Gestione informatica dei documenti e formazione dell'archivio

Stefano Pigliapoco

Introduzione

Uno dei fenomeni che maggiormente caratterizza il nostro tempo è la convergenza dei sistemi di comunicazione sul digitale.

Qualche decennio fa esistevano quattro distinte tipologie di reti: la rete telefonica, la rete radiofonica, la rete dati, la rete televisiva; e ciascuna rete aveva il suo terminale dedicato: l'apparecchio telefonico, la radio, il computer, il televisore. Oggi questa distinzione non ha più senso; attraverso la rete dati, che può essere rappresentata da una LAN (Local Area Network), una WAN (Wide Area Network) o Internet, e un terminale intelligente, come ad esempio un PC, un palmare, un notebook, uno smartphone, un set-top-box avanzato, è possibile trasmettere e ricevere messaggi vocali, testi, informazioni multimediali, trasmissioni televisive (TV Digitale Terrestre), trasmissioni radiofoniche, SMS e MMS. Ogni contenuto informativo che non nasce in formato digitale è digitalizzato alla fonte, trasmesso attraverso la rete dati e ricevuto con apparecchiature che ne assicurano la riproduzione a livello utente.

Questa convergenza dei sistemi di comunicazione sul digitale trova la sua motivazione nella crescente esigenza delle organizzazioni di avere accesso, in ogni luogo, in qualsiasi momento, in modo rapido e a costi contenuti, alle informazioni e ai documenti di cui hanno bisogno. Non solo di avere accesso, ma anche di interagire con i propri interlocutori attraverso canali di comunicazione attivabili con modalità sincrone o asincrone. Ad esempio, con un apparecchio telefonico digitale intelligente si possono ascoltare messaggi vocali registrati nella segreteria telefonica, programmare in anticipo le telefonate, farsi leggere una e-mail urgente e dettare la risposta che sarà digitalizzata e trasmessa al destinatario come allegato a un messaggio di posta elettronica.

In questo contesto, è facile comprendere l'interesse dei Governi – di quello italiano ma anche degli altri Stati membri dell'Unione

europea – verso la digitalizzazione delle comunicazioni e dei documenti, che viene vista come la soluzione ottimale per ridurre i costi e aumentare l'efficienza delle organizzazioni. La spinta dei Governi verso il digitale e la disponibilità di strumenti tecnologicamente avanzati a costi accessibili fanno prevedere nell'immediato futuro un aumento consistente della quantità di documenti informatici prodotti e scambiati tra le pubbliche amministrazioni e tra queste e i loro utenti.

Questa facile previsione trova ampia conferma nei numerosi progetti di dematerializzazione[1] che sono in fase di realizzazione sia in ambito pubblico che privato. Le nuove norme che introducono la fatturazione elettronica in sostituzione di quella cartacea e regolano l'archiviazione su base informatica dei documenti di rilevanza fiscale e tributaria stanno spingendo le imprese a riprogettare il processo di gestione delle fatture attive e passive eliminando la produzione del cartaceo[2]. Inoltre:

a - un numero rilevante di enti pubblici ha attivato procedure di acquisto per via telematica ed ha iniziato ad emettere mandati di pagamento informatici;

b - le Camere di Commercio gestiscono da anni il Registro delle Imprese esclusivamente su supporto digitale;

c - il Ministero della Giustizia ha progettato il processo telematico;

---

[1] Il Centro nazionale per l'informatica nella pubblica amministrazione (DigitPA), sul suo sito www.cnipa.gov.it, ha chiarito il significato del termine dematerializzazione utilizzato nelle norme e nelle specifiche tecniche inerenti alla digitalizzazione dei documenti. Questo è il testo pubblicato sul sito di DigitPA: il termine "dematerializzazione" ha fatto la sua prima apparizione durante gli anni '80 nel settore finanziario, con particolare riferimento ai titoli di credito al fine di superarne la fisicità e consentire forme di circolazione virtuali. Da allora è entrato a far parte del lessico giuridico (vedi: articolo 10, Legge 17 dicembre 1997, n. 433; titolo V, Decreto legislativo 24 giugno 1998, n. 213) fino ad arrivare all'articolo 42 del Decreto legislativo 7 marzo 2005, n. 82, recante il Codice dell'Amministrazione Digitale, dove viene usato per i documenti e gli atti cartacei delle pubbliche amministrazioni identificando la progressiva perdita di consistenza fisica da parte degli archivi, tradizionalmente costituiti da documentazione cartacea, all'atto della loro sostituzione con documenti informatici. In questo senso il concetto di "dematerializzazione" si può considerare come l'estensione alla pubblica amministrazione della generale tendenza, invalsa nel settore privato, dell'uso degli strumenti ICT (*Information and Communication Technology)* per il trattamento automatizzato dell'informazione nei processi produttivi.

[2] Tali norme sono rappresentate dal D.Lgs. 20 febbraio 2004, n. 52, emanato in attuazione della direttiva 2001/115/CE, volta a semplificare ed armonizzare le modalità di fatturazione in materia di IVA, e dal Decreto del Ministero dell'Economia e delle Finanze 23 gennaio 2004, concernente le modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto.

d - il Ministero del Lavoro ha definito gli standard e le regole per la trasmissione informatica delle comunicazioni di instaurazione, trasformazione, proroga e cessazione dei rapporti di lavoro, che i datori di lavoro pubblici e privati e le agenzie di somministrazione sono tenuti ad effettuare ai servizi per l'impiego;

e - diversi Ministeri hanno pianificato nel breve periodo la sostituzione delle tradizionali comunicazioni cartacee con comunicazioni telematiche equivalenti.

Il processo di dematerializzazione in atto in Italia appare in tutta la sua estensione nel piano di *e*-government 2012, che è stato predisposto dal Ministero per la Pubblica Amministrazione e l'Innovazione. Si tratta di un piano da realizzare entro il 2012, composto da 27 obiettivi organizzati in quattro ambiti di intervento prioritari:

f - *Obiettivi settoriali*: sono gli obiettivi riferiti alle Amministrazioni centrali dello Stato e alle Università;

g - *Obiettivi territoriali*: sono gli obiettivi riferiti alle Regioni e ai capoluoghi;

h - *Obiettivi di sistema*: sono gli obiettivi mirati allo sviluppo di infrastrutture;

i - *Obiettivi internazionali*: comprende le azioni per lo sviluppo della rete europea dell'innovazione e delle *best practice.*

Nella seguente tabella sono evidenziati i progetti previsti nel piano *e*-gov 2012 che avranno un forte impatto sulla gestione informatica dei documenti e la formazione degli archivi.

Obiettivo 3. Giustizia	Progetto 1. Notificazioni telematiche delle comunicazioni e degli atti praocessuali Progetto 2. Rilascio telematico di certificati giudiziari Progetto 3. Trasmissione telematica delle notizie di reato tra forze di polizia e procure della Repubblica Progetto 4. Accesso on-line alle sentenze e ai dati dei procedimenti
Obiettivo 4. Salute	Progetto 1. Digitalizzazione del ciclo delle prescrizioni e dei certificati medici Progetto 2. Fascicolo sanitario elettronico
Obiettivo 6. Sicurezza e libertà civili	Progetto 1. Passaporto e carta d'identità elettronica
Obiettivo 17. Carte dei servizi	Progetto 1. Integrazione tessera sanitaria e carta regionale dei servizi

Obiettivo 20. Dematerializzazione	Progetto 1. Casella elettronica certificata per i cittadini, le amministrazioni pubbliche, le imprese e i professionisti Progetto 2. Fatturazione elettronica verso la pubblica amministrazione Progetto 3. Pagamenti *on-line* verso la pubblica amministrazione Progetto 4. Documento Unico di Regolarità Contributiva (DURC) *on-line* Progetto 5. Attuazione del Codice dell'amministrazione digitale Progetto 6. Gestione documentale elettronica

Tutte queste iniziative porteranno inevitabilmente alla produzione di una grande quantità di documenti informatici che si affiancheranno a quelli cartacei, rendendo sempre più complesse le attività inerenti alla formazione, gestione e conservazione degli archivi. Di conseguenza, ai Responsabili dei sistemi documentali saranno richieste non soltanto competenze in materia di archivistica e diplomatica, ma anche conoscenze nel campo dell'informatica, del diritto e dell'organizzazione[3].

I. - Firma elettronica e firma digitale

Il complesso delle norme che disciplinano la produzione dei documenti informatici attraverso l'uso delle firme elettroniche poggia essenzialmente sulla Direttiva 13 dicembre 1999, n. 93/CE, del Parlamento europeo e del Consiglio, relativa ad un quadro comunitario per le firme elettroniche, entrata in vigore il 19 gennaio 2000.

Tale Direttiva è stata emanata nella convinzione che[4]:

a - la firma elettronica è uno strumento indispensabile per lo sviluppo del commercio elettronico e delle comunicazioni elettroniche, in quanto contribuisce ad accrescere la fiducia degli utenti nelle transazioni eseguite su base informatica;

b - la divergenza delle norme in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati membri costituisce un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico;

c - la rapida evoluzione tecnologica e il carattere globale di Internet rendono necessario un approccio aperto alle varie tecnologie e servizi che consentono di autenticare i dati in modo elettronico.

---

[3] Per ulteriori approfondimenti si rinvia al piano *e*-gov 2012 pubblicato sul sito www.innovazionepa.gov.it.

[4] Si veda il testo introduttivo agli articoli della Direttiva n. 1999/93/CE.

Allo scopo di evitare che gli Stati membri dell'Unione europea adottassero autonomamente le regole tecniche per la generazione e la verifica delle firme elettroniche, rischiando così l'incompatibilità, l'art. 9 della Direttiva n. 1999/93/CE ha istituito un "Comitato per la firma elettronica" e l'art. 10 gli ha assegnato i seguenti compiti:

d - definire i requisiti relativi ai certificati elettronici qualificati, ai prestatori di servizi di certificazione che rilasciano certificati qualificati e ai dispositivi per la creazione di una firma sicura[5];

e - fissare i criteri in base ai quali gli Stati membri stabiliscono se un organismo pubblico può essere designato per la determinazione della conformità dei dispositivi di firma sicura ai requisiti fissati dal Comitato;

f - emanare le norme generalmente riconosciute relative ai prodotti di firma elettronica[6].

Le specifiche tecniche per la generazione e la verifica delle firme elettroniche, pertanto, sono definite ed aggiornate a livello europeo; gli Stati membri devono recepirle, adeguando periodicamente la propria base normativa e regolamentare.

I.1. - Quadro normativo di riferimento

Lo Stato italiano, in attuazione alla Direttiva europea citata, ha emanato un complesso di norme che oggi, dopo diverse modifiche, abrogazioni e integrazioni, comprende:

a - il D.Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale;

b - il D.P.C.M. 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici;

c - la Circolare CNIPA 21 maggio 2009, n. 45 - Regole per il riconoscimento e la verifica del documento informatico.

Tali norme, in accordo con le disposizioni contenute nella Direttiva europea citata, prevedono la possibilità di generare firme elettroniche aventi valenza giuridica e forza probatoria differente in funzione del livello garantito di sicurezza e affidabilità.

---

[5] Si vedano le definizioni riportate nei successivi paragrafi.

[6] L'art. 2, c. 12, della Direttiva n. 1999/93/CE, definisce prodotto di firma elettronica "un hardware o un software, oppure i componenti pertinenti dei medesimi, destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica oppure per la creazione o la verifica di firme elettroniche".

I.2. - Firma elettronica

L'art. 1, c. 1, lett. q), del D.Lgs. n. 82/2005, recante il Codice dell'Amministrazione Digitale, definisce firma elettronica i "dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzati come metodo di identificazione informatica". Essa può essere generata con un qualsiasi dispositivo, un software configurato o un hardware, che permetta di applicare i dati per la creazione di una firma[7] a un contenuto informativo elettronico.

Siccome non sono richiesti particolari requisiti tecnici per il dispositivo né sono previste misure specifiche per garantire la connessione univoca tra un soggetto e i dati per la creazione della firma elettronica, questa può essere caratterizzata da un livello basso di sicurezza e affidabilità. In questo caso si parla di "firma debole".

Allo stesso tempo, però, può verificarsi il caso che, pur non rispettando tutti i requisiti previsti per le firme elettroniche qualificate descritte nel successivo paragrafo, gli strumenti tecnologici utilizzati e le procedure di rilascio dei dati personali siano tali da garantire un sufficiente grado di attendibilità delle firme elettroniche generate in rapporto alla tipologia dei documenti siglati.

In considerazione della variabilità del grado di certezza attribuibile a una firma elettronica, il legislatore europeo, con la Direttiva n. 1999/93/CE, precisamente l'art. 5, c. 2, ha imposto agli Stati membri di non considerarla "legalmente inefficace o inammissibile come prova in giudizio unicamente a causa del fatto che è in forma elettronica, o non basata su un certificato qualificato, o non basata su un certificato qualificato rilasciato da un prestatore di servizi di certificazione accreditato, ovvero non creata da un dispositivo per la creazione di una firma sicura"[8].

I.3. - Firma elettronica qualificata

L'art. 1, c. 1, lett. r), del Codice dell'Amministrazione Digitale, definisce firma elettronica qualificata "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in

---

[7] L'art. 1, c. 1, lett. e), del D.P.C.M. 30 marzo 2009, definisce dati per la creazione di una firma "l'insieme dei codici personali e delle chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica".

[8] Si vedano le definizioni riportate nel successivo paragrafo.

modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma". Si tratta, cioè, di una firma elettronica caratterizzata dal più alto grado di sicurezza e affidabilità.

Per comprendere la consistenza di una firma elettronica qualificata occorre chiarire il significato dei termini: certificatore, certificato elettronico e dispositivo sicuro per la generazione della firma.

I certificatori sono i soggetti che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi a queste ultime[9]. I loro legali rappresentanti ed i soggetti preposti all'amministrazione devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche. I certificatori rilasciano alle persone che ne fanno richiesta i cosiddetti certificati elettronici che, ai sensi dell'art. 1, c. 1, lett. e), del Codice dell'Amministrazione Digitale, sono "attestati elettronici che collegano all'identità del titolare i dati utilizzati per la verifica delle firme elettroniche"[10].

In conformità con quanto stabilito nell'art. 27 del Codice dell'Amministrazione Digitale e nell'allegato II della Direttiva europea n. 1999/93/CE, un certificatore si dice qualificato se, oltre a possedere i requisiti imposti ai certificatori:

a - dimostra l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;

b - impiega personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti;

c - utilizza sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità ai criteri di sicurezza riconosciuti in ambito europeo e internazionale;

d - adotta adeguate misure contro la contraffazione dei certificati.

Un certificatore qualificato può essere accreditato dallo Stato italiano se:

e - è una società di capitali con capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria;

f - garantisce il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti all'amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di

---

[9] Si veda l'art. 1, c. 1, lett. g), del Codice dell'Amministrazione Digitale.

[10] Ai sensi dell'art. 1, c. 1, lett. aa), del D.Lgs. n. 82/2005, per titolare s'intende la persona fisica che ha accesso ai dispositivi per la creazione della firma elettronica.

onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche;

g - ottiene dal CNIPA, su apposita richiesta, il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza.

L'elenco dei certificatori accreditati è tenuto da DigitPA ed è consultabile per via telematica sul sito www.cnipa.gov.it.

I certificatori qualificati, ed eventualmente accreditati, rilasciano certificati elettronici qualificati che, in conformità con quanto stabilito nell'allegato I della Direttiva europea recante il quadro comunitario delle firme elettroniche, contengono le seguenti informazioni[11]:

h - indicazione che il certificato elettronico è un certificato qualificato;

i - numero di serie o altro codice identificativo del certificato;

l - nome, ragione o denominazione sociale del certificatore e lo Stato nel quale è stabilito;

m - nome, cognome, o uno pseudonimo chiaramente identificato come tale, e codice fiscale del titolare del certificato;

n - dati per la verifica della firma corrispondenti ai dati per la creazione della stessa in possesso del titolare;

o - indicazione del termine iniziale e finale del periodo di validità del certificato;

p - firma elettronica del certificatore che rilascia il certificato, idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.

In via opzionale, in un certificato elettronico qualificato è possibile inserire:

q - le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché i poteri di rappresentanza;

r - i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarietà delle qualifiche e dei poteri di rappresentanza di cui alla precedente lettera q);

s - i limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato.

Per ragioni di sicurezza, a un certificato elettronico qualificato è attribuito un periodo di validità[12], che decorre dalla data di pubblicazione del suo codice identificativo nella lista dei certificati emessi.

---

[11] Si veda l'art. 28 del Codice dell'Amministrazione Digitale.

[12] Attualmente, il periodo di validità di un certificato elettronico qualificato è di circa tre anni.

Può accadere, tuttavia, che il titolare ritenga compromessa la segretezza del suo codice privato o la sicurezza del suo dispositivo di firma, ad esempio per smarrimento, furto o distruzione accidentale. In tal caso egli può richiedere al certificatore, con le procedure di cui al D.P.C.M. 30 marzo 2009, la revoca o la sospensione del suo certificato elettronico, che avverrà mediante la pubblicazione del relativo codice identificativo nelle liste dei certificati revocati o sospesi (CRL e CSL).

In un determinato momento, pertanto, un certificato elettronico qualificato, rilasciato da un certificatore a un titolare, può trovarsi in uno dei seguenti quattro stati: in corso di validità, scaduto, sospeso o revocato.

A completamento delle disposizioni che regolano l'emissione dei certificati di firma, l'art. 32, c. 3, lett. j), del D.Lgs. n. 82/2005, impone ai certificatori qualificati l'obbligo di "tenere registrazione, anche elettronica, di tutte le informazioni relative ad un certificato qualificato, dal momento della sua emissione per almeno venti anni, anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari".

Relativamente ai dispositivi sicuri per la generazione di una firma elettronica qualificata, l'art. 35 del D.Lgs. n. 82/2005 e l'art. 9 del D.P.C.M. 30 marzo 2009, coerentemente con quanto stabilito nell'Allegato III della Direttiva dell'Unione europea n. 1999/93/CE, dichiara che essi devono possedere caratteristiche tali da garantire che:

t - la chiave privata sia riservata, non possa essere derivata e sia sufficientemente protetta dal titolare dall'uso da parte di terzi;

u - siano generate firme protette da contraffazioni e capaci di garantire l'integrità dei documenti informatici a cui le firme si riferiscono;

v - i documenti informatici siano presentati al titolare prima dell'apposizione della firma, chiaramente e senza ambiguità, e sia richiesta la conferma della volontà di sottoscrizione;

z - la generazione di una firma avvenga all'interno del dispositivo sicuro, così che non sia possibile l'intercettazione della chiave privata utilizzata;

x - il dispositivo sicuro possa essere attivato esclusivamente dal titolare mediante codici personali.

In sintesi, per generare una firma elettronica qualificata occorre munirsi di un certificato elettronico qualificato, che può essere rilasciato da un certificatore qualificato o accreditato, e utilizzare un dispositivo per la creazione di una firma sicura, sul quale il firmatario possa conservare un controllo esclusivo.

II. - *Firma digitale*

L'art. 1, c. 1, lett. s), del Codice dell'Amministrazione Digitale, definisce firma digitale "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

Sotto il profilo tecnico, la firma digitale è il risultato di un algoritmo crittografico a chiavi asimmetriche[13], precisamente dell'algoritmo RSA (dalle iniziali dei nomi degli inventori Rivest, Shamir, Adleman) applicato al file contenente la rappresentazione digitale del documento che si vuole sottoscrivere.

Per generare firme digitali, una persona deve munirsi degli strumenti necessari richiedendoli a un certificatore qualificato, meglio se accreditato. Questi, dopo aver identificato con certezza il soggetto che fa richiesta della certificazione[14], gli fornisce il dispositivo di firma sicuro all'interno del quale è generata una coppia di chiavi crittografiche di lunghezza minima 1024 bit e memorizzato il certificato elettronico qualificato.

II.1. - Generazione di una firma digitale

La firma digitale è generata con un processo che si compone di 4 fasi:

Fase 1 - Il titolare attiva il software che gli ha fornito il certificatore per la generazione della firma digitale, specificando il nome del file che contiene il documento da sottoscrivere;

Fase 2 - Al file selezionato (e visualizzato dal titolare) viene applicata una funzione matematica – l'HASH crittografico conforme alla norma ISO/IEC 10118-3:2004 – che genera impronte digitali a

---

[13] La crittografia è la scienza che studia i sistemi e i metodi per rendere un testo comprensibile solo a chi conosce un determinato codice o chiave crittografica. Nello specifico, l'algoritmo crittografico asimmetrico prevede la generazione di una coppia di chiavi, una pubblica e l'altra segreta, con modalità tali da soddisfare queste due condizioni: 1) da una chiave della coppia non è possibile risalire all'altra chiave della stessa coppia; 2) se la crittografia di un file è eseguita con la chiave di una coppia, l'operazione inversa di decodifica può essere effettuata solo con l'altra chiave della stessa coppia.

[14] Si veda l'art. 32, c. 3, lett. a) e c. 4, del Codice dell'Amministrazione Digitale.

160 bit[15]. Tale funzione garantisce, con un sufficiente livello di sicurezza:

a - l'unidirezionalità, cioè l'impossibilità di risalire al documento informatico partendo dalla sua impronta digitale;

b - la resistenza alle collisioni, cioè l'impossibilità di generare una stessa impronta digitale a partire da due file diversi;

Fase 3 - L'impronta digitale del documento viene inviata all'interno del dispositivo sicuro, attivato dal titolare con un PIN (Personal Identification Number), dove viene generata la firma digitale. Essa è la sequenza binaria risultante dall'applicazione dell'algoritmo crittografico asimmetrico all'impronta digitale di 160 bit e alla chiave segreta del titolare;

Fase 4 - Viene generato il documento informatico che, nel formato standard PKCS#7 (.p7m), si compone: del file originario contenente il testo del documento, della firma digitale e del certificato elettronico qualificato del sottoscrittore estratto dal dispositivo sicuro[16].

Lo schema rappresentativo del processo di generazione di una firma digitale è riportato in figura 1, mentre la figura 2 mostra la composizione di un documento firmato digitalmente e prodotto in formato .p7m.

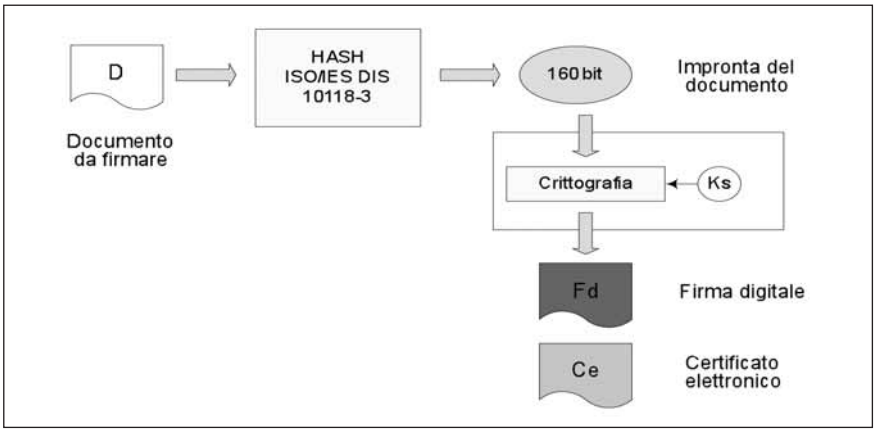

Fig. 1. Schema del processo di generazione della firma digitale

---

[15] L'art. 1, c. 1, lett. h), del D.P.C.M. 30 marzo 2009, definisce impronta digitale di un file "una sequenza di simboli binari (bit) di lunghezza predefinita, generata mediante l'applicazione al primo di un'opportuna funzione di HASH".

[16] Si segnala che oltre al formato .p7m, il CNIPA ha ammesso altri due formati per la firma digitale: il PDF, a seguito di un protocollo d'intesa siglato con la società Adobe Systems Inc. nel mese di marzo 2006, e l'XML, con l'emanazione della Deliberazione 18 maggio 2006, n. 34, recante le regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in formato XML.

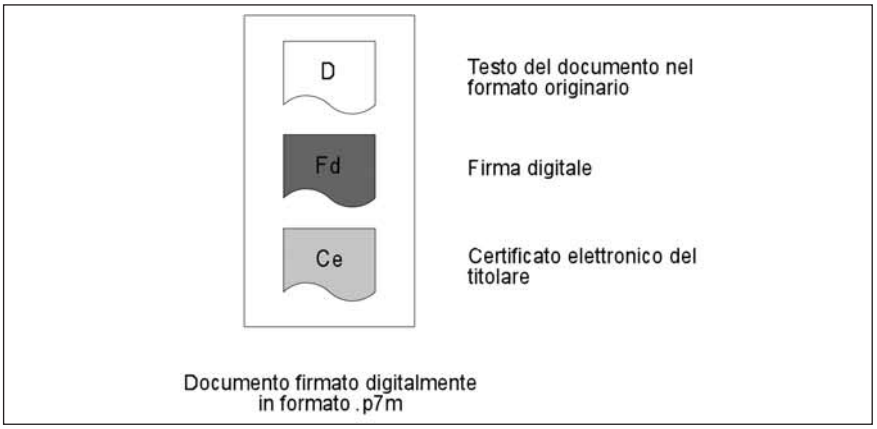

Fig. 2. Composizione di un documento sottoscritto con firma digitale in formato .p7m

II.2. - Verifica di una firma digitale

Il processo di verifica di una firma digitale apposta a un documento informatico e generata in formato .p7m si articola anch'esso in 4 fasi:

Fase 1 - Viene attivato il software per la verifica delle firme digitali fornito dal certificatore, specificando il nome del file che contiene il documento informatico da leggere;

Fase 2 - Il software esegue automaticamente due operazioni:

a - applica la funzione di HASH al testo del documento nel formato originario privo della firma digitale, generando la sua impronta di 160 bit;

b - decodifica la firma digitale con la chiave pubblica del sottoscrittore memorizzata nel certificato elettronico contenuto nel file .p7m, ottenendo l'impronta digitale di 160 bit che le corrisponde;

Fase 3 - il software confronta le due impronte digitali e se coincidono:

c - si ha la certezza che la firma digitale corrisponde al testo del documento, ovvero che questi non è stato modificato dopo la sottoscrizione (garanzia dell'integrità);

d - si presume che il sottoscrittore sia il titolare del certificato elettronico dal quale è stata prelevata la chiave pubblica utilizzata per la decodifica della firma (funzione indicativa e dichiarativa)[17];

[17] È evidente che se il titolare consegna il suo dispositivo sicuro ad un'altra persona e gli comunica anche il PIN necessario per attivarlo, questa può generare esattamente la sua firma digitale.

Fase 4 - Il testo del documento è visualizzato a video insieme ai dati identificativi del sottoscrittore prelevati dal certificato elettronico contenuto nel file .p7m.

Lo schema che rappresenta il processo di verifica di una firma digitale è riportato in figura 3.

In base alle nuove regole tecniche per il riconoscimento e la verifica del documento informatico, contenute nella Circolare CNIPA 21 maggio 2009, n. 45, a decorrere dal mese di settembre 2010, allo scopo di garantire una maggiore sicurezza, per la generazione e la verifica delle firme digitali si dovrà utilizzare la funzione di HASH SHA-256, che genera impronte di 256 bit, in sostituzione della funzione SHA-1, che le produce di 160 bit.

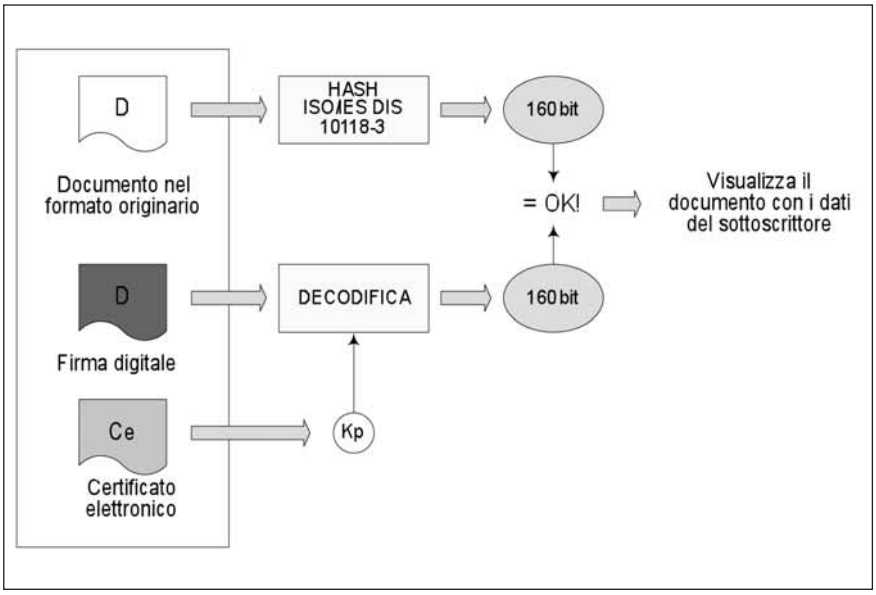

Fig. 3. Schema del processo di verifica di una firma digitale

III. - Documento informatico

L'art. 1, c. 1, lett. p), del Codice dell'Amministrazione Digitale, definisce documento informatico "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

In linea di principio, esso dovrebbe essere la traslazione su base digitale del documento cartaceo tradizionale, ma non è così semplice. Le caratteristiche intrinseche degli oggetti digitali e l'esigenza di soddisfare i requisiti che sono alla base della teoria giuridica del

documento in un contesto tecnologico in continua evoluzione, fanno assumere ai processi di produzione, gestione e conservazione dei documenti informatici una loro specifica connotazione, sostanzialmente diversa da quella dei processi analoghi applicati ai documenti cartacei.

III.1. - Documento informatico non sottoscritto digitalmente

Un documento informatico può essere digitato su computer con l'ausilio di un software di office automation, oppure può essere ottenuto con un processo di digitalizzazione applicato a un documento analogico (ad esempio la scansione di un documento cartaceo), o generato automaticamente da un apparato hardware e software opportunamente programmato. In ogni caso, senza l'adozione di particolari accorgimenti tecnici e la protezione di un sistema di archiviazione digitale, un documento informatico può essere modificato in qualsiasi momento, anche dopo la sua produzione e anche senza la volontà esplicita dell'autore.

Pertanto, ai documenti informatici non sottoscritti digitalmente è riconosciuta la forza giuridica delle riproduzioni meccaniche, che è specificata nell'articolo 2712 del Codice Civile[18].

III.2. - Documento informatico sottoscritto con firma elettronica

Come esposto nel paragrafo II.2., a una firma elettronica si riconosce un livello di sicurezza e di affidabilità variabile in funzione degli strumenti tecnologici utilizzati per la sua generazione e delle procedure seguite per il rilascio ai titolari dei codici personali.

Di conseguenza, ai sensi dell'art. 21, c. 1, del Codice dell'Amministrazione Digitale, "il documento informatico cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità". In altri termini, in caso di contenzioso, il giudice può liberamente stabilire la validità di un documento sottoscritto con una firma elettronica, valutando il grado di sicurezza e di affidabilità che le può essere riconosciuto.

---

[18] L'art. 2712 del Codice Civile stabilisce che "le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fotografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime".

III.3. - Documento informatico sottoscritto con firma elettronica qualificata o firma digitale

In considerazione delle più ampie garanzie di sicurezza fornite da una firma elettronica qualificata, l'art. 21, c. 2, del D.Lgs. n. 82/2005, riconosce al "documento informatico sottoscritto con una firma digitale, o un altro tipo di firma elettronica qualificata, l'efficacia prevista dall'art. 2702 del Codice Civile"[19], affermando che "l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria".

Al documento informatico sottoscritto con firma digitale, quindi, è attribuito un valore giuridico equivalente a una scrittura privata, con in più l'onere, per chi non riconosce come propria una firma digitale che il processo di verifica gli attribuisce, di dover fornire egli stesso la prova dell'esistenza di una qualche manomissione o anomalia[20].

L'apposizione di una firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente[21].

III.4. - Marcatura o riferimento temporale

Non sempre è possibile attribuire a una firma digitale l'efficacia di una sottoscrizione autografa. L'art. 21, c. 3, del D.Lgs. n. 82/2005, infatti, afferma in modo esplicito che "l'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione".

Pertanto, per stabilire la validità di una firma digitale apposta ad un documento informatico occorre accertare che il certificato elettronico del firmatario non risulti inserito nelle liste dei certificati scaduti, revocati o sospesi (CRL e CSL) tenute dal suo certificatore. E questo controllo è eseguito automaticamente durante il processo di verifica della

---

[19] L'art. 2702 del Codice Civile riguarda la scrittura privata e stabilisce che essa "fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata riconosciuta".

[20] Si ricorda quanto stabilito dall'art. 32, c. 1, del D.Lgs. n. 82/2005: "il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma".

[21] Si veda l'art. 24, c. 2, del Codice dell'Amministrazione Digitale.

firma digitale purché la stazione di lavoro utilizzata sia connessa ad Internet.

Tuttavia, un documento informatico può avere piena valenza giuridica anche se al momento della verifica della firma digitale il certificato del firmatario risulta essere scaduto, revocato o sospeso. Si pensi, ad esempio, a una firma digitale prodotta con un certificato elettronico qualificato in corso di validità e verificata dopo cinque o più anni, quando cioè il certificato risulterà scaduto.

Ai fini dell'accertamento della validità di una firma digitale apposta ad un documento informatico, è necessario stabilire se al momento della sottoscrizione il certificato elettronico del firmatario era scaduto, revocato o sospeso. L'art. 51 del D.P.C.M. 30 marzo 2009, infatti, dichiara che "la firma digitale, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, è valida se alla stessa è associabile un riferimento temporale opponibile ai terzi che colloca la generazione di detta firma digitale in un momento precedente alla sospensione, scadenza o revoca del suddetto certificato".

Per attribuire ad un documento informatico una data certa, il legislatore ha previsto la generazione delle marche temporali che, con l'ausilio di determinate procedure informatiche, permettono di eseguire la cosiddetta validazione temporale[22].

Il processo di generazione di una marca temporale per un documento informatico si articola in quattro fasi:

Fase 1 - Applicazione della funzione di HASH al documento informatico a cui si vuole associare una marca temporale, con conseguente generazione della sua impronta digitale;

Fase 2 - Trasmissione dell'impronta digitale così calcolata al sistema informatico del certificatore che eroga il servizio di marcatura temporale;

Fase 3 - Generazione e firma della marca temporale;

Fase 4 - Trasmissione della marca temporale al soggetto richiedente.

Lo schema che rappresenta il processo di marcatura temporale è riportato in figura 4.

---

[22] L'art. 1, c. 1, del D.P.C.M. 30 marzo 2009, e l'art. 1, c. 1, lett. bb), del Codice dell'Amministrazione Digitale, propongono le seguenti definizioni:
x - per riferimento temporale, un'informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
y - per marca temporale, il riferimento temporale che consente la validazione temporale;
z - per validazione temporale, il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data e un orario opponibili ai terzi.

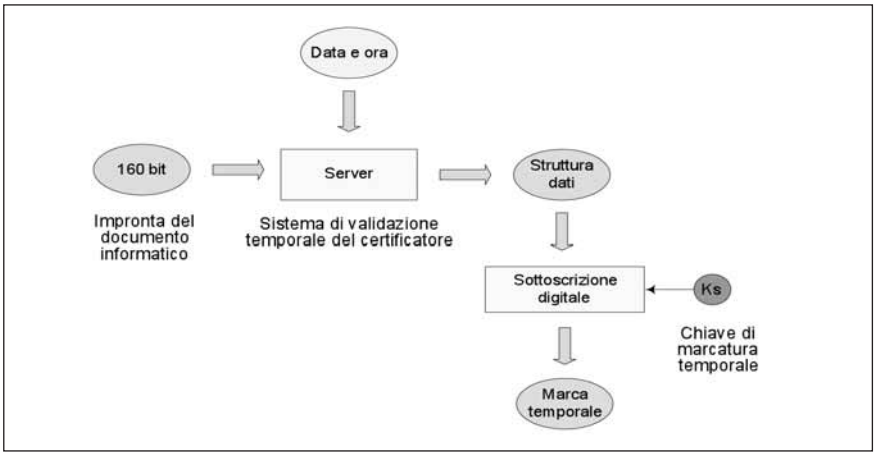

Fig. 4. Schema del processo di generazione di una marca temporale

L'art. 48 del D.P.C.M. 30 marzo 2009 specifica i requisiti tecnici dei sistemi di validazione temporale, mentre l'art. 49 fissa a venti anni il periodo minimo di conservazione e quindi di validità delle marche temporali[23].

In mancanza di una marca temporale apposta o associata ad un documento informatico, ai sensi dell'art. 37, c. 4, del D.P.C.M. 30 marzo 2009, costituiscono validazione temporale:

a - il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del D.P.C.M. 31 ottobre 2000, recante le Regole tecniche per il protocollo informatico;

b - il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;

c - il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del Codice dell'Amministrazione Digitale;

d - il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14 , comma 1, punto 1.4, della Convenzione postale universale.

---

[23] L'art. 49, c. 1, del D.P.C.M. 30 marzo 2009, stabilisce che "tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni, ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore". Il c. 2 precisa che "la marca temporale è valida per il periodo di conservazione stabilito o concordato con il certificatore di cui al comma 1".

Pertanto, in presenza di un documento informatico per il quale non è stata generata una marca temporale, la verifica della validità della firma digitale ad esso apposta può essere effettuata prendendo come riferimento temporale una delle date sopra elencate. In particolare, costituisce valido riferimento temporale la data della registrazione di protocollo.

III.5. - Validità di una firma digitale nel tempo

Come dimostrato nei precedenti paragrafi, la firma digitale permette di accertare l'integrità di un documento informatico e di identificare il sottoscrittore, attribuendogli le dichiarazioni contenute nel documento. Queste potenzialità, però, le sono riconosciute per un periodo di tempo relativamente breve dalla data di sottoscrizione, in quanto successivamente intervengono altri fattori che la rendono inefficace o, comunque sia, non più in grado di fornire le stesse certezze giuridiche di una firma autografa.

In primo luogo, l'evoluzione tecnologica renderà disponibili sistemi di elaborazione così veloci da ridurre drasticamente il livello di sicurezza garantito da una firma digitale "vecchia" di cinque o più anni. In secondo luogo, la firma digitale è costituita da una sequenza binaria organizzata secondo un determinato formato e quindi è soggetta ad obsolescenza tecnologica come qualsiasi altro contenuto digitale[24]. In ultimo, l'obbligo imposto ai certificatori qualificati dall'art. 32, c. 3, lett. j), del D.Lgs. n. 82/2005, di "tenere registrazione, anche elettronica, di tutte le informazioni relative ad un certificato qualificato, dal momento della sua emissione per almeno venti anni", appare del tutto insufficiente per garantire la verifica delle firme digitali apposte ai documenti di interesse storico destinati alla conservazione permanente[25].

III.6. - Requisiti dei formati elettronici

Alcuni formati elettronici, tra cui il diffusissimo .doc della Microsoft, ma anche il .pdf nelle versioni più recenti, permettono di inserire campi dinamici nel testo del documento, ovvero sequenze di istruzioni (macroistruzioni) che il software esegue automaticamente in

---

[24] Cfr. S. PIGLIAPOCO, S. ALLEGREZZA, *Produzione e conservazione del documento digitale. Requisiti e standard dei formati elettronici*, Macerata, EUM, 2008.

[25] E' evidente che se si cancellano tutte le informazioni relative ad un certificato elettronico qualificato, archiviate presso il certificatore, non sarà più possibile accertare la validità delle firme digitali basate su di esso.

fase di lettura, inserendo i risultati nella rappresentazione del documento come se fossero stati digitati insieme agli altri caratteri[26].

E' possibile, quindi, che un documento sottoscritto digitalmente e archiviato con un sistema che ne impedisce qualsiasi modifica, si presenti all'utente con un contenuto diverso da quello originario per effetto della presenza al suo interno di macroistruzioni che producono risultati dipendenti da parametri esterni al documento stesso, i quali possono cambiare di giorno in giorno e/o da computer a computer.

Il legislatore, nell'art. 3, c. 3, del D.P.C.M. 30 marzo 2009, ha chiarito che un documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica qualificata, non produce gli effetti dell'art. 21, c. 2, del Codice dell'Amministrazione Digitale, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.

Da qui l'esigenza di utilizzare per la produzione di documenti formati elettronici che, al minimo, soddisfano i seguenti requisiti[27]:

a - non devono poter contenere macroistruzioni o codici eseguibili, ovvero devono essere disponibili gli strumenti capaci di rilevarne la presenza con sufficiente sicurezza;

b - devono essere aperti, standard e documentati, ovvero le relative specifiche devono essere pubblicamente accessibili, complete ed esaustive;

c - devono essere robusti, accurati, ampiamente adottati ed usabili[28];

d - devono essere indipendenti dalle piattaforme tecnologiche, in modo da poter visualizzare un documento senza particolari vincoli di natura informatica o il pagamento di royalty;

e - devono essere conformi alle disposizioni emanate dalle autorità competenti in materia di archiviazione e conservazione digitale.

IV. - Posta elettronica certificata

La trasmissione e la ricezione di documenti informatici avvengono di solito tramite il servizio di posta elettronica convenzionale, che ormai tutti noi abbiamo attivato sulla nostra stazione di lavoro.

---

[26] Esempi di campi dinamici sono: la data e l'ora del documento, il nome del *file*, i dati identificativi dell'autore.

[27] Per lo studio dei requisiti tecnici dei formati elettronici si rinvia al volume di S. PIGLIAPOCO, S. ALLEGREZZA, *op. cit.*

[28] Il coefficiente di robustezza di un formato elettronico indica la probabilità, in caso di corruzione di un *file*, di recuperare tutto o parte del suo contenuto.

Tuttavia, nella sua configurazione standard, questo servizio espone il mittente e il destinatario a rischi rappresentati da:

a - virus informatici;

b - lettura dei messaggi da parte di sconosciuti, con conseguente violazione della privacy;

c - modifica dei messaggi da parte di "malintenzionati", con conseguente abbattimento delle certezze relative alla provenienza, alla data di spedizione, all'integrità del testo e degli allegati;

d - deviazione o annullamento dei messaggi con conseguente incertezza sulla data di consegna.

Il servizio di posta elettronica certificata (PEC) è stato introdotto dal legislatore con l'obiettivo di eliminare questi rischi e fornire ampie garanzie nelle comunicazioni per via telematica[29]. La base normativa di riferimento è costituita da:

e - D.P.R. 11 febbraio 2005, n. 68 - Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27 della Legge n. 3/2003;

f - Decreto del Ministero per l'Innovazione e le Tecnologie, 2 novembre 2005 - Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata.

Il servizio di posta elettronica certificata può essere erogato solo dai gestori che possiedono i requisiti di cui all'art. 14 del D.P.R. n. 68/2005 e sono inseriti in un elenco gestito dal Centro nazionale per l'informatica nella pubblica amministrazione (DigitPA). Fanno eccezione le pubbliche amministrazioni alle quali è riconosciuta la facoltà di attivare autonomamente un servizio di PEC, rispettando le regole tecniche e di sicurezza previste dalla normativa vigente.

Il titolare di una casella di PEC, all'atto della connessione al punto di accesso del suo gestore del servizio di posta certificata[30], deve autenticarsi fornendo le credenziali di identificazione (user-id e password) che gli sono state fornite al momento del rilascio dell'indirizzo di PEC. L'autenticazione è funzionale alla certificazione della provenienza del messaggio.

I canali di comunicazione attraverso i quali transitano i messaggi scambiati tra gli utenti e i gestori del servizio di PEC e tra i

---

[29] L'art. 1, c. 1, lett. g), del D.P.R. n. 68/2005, definisce posta elettronica certificata "ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici".

[30] Ai sensi dell'art. 1, c. 1, lett. a) del D.M. 2 novembre 2005, per punto di accesso s'intende "il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto".

gestori medesimi, sono realizzati con protocolli sicuri che garantiscono la riservatezza delle comunicazioni. Inoltre, i sistemi dei gestori di PEC controllano sistematicamente i messaggi per individuare l'eventuale presenza di virus informatici e, in caso affermativo, non li accettano, segnalando l'anomalia al mittente[31]. In ogni caso, se un messaggio non è consegnabile al destinatario, è garantita la spedizione al mittente di un messaggio di anomalia entro 24 ore dall'invio.

Il punto di accesso di un gestore del servizio di PEC, dopo aver eseguito i controlli sul messaggio in ingresso, se non riscontra anomalie, invia al mittente una ricevuta di accettazione nella quale sono riportati i dati di certificazione[32]. Tale ricevuta è sottoscritta digitalmente ed ha effetti probatori[33].

Dopo l'emissione della ricevuta di accettazione, il sistema del gestore del servizio di PEC del mittente genera una busta di trasporto contenente il messaggio originale e i dati di certificazione, la firma digitalmente e la invia al punto di ricezione[34] del gestore della PEC del destinatario.

Il punto di ricezione, a fronte dell'acquisizione di un messaggio proveniente da un gestore del servizio di PEC, verifica la firma elettronica associata alla busta di trasporto per accertare l'integrità della comunicazione. In caso di esito favorevole, rilascia una ricevuta di presa in carico firmata digitalmente e trasmette la busta al punto di consegna[35]. Se il messaggio ricevuto contiene errori o proviene da una casella di posta elettronica non certificata (posta elettronica convenzionale), il punto di ricezione non emette la ricevuta di presa in carico, ma genera una busta di anomalia, includendovi il messaggio ricevuto con la specifica della natura dei problemi riscontrati. Tale busta è firmata digitalmente e inoltrata al punto di consegna.

Il punto di consegna, a fronte della ricezione di una busta di trasporto o una busta di anomalia, esegue gli stessi controlli del punto di ricezione e, in caso di esito favorevole, deposita il messaggio nella casella di PEC del destinatario. Se il messaggio depositato è una busta

---

[31] Il gestore della PEC è tenuto a conservare il messaggio contenente virus per un periodo non inferiore a 30 mesi.

[32] I dati di certificazione comprendono: la data e l'ora d'invio, le informazioni sul mittente e il destinatario, l'oggetto e l'identificativo del messaggio.

[33] La ricevuta di accettazione costituisce prova opponibile a terzi dell'avvenuta spedizione di un messaggio di PEC.

[34] Per punto di ricezione s'intende il punto che riceve il messaggio all'interno di un dominio di posta elettronica certificata.

[35] Per punto di consegna s'intende il punto che compie la consegna del messaggio nella casella di posta elettronica certificata del destinatario, verifica la provenienza/correttezza del messaggio, emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna.

di trasporto, è inviata al mittente una ricevuta di avvenuta consegna nella quale sono riportati i dati di certificazione, una copia del messaggio[36], la data e l'ora di consegna. Tale ricevuta è sottoscritta digitalmente ed ha effetti probatori[37]. Se, invece, è una busta di anomalia, non è generata alcuna ricevuta di consegna.

Gli schemi che mostrano il funzionamento di un servizio di posta elettronica certificata sono riportati nelle figure 5, 6 e 7. Tali schemi sono tratti dalle specifiche tecniche del servizio di PEC contenute nel D.M. 2 novembre 2005.

Come si vede dalle figure, è possibile inviare un messaggio da un indirizzo di posta elettronica convenzionale ad uno di PEC e viceversa. Ovviamente, nel primo caso, al mittente non sarà recapita la ricevuta di accettazione né quella di avvenuta consegna, mentre al destinatario sarà segnalata "l'anomalia". Nel secondo caso, invece, il mittente si vedrà recapitare la ricevuta di accettazione, ma non quella di avvenuta consegna.

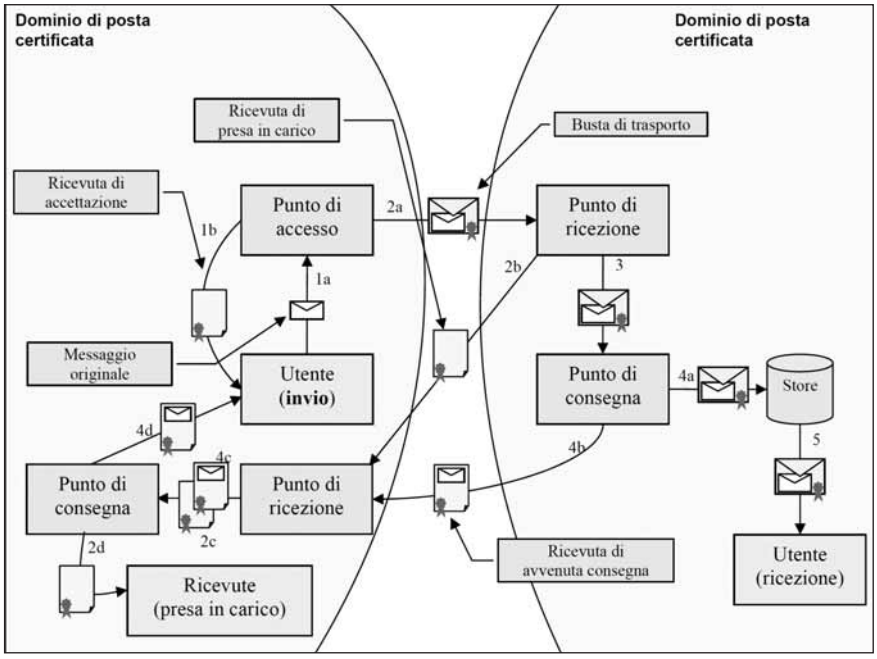

Fig. 5. Trasmissione di un messaggio tra due indirizzi di posta elettronica certificata

---

[36] La copia del messaggio è allegata solo alle ricevute che attestano l'avvenuta consegna ai destinatari primari (specificati nel campo "To:" del messaggio)

[37] Si noti che la ricevuta di avvenuta consegna è rilasciata contestualmente al deposito del messaggio di posta elettronica certificata nella casella *e*-mail del destinatario, indipendentemente dall'avvenuta lettura da parte di questi. Tale ricevuta fornisce al mittente prova che il suo messaggio è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica il momento della consegna.

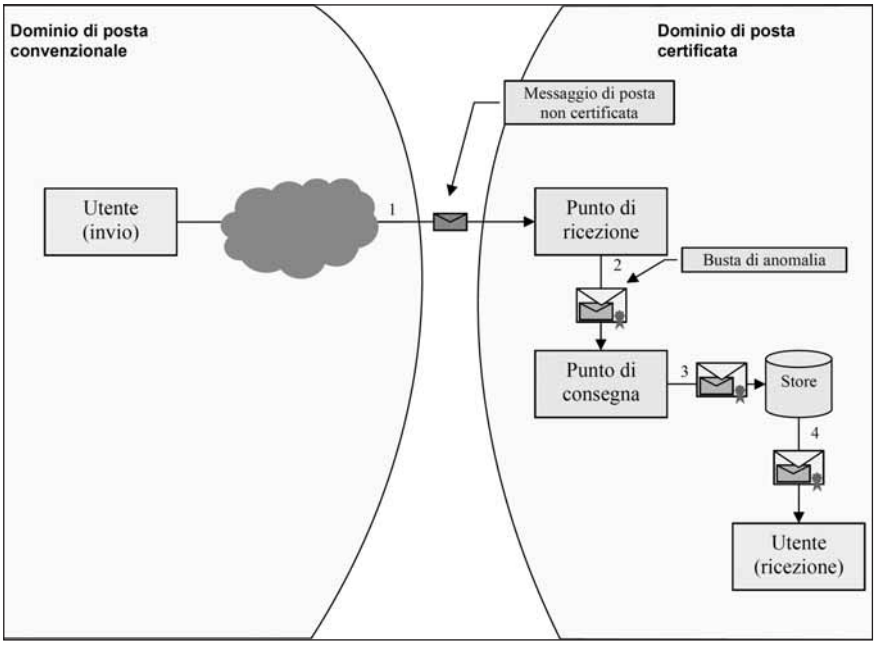

Fig. 6. Trasmissione di un messaggio da un indirizzo e-mail convenzionale a un indirizzo di PEC

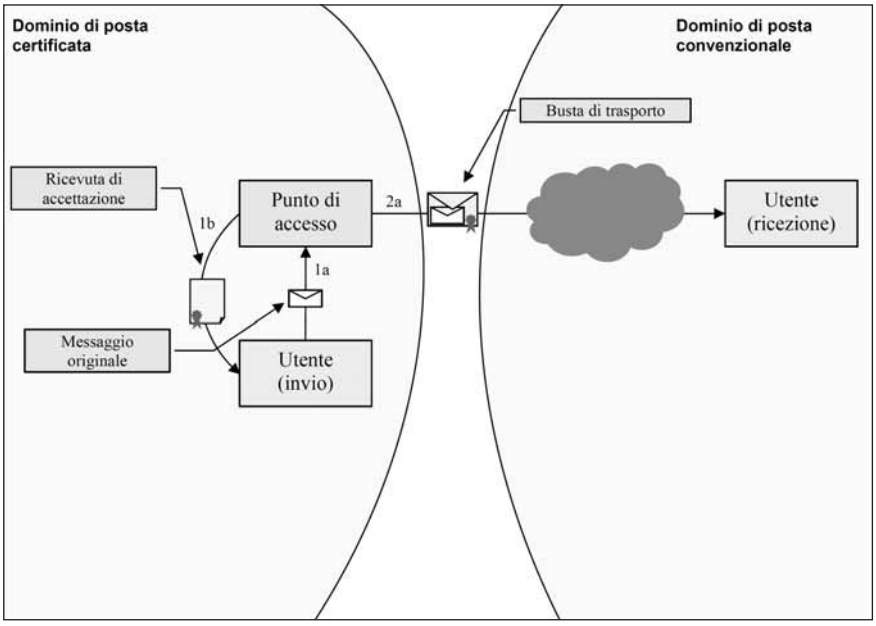

Fig. 7. Trasmissione di un messaggio da un indirizzo di PEC a un indirizzo e-mail convenzionale

I gestori del servizio di PEC devono tenere traccia delle operazioni effettuate per la trasmissione dei messaggi in un registro informatico, denominato log dei messaggi, che deve essere conservato per trenta mesi con modalità tali da assicurare la riservatezza, sicurezza, integrità ed inalterabilità nel tempo delle informazioni in esso contenute.

Il Codice dell'Amministrazione Digitale riconosce la piena efficacia delle trasmissioni di documenti informatici eseguite con un servizio di PEC:

a - l'art. 45, c. 1, dichiara che "i documenti trasmessi da chiunque a una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale";

b - l'art. 48, c. 2 , afferma che "la trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalle legge, alla notificazione a mezzo della posta", mentre il c. 3 chiarisce che "la data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al D.P.R. n. 68/2005 ed alle relative regole tecniche".

La disponibilità del servizio di posta elettronica certificata ha determinato l'emanazione di una serie di disposizioni – di seguito riportate – che spingono le pubbliche amministrazioni, i professionisti, le imprese e anche i cittadini a dotarsi di un indirizzo elettronico dichiarato.

L'art. 16, c. 8, della Legge 28 gennaio 2009, n. 2, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale, obbliga le pubbliche amministrazioni di cui all'art. 1, c. 2, del D.Lgs. 30 marzo 2001, n. 165, e successive modificazioni, ad istituire una casella di posta certificata, o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali[38], per ciascun

---

[38] Questa apertura verso un servizio di posta elettronica alternativo alla PEC, comunque capace di certificare la data e l'ora dell'invio e della ricezione delle comunicazioni, nonché l'integrità del contenuto delle stesse, sembra essere la risposta del legislatore a quanti avevano sollevato perplessità sulla incompatibilità del servizio di posta elettronica certificata con gli analoghi sistemi internazionali. Al riguardo, l'art. 35 della Legge 18 giugno 2009, n. 69, recante disposizioni per lo sviluppo economico, la semplificazione, la competitività nonchè in materia di processo civile, impegna il Governo a modificare il D.P.R. n. 68/2005 per garantire l'interoperabilità del servizio di posta elettronica certificata con analoghi sistemi internazionali.

registro di protocollo, dandone comunicazione al Centro nazionale per l'informatica nella pubblica amministrazione (DigitPA), il quale deve provvedere alla pubblicazione di tali caselle in un elenco consultabile per via telematica[39]. Il c. 6, dello stesso articolo, impone alle imprese costituite in forma societaria di indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese, o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali[40]. Il c. 7, invece, riguarda i professionisti iscritti in albi ed elenchi istituiti con Legge dello Stato e li obbliga a comunicare, entro un anno dalla data di entrata in vigore della norma, ai rispettivi ordini o collegi, il proprio indirizzo di posta elettronica certificata, o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali. Gli ordini e i collegi, a loro volta, devono pubblicare in un elenco riservato, consultabile per via telematica esclusivamente dalle pubbliche amministrazioni, i dati identificativi degli iscritti con il relativo indirizzo di posta elettronica dichiarato. Il c. 9, infine, delinea chiaramente uno scenario in cui le comunicazioni tra le pubbliche amministrazioni, i professionisti e le imprese, che hanno dichiarato il loro indirizzo nei modi sopra descritti, possono avvenire per posta elettronica certificata senza che il destinatario debba dichiarare preventivamente la propria disponibilità ad accettarne l'utilizzo.

Il D.P.C.M. 6 maggio 2009, recante disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini, completa l'attuale quadro normativo. Esso prevede la possibilità per i cittadini di ottenere un indirizzo di PEC gratuitamente, richiedendola, direttamente o tramite l'affidatario del servizio, al Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri. Una volta assegnata, la casella di PEC diventa

---

[39] Si segnala che l'obbligo per le pubbliche amministrazioni di attivare un indirizzo di posta elettronica da adibire alla ricezione dei documenti informatici, registrandolo sull'indice delle amministrazioni pubbliche e delle aree organizzative omogenee gestito dal CNIPA (www.indicepa.gov.it), era già stato previsto nel D.P.C.M. 31 ottobre 2000, contenente le regole tecniche per il protocollo informatico, e nella circolare AIPA n. 28/2001, recante standard, modalità di trasmissione, formato e definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni.

[40] Le imprese già costituite alla data di entrata in vigore della L. n. 2/2009 hanno tre anni di tempo per comunicare al registro delle imprese il loro indirizzo di posta elettronica certificata.

per il titolare un indirizzo valido, ad ogni effetto giuridico, ai fini dei rapporti con le pubbliche amministrazioni, e la volontà da questi espressa all'atto della richiesta rappresenta l'esplicita accettazione dell'invio, tramite essa, da parte delle pubbliche amministrazioni, di tutti i provvedimenti e gli atti che lo riguardano.

Il disciplinare di gara, elaborato dal Dipartimento per la Digitalizzazione della P.A. e l'Innovazione tecnologica (DDI) per la concessione del servizio di PEC per i cittadini ha inaspettatamente disegnato un servizio simile, ma non coincidente con la PEC. Lo dimostra il fatto che tra i requisiti del servizio oggetto della concessione figura "l'interoperabilità con i servizi erogati nei domini di PEC conformi al D.P.R. n. 68/2005". Insomma, un altro servizio di comunicazione elettronica certificata, il CEC-PAC, che deve garantire:

c - il rilascio delle caselle di posta elettronica per ogni cittadino maggiorenne che ne faccia richiesta, destinate esclusivamente alle comunicazioni tra P.A. e cittadino;

d - la possibilità di attivare la funzionalità aggiuntiva della ricevuta di presa visione da parte dell'utente;

e - il servizio di notifica dell'avvenuta ricezione di un messaggio sulla casella CEC-PAC tramite canali di comunicazione tradizionali[41];

f - la formazione del fascicolo elettronico personale del cittadino con i documenti ricevuti e trasmessi alle pubbliche amministrazioni.

V. - Carta d'identità elettronica e carta nazionale dei servizi

L'erogazione on line dei servizi delle pubbliche amministrazioni presuppone che i soggetti fruitori siano dotati di strumenti tecnologici e dati personali che, in quanto da loro conosciuti o ad essi univocamente associati, ne permettono l'identificazione in rete.

Il legislatore italiano, con l'obiettivo di soddisfare questa esigenza, ha emanato il D.P.C.M. 22 ottobre 1999, n. 437, che definisce le caratteristiche e le modalità di rilascio della carta d'identità elettronica (CIE) in sostituzione di quella tradizionale cartacea.

La CIE è un "documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica

---

[41] In aggiunta al servizio base di notifica tramite *e*-mail è prevista per il cittadino, a pagamento, la possibilità di ricevere le stesse segnalazioni anche via SMS, IVR e posta cartacea.

del suo titolare"[42]. Di fatto, è una carta ibrida in grado di integrare nel supporto fisico sia una banda a memoria ottica che un microprocessore[43]. Nella banda ottica a lettura laser sono memorizzati, con modalità informatiche di sicurezza, i dati riportati graficamente sul documento ai fini della salvaguardia delle esigenze di pubblica sicurezza. Il microprocessore, invece, è utilizzato per la memorizzazione dell'insieme dei dati riferiti alla persona e per le operazioni connesse alle procedure di identificazione in rete del titolare.

In via opzionale, nella CIE possono essere registrate, a richiesta dell'interessato ove si tratti di dati sensibili, le informazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attività amministrative e per l'erogazione di servizi al cittadino. L'art. 66, c. 4, del Codice dell'Amministrazione Digitale, include tra questi dati:

a - il gruppo sanguigno;

b - le opzioni di carattere sanitario previste per legge;

c - i dati biometrici della persona ad esclusione del DNA;

d - le procedure informatiche e le informazioni occorrenti per la firma elettronica.

Nel 2004, preso atto della limitata diffusione della carta d'identità elettronica a causa della dilatazione dei tempi di progettazione delle misure di sicurezza, dell'inerzia delle pubbliche amministrazioni coinvolte nell'iniziativa e soprattutto degli alti costi di realizzazione a carico del Ministero dell'Interno e delle amministrazioni comunali, il legislatore ha ritenuto opportuno introdurre un altro strumento per l'identificazione in rete: la carta nazionale dei servizi (CNS). L'art. 2, c. 1, del D.P.R. 2 marzo 2004, n. 117, recante il regolamento per la diffusione della carta nazionale dei servizi, afferma, infatti, che "la carta nazionale dei servizi, in attesa della carta d'identità elettronica, è emessa dalle pubbliche amministrazioni interessate al fine di anticiparne le funzioni di accesso ai servizi in rete delle pubbliche amministrazioni".

La CNS può essere emessa da una qualsiasi pubblica amministrazione, previa identificazione del titolare, con le modalità descritte nel D.P.R. n. 117/2004 e nelle regole tecniche e di sicurezza emanate il 9 dicembre 2004 con un Decreto congiunto del Ministro

---

[42] Si veda la definizione di carta d'identità elettronica riportata nell'art. 1, c. 1, lett. c) del D.Lgs. 7 marzo 2005, n. 82, recante il Codice dell'Amministrazione Digitale.

[43] Il supporto fisico è stampato con le tecniche tipiche della produzione delle carte valori ed è dotato degli elementi fisici di sicurezza atti a consentire il controllo dell'autenticità del documento, visivamente e mediante strumenti portatili e di laboratorio.

dell'Interno, Ministro per l'Innovazione e le Tecnologie e Ministro dell'Economia e delle Finanze. Essa contiene un certificato di autenticazione rilasciato da un certificatore accreditato[44], consistente nell'attestato elettronico che assicura l'autenticità delle informazioni necessarie per l'identificazione in rete del titolare. A differenza della CIE, che rimane valida per 10 anni dalla data di emissione, la CNS ha la validità temporale determinata dall'amministrazione emittente e comunque non superiore a 6 anni[45].

Sotto il profilo tecnologico, le due carte sono interoperabili e presentano le stesse caratteristiche funzionali, ma mentre la CIE contiene gli elementi esterni necessari per l'identificazione del titolare anche senza l'ausilio del computer (gli ologrammi prodotti dall'Istituto Poligrafico e Zecca dello Stato e la banda ottica presente sul retro), la CNS non richiede la presenza sull'involucro esterno di segni particolari[46] e quindi risulta essere meno costosa e più facile da emettere.

I servizi erogabili attraverso l'uso della carta d'identità elettronica o della carta nazionale dei servizi si dividono in due categorie: servizi standard e servizi qualificati. I primi riguardano l'identificazione in rete del titolare per mezzo del certificato di autenticazione memorizzato nel microprocessore della carta; i secondi, invece, richiedono l'installazione sulla carta, per opera delle amministrazioni emittenti, delle informazioni aggiuntive necessarie per l'erogazione *on-line* di determinati servizi. In particolare, la CIE e la CNS possono essere utilizzate per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni e sono predisposte per ospitare il servizio di firma digitale.

L'art. 64, c. 1, del Codice dell'Amministrazione Digitale, individua chiaramente nella carta d'identità elettronica e nella carta nazionale dei servizi gli "strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica".

In ragione dell'elevato livello di sicurezza garantito, ai sensi dell'art. 65, c. 1-2 del Codice dell'Amministrazione Digitale, "le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica (…) sono valide (…) quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi (…). Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal c. 1 sono equivalenti alle

---

[44] Si veda l'art. 3, c. 1, del D.P.R. n. 117/2004.
[45] Si veda l'art. 5, c. 1, del D.P.R. n. 117/2004.
[46] Ai sensi dell'art. 3, c. 4, del D.P.R. n. 117/2004, la carta nazionale dei servizi deve riportare impresso in modo leggibile, sul dorso, la dicitura «CARTA NAZIONALE DEI SERVIZI» ed il nome della pubblica amministrazione che la emette.

istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento; resta salva la facoltà della pubblica amministrazione di stabilire i casi in cui è necessaria la sottoscrizione mediante firma digitale".

VI. - Gestione informatica dei documenti e formazione dell'archivio

L'introduzione del documento informatico nel nostro ordinamento giuridico e lo sviluppo di strumenti tecnologici affidabili per le comunicazioni elettroniche hanno aggiunto nuovi elementi di complessità nei processi inerenti alla formazione e alla conservazione dell'archivio. Da un lato, infatti, occorre governare i processi che attengono all'organizzazione dei documenti, sia cartacei sia digitali, dall'altro si devono utilizzare al meglio le tecnologie informatiche per migliorare il livello di efficacia e di efficienza dell'azione amministrativa, velocizzando al massimo i flussi di lavoro.

La convinzione che le problematiche connesse alla gestione dei documenti potessero essere risolte rapidamente con l'introduzione delle tecnologie dell'informazione e della comunicazione (ICT), ha oggi lasciato il posto alla consapevolezza che la digitalizzazione dei documenti può produrre benefici solo con un approccio progettuale che prenda in considerazione gli aspetti tecnologici unitamente a quelli organizzativi, archivistici e giuridici. Tale approccio progettuale trova nella norma ISO 15489:2001 il principale standard di riferimento.

VI.1. - Norma ISO 15489:2001

Nel mese di ottobre 2001, su input del Comitato Tecnico ISO/TC 46, Information and documentation, Sottocomitato 11, archives/records management, l'International Organization for Standardization (ISO) ha emanato la norma ISO 15489:2001 allo scopo di delineare i migliori metodi operativi internazionali per la gestione dei documenti. Essa si compone di una parte generale (ISO 15489-1, Part 1: General) e di un rapporto tecnico che fornisce una guida per l'applicazione pratica delle regole generali (ISO 15489-2, Part 2: Guidelines).

La norma ISO 15489:2001 non si applica alla gestione degli archivi storici, bensì al records management, cioè all'insieme delle operazioni finalizzate al controllo della produzione, ricezione, tenuta, uso e destinazione finale dei documenti ricevuti o prodotti da un'organizzazione, o una persona fisica, durante lo svolgimento della sua attività, indipendentemente dal supporto sul quale sono formati.

Essa fornisce una guida per la progettazione e la realizzazione di sistemi documentali di qualità, tralasciando gli aspetti tecnologici in senso stretto e concentrandosi sulle politiche, procedure, metodi operativi e responsabilità.

La metodologia proposta dalla norma ISO 15489 si articola in otto fasi[47]:

a - indagine preliminare;

b - analisi delle attività;

c - identificazione dei requisiti per i documenti;

d - valutazione dei sistemi esistenti;

e - identificazione delle strategie per soddisfare i requisiti di cui alla fase c);

f - progettazione del sistema documentale;

g - implementazione del sistema documentale;

h - controlli e verifiche post-implementazione.

Le prime quattro fasi permettono di esplicitare le relazioni esistenti tra la produzione documentaria e le attività dell'organizzazione[48], il contesto normativo e regolamentare di riferimento, le esigenze di natura pratica-operativa. La rilevazione e l'analisi dei processi rappresentano un passaggio fondamentale della progettazione di un sistema documentale perché permettono di individuare i documenti ricevuti o prodotti nell'ambito delle attività dell'organizzazione, specificando la loro natura (atto pubblico, scrittura privata, provvedimento amministrativo, etc.), i contenuti minimi essenziali e accidentali, il periodo di conservazione, le esigenze in termini di accessibilità, riproducibilità e riservatezza.

La fase e) è finalizzata all'identificazione delle strategie, delle politiche, degli standard, degli strumenti e dei metodi operativi che permettono all'organizzazione di soddisfare i requisiti specificati nelle fasi precedenti.

La fase f) riguarda la progettazione vera e propria del sistema documentale, che dovrebbe essere eseguita mantenendo separati la definizione concettuale del modello organizzativo e archivistico dal disegno tecnologico e funzionale del sistema documentale che lo implementerà.

Le ultime due fasi forniscono indicazioni per l'implementazione del sistema documentale e il controllo della sua operatività.

---

[47] Per ulteriori approfondimenti sulla metodologia di progettazione di sistemi documentali di qualità si veda S. PIGLIAPOCO, *La qualità nella gestione dei documenti: la norma ISO 15489*, in *Una mente colorata. Studi in onore di Attilio Mauro Caproni per i suoi 65 anni*, a cura di C. Cavallaro, Roma, Vecchiarelli editore, 2007. Si veda inoltre G. MICHETTI, *Uno standard per la gestione documentale: il modello ISO 15489*, in «Archivi & Computer», (1) 2005, S. Miniato (PI), Titivillus Edizioni, 2005, pp. 63-82.

[48] Con il termine organizzazione qui s'intende l'ente che produce i documenti e che li vuole gestire con criteri e modalità conformi alla norma ISO 15489.

VI.2. - Registrazione di protocollo, classificazione e fascicolazione dei documenti

Le operazioni che permettono di identificare i documenti e le unità archivistiche, mostrando le relazioni che esistono tra di esse e con le attività del soggetto produttore sono: la registrazione di protocollo, la classificazione e la formazione dei fascicoli

La registrazione di protocollo è l'operazione che permette di identificare e descrivere i documenti ricevuti o spediti da un ente, fissando con certezza giuridica la data dell'ingresso o dell'uscita. Il sistema di registrare in ordine cronologico i dati essenziali dei singoli documenti nasce in area germanica e si diffonde in Italia all'inizio dell'Ottocento con la finalità principale di predisporre strumenti razionali di gestione dei documenti[49]. Il registro di protocollo oltre ad avere grande rilevanza sotto il profilo archivistico ha anche valenza giuridica; esso, infatti, è un atto pubblico cui è riconosciuta la fede privilegiata[50] in virtù "del rapporto assolutamente inscindibile che collega o almeno che dovrebbe collegare tra di loro il numero progressivo, gli estremi cronologici relativi al preciso momento dell'ingresso in memoria, l'indicazione del mittente o del destinatario e la descrizione dell'oggetto"[51].

Ai sensi dell'art. 53, c. 5, del D.P.R. 28 dicembre 2000, n. 445, recante il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, la registrazione di protocollo è un'operazione obbligatoria per i documenti ricevuti o spediti da una pubblica amministrazione e per tutti i documenti informatici. Non sono soggetti a tale obbligo: "le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione"[52].

---

[49] Cfr. G. Bonfiglio-Dosio, *Primi passi nel mondo degli archivi*, Padova, CLEUP, 2007, pp. 45-50. Si veda inoltre P. Carucci, M. Guercio, *Manule di archivistica*, Roma, Carocci editore, 2008, pp. 203-208.

[50] Sentenza della Cassazione penale, sez. V, del 6 ottobre 1987.

[51] Cfr. A. Romiti, *Le principali sentenze sul protocollo delle pubbliche amministrazioni: casistica, commento e note sentenza per sentenza*, Viareggio, SAL editoriale, 1995, p. 43.

[52] Per documenti già soggetti a registrazione particolare dell'amministrazione s'intendono quei documenti che sono registrati per obbligo di legge in repertori o registri diversi dal protocollo generale. È il caso, ad esempio, delle fatture ricevute, che devono essere registrate nel registro IVA e in altri libri contabili, degli atti deliberativi e dei contratti, che devono essere annotati in appositi repertori. Per queste tipologie di documenti il legislatore ha voluto evitare la doppia registrazione.

Una registrazione di protocollo contiene dati obbligatori e dati accessori. I dati obbligatori sono:

a - numero di protocollo, generato automaticamente dal sistema[53];

b - data di registrazione di protocollo, assegnata automaticamente dal sistema;

c - mittente per i documenti ricevuti, o destinatario per i documenti spediti;

d - oggetto del documento[54];

e - data e numero di protocollo del documento ricevuto, se disponibili.

Sono accessori i seguenti dati:

f - data di arrivo (per i documenti in entrata);

g - luogo di provenienza o di destinazione;

h - numero degli allegati (se esistono) e descrizione sintetica degli allegati;

i - estremi dell'autorizzazione al differimento della registrazione;

l - mezzo di ricezione o di spedizione;

m - ufficio di competenza;

n - copie per conoscenza;

o - tipo di documento.

Nel caso dei documenti informatici, la registrazione di protocollo determina la loro memorizzazione nell'archivio digitale: da quel momento in poi non potranno più essere modificati né cancellati[55].

Sotto il profilo pratico-operativo, la registrazione di protocollo di un documento informatico comprende, in aggiunta ai dati obbligatori sopra citati, la sua impronta digitale di 160 bit[56]; inoltre, se il documento è ricevuto per posta elettronica, essa deve corrispondere all'intero messaggio.

Ogni registrazione deve essere completata con la segnatura di protocollo che, ai sensi dell'art. 1, c. 1, lett. s), del D.P.R. n. 445/2000, consiste "nell'apposizione o nell'associazione all'originale del documento, in forma permanente e non modificabile, delle informazioni riguardanti il documento stesso". Per i documenti cartacei essa si

---

[53] È un numero progressivo costituito da almeno sette cifre numeriche, che ricomincia da 1 all'inizio di ogni anno.

[54] È una sintesi del documento che deve dare un'idea precisa del contenuto anche in assenza dell'originale.

[55] Un documento informatico archiviato segue le stesse vicende della relativa registrazione di protocollo la quale, ai sensi dell'art. 54 del D.P.R. n. 445/2000, può essere annullata, ma deve rimanere memorizzata nella base di dati per consentire la lettura di tutte le informazioni originarie.

[56] Si veda l'art. 53, c. 1, lett. f), del D.P.R. 28 dicembre 2000, n. 445.

realizza apponendo su di essi un timbro di protocollo nel quale sono riportati i dati identificativi dell'ente, la data e il numero di protocollo, l'indice di classificazione e il numero del fascicolo. Per quelli informatici, invece, la normativa vigente[57] prevede la produzione della segnatura informatica di protocollo, rappresentata da un *file* conforme alle specifiche dell'XML compatibili con la DTD (Document Type Definition) definita dal CNIPA e contenente sia le informazioni del timbro di protocollo, sia altri dati utili ai fini dell'ottimizzazione dei processi di gestione documentale.

Come sopra accennato, le registrazioni di protocollo possono essere annullate su autorizzazione del Responsabile del Servizio per la tenuta del protocollo informatico[58], ma non cancellate fisicamente; esse devono rimanere memorizzate nella base di dati e sono evidenziate dal sistema di gestione informatica dei documenti con un simbolo o una dicitura.

Qualora per cause tecniche non sia possibile utilizzare il sistema di gestione informatica dei documenti, il Responsabile del Servizio per la tenuta del protocollo informatico può autorizzare lo svolgimento, anche manuale, delle operazioni di registrazione di protocollo su registri di emergenza[59]. Al ripristino delle funzionalità del sistema, le informazioni relative ai documenti protocollati in emergenza dovranno essere riportate su di esso senza ritardo, utilizzando un'apposita funzione di recupero dei dati. A ciascun documento registrato in emergenza sarà attribuito un nuovo numero di protocollo mantenendo, però, stabilmente la correlazione con il numero utilizzato in emergenza.

La registrazione di protocollo eseguita nei modi sopra descritti è un'operazione necessaria, ma non sufficiente. Essa, infatti, permette di identificare e descrivere sinteticamente i documenti che entrano nella memoria dell'ente, fissandone la data esatta dell'ingresso, ma non di esplicitare il *vincolo o nesso archivistico*, che è l'elemento costitutivo dell'archivio ed è rappresentato dall'insieme delle relazioni logiche e formali esistenti tra i documenti che lo compongono[60].

---

[57] Si veda l'art. 18 del D.P.C.M. 31 ottobre 2000 e la Circolare AIPA n. 28/2001.
[58] Si veda il successivo paragrafo VI.3.
[59] Si veda l'art. 63 del D.P.R. n. 445/2000.
[60] Cfr. R. De Felice, *L'archivio contemporaneo*, Roma, La Nuova Italia Scientifica, 1998. Sul vincolo archivistico si veda anche A. Romiti, *Archivistica generale: primi elementi*, Lucca, Civita editoriale, 2009, pp. 47-55, dove l'autore ne analizza la natura, proponendone una distinzione in quattro tipologie: 1) vincolo archivistico interno, che attiene al nesso esistente nella documentazione realizzata e conservata dall'entità produttrice; 2) vincolo archivistico esterno, che si propone nel rapporto tra l'unità produttrice, le unità referenti e l'archivio prodotto; 3) il vincolo istituzionale esterno, che può essere individuato nel collegamento che intercorre tra l'entità produttrice dell'archivio e la realtà istituzionale, a livello territoriale, nel quale tale soggetto opera; 4) vincolo istituzionale interno, che si sviluppa nel rapporto tra l'entità produttrice e le altre realtà sociali che si pongono in collegamento con essa.

Le operazioni che rendono evidenti le relazioni esistenti tra i documenti di un archivio e tra questi e le attività del soggetto produttore sono la classificazione e la fascicolazione che, insieme alla registrazione e segnatura di protocollo, costituiscono le "operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni"[61].

I fascicoli sono le unità archivistiche di base dell'archivio; essi riuniscono in un unico contenitore, cartaceo o digitale, i documenti relativi ad un procedimento amministrativo, una persona fisica o giuridica, un oggetto specifico dell'attività del soggetto produttore. Un fascicolo può essere organizzato in sottofascicoli e questi a loro volta in inserti; al loro interno i documenti sono posti in ordine cronologico di archiviazione.

La formazione dei fascicoli avviene a cura delle unità organizzative responsabili della trattazione delle pratiche ed è guidata dal titolario di classificazione, che è uno strumento archivistico di fondamentale importanza. Esso è costituito dall'insieme delle partizioni astratte (ad esempio denominate categorie, classi e sottoclassi), gerarchicamente ordinate (una categoria si compone di più classi che a loro volta si articolano in sottoclassi), che rispecchiano le funzioni del soggetto produttore. Un titolario deve essere sufficientemente dettagliato, ma senza far perdere la visione d'insieme delle attività complessivamente svolte dall'ente produttore dell'archivio. I fascicoli sono gli elementi terminali del titolario di classificazione e si dispongono nelle varie partizioni precostituite (categorie, classi e sottoclassi) in base all'oggetto cui si riferiscono. In questo modo, gli uffici produttori alimentano continuamente l'archivio con i loro documenti, mutuando la struttura logica, unitaria, disegnata nel titolario di classificazione.

In termini pratici, classificare un documento significa associarlo alla partizione del titolario che individua la funzione cui si riferisce, mentre l'operazione di fascicolazione attiene all'inserimento del documento nell'unità archivistica che raccoglie i suoi precedenti o, comunque sia, gli atti relativi allo stesso oggetto o stessa persona.

Sul sistema di gestione informatica dei documenti, per ogni fascicolo, al minimo, si devono registrare le seguenti informazioni:

p - indice di classificazione;

q - numero del fascicolo, che è un numero progressivo nell'ambito della voce di classificazione;

r - oggetto del fascicolo;

s - data di formazione;

t - data di chiusura;

u - ente e ufficio produttore.

---

[61] Se veda l'art. 56 del D.P.R. n. 445/2000.

Gli estremi identificativi dei fascicoli, sottofascicoli e inserti, devono essere riportati, unitamente alle informazioni sui loro movimenti interni all'organizzazione, nel repertorio dei fascicoli, che è un elenco ordinato in base alle partizioni del titolario di classificazione.

VI.3. - Aspetti organizzativi e responsabilità

Lo standard internazionale ISO 15489, oltre a fornire indicazioni sulla metodologia di progettazione dei sistemi documentali di qualità, spinge le organizzazioni ad assegnare alle unità di personale un livello di responsabilità nella trattazione dei documenti commisurato al ruolo ricoperto e alle mansioni svolte.

Il legislatore italiano ha regolamentato gli aspetti organizzativi connessi alla gestione informatica dei documenti con gli articoli 50 e 61 del D.P.R. n. 445/2000. Il primo spinge le pubbliche amministrazioni a costituire "aree organizzative omogenee (AOO)", ovvero insiemi di uffici aventi l'esigenza di gestire la documentazione in modo unitario, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse, mentre il secondo decreta la nascita, in ogni AOO, di un Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, a capo del quale deve essere posto "un dirigente, ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione".

Ai sensi dell'art. 61, c. 3, del D.P.R. citato, il Servizio per la tenuta del protocollo informatico deve:

a - garantire il corretto svolgimento delle attività di gestione dei documenti, nonché la formazione, gestione, conservazione e fruizione dell'archivio;

b - attribuire il livello di autorizzazione per l'accesso alle funzioni del sistema di gestione informatica dei documenti, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;

c - garantire che le operazioni di registrazione e segnatura di protocollo si svolgano nel rispetto della normativa vigente;

d - garantire la corretta produzione e conservazione del registro di protocollo;

e - predisporre e mantenere aggiornati il titolario di classificazione e il piano di conservazione dell'archivio[62], compresi gli indici e gli altri strumenti archivistici necessari;

---

[62] Il piano di conservazione dell'archivio è il piano, integrato con il titolario di classificazione, contenente i criteri di organizzazione dell'archivio, di selezione periodica e

f - autorizzare le operazioni di annullamento delle registrazioni di protocollo.

Tra i compiti attribuiti al Responsabile del Servizio per la tenuta del protocollo informatico, assume particolare rilevanza la predisposizione e il continuo aggiornamento del manuale di gestione dei documenti, nonché il controllo dell'effettiva applicazione delle disposizioni in esso contenute da parte del personale dell'organizzazione.

VI.4. - Manuale di gestione dei documenti

In un contesto dove la gestione dei documenti è effettuata su base informatica e decentrata nelle unità organizzative, fornire al personale dell'ente le istruzioni e le regole per svolgere correttamente le attività di registrazione, classificazione e archiviazione dei documenti è una necessità assoluta.

A questo fine e ai sensi degli articoli 3 e 5 del D.P.C.M. 31 ottobre 2000, recante le regole tecniche per il protocollo informatico, il Responsabile del Servizio per la tenuta del protocollo informatico deve predisporre un manuale di gestione dei documenti, i cui contenuti devono riguardare:

a - l'assetto organizzativo adottato dall'ente per la gestione dei documenti:

1. elenco delle aree organizzative omogenee (AOO) istituite, con l'indicazione, per ciascuna di esse, delle informazioni di cui all'art. 12, c. 2, del D.P.C.M. 31 ottobre 2000;

2. individuazione, in ogni AOO, del Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, e l'identificazione del relativo Responsabile;

b - i principali strumenti archivistici utilizzati per la formazione e la conservazione dell'archivio:

1. titolario di classificazione dei documenti con i relativi indici sistematico e alfabetico;

2. piano di conservazione dell'archivio di cui all'art. 68, c. 1, del D.P.R. n. 445/2000;

c - le fasi della gestione dei documenti:

1. istruzioni per la produzione, ricezione, registrazione, classificazione e fascicolazione dei documenti;

2. regole per l'annullamento o la modifica di una registrazione di protocollo;

---

conservazione permanente dei documenti, nel rispetto delle vigenti disposizioni in materia di tutela dei beni culturali.

3. modalità di produzione e conservazione del registro di protocollo;
4. istruzioni per la tenuta del registro di emergenza;
5. modalità di gestione dei flussi documentali e dei procedimenti amministrativi;
6. istruzioni per la tenuta, conservazione e fruizione dell'archivio;

d - l'accessibilità e la sicurezza dei dati e dei documenti:

1. insieme delle regole (policy) e delle soluzioni tecnologiche da implementare per garantire l'accesso alla base documentale in condizioni di sicurezza e riservatezza.

Il manuale di gestione dei documenti deve essere adottato con atto formale, reso pubblico e comunicato a tutto il personale dell'ente, il quale è tenuto ad applicare le regole ivi contenute sotto il controllo e la supervisione del Responsabile del Servizio per la tenuta del protocollo informatico.

VI.5. - Requisiti funzionali e tecnologici dei sistemi di gestione informatica dei documenti

I requisiti funzionali dei sistemi di gestione informatica dei documenti (ERMS - Electronic Records Management Systems) sono stati oggetto di studio a livello europeo e dettagliatamente descritti nelle specifiche MoReq2 (Model Requirements for the management of electronic records)[63].

Le specifiche MoReq sono state elaborate tra il 2000 e il 2001 da un gruppo di consulenti specializzati di Cornwell Affiliates plc. su incarico della Commissione europea nell'ambito del programma IDA (Interchange of Data between Administrations) e sono state ampiamente utilizzate in Europa e in altri paesi. L'evoluzione tecnologica, i cambiamenti della normativa e le trasformazioni dei modelli organizzativi indotte dalla globalizzazione dei mercati hanno determinato l'esigenza di un aggiornamento che ha portato alla pubblicazione, nel 2008, della nuova versione delle specifiche: MoReq2.

Le specifiche MoReq2, come del resto la prima versione del 2001, non sono legate ad una determinata piattaforma tecnologica e vogliono fornire indicazioni di carattere generale, effettivamente utili a livello pratico (usabilità), sia ad organizzazioni pubbliche che private.

Le principali novità hanno riguardato:

a - una maggiore modularità, che consente di adattarle ai diversi contesti giuridici, pratiche archivistiche ed esigenze di gestione

---

[63] Nelle specifiche MoReq2, con il termine *record* s'intendono le informazioni prodotte, ricevute e conservate ai fini probatori e informativi da una persona fisica o giuridica per soddisfare obblighi legali o per lo svolgimento delle proprie attività.

documentale. Esse comprendono un modulo di base, che contiene i requisiti fondamentali necessari a fornire un'affidabile gestione dei documenti informatici, e moduli opzionali, che descrivono funzionalità supplementari;

b - l'elaborazione di un capitolo introduttivo (il capitolo zero), con il quale si è inteso fornire agli Stati membri la possibilità di aggiungere i propri requisiti nazionali specifici, tenendo così conto delle diverse lingue, legislazioni, regolamenti e tradizioni archivistiche;

c - la disponibilità di test per la verifica della conformità ai requisiti MoReq2[64], che ha permesso di migliorare la comprensione delle specifiche e di conseguire una maggiore coerenza terminologica, anche in relazione ad altri standard di riferimento quali ISO 15489 e il progetto di ricerca internazionale InterPARES.

Le specifiche MoReq2 riconoscono allo schema di classificazione dei documenti, predisposto con le modalità descritte nel precedente paragrafo VI.2., un ruolo centrale nella gestione dei documenti e propongono il modello riportato in figura 8.

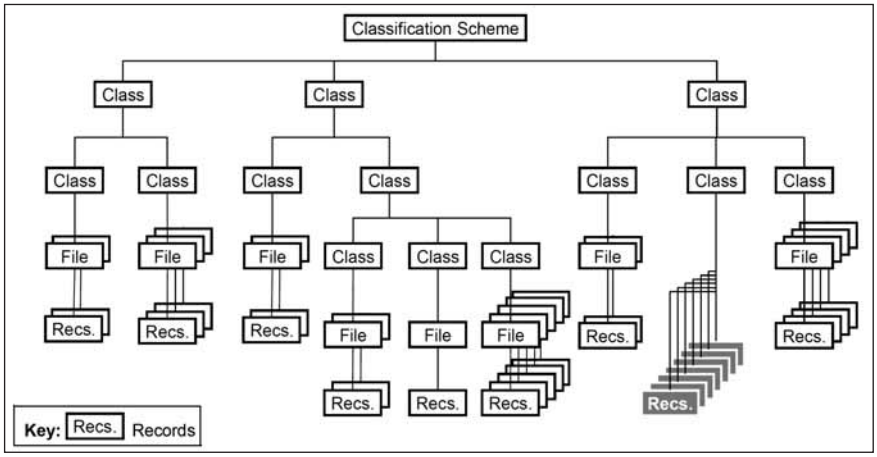

Fig. 8. Schema di classificazione dei documenti proposto in MoReq2

Come si vede dalla figura, lo schema di classificazione proposto in MoReq2 prevede di raggruppare le funzioni del soggetto produttore in classi le quali possono essere suddivise in sottoclassi le quali, a loro volta, possono essere ulteriormente ripartite in altre entità di livello più specifico. L'elemento terminale di una catena di classi ed eventuali

[64] I requisiti per i quali è disponibile un ambiente di test per la verifica della conformità riportano nel campo Test una "Y", se il test permette una verifica totale, o una "P", se il test consente una verifica parziale.

sottoclassi è il fascicolo (file)[65], il quale si compone di documenti (records) ed eventualmente di sottofascicoli contenenti altri records. Un fascicolo o sottofascicolo può essere organizzato in volumi per formare entità elettroniche di dimensione più gestibile. A differenza della prima versione, le specifiche MoReq2 contemplano anche la possibilità di associare uno o più documenti direttamente ad una classe.

Tra le funzioni che un sistema ERMS deve presentare per la gestione dello schema di classificazione, si evidenziano: la possibilità di aggiungere in qualsiasi momento nuove classi; la storicizzazione delle modifiche apportate allo schema nel corso degli anni; la possibilità di spostare uno o più fascicoli da una classe ad un'altra; l'implementazione delle regole che governano la chiusura dei fascicoli; la capacità di associare un documento a più fascicoli e a più classi; la gestione delle attività inerenti alla sostituzione di uno schema in uso con un altro di nuova concezione.

Nel documento MoReq2, le specifiche funzionali del sistema di gestione informatica dei documenti (ERMS) sono riportate nei capitoli dal 3 al 9, mentre il capitolo 10 descrive i moduli opzionali, il capitolo 11 espone i requisiti non funzionali, il capitolo 12 si occupa dei metadati e il capitolo 13 propone un modello funzionale di sistema ERMS. Nel seguito sono commentati, con riferimento ai capitoli che li contengono, i requisiti funzionali più significativi descritti in MoReq2, anche in rapporto alla normativa vigente in Italia, rinviando ogni approfondimento al testo completo delle specifiche reperibile sul sito www.DLM-Network.org/moreq2.

Controlli e sicurezza (capitolo 4)

Nel capitolo 4 del documento MoReq2 sono analizzate le esigenze in termini di sicurezza, integrità e riservatezza dei documenti immessi nel sistema ERMS, e individuati i requisiti funzionali, che trovano nella normativa vigente in Italia un utile completamento.

Il sistema operativo dell'elaboratore su cui è implementato il sistema di gestione informatica dei documenti, ai sensi dell'art. 7 del D.P.C.M. 31 ottobre 2000, deve assicurare:

a - l'univoca identificazione ed autenticazione degli utenti;

b - la protezione delle informazioni relative a ciascun utente nei confronti degli altri;

c - la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;

---

[65] Nelle specifiche MoReq2, con il termine file s'intende un fascicolo, cioè un insieme organizzato di documenti, raggruppati insieme perché relativi a un medesimo oggetto, alla medesima attività o allo stesso procedimento.

d - la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo da garantire l'identificabilità dell'utente stesso (audit trail[66]). Tali registrazioni devono essere protette da modifiche non autorizzate e conservate.

Il software utilizzato per la gestione informatica dei documenti, inoltre, deve avere caratteristiche tali da assicurare:

e - il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppi di utenti, garantendo il pieno rispetto delle disposizioni contenute nel D.Lgs. n. 196/2003, recante il Codice in materia di protezione dei dati personali;

f - il tracciamento di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore. Tali registrazioni devono essere protette da modifiche non autorizzate e conservate.

Infine, deve essere garantita la puntuale esecuzione, da parte di personale autorizzato, delle operazioni di backup dei dati e dei documenti memorizzati sul sistema ERMS, con particolare attenzione a quelli definiti "vitali" per l'organizzazione, conservando le copie in locali sicuri e differenti (disaster recovery). Ogni attività di manutenzione, backup o restore, eseguita sul sistema deve essere monitorata e tracciata, verificando sistematicamente il buon esito dell'operazione.

Conservazione e disposizioni finali (capitolo 5)

I sistemi ERMS devono presentare idonee funzionalità per individuare ed eventualmente eliminare i documenti per i quali è trascorso il periodo minimo di conservazione stabilito con appositi programmi[67]. Inoltre, devono essere in grado di gestire i processi di trasferimento, esportazione e distruzione del materiale documentario archiviato[68]. Per quanto concerne i requisiti funzionali inerenti alla conservazione a lungo termine di complessi documentari digitali, alla selezione o scarto archivistico, si veda il testo di Maria Guercio riportato nel capitolo precedente.

---

[66] Nelle specifiche MoReq2 per audit trail s'intende la memorizzazione delle transazioni che riguardano il sistema di gestione informatica dei documenti, sia le azioni intraprese dagli utenti e dagli amministratori sia quelle automaticamente determinate dal sistema medesimo sulla base di parametri predefiniti.

[67] Si tratta del piano di conservazione dell'archivio citato nel paragrafo VI.3.

[68] Il trasferimento di documenti da un sistema ERMS ad un altro può rendersi necessario nel caso di passaggio di funzioni tra enti o per questioni di natura giuridica o amministrativa. Il termine "esportazione"si riferisce invece al processo di produzione di una copia dei documenti e delle relative aggregazioni archivistiche per un altro sistema.

Acquisizione e riconoscimento dei documenti (capitolo 6)

Acquisire un documento significa registrarlo nel sistema ERMS, associarlo ad un fascicolo afferente ad una classe dello schema di classificazione e memorizzarlo nel dispositivo di storage. Unitamente ai documenti devono essere acquisiti i relativi metadati definiti in fase di configurazione del sistema.

I principali requisiti funzionali specificati per lo svolgimento di queste operazioni sono: la disponibilità di meccanismi atti a garantire l'immodificabilità del contenuto dei documenti informatici durante la fase di acquisizione; la capacità di identificare il formato di un oggetto elettronico e di memorizzare le relative informazioni per poterle utilizzare nei processi di conservazione e accesso; il controllo dell'esistenza di documenti archiviati aventi lo stesso oggetto di quello in via di acquisizione; la possibilità di registrare i metadati relativi ad un documento sia in modo automatico sia manualmente.

In questo capitolo delle specifiche MoReq2 sono analizzate anche le problematiche connesse all'acquisizione dei documenti ricevuti attraverso un servizio di posta elettronica, o prodotti con un processo di scansione.

Per quanto concerne la trattazione dei documenti informatici ricevuti per posta elettronica, il tema è stato affrontato nel precedente paragrafo IV; le specifiche MoReq2 sottolineano la necessità che il sistema ERMS sia integrato con il servizio di posta elettronica e sia in grado di catturare le e-mail a prescindere dal loro valore, che dovrà essere valutato direttamente dall'utente.

Un processo di scansione, eseguito in modo interattivo o batch[69], permette di acquisire in formato elettronico un documento originale cartaceo. Esso comprende le seguenti fasi:

a - acquisizione delle immagini in modo che ad ogni documento, anche composto da più pagine, corrisponda un unico oggetto digitale in formato standard compatibile con il processo di conservazione;

---

[69] Per processo di scansione interattivo s'intende la digitalizzazione dei documenti cartacei al momento della loro registrazione di protocollo, come fase finale dell'inserimento dei dati che li identificano. Un processo di scansione batch, invece, prevede la digitalizzazione di un blocco di documenti già protocollati, anche numericamente consistente, con strumenti tecnologici che permettono di collegare automaticamente le immagini dei documenti alle rispettive registrazioni di protocollo. Normalmente, i processi di scansione batch sono preferiti a quelli di tipo interattivo quando si devono trattare giornalmente una grande quantità di documenti e si dispongono di soluzioni tecnologiche avanzate, quali ad esempio quelle basate sul riconoscimento automatico del codice a barre stampato nella segnatura di protocollo.

b - verifica della qualità delle immagini acquisite;

c - collegamento delle immagini alle rispettive registrazioni di protocollo;

d - memorizzazione delle immagini nel sistema di gestione informatica dei documenti, in modo non modificabile.

Sistemi di identificazione (capitolo 7)

Ogni entità registrata nel sistema ERMS – classe, sottoclasse, fascicolo, sottofascicolo, documento, volume – deve essere identificata in modo univoco in base ad un sistema di codifica predefinito. A questo fine si utilizza la numerazione di protocollo, l'indice di classificazione, la numerazione dei fascicoli, che è progressiva nell'ambito delle rispettive classi, e la numerazione dei sottofascicoli, che invece è progressiva nell'ambito dei fascicoli di appartenenza.

Ricerca, reperimento e riproduzione (capitolo 8)

La ricerca è il processo volto all'individuazione dei documenti e dei fascicoli attraverso un insieme di parametri specificati dall'utente, mentre la riproduzione attiene alla capacità di visualizzare o stampare il documento trovato. Un sistema ERMS deve fornire una serie di strumenti di ricerca in grado di agire sia sui metadati sia sul contenuto dei documenti (ad esempio, ricerche a testo libero). In ogni caso, deve essere garantito il controllo degli accessi attraverso l'autenticazione degli utenti con user-id e password o altri strumenti tecnologici che garantiscono una maggiore sicurezza[70].

Funzioni amministrative (capitolo 9)

Le funzioni amministrative riguardano la gestione della configurazione del sistema (memoria disponibile, utenti, categorie di sicurezza dei documenti, etc.), il monitoraggio dello stato di funzionamento di ogni modulo dell'ERMS e la produzione di report e statistiche per l'amministratore di sistema.

Moduli opzionali (capitolo 10)

Un sistema ERMS deve essere in grado di gestire fascicoli elettronici, fascicoli cartacei e fascicoli ibridi, composti cioè in parte da documenti informatici e in parte da documenti cartacei. Le entità fisiche devono essere descritte e associate allo schema di classificazione come quelle elettroniche, ma per esse si devono gestire anche le informazioni relative alla movimentazione e alla posizione fisica.

---

[70] Si vedano le caratteristiche della carta d'identità elettronica e della carta nazionale dei servizi descritte nel paragrafo V.

Le specifiche MoReq2 pongono l'accento sull'opportunità di integrare un sistema ERMS con un modulo EDMS (Electronic Document Management System)[71] dedicato alla gestione dei processi inerenti alla formazione dei documenti, un modulo WfMS (Workflow Management System) per la gestione dei flussi di lavoro e una piattaforma tecnologica di firma elettronica e crittografia[72].

Particolare rilevanza è attribuita all'integrazione del sistema ERMS con i sistemi per la gestione automatizzata dei processi strutturati, quali sono ad esempio i procedimenti amministrativi di una pubblica amministrazione. Un Workflow Management System (WfMS) è un sistema che definisce, crea e gestisce l'esecuzione dei flussi di lavoro, attraverso l'uso di software che interpretano le definizioni dei processi, interagiscono con i soggetti chiamati a svolgere le attività e, quando necessario, richiamano l'uso di strumenti e applicazioni di Information Technology (IT). Dai documenti elaborati dalla WfMC (Workflow Management Coalition), si possono individuare tre gruppi di funzioni comuni a tutti i sistemi di workflow management:

a - *Build-time functions*: comprende le funzioni per la definizione e la modellazione (prototipazione) dei processi attraverso la specificazione delle attività che li compongono, dell'ordine con cui queste attività devono essere eseguite, delle regole che ne guidano lo svolgimento e delle condizioni d'inizio e di fine del flusso di lavoro;

b - *Run-time functions*: comprende le funzioni per l'esecuzione delle istanze dei processi modellati. A questo livello, la definizione di processo è interpretata da un software responsabile dell'esecuzione delle singole attività, che possono essere assegnate ad unità di personale oppure ad applicazioni informatiche con meccanismi di interoperabilità e cooperazione applicativa tra sistemi;

c - *Interface functions:* comprende le funzioni che realizzano l'interfaccia tra i partecipanti ai flussi di lavoro e il motore di workflow (*Workflow Engine*). Questa interfaccia è realizzata dal cosiddetto *Workflow Handler*, un applicativo che mostra agli attori di un processo, siano essi risorse umane o informatiche, la lista delle attività da svolgere (*worklist*) e l'elenco dei compiti assegnati nell'ambito di ciascuna attività (*workitem*). Allo stesso tempo, consente a ciascun utente di comunicare al *Workflow Engine* le operazioni effettuate e gli eventi accaduti.

---

[71] Un sistema EDMS permette di gestire i documenti in diverse versioni e di modificarli in qualsiasi momento, mentre in un ERMS i documenti sono immodificabili e non possono essere cancellati fisicamente. Inoltre, al contrario dell'ERMS che è destinato a fornire un deposito sicuro di documenti, l'EDMS è prevalentemente destinato a supportare l'uso quotidiano dei documenti per le attività correnti.

[72] Ampiamente descritta nei precedenti paragrafi II e III.

Requisiti non funzionali (capitolo 11)

I requisiti non funzionali riguardano la facilità d'uso del sistema, la sua disponibilità e scalabilità, i vincoli legislativi e normativi, i metodi per fronteggiare l'obsolescenza tecnologica.

Requisiti sui metadati (capitolo 12)

Le specifiche MoReq2 identificano anche i metadati funzionali generici, obbligatori o facoltativi, relativi allo schema di classificazione, ai fascicoli e ai documenti, proponendone un modello molto dettagliato e dichiaratamente conforme allo standard ISO 23081 - Records management processes – Metadata for records[73] – e allo standard ISO 15836 - The Dublin Core metadata element set (for discovery purposes).

[73] In realtà, mentre lo standard ISO 23081 si riferisce ad un ambiente completo di gestione dei documenti, MoReq2 prende in esame solo la parte che riguarda l'operatività dei sistemi ERMS.