

ASPETTI GENERALI SUL PROTOCOLLO INFORMATICO

Chi ha l'obbligo di realizzare la gestione informatica dei documenti ?

Tutte le pubbliche amministrazioni provvedono, entro il 1 gennaio 2004, a realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi.

Ai sensi dell'articolo 1, comma 2 del decreto legislativo 3.2.1993, n. 29, sono amministrazioni pubbliche:

- le amministrazioni dello Stato
- le aziende e le amministrazioni dello Stato ad ordinamento autonomo
- le regioni, le province, i comuni, le comunità montane
- i consorzi e le associazioni dei predetti enti
- gli istituti autonomi case popolari
- le camere di commercio, industria, artigianato e agricoltura, e le loro associazioni
- gli enti pubblici non economici
- gli istituti e le scuole di ogni ordine e grado e le istituzioni educative
- le istituzioni universitarie
- le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale

Quali sono gli obiettivi di carattere generale realizzabili attraverso la gestione informatica dei documenti?

Le disposizioni sulla gestione informatica dei documenti consentono di:

- accrescere l'efficienza delle amministrazioni attraverso l'eliminazione dei registri cartacei, la diminuzione degli uffici di protocollo e la razionalizzazione dei flussi documentali;
- migliorare la trasparenza dell'azione amministrativa tramite strumenti che rendano possibile un effettivo esercizio del diritto di accesso alla documentazione amministrativa da parte dei soggetti interessati.

Ciascuna amministrazione deve:

- definire un adeguato piano di sviluppo dei sistemi informativi automatizzati
- individuare le aree organizzative omogenee e i relativi uffici
- istituire i servizi per la gestione informatica dei documenti, dei flussi documentali e degli archivi
- nominare i responsabili di tali servizi
- redigere e adottare il manuale di gestione del sistema documentario
- introdurre un sistema informatico per la gestione documentale che preveda almeno il nucleo minimo del protocollo informatico.

ASPETTI GENERALI SUL PROTOCOLLO INFORMATICO

Cosa si intende per nucleo minimo del protocollo informatico?

Per nucleo minimo s'intende la componente del sistema di protocollo informatico in grado di effettuare le operazioni di registrazione, segnatura e classificazione dei documenti. Tali operazioni costituiscono le operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni.

In cosa consiste, praticamente, l'operazione di registrazione di protocollo?

Le disposizioni sulla gestione informatica dei documenti consentono di:

- numero di protocollo e data di registrazione del documento spedito, generati automaticamente dal sistema
- mittente (per i documenti ricevuti) o destinatario (per i documenti spediti)
- oggetto del documento
- impronta del documento informatico, se trasmesso per via telematica

La registrazione di tali informazioni deve avvenire in forma non modificabile. Inoltre, se disponibili all'atto della registrazione, devono essere memorizzati anche:

- numero di protocollo e data di registrazione del documento ricevuto.

Cosa è l'impronta di un documento informatico?

L'impronta del documento è una sequenza di lunghezza fissa simboli binari ottenuta attraverso l'applicazione di una specifica funzione di calcolo che garantisce una associazione biunivoca (a meno di eccezioni statisticamente irrilevanti) tra l'impronta stessa ed il documento originatore

Perché si deve registrare anche l'impronta?

Perché attraverso la registrazione dell'impronta del documento informatico in modo non modificabile si ha la certezza di aver registrato esattamente uno specifico documento (integrità del documento), rendendo in tal modo il sistema di protocollo più sicuro rispetto alla sua funzione di sistema di certificazione interna degli eventi di transito dei documenti attraverso i confini di una AOO. Lo stesso livello di garanzia non è ottenibile per i documenti cartacei per i quali si ricorre alla registrazione dell'oggetto e del mittente o destinatario effettuata contemporaneamente alla operazione di segnatura. Nella trasmissione di un documento informatico non è necessario inviare anche l'impronta in quanto questa può essere calcolata dal ricevente (purchè nota la funzione di calcolo). La cosa importante è che l'impronta venga univocamente e permanentemente associata ai dati di protocollo.

Cosa è la segnatura?

La segnatura di protocollo consiste nell'associare in modo permanente e non modificabile delle informazioni al documento. In particolare la segnatura deve contenere per lo meno:

- indicazione o codice dell'amministrazione
- indicazione o codice della AOO
- numero di protocollo
- data di protocollo

A quali documenti si applica la segnatura?

Per i documenti cartacei la segnatura si applica sia ai documenti in ingresso che ai documenti in uscita e deve avvenire contemporaneamente alla operazione di registrazione.

Qual è lo scopo della segnatura?

Lo scopo di una segnatura apposta su un documento cartaceo è quello di mantenere una associazione indissolubile e direttamente leggibile tra il documento stesso e la corrispondente registrazione di protocollo.

Perché registrazione e segnatura devono avvenire contemporaneamente?

L'operazione di segnatura deve avvenire contemporaneamente a quella di registrazione per garantire che ogni registrazione venga eseguita effettivamente a fronte di un documento pervenuto o inviato dalla AOO. In altre parole non deve essere consentito, nel modo più assoluto, che si effettuino registrazioni di protocollo senza disporre del documento a cui la registrazione si riferisce.

Come può applicare, in pratica, la segnatura su un documento cartaceo?

Come può applicare, in pratica, la segnatura su un documento cartaceo? Lo scopo di una segnatura apposta su un documento cartaceo è quello di mantenere una associazione indissolubile e direttamente leggibile tra il documento stesso e la corrispondente registrazione di protocollo.

La segnatura si applica anche sui documenti informatici?

Sì, ma solo sui documenti in uscita ed ha una funzione diversa. Nel caso di un documento informatico la funzione di stabilire un legame indissolubile tra documento e registrazione di protocollo è garantita dalla

presenza dell'impronta del documento nella registrazione stessa. L'altra funzione -propria della segnatura - di rendere accessibili le informazioni di registrazione a partire da un documento, può essere fornita direttamente dal sistema informatico. Se i documenti informatici sono accessibili esclusivamente attraverso l'applicazione che gestisce anche il protocollo allora tale funzione associativa è svolta in modo diretto, se viceversa, i documenti informatici sono gestiti anche da altri sistemi allora il sistema di protocollo dovrà offrire una specifica funzione di ricerca che a partire da un documento informatico fornisca le corrispondenti informazioni di registrazione. Per i documenti informatici la segnatura si applica ai soli documenti in uscita ed ha uno scopo molto più ampio, ovvero consentire la codifica strutturata delle informazioni archivistiche relative al documento inviato, le informazioni sul procedimento amministrativo ed altre informazioni utili al trattamento del documento. La segnatura informatica è codificata per mezzo del linguaggio XML ed è alla base dell'interoperabilità dei sistemi di protocollo informatico in rete.

Quali sono i tempi imposti dalla normativa?

Le pubbliche amministrazioni devono provvedere entro il 1° gennaio 2004 a realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi in conformità alle disposizioni del dpr 445/2000 ed alle disposizioni della legge 31 dicembre 1996, n. 675, nonché dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 e dei relativi regolamenti di attuazione.

Come si può realizzare, in pratica la contemporaneità tra registrazione e segnatura?

Il vincolo di contemporaneità tra le operazioni di registrazione e segnatura stabilisce che le due operazioni siano un'unica operazione informatica, ovvero debbono essere eseguite entrambe con successo entro un breve intervallo di tempo pena l'annullamento degli eventuali risultati intermedi. Il concetto di "breve intervallo" va calato nei diversi contesti organizzativi in cui si colloca il protocollo informatico. In ogni caso il dettaglio della procedura di segnatura, e quindi la valorizzazione dell'intervallo di tempo entro il quale questa deve essere eseguita subito dopo la registrazione, costituiscono elementi da specificare nel manuale di gestione. Un esempio può essere dato dalla segnatura apposta con speciali stampanti di etichette: in questo caso la contemporaneità può essere stabilita con una regola organizzativa interna che impone l'apposizione dell'etichetta entro -ad esempio- un minuto dall'avvenuta registrazione. Il sistema di protocollo potrebbe essere strutturato in modo da chiedere all'operatore conferma dell'avvenuta segnatura e se entro l'intervallo stabilito tale conferma non dovesse essere fornita, il sistema deve annullare automaticamente la registrazione.

La segnatura si applica anche sui documenti informatici?

Sì, ma solo sui documenti in uscita ed ha una funzione diversa. Nel caso di un documento informatico la funzione di stabilire un legame indissolubile tra documento e registrazione di protocollo è garantita dalla presenza dell'impronta del documento nella registrazione stessa. L'altra funzione -propria della segnatura - di rendere accessibili le informazioni di registrazione a partire da un documento, può essere fornita direttamente dal sistema informatico. Se i documenti informatici sono accessibili esclusivamente attraverso l'applicazione che gestisce anche il protocollo allora tale funzione associativa è svolta in modo diretto, se viceversa, i documenti informatici sono gestiti anche da altri sistemi allora il sistema di protocollo dovrà offrire una specifica funzione di ricerca che a partire da un documento informatico fornisca le corrispondenti informazioni di registrazione. Per i documenti informatici la segnatura si applica ai soli documenti in uscita ed ha uno scopo molto più ampio, ovvero consentire la codifica strutturata delle informazioni archivistiche relative al documento inviato, le informazioni sul procedimento amministrativo ed altre informazioni utili al trattamento del documento. La segnatura informatica è codificata per mezzo del linguaggio XML ed è alla base dell'interoperabilità dei sistemi di protocollo informatico in rete.

Quali sono i tempi imposti dalla normativa?

Le pubbliche amministrazioni devono provvedere entro il 1° gennaio 2004 a realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi in conformità alle disposizioni del dpr 445/2000 ed alle disposizioni della legge 31 dicembre 1996, n. 675, nonché dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 e dei relativi regolamenti di attuazione.

Cosa sono le AOO?

Si definisce AOO (Area Organizzativa Omogenea) un insieme di unità organizzative dell'amministrazione che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali. In particolare, all'interno di una AOO esiste un solo servizio di protocollazione dei documenti in entrata ed in uscita, che adotta una unica sequenza numerica per l'attribuzione del numero di protocollo, rinnovata ad ogni anno solare.

Perché istituire una AOO

I principali vantaggi che derivano dalla istituzione delle AOO sono:
riduzione della frammentazione degli uffici di protocollo, e quindi ottimizzazione e riqualificazione dell'uso delle risorse
potenziamento delle capacità di accesso e ricerca alle informazioni e ai documenti stessi
migliore circolazione di informazioni e documenti tra gli uffici
maggiore trasparenza, grazie ad un più razionale accesso alla documentazione amministrativa da parte dei soggetti interessati
migliore organizzazione dell'archivio attraverso l'adozione di un unico piano di classificazione all'interno dell'area.

Come individuare le unità organizzative che compongono una AOO

Una AOO è individuata da un insieme di uffici che, per tipologia di mandato istituzionale, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

Quali criteri adottare per la definizione delle AOO

Per definire al meglio le AOO da istituire, l'amministrazione deve effettuare una analisi della propria struttura organizzativa e il proprio modello funzionale, valutando attentamente alcune variabili come:
il grado di omogeneità degli uffici dal punto di vista delle funzioni svolte
il volume e del flusso dei documenti all'interno dell'amministrazione
la dislocazione geografica delle sedi
la cultura informatica del personale interno
l'esistenza di precedenti sistemi informatici di supporto alla gestione documentale
grado di coerenza dell'attività amministrativa svolta dagli uffici.
L'individuazione delle AOO va effettuata dopo un'attenta analisi di tali informazioni e dopo avere evidenziato le criticità della modalità operativa in essere e gli eventuali vincoli organizzativo-logistici esistenti.

La nascita delle AOO ha effetti sui registri di protocollo intermedi?

Una AOO è individuata da un insieme di uffici che, per tipologia di mandato istituzionale, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentano esigenze di gestione della documentazione in modo unitario e coordinato.

Con le AOO si eliminano i registri di protocollo intermedi: come si fa a tenere traccia delle comunicazioni interne agli uffici della AOO stessa?

L'individuazione delle AOO determina l'eliminazione della frammentazione dei sistemi di protocollo e una riorganizzazione dei flussi documentali: all'interno di ogni area, la certificazione del passaggio dei documenti a valenza esterna (registrazione di protocollo) potrà essere separata dal tracciamento dei passaggi dei documenti all'interno della struttura. Inevitabilmente, ciò determina la necessità di sostituire il rudimentale sistema di tracciamento del flusso documentale (costituito dalla sequenza di successive protocollazioni tra aree interne) con un sistema integrato più evoluto e funzionale alle esigenze dell'amministrazione (posta elettronica interna, sistema di groupware, sistema di workflow, ecc.).
Il fax va protocollato?

Il documento, in quanto tale, è indipendente dal supporto sul quale viene scritto e dal mezzo di trasporto sul quale viene veicolato. Recentemente, l'art. 7, comma 3 del dpr 403/1998 ha stabilito che il fax soddisfa il requisito della forma scritta ed è quindi "documento" a tutti gli effetti di legge: come tale e quindi soggetto a protocollazione. In seguito, pervenuto l'originale, non si dovrà procedere ad una nuova registrazione, ma si dovranno riportare tutti i dati della registrazione del documento pervenuto via fax: si tratta infatti del medesimo documento, anche se pervenuto in tempi e con modalità diverse. Un altro importante motivo di tale procedura risiede nel fatto che la registrazione del fax causa l'avvio dei termini del procedimento amministrativo o dell'affare a cui si riferisce in una determinata data. Non è possibile posticipare quest'ultima semplicemente riproccollando il medesimo documento: ciò causerebbe un'incertezza del diritto e, nel caso ipotetico - ma non raro - di assegnazione ad un responsabile del procedimento diverso da quello precedente, anche un'incoerenza dell'azione amministrativa.

ASPETTI ORGANIZZATIVI

Soddisfatti gli adempimenti minimi previsti dalla normativa, quali altre possibilità ci sono?

Oltre all'attuazione del nucleo minimo del protocollo, possono essere individuati tre ulteriori "livelli realizzativi", che consentono di migliorare progressivamente l'efficienza, la trasparenza e la qualità dell'azione amministrativa:

la gestione informatica dei documenti in modalità avanzata (scansione dei documenti cartacei, assegnazione per via telematica all'interessato, gestione avanzata della classificazione, collegamento dei documenti alla gestione dei procedimenti)

la razionalizzazione dei processi documentali

la reingegnerizzazione dei processi primari.

Cosa s'intende per BPR?

BPR è l'acronimo di Business Process Reengineering ed è la tecnica alla base dello studio di fattibilità che deve accompagnare ogni processo di... vedi doc.ne AIPA "Informazioni ..." o web...

Come scegliere il "livello realizzativo" da raggiungere?

Tale scelta si basa su una corretta identificazione delle reali esigenze e degli obiettivi strategici che si vogliono raggiungere, nonché su una precisa analisi della fisiologia dell'Amministrazione, ovvero della struttura in termini di risorse umane e tecnologiche, al fine di determinare l'entità e l'impegno dell'investimento necessario.

Come procedere all'attuazione del progetto?

È necessario creare un apposito gruppo interno di lavoro e posizionarlo al vertice, affinché possa realmente decidere e sostenere le trasformazioni organizzative che il progetto comporta. Il gruppo deve essere composto da esperti nelle diverse materie afferenti al progetto, nonché dai responsabili delle principali unità organizzative; eventualmente possono essere invitati a partecipare anche consulenti esterni, nel caso in cui manchino le specifiche competenze all'interno dell'Amministrazione.

Da dove iniziare l'analisi dei flussi documentali?

Non è importante da dove si parte (documenti in entrata, o in uscita, o ad esclusiva rilevanza interna), quanto piuttosto che non si tralasci alcun tipo di iter documentale.

Quali tipologie di documenti prendere in considerazione nell'analisi dei flussi documentali?

Tale scelta dipende dalla tipologia di intervento che si intende attuare. A livello generale, è comunque opportuno prendere in considerazione tutti i documenti, anche quelli informali, in particolare tutti quelli che concorrono a determinare gli iter di processo, in quanto non solo garantiscono la trasparenza dell'azione amministrativa, ma costituiscono per l'Amministrazione un preciso know-how di cui fare patrimonio.

Quando e come coinvolgere gli archivisti?

Gli archivisti devono essere coinvolti dall'inizio, come partecipanti al gruppo di progetto. Nella fase di rilevazione, essi dovranno analizzare lo stato pregresso del sistema di gestione dei documenti dell'ente e valutare le esigenze degli utenti interni; nella fase di riprogettazione organizzativa, dovranno definire i nuovi piani di classificazione e conservazione dei documenti e gestire tutte le problematiche connesse (ad esempio, l'organizzazione e l'allocazione dell'eventuale archivio cartaceo e l'integrazione tra l'archivio cartaceo e il nuovo sistema documentale informatico).

Quando e come coinvolgere gli informatici?

Gli informatici devono essere coinvolti dall'inizio, come partecipanti al gruppo di progetto. Nella fase di rilevazione, essi avranno il compito di censire il parco tecnologico; nella fase di analisi e riprogettazione, dovranno individuare le criticità e proporre le relative soluzioni tecnologiche; nella fase di realizzazione

del progetto informatico, infine, lavoreranno pressoché in autonomia, coerentemente con gli indirizzi espressi nello studio di fattibilità.

Come scegliere le unità pilota del progetto di informatizzazione?

Nell'individuazione delle unità pilota possono essere scelte strutture che si candidano autonomamente, oppure quelle a più elevato tasso di informatizzazione, o ancora quelle di dimensioni più ridotte: tale scelta ha il vantaggio di conseguire l'operatività del prototipo in tempi brevi, ma non risolve l'incognita dei tempi e dei costi necessari alla diffusione generalizzata. Al contrario, la scelta di una struttura caratterizzata da numerose problematiche allunga certo i tempi di prima attuazione, ma assicura tempi e costi contenuti per la completa diffusione, in quanto l'analisi necessariamente più complessa permette di capitalizzare sul know-how acquisito a vantaggio delle altre unità organizzative.

Come condurre la fase di rilevazione e a chi fare le interviste?

Le informazioni devono essere raccolte e strutturate secondo una griglia comune, capace di rilevare le maggiori criticità ed opportunità. In linea di massima devono essere sentiti tutti i responsabili delle unità organizzative, fino ad un ragionevole livello di dettaglio, coerentemente con l'esigenza di disegnare un quadro sufficientemente chiaro dei processi documentali.

Come fare per garantire il coordinamento fra le diverse AOO all'interno di un'unica Amministrazione?

Può essere utile prevedere un "decollo" uniforme, al fine di tracciare un percorso di riferimento, in seguito liberamente personalizzabile da ciascuna AOO nell'ambito della propria analisi specifica. Allo scopo si può predisporre un primo gruppo di lavoro, di altissimo livello e trasversale a tutte le AOO, che individui le linee guida generali dell'assetto organizzativo-documentale auspicato; in merito a quest'ultimo obiettivo, si segnala l'attività del gruppo di lavoro della Scuola superiore della pubblica amministrazione, che ha recentemente prodotto delle linee guida per "La gestione elettronica dei documenti e la tenuta degli archivi".

CONSERVAZIONE DEI DOCUMENTI ELETTRONICI

Che cos'è la conservazione digitale?

La conservazione digitale è il processo effettuato con le modalità previste dalla Deliberazione 42/2001 e finalizzato a rendere non deteriorabile e quindi disponibile nel tempo, in tutta la sua integrità ed autenticità, un documento. E' sempre generato da documenti digitali, opportunamente differenziati per la loro tipologia d'origine (digitali, analogici unici e non unici).

Nella Deliberazione 42/2001 vengono mantenuti nettamente distinti il processo di conservazione da quello di archiviazione, vista la diversa natura e le differenti finalità che li contraddistinguono.

L'archiviazione digitale, infatti, è il processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti digitali, anche informatici, univocamente identificati mediante un codice di riferimento, processo antecedente e quello di conservazione.

Per l'archiviazione digitale non vengono indicate regole o metodi da adottare ma la sua eventuale attuazione viene lasciata alla libera iniziativa del Responsabile della conservazione.

Qual'è la differenza tra riversamento diretto e sostitutivo?

Il riversamento è il processo che può distinguersi in diretto o sostitutivo, se trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, rispettivamente, non alterando o modificando la loro rappresentazione digitale.

Il riversamento diretto può paragonarsi al backup di un file mentre quello sostitutivo consente l'aggiornamento tecnologico dell'archivio quando non sia possibile o conveniente conservare il formato della rappresentazione digitale dei documenti.

Che cos'è l'accesso o esibizione del del documento conservato?

L'accesso o esibizione è l'operazione che consente di ritrovare, leggere, visualizzare (nel caso anche per via telematica) un documento conservato e di ottenere l'eventuale copia su supporto cartaceo.

Quali sono i documenti analogici originali non unici?

Sono quei documenti, come la fattura o la lettera o il telegramma ricevuto da un imprenditore, i quali vengono emessi dal soggetto mittente, che assume l'obbligo di conservazione della copia, quindi ricevuti dal soggetto destinatario che è tenuto a conservare il documento stesso come originale.

Poiché destano preoccupazioni gestionali per la quantità della loro produzione e, conseguentemente, per

semplificarne il processo di conservazione, i documenti analogici originali non unici vengono trattati come le copie, svincolati quindi dalla necessità di attestazione di conformità all'originale da parte del pubblico ufficiale (o notaio, nel caso dei privati).

Che cos'è il riferimento temporale?

Il riferimento temporale previsto dalla Deliberazione 42/2001 deve essere considerato come l'informazione, da associarsi all'insieme dei documenti che sono stati sottoposti al processo di conservazione, che attesta la corretta conclusione di tale processo. Con la successiva apposizione della firma digitale tale riferimento viene "bloccato" al contenuto dei documenti a cui si riferisce.

Per motivi improntati ad una semplificazione operativa del processo di conservazione, si è voluto utilizzare il riferimento temporale senza ricorrere necessariamente alla marca temporale, pertanto è sufficiente che la procura di generazione del riferimento temporale venga decisa, definita e documentata dal Responsabile della conservazione nell'ambito delle procedure di sicurezza che il Responsabile stesso intende adottare nel processo di conservazione.

Qual'è il ruolo del Responsabile della conservazione?

La Deliberazione 42/2001 tende a dare un significativo risalto al Responsabile della conservazione, attribuendogli con l'articolo 5 precisi compiti e responsabilità.

In particolare viene affidato al Responsabile della conservazione la realizzazione dell'archivio di conservazione con procedure applicative autonomamente realizzate, quindi personalizzate al proprio ambiente operativo, con il vincolo che siano documentate e che garantiscano la tracciabilità del singolo documento, allo scopo sia di mantenere nel tempo l'integrità del suo contenuto, che di consentirne l'accesso e l'esibizione.

A differenza della precedente deliberazione, non si richiede il rispetto di particolari standard per i supporti di memorizzazione, lasciando libertà per l'adozione di una qualsiasi tipologia, ritenendo di poter anche prescindere dall'impiego della tecnologia laser. Sono stati eliminati gli adempimenti relativi al contenuto obbligatorio del supporto di memorizzazione che comportavano onerosi adempimenti da parte di del Responsabile. Sono state anche abolite sia le operazioni di chiusura del supporto di memorizzazione che di collaudo preventivo.

Tali semplificazioni si sono rese possibili grazie all'impiego del tecnicismo del riferimento temporale e della firma digitale.

La firma digitale deve necessariamente essere apposta dal Responsabile della conservazione?

Secondo gli articoli 3 e 4 della Deliberazione 42/2001, la firma digitale va apposta da parte del Responsabile della conservazione al termine del processo di conservazione di documenti digitali o di documenti analogici memorizzati su supporti di memorizzazione o al termine del processo di riversamento sostitutivo di documenti conservati.

Inoltre, secondo l'articolo 5 della suddetta deliberazione il Responsabile della conservazione può sia delegare in tutto o in parte le proprie attività, sia affidare in tutto o in parte il procedimento di conservazione.

Ciò intende che il responsabile può delegare soggetti interni alla struttura per lo svolgimento delle proprie attività, compresa l'apposizione della firma digitale, o può affidare in outsourcing ad altra società l'intero processo di conservazione, e di conseguenza, anche l'apposizione della firma digitale.

E' possibile conservare su supporto informatico documenti contabili/fiscali e distruggere gli originali cartacei?

Le attuali risoluzioni del Ministero dell'Economia e delle Finanze in materia di scritture e documenti contabili prevedono che i documenti fiscali vengano comunque sempre conservati su supporto cartaceo, prescindendo dalla loro acquisizione sotto forma di immagini.

Pertanto una soluzione definitiva al problema è da rinviarsi a dopo la pubblicazione dell'apposito regolamento per la conservazione della documentazione di rilevanza tributaria, in fase di emanazione da parte dello stesso ministero dell'Economia e delle Finanze alla luce della deliberazione 42/2001 dell'AIPA.

La conservazione digitale è adottabile anche per le cartelle cliniche ed è possibile distruggerne gli originali cartacei?

Per quanto attiene le cartelle cliniche, esse sono soggette a quanto previsto dalle risoluzioni del Ministero della Salute in materia. Tali risoluzioni sono attualmente in fase di revisione alla luce della Deliberazione 42/2001 dell'AIPA. In particolare, esse dovrebbero dare precise disposizioni su come debbano essere

considerate le cartelle cliniche, e cioè se esse debbano essere trattate come documenti originali unici o non unici e su come si possa operare per l'eventuale distruzione del cartaceo dopo il completamento della procedura di conservazione digitale.

FIRMA ELETTRONICA

Che cos'è la firma digitale?

La firma digitale è il risultato di un processo di calcolo che, a partire da un oggetto informatico (tipicamente, un documento) e da alcune informazioni strettamente associate alla persona (coppia di chiave asimmetriche), produce un secondo oggetto informatico (il documento firmato) che attesta la volontà espressa dalla persona nel sottoscrivere l'oggetto originario al quale è stato applicato il processo di firma.

Come si ottiene una firma digitale?

La firma digitale si ottiene applicando ad un oggetto informatico (ad esempio un documento) una procedura di calcolo basata sui principi della crittografia asimmetrica, dove entrano in gioco coppie di chiavi, una utilizzata per cifrare e l'altra per decifrare. La firma digitale non deve essere confusa, nel modo più assoluto, con la digitalizzazione della firma autografa, ovvero la rappresentazione digitale di un'immagine corrispondente alla firma autografa.

In sintesi, qual è la procedura per la generazione di un documento firmato digitalmente?

Il titolare di una coppia di chiavi attesta la sua volontà di sottoscrizione adottando la seguente procedura (totalmente automatizzabile):

calcola l'impronta del documento

esegue la cifratura dell'impronta del documento utilizzando la chiave privata

allega il certificato rilasciato dall'Autorità di certificazione

allega il documento in chiaro

spedisce il tutto in una busta (formato standard PKCS#7) al destinatario.

Il destinatario, per essere certo dell'autenticità e l'integrità del messaggio arrivato, effettua la procedura di verifica, che consiste nei seguenti passi:

apre la busta

accede al certificato del mittente

eventualmente accede ai servizi dell'Autorità di certificazione che ha rilasciato il certificato per verificare che non ci siano atti di revoca o di sospensione nei confronti dello stesso.

decodifica il messaggio con la chiave pubblica del mittente, ottenendo l'impronta del documento originario. Se l'esito dell'operazione è positivo, significa che il certificato è valido e che il messaggio ha come paternità il mittente (in quanto esiste ed è valido l'abbinamento chiave pubblica/chiave privata)

Poi, per essere sicuro dell'integrità del messaggio:

calcola l'impronta del documento in chiaro allegato

confronta l'impronta ottenuta con quella arrivata. Se l'esito del risultato è positivo, il documento non è stato manomesso ed è perfettamente corrispondente a quello che il mittente ha firmato.

A cosa serve la firma digitale?

In modo analogo alla tradizionale sottoscrizione autografa dei documenti cartacei, la firma digitale attesta la volontà del titolare della chiave privata di sottoscrivere il documento informatico e quindi di assumere la responsabilità del suo contenuto. Il processo di firma, oltre all'autenticità del mittente, attesta l'integrità del documento firmato e il principio del non ripudio che non permette il disconoscimento di quanto firmato.

Cos'è l'impronta del documento?

L'impronta è il processo tramite il quale è possibile ottenere da un qualsiasi oggetto informatico (ad esempio, un documento lungo e complesso a piacere) una sequenza di bit a lunghezza fissa (128 o 160 bit). L'operazione è necessaria per garantire il requisito di integrità del messaggio firmato e spedito, in quanto permette il confronto tra l'impronta del documento originario (allegata dal mittente nel messaggio spedito al destinatario) e quella calcolata dal destinatario sul documento in chiaro ricevuto (ottenuta durante il processo di verifica). Poiché è praticamente impossibile (possibilità di collisione uguale a 10 alla -48) che due documenti diversi (differenti anche per un solo bit) abbiano stesse impronte, se l'esito del confronto è positivo si ha la certezza che il documento non è stato alterato da nessuno dopo che il mittente lo ha firmato e spedito. Ricondurre documenti di qualunque dimensione ad un stringa di bit molto corta permette di effettuare confronti molto più veloci rispetto a quelli necessari nel caso in cui l'operazione dovesse effettuarsi sul documento intero.

Che relazione c'è tra firma digitale e crittografia?

La firma digitale è un processo che utilizza tecniche crittografiche come strumento per raggiungere gli obiettivi di autenticità del mittente e di integrità del messaggio; essa attesta la precisa volontà di sottoscrizione del possessore della chiave privata certificata.

Qual è la differenza tra firma digitale e strumenti di sicurezza come il protocollo SSL?

I vari protocolli del tipo SSL o SET sono dei sistemi di crittografia: hanno pertanto la funzione di garantire la segretezza del messaggio spedito. In verità, con tali protocolli si riesce a garantire anche l'autenticità del server di posta utilizzato, in quanto è prevista una procedura di certificazione (ma non ai sensi della normativa vigente in Italia) del server di comunicazione. L'impiego di tali protocolli è quindi inutile qualora, come nel caso della firma digitale, sia necessario garantire l'autenticità del mittente, cioè la volontà di sottoscrizione del messaggio da parte del mittente.

Cos'è il certificato?

Un certificato è strettamente connesso alla tipologia della coppia di chiavi a cui esso si riferisce. Le chiavi possono essere:

di sottoscrizione, se utilizzate dagli utenti per esprimere la volontà di firma del possessore di certificazione, se utilizzate dalla Certification Authority per sottoscrivere una propria attestazione di validità temporale, se utilizzate dalle Certification Authority per attestare la collocazione temporale del documento.

I certificati, in funzione del loro utilizzo, possono essere:

di sottoscrizione, i più frequenti e quelli che in genere prendono impropriamente il solo nome di certificato di autenticazione, utilizzati per essere riconosciuti via web o per la sottoscrizione della posta elettronica di crittografia, utilizzati per il solo scopo della crittografia di documenti riservati di attributo, per attestare il ruolo ed i poteri di firma del possessore.

Il certificato di sottoscrizione è lo strumento attraverso il quale la Certification Authority (Trusted Party) attesta l'identità della persona che detiene il certificato. Le informazioni minime contenute nel certificato sono di tre tipi:

informazioni proprie del certificato, come identificativo, validità temporale e algoritmo da utilizzare per il processo di verifica (cioè l'algoritmo usato per generare l'impronta del documento)

informazioni riguardanti il possessore del certificato, come dati anagrafici del possessore e sua chiave pubblica

informazioni riguardanti chi ha emesso il certificato, come dati identificativi della Certification Authority e sua firma digitale.

Se il certificato si riferisce a una coppia di chiavi di certificazione, oltre alle precedenti informazioni, devono essere presenti informazioni relative all'uso delle chiavi di certificazione. Se il certificato si riferisce ad una coppia di chiavi di marcatura temporale, oltre alle precedenti informazioni, devono essere presenti informazioni relative al sistema di marcatura temporale utilizzato per determinare la marcatura temporale (il timestamping).

Chi è il certificatore?

È la terza parte di fiducia (Trusted Part) che, in un processo di crittografia asimmetrica basato sull'uso della coppia di chiavi privata/pubblica, identifica la persona a cui sarà rilasciata sia la chiave privata sia un certificato contenente le informazioni necessarie per il processo di verifica della firma, ivi compresa la chiave pubblica. Nella normativa vigente, la Trusted Part è la Certification Authority (CA) che deve essere obbligatoriamente iscritta all'albo pubblico dell'AIPA nel caso in cui debba rilasciare certificati di sottoscrizione alla Pubblica Amministrazione. La CA fornisce anche il servizio di marcatura temporale che serve ad estendere la validità temporale di un documento informatico.

Cos'è la marca temporale e a cosa serve?

Se un documento informatico viene firmato digitalmente, la sua validità temporale è data dalla validità temporale del certificato utilizzato dal sottoscrittore. Molti documenti però hanno una validità temporale che si protrae oltre la scadenza del certificato di sottoscrizione. Per attribuire a questi documenti una ulteriore validità temporale si utilizza la marca temporale. La marca temporale è un servizio offerto dalla Certification Authority e può essere applicata, per motivi di riservatezza, anche all'impronta del documento di cui si vuole protrarre la validità temporale. Inoltre, il processo è iterativo, per cui si può aggiungere una marca temporale anche ad un documento che precedentemente è stato oggetto di marcatura temporale. Tale processo presenta interessanti analogie con quello del timbro postale utilizzato per attestare la certezza temporale del momento in cui è stata fatta la spedizione.

Qual è la differenza tra firma debole e firma forte?

In base alla normativa vigente, la firma forte è l'unica firma che attribuisce al documento informatico una valenza probatoria. La firma forte è regolamentata dal d.P.R. 445/2000 che, per il processo di firma, prevede la presenza di una Certification Authority iscritta all'albo dell'AIPA e l'utilizzo di un dispositivo di firma sicuro (ad esempio una smart card). Una firma debole è una firma che non possiede i requisiti

precedenti. In pratica, è una firma che consente l'identificazione e l'autenticazione in rete, ma non di colui che fisicamente sottoscrive il documento. In quest'ultimo caso, la valenza probatoria del documento firmato è soggetta alla discrezionalità del giudice.

Cos'è un dispositivo di firma sicuro?

È il dispositivo utilizzato dal possessore di un certificato di sottoscrizione rilasciato da una Certification Authority per generare il processo di cifratura dell'impronta del documento che si vuole sottoscrivere attraverso l'utilizzo della chiave privata. La caratteristica peculiare di un dispositivo di firma sicuro risiede nel fatto che la chiave privata, una volta generata (dal Certificatore o dal possessore del dispositivo) non può essere esportata al suo esterno, né può essere conosciuta da persone diverse dal suo possessore.

Cosa si intende per interoperabilità della firma digitale?

L'interoperabilità della firma digitale è alla base del processo di diffusione ed utilizzo della firma. Consiste nel fatto che un certificato emesso da una determinata Certification Authority (CA) possa essere letto e validato da un utente che si avvale dei servizi una diversa CA. L'AIPA ha emesso delle linee guida, che per le CA della Pubblica Amministrazione sono cogenti. Tali linee guida permettono la completa interoperabilità delle CA relativamente a:

formato dei certificati

formato delle estensioni dei certificati

formato delle liste di revoca e sospensione dei certificati

formato della marcatura temporale.

La firma digitale è operativa?

Sì. Ci sono già quindici soggetti iscritti nell'elenco pubblico dei certificatori consultabile sul sito dell'AIPA. A dicembre 2002 sono stati stimati 500.000 i titolari di certificati per la sottoscrizione con firma digitale di documenti informatici. La firma digitale trova applicazione in diversi progetti fra cui il protocollo elettronico, il mandato informatico di pagamento, processo telematico, archiviazione ottica, servizi camerali, procedure telematiche d'acquisto.

Come posso dotarmi di firma digitale?

Per ottenere gli strumenti necessari per usare la firma digitale è necessario:

recarsi presso la CA e farsi riconoscere fisicamente attraverso documenti ufficiali e/o testimoni

installare nel proprio PC il software (ed eventualmente l'hardware) fornito dalla CA

generare all'interno del dispositivo di firma la coppia di chiavi o richiederne la generazione alla CA

spedire alla CA la chiave pubblica da rendere nota a tutti e richiedere l'emissione di un certificato di sottoscrizione

attendere la risposta di emissione certificato da parte della CA.

Le operazioni di generazione delle chiavi e di richiesta di certificazione sono usualmente eseguibili direttamente presso il certificatore.

Qual è il rapporto tra la firma digitale prevista dalla normativa italiana e la firma elettronica prevista dalla direttiva europea?

La direttiva europea (n. 93 del 13 dicembre 1999) ha una impostazione rivolta al commercio elettronico piuttosto che allo scambio di documenti tra Pubbliche Amministrazioni: pertanto si parla di firma elettronica piuttosto che di firma digitale. La differenza fondamentale tra le due firme è che la firma elettronica non prevede procedure di certificazione per i fornitori dei certificati di sottoscrizione. In altre parole, la direttiva europea introduce il concetto di firma debole oltre a quello di firma forte o di certificati qualificati, comunque previsto e regolamentato in maniera analoga alla normativa vigente in Italia.

Con le nuove norme che recepiscono la Direttiva europea sulle firme elettroniche, vi saranno diverse tipologie di certificatori?

Sì, a seguito del recepimento avremo tre tipologie principali:

Certificatori che rilasciano al pubblico certificati qualificati (certificatori notificati)

Certificatori che rilasciano al pubblico certificati qualificati e che hanno richiesto il riconoscimento del possesso di più alti requisiti di qualità e sicurezza (certificatori accreditati)

Certificatori che rilasciano certificati non qualificati

Sarà possibile avere certificato e chiavi per la firma digitale sulla Carta d'Identità Elettronica, o dovrò dotarmi di due distinte smartcard?

Sì. E' previsto che tanto la C.I.E. che la C.N.S. (Carta Nazionale Servizi) possano ospitare quanto necessario per sottoscrivere con firma digitale documenti informatici. In questo modo si potrà disporre di un unico strumento per identificarsi in rete, accedere e prendere visione di dati personali, sottoscrivere con firma digitale eventuali dichiarazioni, istanze, atti.

Si possono firmare digitalmente pagine web?

In teoria è possibile firmare digitalmente pagine web, ma il problema presenta delle difficoltà tecniche e giuridiche non banali, legate al processo di firma. Come noto, la firma consiste nella cifratura, con la chiave privata del sottoscrittore, dell'impronta del documento. Nel caso della pagina web, il documento in cosa consiste? Nella pagina nella sua interezza o nei soli dati aggiunti da chi sta riempiendo la pagina che poi sottoscriverà e spedisce? Esprimendo la firma digitale una volontà di sottoscrizione del possessore della chiave privata, è da considerarsi legale far viaggiare sulla rete soltanto i dati inseriti da un utente o deve necessariamente viaggiare l'intera pagina? Al momento, il processo è al vaglio delle sedi competenti: rimane però certa la discrezionalità del giudice in caso di contenzioso.

Per i contratti in rete si deve utilizzare la firma digitale?

Dipende dal tipo di contratto. Qualora la tipologia di contratto cartaceo è tale da non prevedere la sottoscrizione autografa, non è necessario l'uso della firma digitale per sottoscrivere l'equivalente contratto informatico.

Come avviene il processo di autenticazione?

L'autenticazione della firma digitale avviene attraverso l'apposizione della firma digitale del notaio o altro pubblico ufficiale autorizzato al documento informatico digitalmente firmato, in sua presenza, dalle parti. L'identità personale deve essere opportunamente accertata attraverso le procedure di norma e la validità dei certificati di firma delle parti deve essere accertata attraverso il processo di verifica della chiave pubblica presso il Certificatore.

CLASSIFICAZIONE E FASCICOLAZIONE

Cos'è la classificazione?

La classificazione è un'attività che consente di organizzare tutti i documenti correnti prodotti da un determinato soggetto (nel caso specifico, da una Area Organizzativa Omogenea), protocollati e non, secondo uno schema articolato di voci (il piano di classificazione, comunemente detto titolare) che descrive l'attività del soggetto produttore identificandone funzioni e competenze.

Quali documenti devono essere classificati?

Sono soggetti a classificazione tutti i documenti che entrano a far parte di un sistema documentale, a prescindere dal loro stato di trasmissione (a prescindere cioè dal fatto che siano documenti ricevuti, spediti o interni) e dal supporto utilizzato (a prescindere cioè dal fatto che si tratti di documenti cartacei o informatici). In quanto strumento di prima organizzazione dei documenti, la classificazione si applica contestualmente allo svolgimento delle attività correnti e mai a posteriori in archivi già formati secondo criteri diversi.

Cos'è la fascicolazione?

La fascicolazione è l'attività di riconduzione logica (e, nel caso di documenti cartacei, anche fisica) di un documento all'interno dell'unità archivistica che ne raccoglie i precedenti, al fine di mantenere vivo il vincolo archivistico che lega ogni singolo documento alla pratica relativa. Tale attività permette di costruire un sistema basato sull'organizzazione funzionale dei documenti in unità complesse stabili nel tempo (i fascicoli), che riflettono la concreta attività del soggetto produttore. La classificazione e la fascicolazione favoriscono la sedimentazione stabile dei documenti prodotti e acquisiti dall'Amministrazione nel corso della propria attività: solo così si assicura la possibilità per l'Amministrazione stessa e per il cittadino di accedere ad una informazione contestualizzata, che dia conto del patrimonio informativo utilizzato a supporto di una determinata attività amministrativa.

Perché creare un piano di classificazione condiviso da tutta l'AOO?

La normativa vigente prevede che le amministrazioni individuino gli uffici da considerare ai fini della gestione unica e coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse (dpr 445/2001, art. 50, comma 4).

È corretto creare un piano di classificazione basato sull'organigramma dell'Ente?

La rapida trasformazione delle strutture organizzative dell'Amministrazione scoraggia l'adozione di piani di classificazione ritagliati sull'organigramma: meglio basarsi sull'analisi delle competenze, delle funzioni e delle attività, che solitamente si rivelano più durature nel tempo.