L'archiviazione elettronica dei documenti

Introduzione

Grazie alle normative pubblicate negli ultimi anni in relazione all'archiviazione ottica documentale ed alla firma digitale:

- Decreto Legislativo n. 52/2004 - Regolamento fattura elettronica
- Decreto Legislativo n. 10/2002 - Firma digitale
- Codice Amministrazione Digitale (*ora DECRETO LEGISLATIVO 30 dicembre 2010, n. 235 - Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69, n.d.a.)*

è possibile, per tutte le organizzazioni, gestire qualsiasi tipo di documento interno che abbia valore legale (documenti contabili, elaborati progettuali, contratti, offerte, ecc.) solamente su supporto elettronico. Questo significa che il documento avente valore legale è quello informatico, eventuali stampe prodotte da esso possono essere cestinate quando non servono più!

Le soluzioni, per le aziende che vogliono avvalersi di questa opportunità per ridurre gli spazi ed i costi per l'archiviazione su supporto cartaceo, sono estremamente ampie. Si parte dalla piccola organizzazione che - disponendo di firma digitale qualificata con marca temporale per il Legale Rappresentante e per tutti i responsabili che hanno potere di firmare ed approvare documenti (ad es. Responsabile Amministrativo, Responsabile Commerciale...) - si auto-gestisce l'archiviazione elettronica documentale firmando digitalmente i documenti emessi e quelli ricevuti, dopo averli scannerizzati, in formato PDF. E si finisce alla grande azienda che si serve di un fornitore esterno che - in outsourcing e via internet - gli gestisce l'intero archivio di documenti elettronici.

Il documento informatico

Ma cos'è il documento informatico? La legge n. 59 del 1997 - articolo 15 – stabilisce che "gli atti, dati e documenti, formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge". Il DPR 445 del 28 dicembre 2000 ha fissato i requisiti che il documento informatico inteso come "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" deve rispettare per avere pieno valore legale.

Con il termine documento cartaceo si intende invece sia il supporto, sia il contenuto che in esso viene rappresentato; tramite la sottoscrizione autografa viene identificata la persona che ne assume la paternità, se ne sancisce l'autenticità ed il sottoscrittore stesso fa propri i contenuti rappresentati nel documento. Un documento informatico può essere invece modificato o riprodotto infinite volte, ottenendo copie assolutamente identiche all'originale. Il contenuto è svincolato dal supporto. Per restituire al documento informatico gli stessi requisiti assolti dalla sottoscrizione autografa di un documento cartaceo occorre, quindi, un tipo di autenticazione come la firma digitale, che attribuisca al contenuto del documento informatico piena validità legale.

La firma digitale garantisce, nei confronti dei documenti informatici, la presenza degli stessi requisiti che la firma autografa garantisce nei confronti dei documenti cartacei. Grazie alla tecnologia della firma digitale e per mezzo del sistema a "chiavi pubbliche", il destinatario del documento ha la garanzia di disporre di un testo integro e proveniente da una fonte ben precisa. La sequenza di simboli che chiamiamo firma digitale, generata da algoritmi matematici, si riferisce univocamente ad i contenuti di un preciso documento, la modifica anche di un solo carattere sarebbe immediatamente rilevata al momento della verifica.

Altre definizioni importanti sono le seguenti (D.P.C.M. 13/1/2004 (G.U. nr 98 del 27/4/2004):

- **Riferimento temporale** = "Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici"
- **Marca temporale** = "Evidenza informatica che consente la validazione temporale"
- **Validazione temporale** = "Il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici , un riferimento temporale opponibile a terzi".

Per fornire adeguata fiducia - anche dal punto di vista legale - i documenti informatici devono essere non modificabili e devono essere emessi garantendo l'attestazione temporale (marca temporale), l'integrità e l'autenticità (tramite sottoscrizione elettronica con firma digitale qualificata).

Dunque la firma digitale, associata alla marca temporale, è in grado di attestare la completa validità di un documento informatico e, quindi, permette di poter rinunciare al supporto cartaceo.

L'archiviazione ottica sostitutiva dei documenti si occupa proprio di questo: dare valenza ai documenti informatici aventi determinate caratteristiche al fine di sostituire pienamente la copia cartacea, eliminandola fisicamente dagli archivi.

I documenti - a valenza fiscale - che si possono smaterializzare sono i seguenti:

- Fatture, lettere e telegrammi ricevuti (Art. 2220 codice civile)
- Copie delle fatture, delle lettere e dei telegrammi spediti (Art. 2220 codice civile)
- Libro giornale e libro degli inventari (Art. 2215 codice civile e Art. 14 comma 1, lettera a, D.P.R. 600/1973)
- Registri prescritti ai fini dell'IVA (Art. 14 comma 1, lettera b, D.P.R. 600/1973)
- Scritture ausiliarie nelle quali devono essere registrati gli elementi patrimoniali e reddituali, raggruppati in categorie omogenee, in modo da consentire di desumerne chiaramente e distintamente i componenti positivi e negativi che concorrono alla determinazione del reddito (Art. 14 comma 1 , lettera c , D.P.R. 600/1973)
- Scritture ausiliarie di magazzino (Art. 14 comma 1, lettera d, D.P.R. 600/1973)
- Registro dei beni ammortizzabili (Art. 16 , D.P.R. 600/1973)
- Libro dei soci
- Libro delle obbligazioni
- Libro delle adunanze e delle deliberazioni delle assemblee
- Libro delle adunanze e delle deliberazioni del consiglio di amministrazione o del consiglio di gestione
- Libro delle adunanze e delle deliberazioni del collegio sindacale ovvero del consiglio di sorveglianza o del comitato per il controllo sulla gestione
- Libri sociali obbligatori (art.2421 c.c.)
- Libro delle adunanze e delle deliberazioni del comitato esecutivo
- Libro delle adunanze e delle deliberazioni delle assemblee degli obbligazionisti
- Libro degli strumenti finanziari emessi ai sensi dell'art.2447-sexies
- Bilancio di esercizio (art.2423 c.c.)
- Stato patrimoniale (art.2424 c.c.)

- Conto economico (art.2425 c.c.)
- Nota integrativa (art.2427 c.c.)
- Relazione sulla gestione (art.2428 c.c.)
- Relazione dei sindaci (art.2429 c.c.)
- Relazione dei revisori contabili (D.Lgs. n.58 del 1998)
- Dichiarazione dei redditi, Irap, Iva e sostituti (DPR n.322 del 22 luglio 1998)
- Documento di trasporto (DPR n. 472 del 14 agosto 1996)
- Giornale di fondo elettronico degli scontrini fiscali-(D.M. 23 marzo 1983)
- Libro matricola e libro paga (art.21 DPR 600/73)

Naturalmente, oltre ai documenti a carattere amministrativo, può essere utile gestire in formato elettronico anche altri documenti che vengono conservati, quali offerte, ordini, contratti, elaborati progettuali, rapporti, ecc..

La firma digitale e la marca temporale

Ma come avviene l'archiviazione ottica sostitutiva? Come funzionano la firma digitale e la marca temporale?

La **Firma Digitale** è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti tradizionali. La differenza tra firma autografa e firma digitale è che la prima è legata alla caratteristica fisica della persona che appone la firma, vale a dire la grafia, mentre la seconda al possesso di uno strumento informatico e di un PIN di abilitazione, da parte del firmatario

La firma digitale 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.

La procedura di marcatura temporale serve ad attestare l'esistenza di un documento informatico rispetto ad una data certa; è inoltre essenziale per evitare che documenti redatti utilizzando certificati revocati o scaduti vengano utilizzati a scopi fraudolenti.

Tale procedura prevede la generazione di una marca temporale, da parte di un sistema dedicato, che indica l'ora e il giorno certi in per cui il documento informatico è stata emessa la marca che ne attesta l'esistenza.

L'infrastruttura a chiave pubblica è un insieme di apparati, regole di sicurezza, procedure operative e servizi che rendono possibile la gestione affidabile ed efficiente di applicazioni per la firma digitale, l'autenticazione, la protezione della riservatezza e la marcatura temporale dei documenti informatici. Si basa sulla crittografia asimmetrica a chiave pubblica e svolge le seguenti funzioni principali.

- generazione e distribuzione di coppie di chiavi digitali;
- verifica dell'identità dei richiedenti i certificati;
- emissione e pubblicazione dei certificati;
- gestione del ciclo di vita dei certificati (sospensione, revoca, rinnovo).

La chiave privata utilizzata per la firma dei documenti informatici deve essere conservata in maniera sicura e segreta dal Titolare che ne è responsabile, per tale ragione le smart card crittografiche, opportunamente protette da PIN di accesso, sono state individuate come un valido supporto, in quanto oltre a permettere la generazione delle chiavi al loro interno e l' applicazione della firma digitale, dispongono di sistemi di sicurezza che impediscono l'esportazione e la copia della chiave privata, fuori dalla smart card in cui è stata generata.

La diffusione della chiave pubblica, invece, consente a tutti i possibili destinatari dei documenti informatici di disporre della chiave necessaria per la verifica dei documenti. Per individuare in maniera sicura il sottoscrittore del documento, deve essere legata in maniera certa al titolare della corrispondente chiave privata.

Dispositivo di firma

Per la normativa italiana con dispositivo di firma si intende "un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto la chiave privata e generare al suo interno le firme digitali."

Uno degli strumenti che è possibile utilizzare come dispositivo di firma è la smart card crittografica. Anche altri dispositivi, quali token USB possono fungere da dispositivo di firma con i medesimi requisiti legali, ma con maggiore praticità (non necessitano di lettore apposito come per le smart card in quanto sono direttamente collegabili al PC).

Il certificato digitale

Il certificato è il mezzo di cui dispone il destinatario per avere la garanzia sull'identità del suo interlocutore e per venire in possesso della chiave pubblica di quest'ultimo.

Per tale ragione il certificato contiene, oltre la chiave pubblica per la verifica della firma, anche i dati del titolare; è garantito e firmato da una "terza parte fidata": il certificatore.

Per la normativa italiane deve contenere almeno le seguenti informazioni:

- numero di serie del certificato
- ragione e denominazione sociale del certificatore
- codice identificativo del titolare presso il certificatore
- nome, cognome e data di nascita ovvero ragione o denominazione sociale del titolare
- valore della chiave pubblica
- algoritmi di generazione e verifica utilizzabili
- inizio e fine del periodo di validità delle chiavi
- algoritmo di sottoscrizione del certificato

Il certificato in formato X.509, contiene in uno standard riconosciuto, una serie di campi per dati obbligatori ai quali possono essere aggiunte ulteriori estensioni per riportare informazioni aggiuntive.

La Posta Elettronica Certificata (PEC)

L'e-mail è ormai lo strumento di comunicazione elettronica più utilizzato per lo scambio di comunicazioni. La posta elettronica o e-mail è un mezzo di comunicazione in forma scritta via Internet. Il principale vantaggio dell'e-mail è l'immediatezza. I messaggi possono includere testo, immagini, audio, video o qualsiasi tipo di file.

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici. "Certificare" l'invio e la ricezione - i due momenti fondamentali nella trasmissione dei documenti informatici - significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione. Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale. Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte venga conservata per un periodo di tempo definito a cura dei gestori, con lo stesso valore giuridico delle ricevute.

- il DPR 11 febbraio 2005, n. 68 (G.U. 28 aprile 2005, n. 97) disciplina le modalità di utilizzo della Posta Elettronica Certificata (PEC) non solo nei rapporti con la PA, ma anche tra privati cittadini. In sintesi le novità contenute nel provvedimento:

- nella catena di trasmissione potranno scambiarsi le e-mail certificate sia i privati, sia le PA. Saranno i gestori del servizio (art. 14), iscritti in apposito elenco tenuto dal Cnipa (che verificherà i requisiti soggettivi ed oggettivi inerenti ad esempio alla capacità ed esperienza tecnico-organizzativa, alla dimestichezza con procedure e metodi per la gestione della sicurezza, alla certificazione ISO9000 del processo), a fare da garanti dell'avvenuta consegna.

- per iscriversi nell'elenco dovranno possedere un capitale sociale minimo non inferiore a un milione di euro e presentare una polizza assicurativa contro i rischi derivanti dall'attività di gestore;

- i messaggi verranno sottoscritti con la firma digitale avanzata che dovrà essere apposta sia sulla busta, sia sulle ricevute rilasciate dai gestori per assicurare l'integrità e l'autenticità del messaggio;

- i tempi di conservazione: i gestori dovranno conservare traccia delle operazioni per 30 mesi;

- i virus: i gestori sono tenuti a verificare l'eventuale presenza di virus nelle e-mail ed informare in caso positivo il mittente, bloccandone la trasmissione (art. 12);

- le imprese, nei rapporti intercorrenti, potranno dichiarare l'esplicita volontà di accettare l'invio di PEC mediante indicazione nell'atto di iscrizione delle imprese.

Le modalità operative per la gestione della PEC possono essere approfondite nei seguenti documenti:

1. Il Decreto Ministeriale contenente le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" (tutti i requisiti tecnico-funzionali che devono essere rispettati dalle piattaforme utilizzate per erogare il servizio) è stato pubblicato nella G.U. del 15 novembre 2005, n. 266. Il Cnipa effettuerà le attività di vigilanza e controllo assegnategli dalla norma e, con un apposito Centro di competenza, supporterà le PA ai fini dell'introduzione della PEC nei procedimenti amministrativi.

2. La Circolare Cnipa del 24 novembre 2005 n.49, pubblicata nella G.U. del 5 dicembre 2005, n. 283, recante le modalità per presentare domanda di accreditamento nell'elenco pubblico dei Gestori di PEC da parte dei soggetti pubblici e privati che intendono esercitare tale servizio.

In conclusione le novità introdotte dalla legislazione permetteranno di velocizzare notevolmente le attività delle organizzazioni di ogni tipo e di ridurre gli spazi dedicati all'archiviazione cartacea e - quindi - di ridurre i costi.

Il tutto ruota attorno agli strumenti sopra descritti: firma digitale (per assicurare l'autenticazione di un documento), la marca temporale (per attestare la data e l'ora di emissione/approvazione di un documento) e la posta elettronica certificata, che unisce gli strumenti precedenti all'e-mail per garantire la spedizione di una lettera.

Le organizzazioni che meglio potranno beneficiare di questi strumenti sono quelle che hanno un elevato valore e know-how aziendale gestito attraverso documenti prodotti informaticamente e che devono attestare la validità degli stessi documenti anche per soddisfare requisiti di legge e garantire nel tempo le registrazioni sull'attività svolta. Tra esse possiamo indicare, a titolo d'esempio, gli studi professionali (commercialisti, avvocati, notai), le società di ingegneria, le banche, le assicurazioni, le imprese di costruzione e tutte le realtà che operano nel settore degli appalti pubblici, soprattutto perché l'invio di documentazione per partecipare a gare pubbliche può essere effettuato via e-mail.