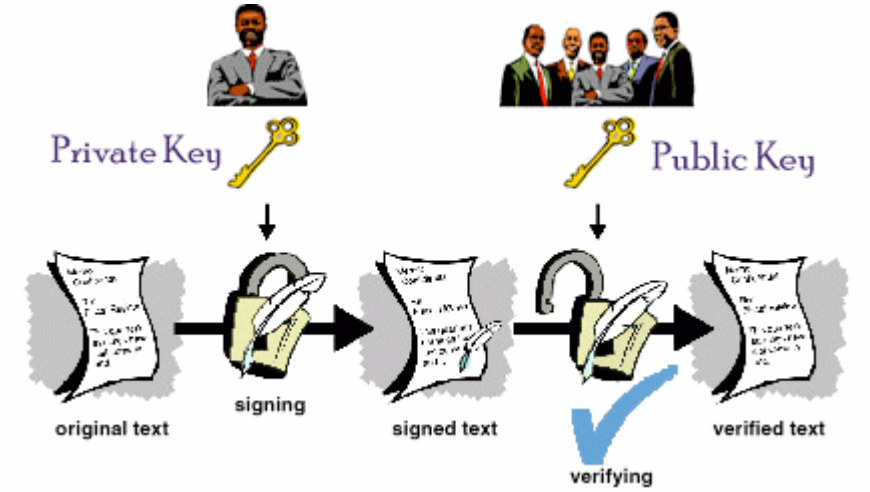
FIRMA DIGITALE e CRITTOGRAFIA



Indice

1 Introduzione

Lo studio della crittografia risale a tempi antichi quando si cercava di rendere segreti i messaggi da trasmettere agli amici, ma da tenere assolutamente nascosti agli occhi dei nemici. Naturalmente ciò che interessa a noi altro non è che la punta dell'iceberg di un mondo infinito e in continua evoluzione.

Infatti quando parliamo di crittografia applicata alla firma digitale ci riferiamo in modo particolare al sistema di "crittografia asimmetrica"; tale sistema permette infatti di dare garanzia che solo le due chiavi, pubblica e privata, possano comunicare tra loro, perché legate da una assoluta dipendenza. È noto infatti che un documento criptato con la chiave privata diventa accessibile solo se decriptato con la chiave pubblica e viceversa.

Tratteremo l'analisi della firma digitale, sia per gli aspetti storico-normativi, sia per gli aspetti tecnici, soffermandoci in modo particolare sul funzionamento pratico e sulle sue implicazioni a livello procedurale.

Di seguito passeremo in rassegna i vantaggi e gli svantaggi, sia organizzativi che economici, che comporta un cambiamento così radicale delle abitudini e del modo di operare di migliaia di aziende e di cittadini; conseguentemente a questi cambiamenti analizzeremo gli impatti di queste nuove tecnologie sull'attività di revisione.

2 La crittografia

2.1 Cenni storici

La crittografia nasce dall'esigenza di nascondere messaggi strategici agli occhi dei nemici già in antichità; nascono così i primi sistemi crittografici come il "cifrario di Cesare" dovuto a Caio Giulio Cesare, oggi banale, ma emblema di quella scienza che ha prodotto sistemi sempre più evoluti e più sicuri. Il *cifrario di Cesare* è il più antico algoritmo crittografico di cui si abbia traccia storica. È un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto. In particolare, Cesare utilizzava uno spostamento di 3 posizioni (la chiave era dunque "3"), secondo il seguente schema:

Testo in chiaro	a b c d e f g h i l m n o p q r s t u v z
Testo cifrato	D E F G H I L M N O P Q R S T U V Z A B C

Per cifrare un messaggio, basta prendere ogni lettera del testo in chiaro e sostituirla con la corrispondente lettera della riga "testo cifrato". Per decifrare, viceversa. Ecco un semplice esempio:

```
Testo in chiaro: attaccare gli irriducibili galli alla ora sesta
```

```
Testo crittato:  DZZDFFDUH LON NUUNGAFNENON LDOON DOOD RUD VHVZD
```

Qualsiasi sia il sistema crittografico utilizzato, la legge fondamentale sul corretto uso di tali tecniche fu scritta da Kerckhoffs (**Legge di Kerckhoffs**) nel suo libro del 1883 "La Cryptographie Militaire" e di seguito riportata:

"La sicurezza di un crittosistema non deve dipendere dal tener celato il crittoalgoritmo. La sicurezza dipenderà solo dal tener celata la chiave."

Nel 1918 Gilbert Vernam propose di usare chiavi lunghe quanto tutto il messaggio, teoria che fu dimostrata essere corretta da Claude Shannon, padre della Teoria dell'Informazione, che dimostrò che questo è l'unico metodo crittografico totalmente sicuro possibile.

Attualmente la ricerca crittografica si occupa di trovare un metodo sicuro ma che non comporti l'utilizzo di una chiave lunga quanto il messaggio da trasmettere, anzi che permetta l'utilizzo di chiavi corte e riutilizzabili senza per questo pregiudicarne la sicurezza.

Fino a qualche anno fa l'unico metodo crittografico era quello della "**crittografia simmetrica**" detta anche a "**chiave unica**" o a "**chiave privata**"; questo metodo richiede che il mittente e il destinatario del messaggio cifrato

facciano uso della medesima chiave, che viene usata prima per codificare e poi per decodificare il messaggio. È necessario quindi che i soggetti si scambino la chiave attraverso un mezzo di comunicazione sicuro. Il più famoso algoritmo a chiave privata è il DES (Data Encryption Standard) sviluppato da IBM nel 1975 e adottato dal National Bureau of Standards. Un'evoluzione del DES è il Triplo DES che consiste nel cifrare un testo usando il DES per tre volte consecutive cambiando ogni volta la chiave.

2.2 La Crittografia oggi

La vera novità del secolo scorso è l'invenzione della "**crittografia asimmetrica**" detta anche a "**chiave doppia**" o a "**chiave pubblica**". Ogni attore coinvolto possiede una coppia di chiavi:

a) la "chiave privata", personale e segreta, che viene utilizzata per decodificare un documento criptato;
b) la "chiave pubblica", che deve essere distribuita, serve a crittare un documento destinato alla persona che possiede la relativa chiave privata.

L'idea base della crittografia con coppia di chiavi diviene più chiara se si usa un'analogia postale, in cui il mittente è Alice ed il destinatario Bob e i lucchetti fanno le veci delle chiavi pubbliche e le chiavi recitano la parte delle chiavi private:

1. Alice chiede a Bob di spedirle il suo lucchetto, già aperto. La chiave dello stesso verrà però gelosamente conservata da Bob.
2. Alice riceve il lucchetto e, con esso, chiude il pacco e lo spedisce a Bob.
3. Bob riceve il pacco e può aprirlo con la chiave di cui è l'unico proprietario.

Se adesso Bob volesse mandare un altro pacco ad Alice, dovrebbe farlo chiudendolo con il lucchetto di Alice, che lei dovrebbe mandare a Bob e che solo lei potrebbe aprire. Si può notare come per segretare i pacchi ci sia bisogno del lucchetto del destinatario mentre per ricevere viene usata esclusivamente la propria chiave segreta, rendendo l'intero processo di criptazione/decriptazione asimmetrico. Questo semplice metodo condivide alcune caratteristiche con la crittografia a chiave pubblica: si tratta di un sistema che risolve efficacemente il classico problema della crittografia tradizionale. Se la sicurezza del sistema dipende dalla segretezza della chiave di codifica utilizzata, allora è necessario

almeno un canale sicuro attraverso il quale trasmettere la chiave. Nella crittografia tradizionale viene utilizzata un'unica chiave sia per codificare, sia per decodificare i messaggi. Le informazioni (la chiave e l'algoritmo) necessarie per chi deve inviare il messaggio sono quindi identiche a quelle necessarie a chi deve riceverlo. Per concordare una chiave con il proprio interlocutore c'è bisogno di mettersi preventivamente in contatto con lui incontrandolo di persona, telefonandogli, scrivendogli una lettera, mandandogli un messaggio o in qualsiasi altro modo. In qualsiasi caso, esiste il pericolo che la chiave venga intercettata durante il tragitto, compromettendo quindi l'intero sistema comunicativo. La crittografia a chiave pubblica permette invece a due (o più) persone di comunicare in tutta riservatezza senza usare la stessa chiave e anche se non si sono mai incontrate precedentemente. Per utilizzare questo tipo di crittografia è necessario creare una coppia di chiavi, una chiave pubblica (da diffondere) ed una chiave privata (da tenere segreta). La proprietà fondamentale della coppia di chiavi pubblica/privata è che un messaggio cifrato usando la chiave pubblica può essere decriptato usando soltanto la chiave privata corrispondente. In pratica, la chiave pubblica serve unicamente per codificare il messaggio, mentre quella privata serve unicamente per decodificarlo. È come se una cassaforte avesse due chiavi distinte, una usata per aprirla e una per chiuderla. La coppia di chiavi pubblica/privata viene generata attraverso un algoritmo (ad esempio RSA o DSA) a partire da dei numeri casuali. Gli algoritmi asimmetrici sono studiati in modo tale che la conoscenza della chiave pubblica e dell'algoritmo stesso non siano sufficienti per risalire alla chiave privata. Tale meccanismo è reso possibile grazie all'uso di funzioni unidirezionali. In realtà, in molti casi, l'impossibilità di risalire alla chiave privata non è dimostrata matematicamente, ma risulta allo stato attuale delle conoscenze in matematica e della potenza di calcolo disponibile un problema complesso. A questo punto il gioco è fatto: ogni utilizzatore si crea la propria (o le proprie, in casi particolari) coppia di chiavi. La chiave privata viene tenuta segreta e non viene mai rivelata a nessuno, nemmeno alle persone con le quali si

comunica; viceversa, la chiave pubblica viene diffusa in vari modi: può essere aggiunta automaticamente in coda a ciascun proprio messaggio, o può essere depositata in archivi pubblici (*keyserver*) a disposizione di chi la desideri. È importante che la chiave pubblica sia liberamente accessibile, perché chiunque voglia comunicare con la persona che l'ha generata dovrà preventivamente munirsi di questa, con la quale cripterà il messaggio. Un altro possibile utilizzo della coppia chiave pubblica/privata riguarda l'idea di firma digitale: in pratica un utente cifra un messaggio con la propria chiave privata; gli altri, una volta ricevuto tale messaggio, riescono a decifrarlo solo con la chiave pubblica relativa a quel particolare mittente, della quale devono essere preventivamente a conoscenza, per cui possono risalire con certezza alla sua identità.

3 La Firma Digitale

3.1 Introduzione

Per comprendere la firma digitale è opportuno esaminare anzitutto i motivi che rendono necessaria la firma di un documento di qualsiasi genere e le proprietà che essa deve di conseguenza possedere. *La firma manuale,* utilizzata comunemente per provare l'autenticità o la paternità di un documento o per siglare un accordo formulato in esso, soddisfa alcuni requisiti fondamentali:

1. La firma è *autentica,* nel senso che chi la riceve è convinto della sua originalità.
2. La firma *non* è falsificabile, e dunque costituisce prova che chi l'ha prodotta è veramente colui che ha sottoscritto il documento.
3. La firma *non è ri-utilizzabile,* e quindi risulta legata strettamente al documento su cui è stata apposta.
4. Il documento firmato *non è alterabile,* e quindi chi ha prodotto la firma è sicuro che questa si riferirà solo al documento sottoscritto nella sua forma originale.
5. La firma *non* può essere *ripudiata* da chi l'ha apposta, e costituisce dunque prova legale di un accordo o di una dichiarazione contenuta nel documento.

Anche se a volte questi requisiti sono annullati da impostori in grado di falsificare perfettamente le firme manuali, essi sono validi nella maggior parte dei casi e la firma rimane il mezzo standard per l'autenticazione di un documento. Una *versione digitale* della firma è quindi utilissima operando sulle reti dove si scambiano quotidianamente innumerevoli transazioni, ma la forma

che essa deve possedere è del tutto nuova. La firma digitale infatti non può semplicemente consistere di una *digitalizzazione* (per esempio attraverso uno scanner) del documento originale firmato manualmente, poiché un crittoanalista potrebbe condurre su di essa attacchi molto semplici, il più rischioso ed elementare dei quali è "tagliare" dal documento digitale la parte contenente la firma e 'copiarla" su di un altro documento Quindi, a differenza dalla firma manuale, la firma digitale deve avere una forma che dipende dal documento su cui viene apposta, per essere inscindibile da questo.

La firma digitale è quindi il risultato di una procedura informatica (validazione) che consente al sottoscrittore di rendere manifesta l'autenticità del documento informatico ed al destinatario di verificarne la provenienza e l'integrità. In sostanza i requisiti assolti sono:

- ***Autenticità***: con un documento firmato digitalmente si può essere certi dell' identità del sottoscrittore;
- ***Integrità***: sicurezza che il documento informatico non è stato modificato dopo la sua sottoscrizione;
- ***Non ripudio***: il documento informatico sottoscritto con firma digitale, ha piena validità legale e non può essere ripudiato dal sottoscrittore.

Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche, attribuite in maniera univoca ad un soggetto detto Titolare della coppia di chiavi. La prima, chiave privata destinata ad essere conosciuta solo dal Titolare, è utilizzata per la generazione della firma digitale da apporre al documento, la seconda, chiave da rendere pubblica, viene utilizzata per verificare l'autenticità della firma. Caratteristica di tale metodo, detto crittografia a doppia chiave, è che, firmato il documento con la chiave privata, la firma può essere verificata con successo esclusivamente con la corrispondente chiave pubblica. La sicurezza è garantita dalla impossibilità di ricostruire la chiave privata (segreta) a partire da quella pubblica, anche se le due chiavi sono univocamente collegate.

3.2 Il quadro normativo

La firma digitale nasce come strumento per la trasmissione in sicurezza dei documenti informatici, sia tra le aziende che tra aziende ed enti pubblici.

I primi accenni legislativi per disciplinare il trattamento dei documenti informatici risale al 1994, anno dal quale è stato permessa la conservazione dei documenti aziendali in formato elettronico. Il primo atto normativo che ha stabilito la validità della firma digitale per la sottoscrizione dei documenti elettronici è stato il DPR 513 del 1997, emanato in attuazione dell'articolo 15 della legge 15 marzo 1997, n. 59. Successivamente, tale normativa è stata trasposta nel DPR n. 445 del 2000 (il Testo Unico sulla documentazione amministrativa), più volte modificato negli anni successivi all'emanazione, per conformare la disciplina italiana alla normativa comunitaria contenuta nella Direttiva 99/93 in materia di firme elettroniche. Oggi, la legge che disciplina la firma digitale è il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale". Tale atto normativo, all'articolo 1, distingue i concetti di "firma elettronica", "firma elettronica qualificata" e "firma digitale".

a) Per "firma elettronica" la legge intende qualunque sistema di autenticazione del documento informatico.
b) La "firma elettronica qualificata" è definita come la firma elettronica basata su una procedura che permetta di identificare in modo univoco il titolare, attraverso mezzi di cui il firmatario deve detenere il controllo esclusivo, e la cui titolarità è certificata da un soggetto terzo. Qualunque tecnologia che permetta tale identificazione univoca, rientra nel concetto di "firma elettronica qualificata".

c) La "firma digitale", è considerata dalla legge come una particolare specie di "firma elettronica qualificata", basata sulla tecnologia della crittografia a chiavi asimmetriche.

Il decreto legislativo 82/2005, quindi, è impostato come se si potessero avere più tipi di firma elettronica qualificata, ossia più sistemi che consentano l'identificazione univoca del titolare, uno solo dei quali è la firma digitale a chiavi asimmetriche. Di fatto, però, nella realtà concreta, la firma digitale è l'unico tipo di firma elettronica avanzata oggi conosciuto e utilizzato, perciò i due concetti tendono a coincidere. Con un rimando al Codice Civile, l'articolo afferma che la firma digitale (o altra firma elettronica qualificata) fa piena prova fino a querela di falso, equiparando così il documento informatico sottoscritto con firma digitale alla scrittura privata sottoscritta con firma autografa.

3.3 Firma Digitale e Firma autografa a confronto

La firma digitale è la versione informatica della firma autografa apposta in calce a un documento cartaceo. Mediante essa si possono firmare documenti predisposti in formato elettronico con la possibilità, per chi riceve il documento, di verificarne la paternità e l'integrità, potendo risolvere eventuali dispute e contenziosi in caso di abusi informatici. Le principali caratteristiche e differenze tra le due tipologie di firme sono:

	FIRMA CONVENZIONALE	FIRMA DIGITALE
CREAZIONE	manuale	mediante algoritmo di creazione
APPOSIZIONE	sul documento: la firma è parte integrante del documento	come allegato: il documento firmato è costituito dalla coppia (documento, firma)
VERIFICA	confronto con una firma autenticata: metodo insicuro	mediante algoritmo di verifica pubblicamente noto: metodo sicuro
DOCUMENTO COPIA	distinguibile	indistinguibile
AUTOMAZIONE DI PROCESSI	non possibile	possibile

Il concetto di firma elettronica è stato ufficialmente introdotto nella definizione della direttiva n. 93/1999/CE. Obiettivo del legislatore comunitario è stato

quello di regolamentare i meccanismi di autenticazione della persona fisica che opera in un contesto di commercio elettronico e che, connessa alla rete, interagisce con una controparte garantendo differenti livelli di fiducia nell'autenticazione della propria persona in base alla tipologia delle operazioni in corso.

3.4 Come ottenere la Firma Digitale: i Certificatori

Per poter utilizzare la firma digitale è necessario possedere un apposito documento, il Certificato, che confermi le generalità dell'utente. Il certificato è un documento elettronico, contenente informazioni relative al titolare e la chiave pubblica di firma del Titolare. E' il risultato di una apposita procedura di certificazione che garantisce la corrispondenza biunivoca tra una chiave pubblica ed il soggetto a cui essa appartiene. Affinché i soggetti possano riporre completa fiducia nei certificati digitali e nei dati in essi contenuti, occorre che una "terza parte fidata" - il Certificatore - garantisca l'affidabilità dei dati contenuti nel certificato, occupandosi quindi del suo rilascio e pubblicazione su un apposito registro accessibile *online*. La "certificazione" è quella "procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca *tra* chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni". La procedura di certificazione, pertanto, ha per oggetto la chiave pubblica, la quale è idonea a cifrare i documenti informatici. È opportuno non confondere tale procedura con attività collegate quali il *key escrow* e la *key recorery*. Con la prima locuzione si intende la comunicazione della propria chiave privata a dei soggetti. generalmente pubblici, i quali hanno il compito di monitorare le comunicazioni

telematiche. Come si è visto precedentemente la crittografia assicura la riservatezza delle comunicazioni telematiche e organizzazioni criminali potrebbero avvalersi di tali strumenti software per comunicare indisturbati informazioni illegali. Si pone, pertanto, un'esigenza di ordine pubblico e di sicurezza pubblica che si pensava di risolvere con il monitoraggio delle chiavi private di cifratura, ma ben presto si è rinunciato allo strumento per le forti critiche maturate legate alla violazione della privacy dei titolari delle informazioni riservate. Procedura più complessa è la *key recovery,* la quale consente, sempre ad istituzioni autorizzate, di ricostruire su richiesta la chiave privata dal sistema di crittazione. Anche tale sistema, però, è discutibile in quanto la possibilità di risalire da un documento informatico cifrato alla corrispondente chiave privata pone il problema di assicurare la provenienza della chiave privata dal suo legittimo proprietario, quindi la paternità del documento stesso. Si consideri, infatti, che tale procedura informatica ben potrebbe essere effettuata da soggetti sufficientemente preparati da un punto di vista informatico (si pensi agli *hacker*, *cracker*).

Le principali attività del Certificatore sono le seguenti:

- verificare ed attestare l'identità del richiedente;
- stabilire il termine di scadenza dei certificati, ed il periodo di validità delle chiavi in funzione della loro "robustezza " e degli usi per i quali sono impiegate;
- emettere e pubblicare il certificato, in un archivio pubblico gestito dallo stesso Certificatore;
- revocare o sospendere i certificati.

I certificatori, per l'attuale normativa, sono accreditati presso il Centro nazionale per l'informatica nella pubblica amministrazione ed iscritti in un apposito elenco. Per la legge italiana il Certificatore deve provvedere a verificare l' identità del soggetto che richiede il certificato attraverso procedure appositamente definite.

Il richiedente deve fornire all'Ente di Certificazione la documentazione utile per accertare la sua identità;

Il Certificatore, a sua volta, fornisce al richiedente un codice identificativo univoco;

A seguito della generazione delle chiavi asimmetriche, quella privata da mantenere segreta e quella pubblica da rendere disponibile per la verifica, quest'ultima chiave viene inviata al Certificatore per l'emissione del certificato;

Il Certificatore, infine, genera e pubblica il certificato che contiene i dati del Titolare e la sua chiave pubblica che i destinatari utilizzano per la verifica della firma.

3.5 La Firma Digitale: Il Funzionamento

La prima e più importante differenza nell'uso dei due metodi è che il documento firmato con la penna resta perfettamente leggibile, mentre quello firmato digitalmente cambia il suo stato, la sua forma, e richiede un programma specializzato per la sua apertura.

La firma digitale è un processo matematico che permette di criptare una rappresentazione univoca del file, detta "impronta", e di inserirla nel file stesso trasformandolo in un nuovo tipo di file. Questa in particolare è la caratteristica che va ben compresa: il risultato del processo di firma digitale di un file è un altro file, di formato diverso. Ad esempio il file in formato Microsoft Word "Documento.doc", al termine del processo di firma diventa il file 'Documento.doc.p7m'. L'estensione 'p7m' indica che il file non è più un documento Microsoft Word e quindi non può più essere aperto da questo programma. Per poterlo leggere è necessario l'uso di un nuovo programma, facilmente reperibile su internet, prodotto da vari autori. Questo programma ha

lo scopo di estrarre nuovamente il file originale e di confermare l'autenticità dell'autore del documento.

Attenzione quindi: il file firmato digitalmente non può essere letto con i sistemi oggi comunemente diffusi.

Se, ad esempio, decidiamo di adottare il formato Portable Document Format (PDF) per pubblicare ed inviare i nostri documenti è perché si tratta di un formato ormai capillarmente diffuso che garantisce la leggibilità del documento presso il destinatario. In altre parole non dobbiamo preoccuparci di accordarci con lui per essere certi che sarà in grado di leggere il nostro file. Ma il file firmato non è più in formato PDF, è in formato 'p7m', uno standard in effetti, ma ancora poco diffuso. Molti destinatari del nostro documento non sapranno come aprire il file e saranno costretti a procurarsi un prodotto che sia in grado di farlo. Va detto che lo scopo di questa trasformazione non è nascondere il contenuto del file, tutt'altro: chiunque potrà aprire ed estrarre il file originale ed infine consultarlo, ma il nuovo formato è una necessaria trasformazione per aggiungere le informazioni che garantiscono l'originalità del file e la sua provenienza.

Come abbiamo visto la firma digitale è un processo matematico che può essere così sintetizzato.

1) Creazione dell'impronta del documento: attraverso un algoritmo detto 'algoritmo di Hash' (Secure Hash Algoritm, SHA-1) è possibile estrarre un numero di lunghezza fissa (160 bit) che ha la caratteristica di rappresentare univocamente il nostro documento. Se cambiamo anche una sola virgola al documento anche il numero che lo rappresenta cambierà. Questo numero è detto "impronta" del file. Le due caratteristiche importanti sono:

    a) l'impronta rappresenta il file, se il file cambia l'impronta cambia;

b) è un numero.

2) Firma dell'impronta: un altro algoritmo matematico permette di criptare l'impronta (che è un numero) con un altro numero, la chiave privata. Questa operazione è molto semplice da effettuare, ma è computazionalmente molto difficile effettuare l'operazione inversa, cioè ricavare la chiave privata. L'impronta così criptata è sicura e non può essere alterata. La chiave privata viene creata sempre in coppia con un altro numero, la chiave pubblica. Quest'ultima permette di estrarre l'impronta criptata, ma non di criptarla.

3) Creazione del nuovo formato di file. Questa operazione può essere immaginata come la creazione di una sorta di busta all'interno della quale trovano posto:

a) il file originale;

b) l'impronta firmata;

c) la chiave pubblica;

d) il certificato dell'autore.

Quest'ultimo è una vera e propria carta d'identità elettronica e viene rilasciata da una autorità preposta.

Vediamo ora cosa deve fare il destinatario per sapere se il file è originale o se è stato manomesso. Il principio consiste nell'estrarre il file originale e creare una nuova impronta che poi confronteremo con quella criptata contenuta nella busta: se le due impronte coincidono il file è intonso. In sintesi:

1) Estrazione del file originale dalla busta;

2) Creazione di un' impronta attraverso l'applicazione dell'algoritmo SHA-1.
3) Estrazione dell'impronta criptata con la chiave pubblica, anch'essa contenuta nella busta.
4) Confronto delle due impronte.

Queste operazioni vengono svolte da programmi specializzati per la firma e la verifica dei documenti che vengono distribuiti gratuitamente su internet dalle stesse autorità che rilasciano i certificati e le chiavi private e pubbliche per la firma digitale.

Ma chi garantisce l'inviolabilità dei certificati e dalla chiave privata? Le autorità di cui abbiamo parlato, preposte al rilascio dei certificati per firma digitale, installano questi ultimi su supporti che non possono essere contraffati o alterati. Questi supporti sono *smart card* o *token USB*. L'operazione di criptaggio dell'impronta, la firma digitale, avviene attraverso questi supporti: il programma dopo aver estratto l'impronta la invia al supporto che applica la chiave privata e restituisce l'impronta firmata. Il supporto si comporta come una cassaforte intelligente, che non permette l'uscita dei suoi valori, ma è in grado di operare al suo interno.

3.6 Campi di applicazione

La firma digitale trova la sua applicazione principalmente come metodo per snellire l'attività burocratica all'intero della pubblica amministrazione.

Conoscendo le condizioni di difficoltà in cui si trova, il legislatore ha pensato di introdurre l'utilizzo di sistemi informatici per la trasmissione e per l'archiviazione dei documenti informatici, sostituendo allo stesso tempo questi ultimi all'ingombrante documento cartaceo.

Ci troviamo così di fronte ad un ammodernamento di tutto il settore pubblico che porterà enormi vantaggi, sia per gli utenti che si rapportano quotidianamente con il settore pubblico, che per gli stessi dipendenti che vedranno semplificate le normali procedure di gestione.

Da oggi è possibile per l'impresa ammodernare il proprio sistema informatico gestendo in modo completo documenti digitali purché firmati elettronicamente.

L'operatore economico può quindi scambiare corrispondenza digitale ufficiale, emettere ed archiviare documenti digitali validi, ma anche trasmetterli ad altri operatori economici, sia in Italia sia in quei paesi dove sia riconosciuta la firma elettronica. Inoltre può operare l'archiviazione sostitutiva di documenti originari su supporto cartaceo, previa autenticazione degli eventuali documenti unici originali.

Di sicuro all'operatore economico, con le nuove opportunità stabilite dalla legge sulla firma elettronica, non converrà trascurare il proprio ammodernamento tecnologico poiché riceverà da altri soggetti (in primis dalla Pubblica Amministrazione.) documenti elettronici firmati elettronicamente, e quindi dovrà provvedere ad archiviare tali documenti in modo sicuro ed efficiente.

4 L’azienda e la firma digitale

4.1 L’utilità e i vantaggi tratti dall’utilizzo della firma digitale

Un’azienda che si è trovata di fronte all’obbligo di utilizzare la firma digitale per certificare i propri documenti da inviare agli archivi della pubblica amministrazione ha sicuramente giovato dello snellimento di tutte quelle situazioni burocratiche che si venivano a creare ogni volta che ci si rapportava con la realtà pubblica.

Gli operatori economici possono quindi trarre grandi benefici dal processo di digitalizzazione proprio e della Pubblica Amministrazione.

La legge non si limita a rendere legale la firma elettronica, ma si preoccupa di dare validità ai supporti elettronici d’archiviazione e a riconoscere legali i mezzi di trasmissione elettronici. Per cui da oggi è possibile per l’impresa ammodernare il proprio sistema informatico gestendo in modo completo documenti digitali purché firmati elettronicamente.

L’operatore economico può quindi scambiare corrispondenza digitale ufficiale, emettere ed archiviare documenti digitali validi, ma anche trasmetterli ad altri operatori economici. Inoltre, può operare l’archiviazione sostitutiva di documenti originari su supporto cartaceo, previa autenticazione degli eventuali documenti unici originali. Non ci dobbiamo, infatti, illudere che la digitalizzazione faccia d’incanto sparire tutta la documentazione cartacea, sicuramente si avranno flussi digitali e cartacei contemporaneamente almeno per un tempo abbastanza lungo.

Di sicuro all'operatore economico, con le nuove opportunità stabilite dalla legge sulla firma elettronica, non converrà trascurare il proprio ammodernamento tecnologico poiché riceverà da altri soggetti (in primis dalla Pubblica Amministrazione.) documenti elettronici firmati elettronicamente, e quindi dovrà provvedere ad archiviare tali documenti in modo sicuro ed efficiente.

Sarà quindi possibile ridurre drasticamente i costi per la tenuta di archivi cartacei: mi riferisco in modo particolare ai costi per i locali, ai costi per il materiale cartaceo ma anche per la semplice consultazione di un documento passato.

4.2 Gli svantaggi e i costi

Nel considerare gli effetti di un processo di ammodernamento dei sistemi di trasmissione e autenticazione dei documenti aziendali non possiamo tralasciare quelli che sono gli svantaggi e i costi per poter utilizzare questo sistema dalle potenzialità enormi.

Parlando di svantaggi ci si riferisce in modo particolare alla necessità di garantire sempre la piena contabilità dei documenti informatici con i sistemi operativi attuali e futuri: è quindi necessario nominare un incaricato che si preoccupi di fornire sempre gli aggiornamenti necessari per avere la piena disponibilità in ogni momento dei file necessari. Oltre agli aggiornamenti dei file è anche necessario che l'incaricato si preoccupi e certifichi che i dati aggiornati non abbiano subito modifiche o che ci sia stata una perdita di dati tale da rendere inutilizzabile o peggio da fornire informazioni errate.

Nonostante i rischi legati all'archiviazione informatica rispetto a quella cartacea si differenziano notevolmente, dobbiamo sempre considerare valide le attenzioni poste in essere nei confronti di eventuali incendi o allagamenti che andrebbero a danneggiare in modo irreparabile i documenti archiviati in supporti informatici.

Risulta chiaro da queste prime osservazioni che i rischi legati a queste nuove procedure vanno considerati in modo consapevole per non incorrere in problemi più grandi.

Tra i primi costi che un'impresa dovrà affrontare per sfruttare le nuove tecnologie c'è sicuramente quello per l'acquisto o l'aggiornamento dell'hardware e del software necessario per svolgere tutte le funzioni informatiche. È chiaro che tutto dipenderà dalle dimensioni aziendali, ma per le grandi realtà produttive sarà necessario automatizzare i processi contabili. Per quanto riguarda la firma digitale un kit di firma comprendente smart-card, lettore di smart-card e certificato di firma è stato distribuito a tutte le imprese gratuitamente: chi vuole avere la possibilità, per necessità o comodità, di dotare più dipendenti di smart-card per firmare digitalmente i propri documenti deve sborsare 100 €[1] per ogni smart-card aggiuntiva.

Tra costi che si differenziano tra l'archiviazione cartacea e digitale c'è sicuramente la tenuta dell'archivio, che per le imprese di dimensioni considerevoli richiedevano grandi ambienti talvolta di dimensioni maggiori rispetto a quelle delle sale dove si svolge l'attività vera e propria.

L'archiviazione informatica avviene invece su supporti magnetici che riducono lo spazio occupato in maniera considerevole ma per avere la possibilità di una consultazione rapida ed efficace è necessario dotarsi di potenti calcolatori collegati a dei server[2] interni. Oppure in caso di costi troppo elevati è possibile

[1] Fonte: "www.infocamere.it"
[2] Enorme contenitore di dati da consultare tramite postazione informatica

servirsi di web-server, che svolgono la stessa funzione dei server interni ma non sono fisicamente presenti in azienda ma si trovano in un altro luogo, ma collegato alla rete aziendale tramite internet.

Quando si utilizza questo tipo di servizio è importante verificare la solidità degli accessi da parte di personale non autorizzato o addirittura malintenzionato che potrebbe prelevare informazioni riservate con lo scopo di creare un danno all'impresa stessa.

4.3 La sicurezza nello scambio di informazioni societarie

Dall'analisi appena svolta risulta quindi chiaro che l'informatizzazione delle procedure aziendali risulta assolutamente importante per lo snellimento delle normali operazioni di routine ma allo stesso tempo risulta più difficile garantire la sicurezza nello scambio delle informazioni aziendali.

È proprio per superare queste difficoltà che è stata introdotta la firma digitale come strumento di sicurezza nello scambio di informazioni societarie; basta pensare che con l'obbligo di presentare il bilancio in forma elettronica e non più cartacea viene a mancare tutta quella serie di controlli documentali e anagrafici per cui in un successivo controllo si era certi dell'identità di che aveva consegnato il bilancio stesso. Lo stesso vale anche per la controparte alla quale non rimarrebbe traccia dell'avvenuta consegna.

Oggi grazie alla firma digitale è possibile verificare l'identità di chi firma grazie al "Certificato" emesso da apposito ufficio, ma anche che il documento non sia stato contraffatto nel trasferimento perché ad ogni modifica corrisponde una serie binaria diversa[3]. Oltre a questo, un servizio aggiuntivo offerto dal sistema

[3] Grazie all'utilizzo della funzione di Hash

firma digitale è quello della "marca temporale" o "time stamping" che permette di certificare l'orario e la data esatti di invio del documento: questo svolge la duplice funzione sia per colui che invia che per chi riceve in caso di contenzioso.

Importante a questo punto è la sicurezza delle reti che si utilizzano per lo scambio di informazioni: è quindi fondamentale dotarsi di una LAN[4] protetta da possibili intrusioni esterne che potrebbero carpire informazioni riservate. Risulta necessaria l'installazione di un *firewall* che neghi l'accesso a tutti i servizi tranne a quelli autorizzati e che filtri le comunicazioni provenienti dalla linea al fine di proteggere la LAN.

5 La Revisione e la Firma Digitale

5.1 L'importanza della firma digitale per la revisione aziendale

La firma digitale riveste un ruolo fondamentale per la revisione in quanto è possibile risalire con assoluta certezza al creatore di un documento informatico ma è anche possibile, attraverso la tecnica della marca temporale stabilire con assoluta certezza l'ora e la data del documento.

La firma digitale è quindi un vero e proprio strumento della revisione al fine di garantire l'autenticità di una evidenza.

Importante aspetto è quello della certificazione del creatore del messaggio che la Direttiva 1999/93/CEE[5] allarga a tutti gli stati membri dell'Unione l'obbligo

[4] Local Area Network (rete di telecomunicazione informatica locale)
[5] Articolo 7 paragrafo 1

di riconoscere la firma digitale emessa in altro stato purché rilasciata da certificatore riconosciuto.

Con queste premesse è chiaro che in caso di ritrovamento di documenti falsificati all'interno della contabilità di un impresa il revisore potrà dichiararlo nelle sue carte di lavoro e porterà a prova la non presenza della firma digitale applicata su quel documento.