

CAPITOLO QUINTO

Protocollo informatico e firma digitale

Quadro di riferimento normativo

5.1. PREMESSA

Negli ultimi anni, il processo di informatizzazione della pubblica amministrazione ha subito una grande accelerazione anche a fronte di un notevole impegno a livello governativo che ha portato a definire un quadro normativo e tecnico sufficientemente completo per poter utilizzare le nuove tecnologie informatiche in seno alla pubblica amministrazione anche se spesso non direttamente applicabile alla Giustizia Amministrativa.

Il secondo comma dell'art. 15 della legge 15 marzo 1997, n. 59 (c.d. "Bassanini uno") stabilisce che «gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi a tutti gli effetti di legge». Questa legge ha innescato un processo di riforma fondamentale che ha portato alla definizione delle specifiche tecniche della firma digitale ed ha dato impulso alla realizzazione della Rete unitaria della pubblica amministrazione quale mezzo di trasmissione di documenti elettronici. Le norme di attuazione della firma digitale sono le seguenti.

Il regolamento attuativo è contenuto nel d.p.r. 513 del 1997 (pubblicato sulla *Gazzetta ufficiale* n. 60 del 13 marzo 1998) e definisce le modalità di attuazione della firma elettronica nella pubblica amministrazione.

Il regolamento tecnico è contenuto nel d.p.c.m. 8 febbraio 1999, pubblicato sulla *Gazzetta ufficiale* n. 89 del 15 aprile 1999. Il testo è suddiviso in due parti. Le norme vere e proprie in 3 articoli e le regole tecniche contenute in un apposito allegato.

Altra importante innovazione nell'ambito del generale disegno di riforma della pubblica amministrazione è indubbiamente il protocollo informatico poiché, da un lato, esso comporta l'attuazione concreta del diritto di accesso ai documenti amministrativi (introdotto dalla legge 8 agosto 1990, n. 241) dall'altro si pone l'obiettivo di razionalizzare, riorganizzare, ridistribuire, secondo criteri di maggiore efficienza e di riduzione dei costi, le immense risorse umane e materiali attual-

mente destinate alla gestione dei flussi documentali nell'ambito della pubblica amministrazione.

5.2. NORME DI RIFERIMENTO SUL PROTOCOLLO INFORMATICO

Il sistema del protocollo nella pubblica amministrazione si è basato fino ad oggi sul regio decreto n. 35 del 25 gennaio 1900, che prescrive, per ogni amministrazione, l'apposizione di un timbro con la data ed il numero progressivo sui documenti protocollati, la trascrizione di questi su un apposito registro, ed i meccanismi per la fascicolazione (creazione di un fascicolo con documenti correlati), l'invio al destinatario e l'archiviazione. Questa normativa non è più idonea a fornire un servizio adeguato.

Come detto, sulla base di quanto previsto dell'art. 15 della legge n. 59 del 1997, è stato istituito un nuovo sistema di protocollo, con il d.p.r. 20 ottobre 1998, n. 428 «Regolamento recante norme per la gestione del protocollo informatico da parte delle amministrazioni pubbliche».

Il decreto rimanda ad un regolamento tecnico la definizione delle modalità tecniche di gestione del protocollo informatico. Tale regolamento è stato approvato dall'AIPA il 2 dicembre 1999 e trasmesso per la definitiva approvazione nella forma di d.p.c.m. D'ora in poi ci riferiremo a questo testo con il termine "regole tecniche", in breve RT. Deve, inoltre, essere ricordata la direttiva del Presidente del Consiglio dei ministri 28 ottobre 1998 «Gestione informatica dei flussi documentali nelle pubbliche amministrazioni».

Il protocollo informatico è attuato dalla normativa, già in vigore, che introduce il documento elettronico e la firma digitale (d.p.r. n. 513 del 1997 e d.p.c.m. 8 febbraio 1999). A queste normative va aggiunta la deliberazione AIPA n. 24/98, del 30 luglio 1998, che contiene le regole tecniche per l'archiviazione dei documenti su supporti magnetici e ottici.

La nuova normativa, contenuta nel d.p.r. n. 428 del 1998 e nelle successive regole tecniche ridisegna completamente il sistema del protocollo.

La gestione del protocollo avviene con procedure informatiche e quindi, per poter protocollare, ogni amministrazione dovrà dotarsi di un sistema di protocollo informatico che abbia alcune «funzionalità minime» previste dal decreto. Il protocollo informatico deve, secondo l'art. 3, d.p.r. n. 428 del 1998:

- garantire la sicurezza e l'integrità dei dati,
- garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;

- **fornire informazioni sul collegamento** esistente tra ciascun documento ricevuto dall'Amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
- consentire il **reperimento delle informazioni riguardanti i documenti registrati**;
- consentire, in condizioni di sicurezza, l'**accesso alle informazioni da parte dei soggetti interessati, nel rispetto delle disposizioni della legge 31 dicembre 1996, n. 675, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali**;
- **garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato.**

Possiamo sintetizzare dicendo che il sistema di protocollo informatico deve fornire tre tipi di servizi:

- **servizi di certificazione**, in quanto con la «registrazione di protocollo» l'ente certifica che un determinato documento è stato creato o è comunque entrato nell'amministrazione a partire da una certa data oppure è stato trasmesso a qualcuno;
- **servizi di catalogazione**, in quanto i documenti debbono essere correttamente organizzati nell'ambito di un determinato sistema di classificazione, e poi archiviati;
- **servizi di directory** in quanto deve «consentire il reperimento delle informazioni riguardanti i documenti registrati» e «fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali».

Inoltre, deve fornire questi servizi garantendo la sicurezza dei dati, la loro riservatezza, e l'accesso rapido a tutti coloro che ne hanno diritto.

Sono tenuti a realizzare la gestione del protocollo con sistemi informativi automatizzati (art. 1, comma 1, d.p.r. 428/1998) le pubbliche amministrazioni indicate dall'articolo 1, comma 2, del decreto legislativo 3 febbraio 1993, n. 29, che sono «tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le regioni, le province, i comuni, le comunità montane, e loro consorzi ed associazioni, le istituzioni universitarie, gli istituti autonomi case popolari, le camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale».

Il d.p.r. n. 428 del 1998 individua un tempo massimo per la sua attuazione concreta, fissandolo al 31 dicembre 2003, prevedendo, al comma 3 dell'art. 21, che le pubbliche amministrazioni provvedono, entro cinque anni, a partire dal 1° gennaio 1999, a realizzare o revisionare sistemi informativi automatizzati finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi in conformità alle disposizioni del regolamento stesso ed alle disposizioni della legge 31 dicembre 1996, n. 675 (tutela dei dati personali), nonché dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 e dei relativi regolamenti di attuazione» (gestione con strumenti informatici dei documenti e firma digitale).

Esaminiamo più nel dettaglio le disposizioni contenute nel d.p.r. n. 428 del 1998, che riguardano il protocollo informatico, integrate con le regole tecniche previste dall'AIPA.

5.2.1. ALCUNI CONCETTI INTRODOTTI DAL D.P.R. N. 428 DEL 1998 E RELATIVE REGOLE TECNICHE

Il decreto sul protocollo (art. 2) ribadisce che «la gestione dei documenti è effettuata mediante sistemi informativi automatizzati», nell'ambito di «grandi aree organizzative omogenee, entro le quali vengono definiti «criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna fra le aree stesse»

Ogni amministrazione deve individuare gli uffici da considerare Aree Organizzative Omogenee (AOO), una o più a seconda delle dimensioni dell'ente, entro le quali vi sarà un sistema unico di protocollo e gestione documentale. Tutte le AOO dovranno utilizzare «criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse» (art. 2, comma 2). Per ogni AOO verrà istituita una specifica struttura, chiamata «Servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi» (SPIGFD).

Allo SPIGFD «è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente» (art. 12). Tale figura viene definita dal regolamento tecnico «Responsabile del servizio» (art. 2 RT), e deve essere nominata con apposito atto per ciascuna AOO.

Il ruolo del responsabile del servizio dell'AOO è definito dall'art. 12 del decreto e dall'art. 3 delle regole tecniche. Dal ruolo e dalle responsabilità assegnate a questa figura si desume la centralità che il protocollo informatico andrà ad assumere nel contesto della gestione dei flussi documentali nella pubblica amministrazione. Il responsabile del servizio, entro centottanta giorni dalla nomina, predispone il «manuale di gestione» di cui all'art. 4 RT. Ogni AOO dovrà redigere il «manuale di

gestione" del servizio, che «descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio» (art. 4, comma 1, RT).

Inoltre viene istituito l'«Indice delle amministrazioni pubbliche e delle aree organizzative omogenee» (IAP), previsto nel titolo III delle RT. Lo IAP è «destinato alla conservazione e pubblicazione di codici identificativi e dei dati relativi alle amministrazioni, le aree organizzative omogenee e gli uffici che utilizzano i servizi di interoperabilità della Rete unitaria» (art. 11, comma 1, RT).

I dati contenuti nello IAP, per ogni singola amministrazione pubblica, sono indicati nell'art. 10, comma 2, RT. Lo IAP contiene un «codice identificativo» (CI) di ogni pubblica amministrazione e di ogni AOO nelle quali questa sia eventualmente suddivisa, oltre a vari altri dati. Il CI «associato a ciascuna amministrazione è il nome identificativo dell'amministrazione nell'ambito del *directory service* della Rete unitaria» (art. 10, comma 3, RT). Il CI di ciascuna AOO è «generato ed attribuito dall'amministrazione a cui l'area stessa fa riferimento» (art. 10, comma 4 RT).

L'accesso allo IAP sarà garantito, per via telematica (attraverso la RUPA). L'art. 12, comma 1, RT stabilisce che l'«indice delle amministrazioni pubbliche è gestito da un sistema informatico in grado di permettere l'accesso e la consultazione delle informazioni in esso contenute da parte delle amministrazioni o di tutti i soggetti pubblici o privati tramite servizio conforme al *directory service* della Rete unitaria della pubblica amministrazione».

5.2.2. LA REGISTRAZIONE DI PROTOCOLLO

La registrazione di protocollo è un'operazione di memorizzazione di dati in un archivio informatico (art. 4, comma 1, d.p.r. 428/98). Per ogni documento in entrata o uscita, soggetto a registrazione di protocollo, i dati da inserire nell'archivio informatico sono:

- numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile,
- oggetto del documento, registrato in forma non modificabile;
- data e protocollo del documento ricevuto, se disponibili;

- **L'impronta del documento informatico**, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

Riguardo alla generazione dell'impronta le regole tecniche (art. 16) recitano:

«1. Nell'effettuare l'operazione di registrazione di protocollo dei documenti informatici l'impronta di cui all'art. 4 comma 1 lettera f) del decreto va calcolata sull'intero insieme dei computer inviati.

2. La generazione dell'impronta si effettua impiegando la funzione di *hash*, definita nella norma ISO/IEC 10118-3:1998, *Dedicated Hash-Function 3*, corrispondente alla funzione SHA-1.»

Tutte le informazioni devono essere inserite in un'unica sessione, con esclusione di ogni intervento intermedio, anche indiretto, da parte dell'operatore (art. 4, comma 3, d.p.r. 428/98).

Eventuali informazioni annullate «devono rimanere memorizzate nella base di dati per essere sottoposte alle elaborazioni previste dalla procedura. La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie, poi annullate, unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione» (art. 5, comma 1, d.p.r. 428/98).

«L'annullamento anche di una sola delle informazioni registrate in forma non modificabile generate o assegnate automaticamente dal sistema determina l'automatico e contestuale annullamento della registrazione di protocollo» (art. 7, comma 1, RT).

Le informazioni registrate in forma non modificabile possono essere annullate «esclusivamente per la correzione di errori intercorsi nella operazione di registrazione di protocollo che rendono incongruenti le informazioni della registrazione di protocollo con il documento originale»; l'annullamento «determina, relativamente alla medesima registrazione di protocollo, l'automatica e contestuale attivazione di una nuova sessione di attività di registrazione per la sola memorizzazione delle informazioni congruenti» (art. 7, comma 2, RT).

5.2.3. LA SEGNAURA DI PROTOCOLLO

La «segnatura di protocollo» è costituita da «informazioni» associate ad ogni documento, sia cartaceo sia elettronico, che sia stato sottoposto alla registrazione di protocollo. Le informazioni della segnatura di protocollo sono anche parte dei

dati di registrazione, e devono essere rese disponibili per via telematica in formato standard.

«L'associazione della **segnatura** al protocollo da un documento deve essere **permanente e non modificabile**» (art. 1, comma 1, lett. d), d.p.r. n. 428 del 1998) e deve essere effettuata **«contemporaneamente all'operazione di registrazione di protocollo»**.

Le informazioni minime (obbligatorie) da includere nella **segnatura di protocollo** sono (art. 6, comma 1, d.p.r. n. 428/1998 e art. 8, comma 1, e art. 18, comma 1, RT):

- il codice dell'amministrazione;
- il codice dell'AOO;
- la data di protocollo, secondo il formato gg/mm/aaaa;
- il numero progressivo di protocollo, secondo il formato: **numero ordinale** costituito da 7 cifre numeriche e rinnovato ogni anno;
- l'oggetto del documento;
- il mittente del documento;
- il destinatario o i destinatari del documento.

Se necessario, ad esempio nel caso esistano allegati o vi siano altre informazioni essenziali, queste andranno aggiunte alla **segnatura**.

L'art. 17, comma 1, RT specifica che «i **dati relativi alla segnature di protocollo** di un documento **trasmesso da una area organizzativa omogenea** sono contenuti, un'unica volta nell'ambito dello stesso messaggio, in un *computer* conforme alle specifiche dell'XML 1.0, contenente le informazioni minime di cui al comma 1 dell'art. 18 (RT). Le ulteriori informazioni definite al comma 2 dello stesso articolo sono incluse nello stesso *computer*».

5.2.4. REQUISITI DEL SISTEMA DEL PROTOCOLLO

I requisiti minimi, sia dal punto di vista delle regole organizzative sia da quello delle caratteristiche dei sistemi tecnologici, sono definiti dall'art. 7 d.p.r. n. 428 del 1998:

«Le operazioni di registrazione indicate all'articolo 4 e le operazioni di **segnatura di protocollo** di cui all'articolo 6 del presente regolamento nonché le operazioni di classificazione costituiscono operazioni **necessarie e sufficienti per la tenuta del protocollo informatico da parte delle pubbliche amministrazioni**».

Per **ottemperare ai requisiti minimi** ogni amministrazione dovrà identificare le aree organizzative omogenee, e per ognuna di queste istituire un servizio e nominare un responsabile; dovrà dotarsi di un **registro informatico** e dovrà scrivere il «manuale

di gestione». Dovrà inoltre dotarsi di un sistema informatico in grado di immagazzinare i dati delle registrazioni di protocollo, e di consentirne l'inserimento e la ricerca.

La definizione, nel testo delle regole tecniche, dei requisiti minimi ipotizza che il sistema del protocollo informatico, una volta integrato con la firma digitale e con le funzioni di interoperabilità con la rete unitaria, possa essere l'unico sistema informatizzato presente all'interno di una pubblica amministrazione e che con esso si ottemperi alle norme contenute nella legge sul documento informatico. In ogni caso, tra i requisiti minimi del sistema di gestione informatizzata dei procedimenti amministrativi (che deve includere il protocollo), oltre alla «registrazione di protocollo», devono essere incluse le funzionalità previste dall'art. 16 d.p.r. n. 428 del 1998. Tale norma specifica che il sistema di gestione informatizzata dei procedimenti amministrativi, oltre a quanto previsto all'art. 3, deve anche:

- fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
- consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
- fornire informazioni statistiche sull'attività dell'ufficio;
- consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi.

Il d.p.r. n. 428 del 1998 definisce, inoltre, un insieme di «funzionalità aggiuntive», che le amministrazioni possono realizzare sulla base del «rapporto tra costi e benefici nell'ambito dei propri obiettivi di miglioramento dei servizi e di efficienza operativa» (art. 5, comma 2, RT).

Vanno considerate funzionalità aggiuntive al sistema informatico del protocollo, e quindi con questo integrate, tutte le procedure informatiche preesistenti o successivamente realizzate, autonomamente o sulla base di altra normativa (ad esempio le norme sul documento elettronico e sulla firma digitale), che coinvolgano la gestione dei flussi documentali (assegnazione e flusso di pratiche, gestione di procedimenti amministrativi, ecc.).

Le funzionalità aggiuntive devono condividere con la funzionalità minima «almeno i dati di identificazione dei documenti» (art. 5, comma 3, RT).

5.2.5. LE SPECIFICHE PER LA SICUREZZA

Le regole tecniche indicano i requisiti minimi di sicurezza dei sistemi di protocollo informatico (art. 6 RT).

«1. Il sistema operativo, dei cui servizi si avvale il sistema di protocollo informatico, 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;
- d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantire l'identificabilità dell'utente stesso. Tali registrazioni devono essere protette da modifiche non autorizzate.

2. Il sistema di protocollo informatico deve consentire il controllo differenziato dell'accesso alle risorse del sistema per ciascun utente o gruppo di utenti.

3. Il sistema di protocollo informatico deve consentire il tracciamento di qualsiasi evento di modifica delle informazioni trattate, assicurandone la corretta attribuzione al soggetto che lo ha causato. Le registrazioni degli eventi devono essere protette da modifiche non autorizzate.

4. Al fine di garantire la non modificabilità delle operazioni di registrazione, il contenuto del registro informatico di protocollo, almeno al termine della giornata lavorativa, deve essere riversato su supporti informatici non riscrivibili e deve essere conservato dal responsabile della sicurezza o da chi ne fa le veci.»

5.2.6. ACCESSO ESTERNO AL PROTOCOLLO INFORMATICO

Deve essere garantito l'accesso dall'esterno dell'amministrazione alle informazioni contenute nel protocollo informatico, come previsto dagli articoli 10 e 11 d.p.r. n. 428 del 1998.

Tutti i soggetti che, secondo il capo V della legge 7 agosto 1990, n. 241, hanno diritto ad ottenere le informazioni contenute nel protocollo, debbono poter accedere «anche mediante l'impiego di procedure applicative operanti al di fuori del sistema e strumenti che consentono l'acquisizione diretta delle informazioni da parte dell'interessato» (art. 10, comma 1, d.p.r. 428/98).

Per garantire questo diritto, le amministrazioni determinano «criteri tecnici ed organizzativi per l'impiego, anche per via telematica, del sistema di protocollo informatico per il reperimento, la visualizzazione e la stampa delle informazioni», nel rispetto della normativa sulla *privacy* (legge 31 dicembre 1996, n. 675), e nell'ambito delle più generali misure organizzative finalizzate a garantire il diritto di accesso, come previsto dall'articolo 22, comma 3, legge n. 241 del 1990, (art. 10, comma 2, d.p.r. 428/98).

L'accesso dall'esterno dovrà avvenire dietro identificazione dell'utente, «anche mediante l'impiego di strumenti informatici per la firma digitale del documento informatico, come disciplinati dall'articolo 15, comma 2, della legge 15 marzo 1997, n. 59, dal decreto del Presidente della Repubblica 10 novembre 1997, n. 513 e dai relativi regolamenti di attuazione» (art. 10, comma 3, d.p.r. 428/98).

«Nel caso di accesso effettuato da soggetti non appartenenti alla pubblica amministrazione possono utilizzarsi le funzioni di ricerca e di visualizzazione delle informazioni messe a disposizione - anche per via telematica - attraverso gli uffici relazioni col pubblico di cui all'articolo 12 del decreto legislativo 3 febbraio 1993, n. 29» (art. 10, comma 4, d.p.r. 428/98).

5.2.7. ACCESSO DI ALTRE PUBBLICHE AMMINISTRAZIONI

Le altre pubbliche amministrazioni possono accedere al protocollo informatico di una data AOO mediante proprie applicazioni, utilizzando «le modalità di interconnessione stabilite nell'ambito delle norme e dei criteri tecnici emanati per la realizzazione della Rete unitaria della pubblica amministrazione» (art. 11, comma 1, d.p.r. 428/98).

Ogni AAO dovrà esporre un insieme di funzionalità minime (art. 11, comma 2, d.p.r. 428/98), in modo da consentire alle altre pubbliche amministrazioni di ottenere:

- numero e data di registrazione di protocollo dei documenti, ottenuti attraverso l'indicazione alternativa o congiunta dell'oggetto, della data di spedizione, del mittente, del destinatario;
- numero e data di registrazione di protocollo del documento ricevuto, ottenuti attraverso l'indicazione della data e del numero di protocollo attribuiti dall'amministrazione al documento spedito.

Come visto precedentemente, i dati della segnatura di protocollo devono essere resi disponibili sulla Rete unitaria della pubblica amministrazione in formato XML.

Per lo scambio di documenti tra pubbliche amministrazioni, ogni AAO dovrà utilizzare «messaggi conformi ai sistemi di posta elettronica veicolabili dalla Rete unitaria della pubblica amministrazione» (art. 14, comma 1, RT; ovvero gli standard *Internet*).

Infatti il comma 3 dell'articolo 14 delle regole tecniche, afferma che «ciascuna area organizzativa omogenea istituisce una casella di posta elettronica adibita alla protocollazione dei messaggi ricevuti. L'indirizzo di tale casella è pubblicato dall'amministrazione ai sensi dell'art. 10 ed è riportato nell'indice delle amministrazioni pubbliche».

«Ad un messaggio di posta elettronica ricevuto da una area organizzativa omogenea corrisponde una unica operazione di registrazione di protocollo. La registrazione può riferirsi al corpo del messaggio, ovvero all'insieme dei *computer* allegati contenuti nello stesso messaggio» (art. 14, comma 2, RT).

5.2.8. ARCHIVIAZIONE E CONSERVAZIONE DELLE REGISTRAZIONI DI PROTOCOLLO E DEI DOCUMENTI

Le informazioni di protocollo relative ai procedimenti conclusi sono conservate su «supporto informatico rimovibile» (art. 13, comma 1, d.p.r. 428/98), devono sempre poter essere consultabili (art. 13, comma 3, d.p.r. 428/98), e devono essere «parte integrante del sistema di indicizzazione e di organizzazione dei documenti che sono oggetto di procedure di archiviazione ottica sostitutiva» (art. 13, comma 4, d.p.r. 428/98).

Per quanto riguarda i documenti, «ciascuna amministrazione garantisce la leggibilità nel tempo di tutti i documenti trasmessi o ricevuti adottando i formati previsti all'art. 6, comma 1, lettera b) della delibera AIPA n. 24/1998 o comunque non proprietari» (art. 15, comma 2, RT).

I formati previsti dall'art. 6, comma 1, lettera b) della delibera AIPA n. 24/1998 sono quelli conformi «allo standard SGML, "oppure" uno dei seguenti formati: PDF, AFP e Metacode. È altresì possibile la conservazione di tali documenti come puro testo purché questo ne rappresenti integralmente ed in maniera non ambigua il contenuto. Deve essere in ogni caso definito univocamente il set di caratteri utilizzato, del quale deve essere contestualmente registrata l'immagine, e, qualora la formattazione non sia già implicitamente contenuta nel formato del documento, debbono essere specificate almeno la divisione in righe e pagine e la dimensione delle spaziature. Un documento formato secondo i precedenti requisiti costituisce la rappresentazione digitale del documento archiviato. È inoltre consentita l'archiviazione dei documenti formati all'origine su supporto informatico attraverso la conservazione della corrispondente immagine ottenuta per conversione diretta dal formato testuale; è possibile conservare sul medesimo supporto anche il testo del documento per scopi gestionali e documentali».

È utile osservare che il formato SGML (*Standard Generalized Markup Language*) è un formato da cui deriva l'XML. Un documento XML è anche necessariamente un documento SGML (ma non viceversa).

Il PDF (*Portable Document Format*, formato dei documenti del programma Acrobat della Adobe) è un altro formato molto diffuso. Pur essendo un formato proprietario, il lettore di documenti PDF è largamente diffuso e reperibile gratuita-

mente, anche come *plug-in* (componente) del *browser*. È un formato discretamente compresso, e garantisce la fedele riproduzione in stampa del documento.

Il formato AFP (*Advanced Function Printing*) è stato introdotto dall'IBM nel 1984 per i *mainframe*.

Il formato Metacode è quello dei sistemi di stampa Xeros ESS.

5.3. NORME DI RIFERIMENTO SULLA FIRMA DIGITALE

Il ricordato articolo 15 della legge n. 59 del 1997 ha iniziato un processo che ha portato in tempi brevi alla definizione dell'attuale normativa in materia di documento elettronico e firma digitale. L'AIPA ha assunto un ruolo trainante nella predisposizione della normativa del settore, svolgendo un'intensa attività che ha portato al regolamento contenuto nel d.p.r. n. 513 del 1997 ed ha stabilito gli scenari di riferimento giuridici, tecnologici ed organizzativi per ottenere quanto necessario ad un efficace utilizzo del documento informatico e della firma digitale. Il d.p.c.m. 8 febbraio 1999 regola gli aspetti tecnici ed organizzativi di chi usufruisce ed opera con i documenti informatici e la firma digitale. La pubblicazione della circolare dell'AIPA 26 luglio 1999, n. 22, per l'iscrizione all'elenco pubblico dei certificatori costituisce il tassello conclusivo del processo normativo descritto.

La firma digitale rappresenta una componente importante per la Rete unitaria della pubblica amministrazione. Il Centro tecnico della Rete unitaria, iscritto all'elenco pubblico dei certificatori, svolgerà i compiti di certificazione e di validazione temporale per i soggetti che utilizzano la Rete unitaria stessa. Esso avrà anche il ruolo di certificare le chiavi dell'Autorità e di gestire gli accessi all'elenco pubblico garantendo la comunicazione su canale sicuro con i certificatori.

Inoltre, provvederà alla certificazione delle chiavi attinenti a quelle funzioni che nell'ambito della pubblica amministrazione hanno potere di firma.

5.3.1. IL DOCUMENTO ELETTRONICO

L'utilizzo di documenti elettronici è possibile a patto che sia possibile garantire, attraverso strumenti crittografici, che il documento ricevuto per via telematica:

- provenga da uno specifico mittente (garanzia di autenticità);
- non possa essere rinnegato o ripudiato dal mittente (garanzia di non ripudio);
- non sia stato letto da nessuna terza parte durante la trasmissione (garanzia di riservatezza);
- non sia stato modificato da nessuna terza parte durante la trasmissione (garanzia di integrità).

5.3.2. CRITTOGRAFIA A CHIAVI ASIMMETRICHE

Esistono molti algoritmi di crittazione. Questi algoritmi usano una chiave, cioè una stringa di caratteri, per crittografare e decrittografare le informazioni. Inizialmente gli algoritmi di crittazione utilizzavano la stessa chiave per crittare e per decrittare.

La crittografia a chiavi asimmetriche, invece, fa uso di una coppia di chiavi distinte, una usata per crittare e l'altra per decrittare. Ogni soggetto sceglie o genera un'opportuna coppia di chiavi, mantiene segreta una delle due (la chiave privata) mentre rende nota l'altra (la chiave pubblica). In una trasmissione di documenti, ad esempio, un mittente può inviare, ad uno o più destinatari, un messaggio crittandolo mediante la sua chiave privata; ognuno dei destinatari può decrittare il messaggio ricevuto, usando la chiave pubblica del mittente. Analogamente, se un mittente critta un messaggio mediante la chiave pubblica del destinatario, tale messaggio potrà essere decrittato solamente da chi possiede la chiave privata corrispondente.

La crittografia a chiavi asimmetriche si basa sulla teoria dei numeri e, sino ad oggi, molti sono gli algoritmi crittografici proposti quali, ad esempio, *Diffie-Hellman key exchange*, RSA, DSA, ECDSA, DSS.

Come si vedrà meglio in seguito, gli usi principali di questo tipo di crittografia sono la firma elettronica e la crittazione e decrittazione di dati.

Alcuni degli algoritmi elencati in precedenza sono alla base di noti sistemi di crittografia presenti sul mercato. Anche se è ormai sempre più chiaro che i sistemi di crittografia a chiavi asimmetriche sono uno strumento indispensabile per semplificare la gestione delle chiavi e rendere possibile comunicazioni sicure, quello che non è ancora del tutto chiaro è quale sia il miglior sistema tra quelli proposti.

In questo contesto si farà un breve cenno a due di questi algoritmi, RSA e DSA, poiché l'art. 2 delle regole tecniche relative al d.p.r. n. 513 del 1997, riguardante l'algoritmo di generazione e verifica delle firme digitali fa espresso riferimento ad essi.

RSA, proposto nel 1978 da Rivest, Shamir e Adleman, è uno tra i più conosciuti ed usati algoritmi di crittografia a chiavi asimmetriche ed è attualmente coperto da brevetto. Un altro algoritmo è DSA (*Digital Signature Algorithm*), sviluppato nel maggio 1994 presso il *National Institute of Standards and Technology* (NIST) degli Stati Uniti.

Dal punto di vista delle prestazioni, cioè la velocità del processo di firma elettronica o di crittazione (o decrittazione) di un documento, gli algoritmi citati sono stati confrontati in alcuni studi effettuati da ricercatori esperti in crittografia. Da questi studi è emerso che DSA è più veloce in fase di generazione della firma elet-

tronica che in fase di verifica; al contrario, RSA è più veloce in fase di verifica rispetto a quella di generazione della firma. Quindi la scelta dell'algoritmo migliore dipende dal tipo di applicazione in questione; infatti, se, ad esempio, in una applicazione è previsto che la fase di firma sia più ricorrente che quella di verifica, allora la scelta di RSA potrebbe contribuire ad aumentare le prestazioni dell'applicazione.

Una delle più importanti caratteristiche da tenere in considerazione nella scelta di un sistema a chiavi asimmetriche è la sua sicurezza, cioè il grado di difficoltà che può incontrare un malintenzionato nel tentare di derivare la chiave privata di un soggetto essendo in possesso di quella pubblica.

A tal fine, occorre precisare che, alla luce delle attuali conoscenze tecnico-scientifiche, non esiste una garanzia assoluta (dimostrabile) sulla sicurezza degli algoritmi di crittografia e, in particolare, di quelli a chiavi asimmetriche. L'unica certezza è che la sicurezza è tanto maggiore quanto più grande è la lunghezza, espressa in bit, delle chiavi generate. La lunghezza tipica delle chiavi generate da algoritmi quali RSA e DSA è 1024 bit. L'art. 4 comma 6 delle regole tecniche relative al d.p.r. n. 513 del 1997 indica in 1024 bit la lunghezza «minima» prevista per le chiavi.

5.3.3. FIRMA ELETTRONICA E SUO USO COME SISTEMA DI IDENTIFICAZIONE

Una delle più importanti applicazioni della crittografia a chiave pubblica è la firma «elettronica», indicata anche come firma «digitale» (secondo una forse impropria traduzione dell'inglese *digital signature*).

A ciascun soggetto si può associare una coppia di chiavi asimmetriche composta da: una chiave «privata», usata per firmare un documento, ed una chiave «pubblica», usata per verificare l'autenticità del documento firmato in precedenza. L'art. 4, comma 1, delle regole tecniche del d.p.r. n. 513 del 1997 recita che «una coppia di chiavi può essere attribuita ad un solo titolare». La chiave privata viene mantenuta segreta, mentre quella pubblica viene messa a disposizione dei potenziali partner coinvolti nella comunicazione con il titolare delle due chiavi in questione.

La Figura 5.1 schematizza le fasi di «generazione» e «validazione» della firma elettronica di un documento, ottenuta tramite un sistema di crittazione a chiavi asimmetriche. In particolare, la fase di generazione della firma può essere descritta sul modo seguente.

Il documento viene dato in Fig. 1 ad un algoritmo di *hash*, cioè (come descritto nell'art. 1, comma 1, lett. c), regole tecniche del d.p.r. n. 513 del 1997) ad una funzione matematica che genera una impronta (una sequenza di simboli binari di lunghezza predefinita). In letteratura, l'impronta è indicata anche come «riassunto», *message digest*, *hash*). L'art. 3 delle regole tecniche relative al d.p.r. n. 513 del 1997 specifica gli algoritmi di *hash* indicati dall'AIPA (RIPEMD-160 e SHA-1). L'impronta si compone di

una serie di caratteri che vengono ricavati univocamente dal testo del documento, a prescindere dalle sue dimensioni, mediante un procedimento automatico di crittazione. Qualunque sia la lunghezza del documento, la lunghezza dell'impronta è fissa e alquanto contenuta, in termini di numero di caratteri. Se il documento originale subisce anche una benché minima variazione (dovuta, ad esempio, ad un tentativo di contraffazione) il suo riassunto subisce un radicale cambiamento. Ciò significa che confrontando l'impronta di un documento generato prima della trasmissione dello stesso con quella generata una volta che il documento è giunto al destinatario, è possibile capire se il documento è giunto integro a destinazione.

- L'impronta del documento viene crittata (codificata) mediante la chiave privata del mittente. L'impronta codificata costituisce la firma elettronica.
- Il documento originale in formato elettronico (documento «in chiaro») con allegata la sua firma elettronica costituiscono la busta digitale (*digital envelop*).
- La busta digitale viene trasmessa dal mittente al destinatario per via telematica.

La fase di validazione della firma elettronica di un documento, schematizzata in Figura 5.1 è descritta qui di seguito.

- Al ricevimento della busta digitale, il destinatario provvede a decodificare la firma elettronica, utilizzando la chiave pubblica del mittente, ottenendo l'impronta del documento al momento della trasmissione.
- Il destinatario provvede a ricalcolare l'impronta del documento ricevuto e a confrontarla con l'impronta ottenuta al passo precedente. Se le due impronte coincidono, significa che il documento è giunto integro a destinazione. La firma è autentica e, conseguentemente, il mittente risulta riconosciuto.

Però, questo modo di operare non garantisce il destinatario che il mittente sia effettivamente il soggetto con cui si vuole entrare in comunicazione. Ad esempio, nel caso di una operazione di *electronic filing* ad un ufficio giudiziario (destinatario) è possibile che un malintenzionato si spacci per un certo avvocato, comunicando preventivamente al destinatario la propria chiave pubblica. In assenza di contenuti del messaggio, già noti all'altra parte, che possano costituire prova «certa» dell'identità del mittente, la tecnologia di crittazione a chiave pubblica garantisce solo la sicurezza del messaggio, ma non l'identità degli interlocutori coinvolti.

L'Associazione dei Procuratori legali statunitensi, l'ABA (*American Bar Association*) ha sviluppato una serie di regole (*Digital Signature Guidelines*), relative alla firma elettronica, assunte a standard internazionali *de facto*. L'ABA ha prodotto il primo documento legale riguardante l'uso della crittografia, firma elettronica, e autenticazione di entità in una rete aperta tipo *Internet*. Il documento descrive il sistema per assicurare l'identità del proprietario di una chiave privata, per gestire la firma elet-

tronica utilizzabile sia nel commercio elettronico sia nelle procedure legali, per ascrivere responsabilità a chi utilizza il servizio di commercio elettronico e per garantire il non ripudio di una transazione.

Firma elettronica

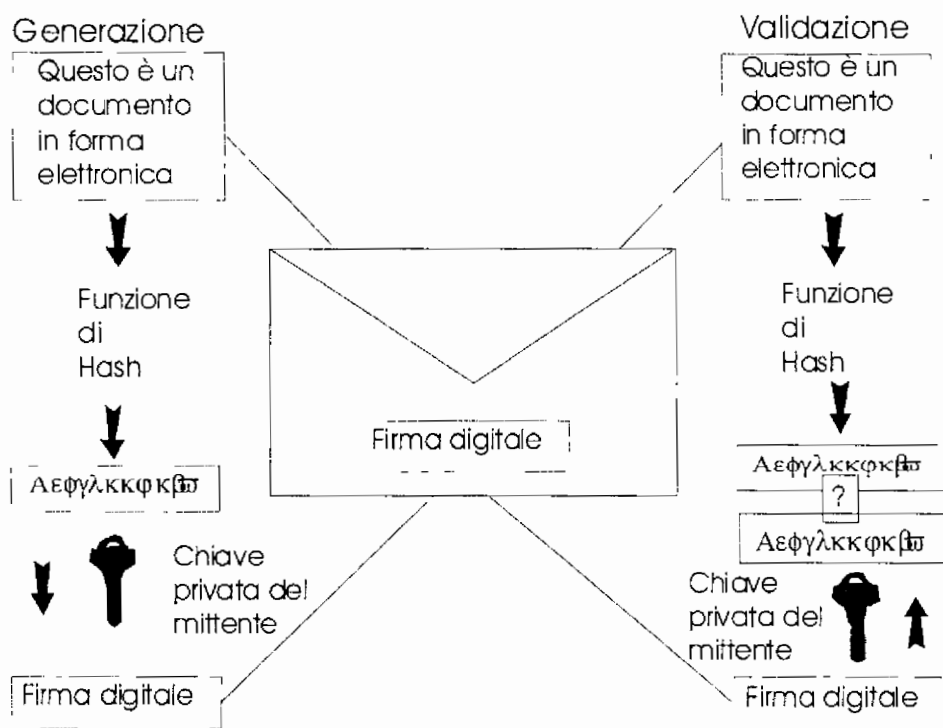


Figura 5.1 - Firma elettronica: generazione e validazione

5.3.4. METODI PER PROTEGGERE LA CHIAVE PRIVATA

Nel precedente paragrafo è stato anticipato che è assolutamente necessario che la chiave privata rimanga segreta e sia protetta da tentativi di individuazione. A tal proposito sono stati sviluppati molti metodi per proteggere le chiavi private e ciascuno di essi ha dei pro e dei contro.

Il metodo più semplice consiste nel memorizzare su *hard disk* la chiave privata, crittandola preventivamente mediante l'uso di una *password*. Questo metodo è usato da applicazioni quali, ad esempio, *Pretty Good Privacy* (PGP) e *Netscape Navigator*. Sebbene alquanto conveniente, questo metodo presenta alcuni svantaggi. Il primo di essi è che un malintenzionato venuto in possesso della *password* potrebbe accedere all'*hard disk* e decrittare la chiave privata. Inoltre, poiché la chiave privata deve

essere necessariamente decrittata dal *computer* prima del suo uso, è possibile che un programma pirata, tipo *Trojan Horse*, ad esempio, possa intercettare la chiave privata decrittata e trasmetterla al malintenzionato che ha inviato il programma pirata.

Il primo dei due svantaggi può essere rimosso memorizzando la chiave privata crittata su un dispositivo di memoria rimovibile quale, ad esempio, un *floppy disk* o un CD-ROM. Purtroppo, questo sistema non risolve il problema generato da un programma pirata.

Attualmente, il modo più sicuro di proteggere la chiave privata consiste sulla sua memorizzazione su dispositivi «intelligenti», quali *smart card*.

Per quanto concerne la legge italiana, l'uso delle *smart card* è previsto dalle regole tecniche, emanate dall'AIPA, relative al d.p.r. n. 513 del 1997 (vedi art. 1); in questo contesto, una *smart card* è definita come «dispositivo di firma», cioè come un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado di conservare in modo protetto le chiavi private e generare al suo interno firme digitali.

Una *smart card* è dotata di un microprocessore in grado di creare e memorizzare una coppia di chiavi pubblica/privata e di una memoria di piccole dimensioni, in grado di memorizzare anche un congruo numero di certificati digitali (descritti in dettaglio più avanti). In questo caso, affinché la chiave privata non sia trasmessa al di fuori della *smart card*, le operazioni di firma elettronica debbono avvenire strettamente all'interno del dispositivo. In base a quanto detto, le *smart card* si apprestano a giocare un ruolo importante nel settore dei sistemi di sicurezza; esse possono essere programmate per richiedere, una volta inserite nel dispositivo di lettura relativo, un codice di identificazione utente (PIN, *Personal Identification Number*) in modo da aumentare i gradi di sicurezza in caso di sottrazione dolosa della *smart card* ad opera di un malintenzionato.

Le *smart card* non sono esenti da problemi quali, ad esempio, fragilità e possibilità di danneggiamento, smarrimento o furto. Nei casi in cui la *smart card* non è più usabile sarà necessario disporre di un duplicato della stessa o di un sistema in grado di produrne uno.

5.3.5. CERTIFICATI DIGITALI E AUTORITÀ DI CERTIFICAZIONE

La firma elettronica garantisce l'autenticazione dei partner di una comunicazione, a patto che non ci siano dubbi sull'autenticità della chiave pubblica impiegata. Quindi, è necessario trasmettere in maniera sicura la chiave pubblica associata ad un certo soggetto. Si potrebbe pensare che quest'ultimo invii direttamente, mediante un canale sicuro, la propria chiave pubblica a tutti i possibili destinatari. Questo metodo risulta poco pratico in alcuni casi perché, ad esempio, può risultare

difficile disporre di un canale sicuro e/o può essere complicato il primo contatto tra due partner di una comunicazione.

Per garantire la diffusione, semplice e sicura, delle chiavi pubbliche sono stati introdotti i **certificati digitali** (*digital certificates*). Un certificato digitale associa i dati identificativi di un soggetto ad una o più sue chiavi pubbliche. La **funzione principale** di un certificato elettronico è quella di fornire alle transazioni effettuate in *Internet/intranet* garanzie di autenticazione simili a quelle offerte attualmente da strumenti quali passaporto, carta di identità, carta di credito, ecc., per l'identificazione delle persone fisiche. Un **certificato elettronico** deve quindi identificare un soggetto con assoluta certezza, permettendogli di **spedire e ricevere documenti firmati digitalmente**, con la garanzia della totale riservatezza delle informazioni trasmesse e con la **sicurezza del riconoscimento** certo del mittente e del destinatario coinvolti nella comunicazione.

Affinché un **certificato digitale** risulti valido, esso deve essere firmato elettronicamente da una Autorità di Certificazione (*Certification Authority*, CA), o anche, in breve, **certificatore**. Una CA è addetta alla distribuzione e alla gestione dei **certificati digitali**, tipicamente in ambiente *Internet/intranet*.

Esistono alcuni standard per definire la **struttura dati dei certificati digitali** e le **procedure relative alla loro distribuzione** da parte della CA. Lo standard più utilizzato dagli attuali sistemi e protocolli di crittografia a chiave pubblica è lo X.509 v3 adottato dall'ISO.

In accordo a questo standard, l'art. 11, comma 1, delle **regole tecniche relative al d.p.r. n. 513 del 1997**, prevede che i **certificati debbono contenere almeno le seguenti informazioni**:

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

Inoltre, se il certificato è relativo ad una coppia di chiavi di sottoscrizione (usate per **firmare elettronicamente un documento**), in aggiunta alle informazioni prescritte dal citato comma 1, possono essere indicati:

- eventuali limitazioni nell'uso della coppia di chiavi;
- eventuali poteri di rappresentanza;
- eventuali abilitazioni professionali.

Al fini di questo studio, è ipotizzabile l'uso di questi campi aggiuntivi per qualificare maggiormente un avvocato da parte del Consiglio dell'ordine di appartenenza.

Il compito di CA può essere svolto da qualunque ente terzo in possesso dei necessari requisiti di fiducia (*trusted third party*), ad esempio, un ente della pubblica amministrazione, un ordine professionale (Consiglio dell'ordine degli avvocati, Consiglio nazionale del notariato, ecc.), un'impresa privata.

Per quanto concerne il nostro Paese, l'art. 14, comma 1, delle regole tecniche relative al d.p.r. n. 513 del 1997 prevede che «chiunque intenda esercitare l'attività di certificatore deve inoltrare all'AIPA, secondo le modalità da questa definite con apposita circolare, domanda di iscrizione nell'elenco pubblico di cui all'articolo 8, comma 3, del d.p.r. 10 settembre 1997, n. 513».

Da quanto detto in precedenza deriva che il soggetto (persona fisica, azienda, banca, ente pubblico, ecc.) che desidera ottenere un certificato digitale deve, in prima istanza, dimostrare la propria identità ed affidabilità ad una CA. Un'identificazione accurata non è un compito banale e comporta, a seconda del tipo di certificato, accertamenti sempre più approfonditi che possono essere condotti direttamente da una CA oppure da una Autorità di registrazione (*Registration Authority*, RA) che fa capo, direttamente o indirettamente, ad una CA. La *Registration Authority* ha la responsabilità di accertare e garantire l'identità del soggetto che chiede un certificato digitale. Invece, il certificato digitale può essere assegnato esclusivamente da una CA.

Una volta identificato dalla RA o dalla CA stessa, il soggetto deve generare, mediante l'utilizzo di software opportuno (ad esempio, un browser quale Microsoft Internet Explorer 3.0 o Netscape Navigator 3.0), la sua coppia di chiavi asimmetriche, l'una pubblica e l'altra privata. La chiave pubblica deve essere comunicata alla CA mentre, per motivi di sicurezza, la chiave privata deve risultare assolutamente segreta e non è opportuno, quindi, che essa sia inclusa nel certificato digitale associato al soggetto.

Il problema della assoluta segretezza della chiave privata è un punto alquanto delicato e, in alcuni Paesi, è in corso un attento dibattito per regolamentarlo. Alcuni governi (ad esempio, quello statunitense), per prevenire l'eventuale uso criminoso delle tecniche crittografiche, vogliono avere le garanzie tecniche ed organizzative necessarie a poter decifrare i messaggi crittografati, quando ritenuto necessario, ad esempio su richiesta dell'autorità giudiziaria.

Affinché gli utenti possano aver fiducia in una CA, occorre che questa soddisfi requisiti di sicurezza rispetto all'*hardware* e *software* che utilizza, alle procedure di distribuzione e verifica dei certificati digitali che mette in atto, e disponga di opportune coperture assicurative rispetto a rischi dell'attività e a possibili danni causabili a terzi. Per quanto riguarda la normativa in vigore, nel nostro Paese, è sufficiente che la CA sia riconosciuta dall'AIPA e risulti iscritta nell'elenco pubblico dei certificatori come previsto dall'art. 17 delle regole tecniche relative al d.p.r. n. 513 del 1997

Revoca e sospensione di un certificato digitale

Tra i compiti di una CA c'è anche quello di revoca di certificati digitali, quando necessario. Ciò potrebbe verificarsi nei seguenti casi:

- un soggetto dichiara che la propria chiave privata è andata persa, distrutta o individuata da un malintenzionato;
- un certificato è stato assegnato per garantire ad un soggetto l'accesso ad una determinata risorsa (servizio) ma lo stesso ha successivamente perso l'autorizzazione ad accedervi;
- la CA scopre di aver emesso un certificato alla persona sbagliata,
- i sistemi della CA potrebbero essere stati seriamente compromessi e qualche malintenzionato potrebbe essere in grado di emettere certificati digitali falsi.

In base a quanto disposto dall'art. 29 delle regole tecniche relative al d.p.r. n. 513 del 1997, la revoca di un certificato determina la cessazione anticipata della sua validità. Essa può avvenire su richiesta scritta del titolare della coppia di chiavi asimmetriche (ad esempio, nei primi due casi) o, in situazioni di motivata urgenza, anche su iniziativa della CA (ad esempio, negli altri casi sopra ricordati). A tale scopo, la CA gestisce una serie di liste di certificati revocati (*Certification Revocation List*, CRL). La revoca del certificato viene effettuata dalla CA mediante il suo inserimento in una di queste liste; solo da quel momento il certificato si intende revocato definitivamente. La richiesta di revoca può anche venire inoltrata ad una CA da parte di un terzo interessato, previa presentazione per iscritto della documentazione giustificativa

Nei casi in cui la CA, ricevuta una richiesta di revoca di un certificato digitale da parte di un ipotetico titolare, non abbia la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato. Gli artt. 33, 34, 35 delle regole tecniche relative al d.p.r. n. 513 del 1997 regolano il processo di sospensione di un certificato.

5.3.6. VALIDAZIONE TEMPORALE DEI DOCUMENTI INFORMATICI

In certi casi può risultare importante validare un documento informatico generando ed applicando una marca temporale (*time stamp*) allo stesso. In questo modo è

possibile conoscere il momento esatto in cui un documento è stato validato. La **marca digitale** viene resa non falsificabile dalla firma digitale. Per avere validità universale, la **marca temporale** deve essere relativa ad un tempo preciso di riferimento. L'art. 53, comma 3, delle regole tecniche relative al d.p.r. n. 513 del 1997, impone che la data e l'ora contenute nella **marca temporale** siano specificate con riferimento al **Tempo Universale Coordinato (UTC)**.

5.3.7. INFRASTRUTTURA A CHIAVE PUBBLICA

In questo paragrafo vengono introdotti i concetti ed i servizi alla base di una **Infrastruttura a chiave pubblica** (*Public Key Infrastructure*, PKI).

Affinché **soggetti** (persone, entità governative, associazioni, aziende, ecc.) possano **cooperare per via telematica**, in **maniera sicura**, mediante sistemi di crittografia a **chiave asimmetrica**, è importante creare una **Infrastruttura a chiave pubblica**. Lo scopo primario di una PKI è quello di consentire l'uso di **certificati X.509** in applicazioni che utilizzano *Internet* o, comunque, una **rete geografica pubblica**, e promuovere l'**interoperabilità tra implementazioni differenti** che fanno uso di certificati.

Come detto precedentemente, i **certificati digitali a chiave pubblica** sono documenti in formato elettronico che contengono almeno il nome e la **chiave pubblica** del soggetto in questione; inoltre, il certificato deve essere **firmato digitalmente** da una *Certification Authority* (CA). Lo scopo di un certificato è di assicurare che l'associazione tra **chiave pubblica e nome del soggetto** sia certa. Oltre alla CA, nell'ambito di una PKI, possono operare altre entità quali la *Registration Authority* (RA), uno o più *Certificate Status Responder* (CPR) e la *Policy Management Authority* (PMA).

Una RA è addetta alla sola **identificazione e registrazione dei soggetti**; questo lavoro può essere svolto anche direttamente da una CA.

I CPR sono dei **serventi accreditati** che forniscono, alle parti in comunicazione, informazioni circa lo stato e la validità dei certificati digitali.

La PMA funge da ispiratrice e coordinatrice delle politiche relative ai certificati digitali; le CA e, eventualmente le RA, dovranno adottare e seguire tali politiche.

La Figura 5.2 mostra la struttura a livelli, tipica di una PKI. Il primo livello, quello più in basso nella figura, rappresenta le funzionalità di base necessarie per la gestione e l'invio dei certificati digitali. Queste funzionalità comprendono: l'invio di un certificato digitale, la sua eventuale revoca, le politiche che regolano l'invio e la revoca dei certificati, l'archiviazione delle informazioni necessarie a validare i certificati.

Al secondo livello si trovano i clienti di una PKI, cioè applicazioni o parti di esse che fanno uso dei certificati digitali. Queste applicazioni eseguono quattro funzioni primitive: la generazione delle coppie di chiavi (pubblica e privata), la genera-

zione e la validazione della firma digitale e la gestione di chiavi segrete (chiavi usate per garantire la riservatezza di una comunicazione, tipicamente usate da un algoritmo a chiavi asimmetriche).

Per quanto concerne la prima funzionalità è bene chiarire che la generazione della coppia di chiavi può essere eseguita sia sotto la assoluta responsabilità del soggetto interessato (il quale, una volta identificato da una RA o CA dovrà comunicare alla CA la propria chiave pubblica) sia direttamente dalla CA. Il primo approccio è quello che, oltre a garantire la integrità del sistema, preserva la proprietà del non ripudio in quanto solamente il soggetto proprietario della chiave privata potrà firmare i documenti.

Al terzo livello si collocano alcuni servizi o agenti che facilitano l'utilizzo di servizi di sicurezza posti al livello superiore. Si precisa che questi servizi non rappresentano tutti quelli possibili, molti dei quali sono ancora oggetto di studio. Tra i servizi più consolidati possono citarsi i seguenti.

- **Notai digitali (Digital Notary).** Forniscono un servizio analogo a quello dei notai, cioè possono sia autenticare elettronicamente un documento, verificandone la firma digitale, sia apporre un sigillo temporale sui documenti per provarne l'esistenza da un dato momento.
- **Agenti per il recovery delle chiavi (Key recovery agent).** Servono per memorizzare, proteggere e accedere in modo assolutamente sicuro un vasto insieme di chiavi private. Ciò permette, ad esempio, di decrittografare dati crittati in precedenza nel caso in cui le chiavi private originarie siano andate smarrite. Questi agenti possono risultare necessari anche nel caso in cui una autorità superiore si trovi nella necessità di decrittare dati codificati, ad esempio, a fronte di una richiesta dell'autorità giudiziaria.
- **Serventi per l'invio di certificati.** Forniscono un servizio in grado di certificare sia l'avvenuta spedizione di un messaggio, in buona fede, da parte di un mittente, sia il non ripudio di un messaggio ricevuto da parte del destinatario (prova che il messaggio è stato realmente ricevuto).
- **Altri Serventi o Agenti.** Altri servizi implementabili, quali, ad esempio, distributori di «biglietti digitali» (*digital ticket*), per permettere l'accesso selettivo ad un servizio.

L'ultimo livello, quello in alto nella Figura 5.2, rappresenta alcuni significativi servizi che possono essere creati utilizzando quanto messo a disposizione dai livelli inferiori. Tra questi servizi, in figura sono mostrati quelli che permettono l'implementazione della firma digitale (servizi di autenticazione, integrità e non ripu-

dio) e la gestione delle chiavi asimmetriche per garantire la riservatezza di una sessione di comunicazione o di un messaggio di posta elettronica.



Figura 5.2 Struttura a livelli di una Infrastruttura a chiave pubblica (PKI)

Le tre strutture dati di base, definite dallo standard X.509, utilizzate da una Infrastruttura a chiave pubblica (PKI) sono: i **certificati digitali**, le **liste dei certificati revocati** e i **certificati incrociati** (*cross certificate*). Nei paragrafi precedenti sono stati descritti sia i certificati digitali sia le relative liste di revoca.

Per **certificazione incrociata** (*cross-certification*) si intende una forma estesa di *third party trust*, cioè una sorta di processo fiduciario «incrociato» tra due CA, secondo il quale esse si **scambiano informazioni riguardanti le chiavi pubbliche** in maniera sicura.

Dal punto di vista tecnico, questo implica la **creazione di *cross certificates*** tra le due CA, cioè ciascuna CA crea e firma elettronicamente un certificato contenente la chiave pubblica dell'altra. In conseguenza di ciò, i **soggetti appartenenti al dominio di certificazione di una CA implicitamente «acquisiscono fiducia»** nei soggetti nel dominio di certificazione dell'altra CA.

La Figura 5.3 schematizza quanto detto; infatti, nel dominio di certificazione della CA UNO, Antonio e Maria, cooperano, ad esempio, scambiandosi messaggi e documenti, in maniera sicura, perché entrambi sono garantiti dai servizi offerti da

CA UNO. Lo stesso discorso vale anche per Aldo e l'ufficio A, appartenenti al dominio di certificazione della CA DUE.

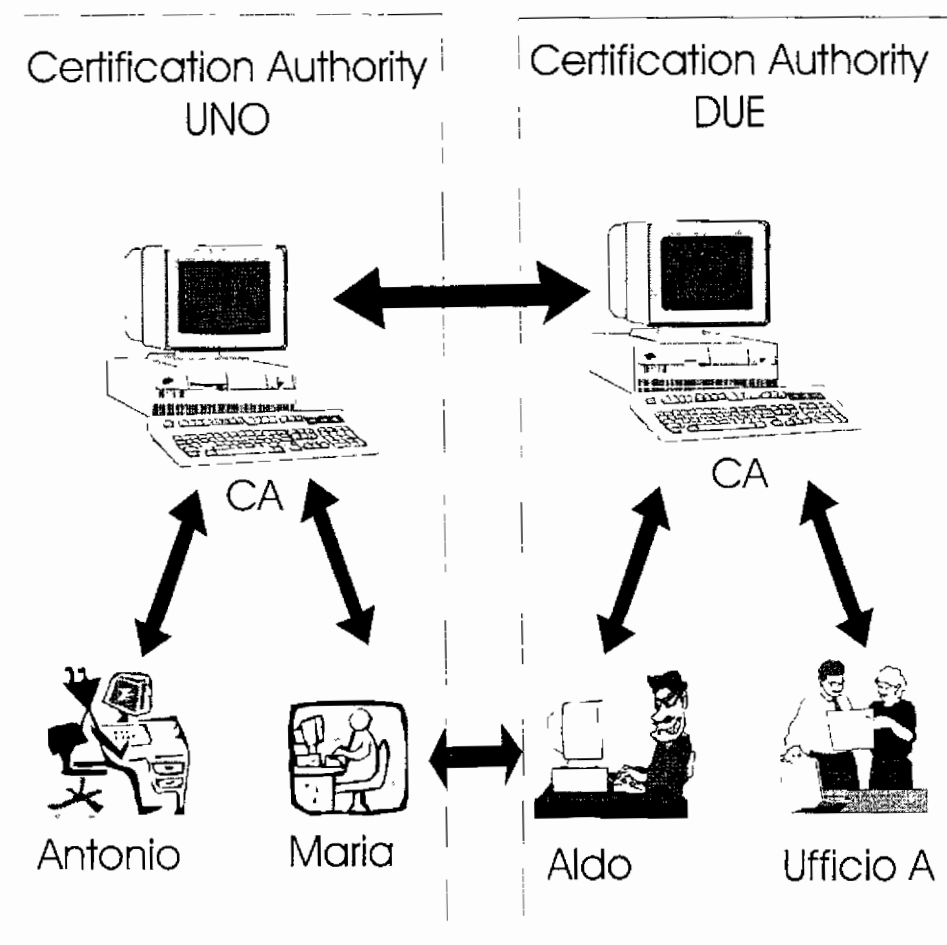


Figura 5.3 - Schematizzazione del processo di cross-certification tra due CA

Inoltre, anche due soggetti appartenenti a domini di certificazione diversi, nella figura, Maria e Aldo, possono cooperare in maniera sicura, perché esiste una *cross-certification* in atto tra la CA UNO e DUE.

L'art. 21, delle regole tecniche relative al d.p.r. n. 513 del 1997 indica che è consentito alle CA definire accordi di certificazione (*cross-certification agreement*). In questo contesto, la certificazione incrociata viene indicata anche come «Certificazione tra certicatori».