazione di un ulteriore firma digitale per il documento marcato. Il servizio di marcatura temporale aggiunge all' impronta ricevuta la data e l' ora ottenendo un' impronta marcata. Il richiedente allega al documento la marca temporale inviategli dal servizio, la quale può essere verificata attraverso la chiave pubblica del servizio stesso.

Le tecniche di firma digitale sono già sperimentate nel continente nord americano, attraverso dei software con caratteristiche come sopra delineate. Per la diffusione nel nostro paese si attende che si giunga alla elaborazione elle regole tecniche, a cura della Autorità per l' Informatica nella Pubblica Amministrazione.

Il settore della informatica è rinomatamente in movimento e sviluppo continuo. Questa situazione potrebbe portare a rapide modifiche di tecnologie nel giro di pochi anni. Ancorché in continua evoluzione, è da ritenere che le basi ed i principi della crittografia asimmetrica non si modificheranno e continueranno ad essere lo strumento di lavoro del sistema della firma digitale.

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 della utente presso un' Autorità di Certificazione (AC)
2. la generazione di una coppia di chiavi Ks e Kp,
3. la certificazione della chiave pubblica Kp,
4. la registrazione della chiave pubblica Kp.

La firma viene apposta, con il processo schematicamente mostrato nella Figura 1, mediante una sequenza di tre operazioni :

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

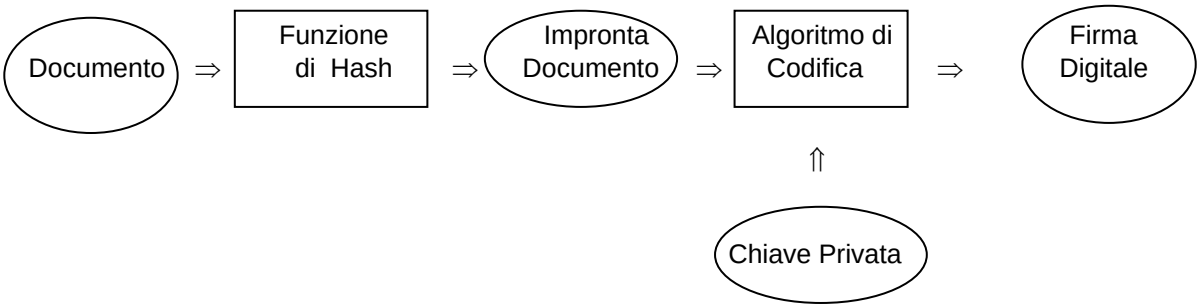

Figura 1 - Generazione della firma digitale

Generazione della 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.

Verifica della firma digitale

L' operazione di verifica della firma digitale, mostrata schematicamente in Figura 2, viene effettuata ricollocando, con la medesima funzione di hash usata nella fase di sottoscrizione, il valore della impronta e controllando che il valore così ottenuto coincida con quello generato per decodifica della firma digitale stessa. La disponibilità del valore della impronta all' interno del messaggio semplifica l' operazione.

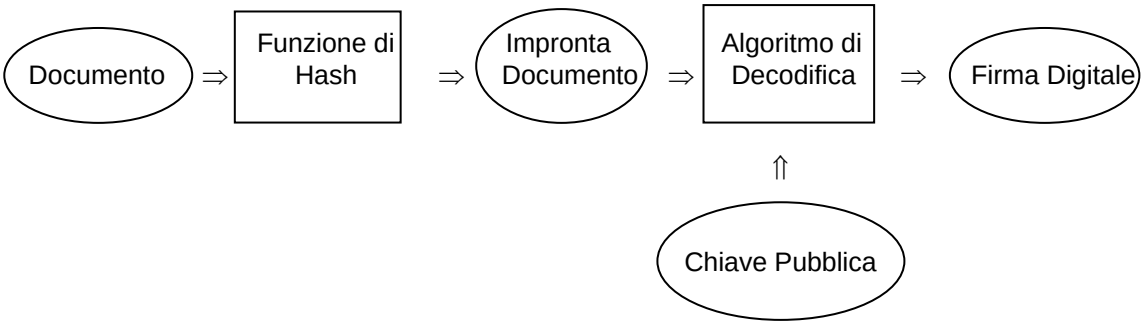

Figura 2 - Verifica della firma digitale

Ecco un esempio di come si usa la firma digitale nello scambio di documenti tra due utenti del servizio :

1. Il mittente A scrive (ad esempio usando un comune word-processor) un documento per un destinatario B.
2. Per essere sicuro che il documento non venga corrotto durante la spedizione, A codifica il documento con un algoritmo di hashing, che dà come risultato un numero (digest).
3. A questo punto A cifra questo risultato con la propria chiave privata (nota soltanto a lui !), firmando di fatto, il messaggio.
4. Affinché unicamente il destinatario B possa leggere il contenuto di tale messaggio, A lo codifica ulteriormente usando la chiave di sessione (ovvero con un algoritmo simmetrico)
5. A spedisce il messaggio così ottenuto tramite un normale sistema di e-mail.
6. Il destinatario B riceve il messaggio con il suo normale software di posta elettronica. Ciò gli consente di visualizzare il contenuto del messaggio.

Aspetti giuridico- legali

La disciplina del d.p.r. 10 novembre 1997, n. 513

In data 31 ottobre 1997 il Consiglio dei Ministri ha approvato il "Regolamento recante criteri e modalità per la formazione, l' archiviazione e la trasmissione di documenti informatici, a norma dell' art. 15, comma 2, della legge 15 marzo 1997, n. 59".

Il risultato, prodotto dalle norme del regolamento, è la piena rilevanza giuridica della documentazione informatica e la sua equiparazione alla tradizionale documentazione "cartacea".

All' intenso valore giuridico della disciplina regolamentare non si accompagna un equivalente valore pragmatico in quanto, per quest' ultimo, occorrerà attendere l' emanazione di ulteriori ed indispensabili regolamenti tecnici di attuazione. Successivamente all' emanazione di tali regolamenti, il d.p.r. 513 diventerà pienamente operativo.

Il regolamento si compone di tre capi.

Il primo di questi, dedicato ai principi generali, si apre con l' enunciazione delle definizioni dei termini di carattere tecnico, utilizzati nel corso della disciplina giuridica. Alla nozione di documento informatico ed alla descrizione dei requisiti che lo caratterizzano, segue la disciplina dell' atto informatico come forma scritta e dell' efficacia probatoria ad esso attribuita ; e quella della validità e rilevanza attribuita alla copia di atti e documenti. Lo stesso capo si occupa (sommariamente) della disciplina della attività da compiersi per il

rilascio delle chiavi asimmetriche all' utente da parte dell' Autorità di Certificazione, nonché degli obblighi inerenti entrambe le parti.

Dopo alcune enunciazioni di carattere funzionale relative alla forme e modalità di utilizzo delle chiavi, il secondo capo, rubricato "firma digitale", si dedica alla validità e rilevanza a tutti gli effetti di legge dei documenti dei contratti stipulati con gli strumenti informatici o per via telematica. L' attenzione è poi rivolta ai criteri di conclusione del contratto e di notificazione del documento informatico, nonché alla segretezza della corrispondenza trasmessa per via informatica ed alla possibilità di effettuare pagamenti elettronici, come pure alla formazione di libri e scritture contabili, a carattere obbligatorio, in formato elettronico.

Le successive disposizioni attengono all'autenticazione della firma digitale, riconosciuta ai sensi dell' art. 2703 cod. civ., ai criteri di validità e di applicazione delle chiavi di cifratura della pubblica amministrazione. Il secondo capo si chiude con la disciplina della firma digitale e del documento informatico, formati dalla pubblica amministrazione.

Le norme di attuazione del regolamento sono contenute nel capo terzo, il quale pone (alle pubbliche amministrazioni) dei termini per l' adozione di piani di sviluppo e di realizzazione nonché di un rapporto tra costi e benefici del recupero su supporto informatico dei documenti e degli atti cartacei.
Il regolamento presenta norme di carattere sostanziale che si inseriscono nel percorso positivo della definizione di documento informatico, per il quale si intende la rappresentazione informatica di atti, fatti, o dati giuridicamente rilevanti (art. 1, a). Nozione breve, che permette di attribuire al documento informatico, da chiunque formato, all' archiviazione e alla trasmissione telematica di questo, validità e rilevanza a tutti gli effetti di legge (art. 2).

Dall' esame dell' art. 1, contenente le definizione dei termini tecnici presenti nelle successivi norme, è possibile richiamare, quasi per intero, la disciplina scelta per il documento informatico firmato digitalmente. Il sistema che attribuisce al documento informatico con firma digitale l' efficacia della scrittura privata (art. 5) è così concepito.
Una Autorità di certificazione (o certificatore), consultata da un utente interessato, descrive a quest' ultimo la procedura e concede il know how per la "generazione" di una coppia di chiavi asimmetriche. L' utente ha il dovere di custodire segretamente la propria " chiave privata" , che utilizzerà per apporre la firma ; tuttavia è data facoltà di depositare in forma segreta la chiave presso un notaio (secondo la disciplina del testamento segreto) . La propria "chiave pubblica" verrà pubblicata in un registro telematico da parte del certificatore. Quest' ultimo, ricevuta la chiave pubblica dell' utente, emette un "certificato", il quale garantisce la corrispondenza biunivoca tra chiave pubblica, necessaria per la verificazione della firma, chiave privata e soggetto titolare. Il contenuto del certificato riguarda l' indicazione delle generalità della persona, della corrispondente chiave pubblica e del termine di scadenza (art.1, h). La validità di tale certificato è stabilita in una durata massima di tre anni, ma può essere revocato, ossia perdere validità irretroattivamente, ovvero sospeso per un periodo di tempo determinato. Il regolamento si occupa di disciplinare i requisiti dei certificatori, i quali hanno il delicato compito di assicurare la corrispondenza, e quindi la titolarità, delle chiavi asimmetriche, e di conseguenza della firma digitale.

Con riferimento al settore privato, per svolgere l' attività di certificatore occorre l' inclusione in un apposito elenco pubblico tenuto dall' Autorità per l' Informatica nella Pubblica Amministrazione (art. 8, comma 3). Si tratta di un regime autorizzatorio i cui requisiti per accedervi sono stati in parte mutuati da quelli richiesti per l' esercizio dell' attività bancaria. Inoltre è data possibilità di agire sul territorio italiano ai certificatori operanti sulla base di licenza od autorizzazione rilasciata da altro Stato membro dell' Unione Europea o dello Spazio economico europeo, purché in possesso dei requisiti equivalenti.

In numerose leggi e progetti di legge stranieri e sovranazionali sulla materia, la struttura ed il quadro di funzionamento delle Autorità di Certificazione sono disciplinati in maniera puntuale ed esaustiva, prevedendo, nella maggior parte dei casi, due livelli gerarchici, con il livello sovraordinato di emanazione statale o pubblica che certifica le autorità sottordinate, normalmente private. Le norme del regolamento necessitano una integrazione che avverrà attraverso l' emanazione dei successivi regolamenti di attuazione previsti dall' art. 3.

Il regolamento prevede la disciplina della "firma digitale autenticata". L' autenticazione consiste nell' attestazione da parte di un pubblico ufficiale che la firma digitale è stata apposta in sua presenza dal titolare. Tale autenticazione deve essere preceduta dall' accertamento dell' identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte e non è in contrasto con l' ordinamento giuridico (art. 16). La funzione di autentica non si esaurisce nella mera certificazione, ma comporta un controllo di legalità sul contenuto del documento informatico sottoscritto. La

firma digitale autenticata si considera come riconosciuta ai sensi dell' art.2703 cod. civ., formando piena prova della provenienza delle dichiarazioni da chi ha sottoscritto il documento informatico.

La disciplina regolamentare incide anche sulla comunicazione telematica del documento informatico. L' art. 12, dedicato alla trasmissione del documento, stabilisce che il documento informatico trasmesso per via telematica si intende pervenuto al destinatario se inviato all' indirizzo elettronico da questi dichiarato. La determinazione della data e dell' orario, opponibili terzi, in cui è avvenuta la conclusione del contratto, dipende dall' adozione di tecniche di validazione temporale.
Come si può notare da questa rassegna il regolamento contiene norme la cui incidenza sul diritto sostanziale è estremamente rilevante, mancando una immediata applicabilità, rinviata a delle emanadande norme tecniche.

L' Autorità per l' informatica nella pubblica amministrazione ha predisposto uno schema di Decreto del Presidente del Consiglio dei Ministri contenente "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi della art. 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513".

La firma digitale nel commercio elettronico

Tutto e' pronto, e a tempo di record , per l'attuazione della firma digitale e per il decollo delle transazioni via internet. Attenzione pero' a non fare confusione: questa formidabile invenzione, denominata firma digitale , che indubbiamente consentira' di effettuare in rete qualsiasi transazione per la quale sia richiesta per legge un documento cartaceo sottoscritto dall'autore, non e' viceversa indispensabile per la realizzazione del commercio elettronico inteso nella sua forma più semplice, di scambio di beni mobili e servizi via internet .

Questo tipo di transazioni, che caratterizzano il commercio elettronico attualmente effettuato in rete, sia nel caso businnes to businnes che nel caso businnes to consumer , potranno continuare a concludersi senza firma digitale, esattamente come è accaduto fino ad oggi,a meno che gli stessi operatori non decidano, per ragioni di opportunità commerciale, di adottare in massa questo strumento.

In altri, termini una volta andata a regime la attività degli enti certificatori e una volta che sarà diffuso l'utilizzo, presso l'utenza consumer , del meccanismo delle doppie chiavi, sarà il mercato a decidere se anche per fare la spesa o acquistare - vendere un libro in rete , sia opportuno utilizzare la firma digitale. Ciò avverrà probabilmente quando l'utilizzo del dispositivo della firma (necessario per creare la coppia di chiavi) e la procedura di certificazione saranno diventati, per economicità e facilità di esercizio, talmente diffusi, un po' come è avvenuto con il bancomat, che verrà naturale apporre la firma digitale anche alle transazioni per le quali la sottoscrizione non è richiesta dalla legge Il fatto che, per esprimere la volontà negoziale, venga utilizzato uno strumento di comunicazione elettronica (invece ad esempio della comunicazione verbale, telefonica o postale) no muta la natura contrattuale delle operazioni per cui continuerà ad applicarsi la disciplina dei contratti prevista dal nostro Codice civile.

A questo proposito il nostro orientamento si è ispirato al principio della cosiddetta libertà di forma, che impone la forma scritta ad substantiam (a pena di nullità) soltanto per alcuni tipi di contratto indicati all'articolo 1350 del Codice civile o da specifiche disposizioni di legge, in considerazione del loro particolare contenuto (ad esempio vendita di beni immobili, locazione di immobili di durata superiore a nove anni, ecc.).

Il criterio generale quindi, ad eccezione dei casi stabiliti espressamente dalla legge, è quello della libertà contrattuale delle parti, in forza del quale i contratti possono essere conclusi a voce, per telefono o con ogni altra forma che venga ritenuta idonea, comprese quindi la e-mail e il World Wide Web. Ciò che rileva è che il contratto è costituito dall'incontro di due volontà e si conclude nel momento in cui chi ha fatto la proposta ha conoscenza dell'accettazione della controparte (articolo 1326 Codice civile). Ciò che farà la differenza, tra l'aver concluso un contratto per la fornitura di un prodotto o un servizio su internet con o senza la firma digitale, sarà la validità o meno delle clausole vessatorie, applicabili comunque soltanto ai contratti businness to businness, e il regime giuridico della prova, con tutte le conseguenze del caso. Da questo punto di vista il Dpr 513/97 ha riconosciuto al documento sottoscritto con firma digitale l'efficacia probatoria della scrittura privata ex articolo 2707 Codice civile (documento sottoscritto dall'autore) mentre, al

documento informatico privo di firma digitale, l'efficacia probatoria delle riproduzioni meccaniche ex articolo 2712 Codice civile.

E' opportuno evidenziare come nella eventualità di patologia del rapporto contrattuale si applicheranno in ogni caso i principi interpretativi generali elaborati da dottrina e giurisprudenza in materia, compatibilmente con la particolare tecnologia utilizzata. In dottrina già si discute, ad esempio , se la firma digitale " validata " , per la quale è quindi da escludere la presenza di atti di revoca o sospensione del certificato, possa o meno essere qualificata come legalmente riconosciuta, ai sensi dell'articolo 2702 Codice civile. L'orientamento prevalente sembra essere di avviso contrario, nel senso della ammissibilità in ogni caso del disconoscimento da parte del titolare, il quale avrà anche l'onere di dimostrare con la querela di falso , le circostanze che hanno consentito ad esempio ai terzi di utilizzare abusivamente la chiave privata, in modo da escludere la propria responsabilità. In attesa che entrino in funzione gli enti certificatori e si diffonda l'uso delle chiavi asimmetriche, è necessario invece che gli operatori di e-commerce rivolti all'utenza consumer provvedano ad adempiere agli obblighi informativi imposti dal Dlgs185/99 (in vigore il 21 Ottobre), adeguando le pagine Web dei propri siti.

Bibliografia :

- www.securteam.it
- www.ilsole24ore.it
- www.aqipa.itwww.comune.bologna.it
- www.interlex.com/inforum/maccaro1.htm
- estratto de IL SOLE 24 ORE / Venerdì 29 ottobre 1999
- www.interlex.com/testi/attiel.htm

STUDENTI : Cifalinò Matteo ; Negri Emanuela ; Saggiomo Ilaria PIACENZA 13/12/1999