INTRODUZIONE ALLA

FIRMA DIGITALE

DEI NOTAI ITALIANI

Consiglio Nazionale del Notariato

SOMMARIO

* le sezioni non firmate sono state predisposte congiuntamente dal Gruppo di lavoro

INTRODUZIONE

di Enrico Santangelo

Ebbene ci siamo. I Notai italiani hanno la firma digitale a norma. L'avventura, iniziata nei primi mesi del 1999, si conclude in questi giorni, e grande è la soddisfazione di chi scrive e dell'intero gruppo che ha reso possibile la sua realizzazione.

E' doveroso, però, che, prima di dare pratica applicazione a questo rivoluzionario strumento, ciascuno di noi conosca non solo come ci si è arrivati, ma anche i punti salienti del quadro normativo, delle possibilità di utilizzazione presenti e future, nonché dei principi basilari anche di natura tecnica.

Si è partiti da un principio che il Legislatore italiano ha scelto nel momento in cui, per la prima volta, si è occupato della firma digitale. La firma digitale a norma sostituisce in tutto e per tutto la firma autografa. Il principio, nella sua semplicità, direi quasi banalità, è però di difficilissima applicazione in quanto il modello cui ci si è ispirati non poteva che essere il modello americano (il più avanzato se non l'unico esistente al mondo), ma tale modello, però, è stato creato ed è ampiamente utilizzato, per il cosiddetto commercio elettronico. Orbene ciò che è valido e funziona perfettamente per il commercio elettronico, non è altrettanto valido allorquando deve essere applicato nei rapporti con la Pubblica Amministrazione.

Mentre, infatti, nel commercio elettronico la firma digitale viene utilizzata per una singola operazione e quindi ha vita brevissima e non necessita di conservazione, nei rapporti con la Pubblica Amministrazione, i documenti sottoscritti con firma digitale si devono poter consultare per un lunghissimo periodo ed in ogni momento deve essere possibile la verifica dei poteri di colui che quel documento ha sottoscritto.

E proprio i poteri del sottoscrittore sono stati la problematica più difficile da risolvere.

Se poi quei poteri sono legati alla funzione notarile, i

problemi si moltiplicano, perché la nostra funzione, proprio perché funzione pubblica, è certificabile esclusivamente dal Presidente del Consiglio Notarile del Distretto cui il Notaio appartiene. E' quindi indispensabile che colui che voglia verificare la veridicità della firma digitale apposta da un Notaio, debba poter verificare non solo l'autenticità di quella firma, ma anche che al momento dell'apposizione colui che l'ha apposta era "Notaio".

Risolvere questo problema è apparso subito il punto focale. Il Gruppo di lavoro della Commissione Informatica del Consiglio Nazionale del Notariato, coordinato dal collega Michele NASTRI con la indispensabile collaborazione dei consulenti professori Antonino MAZZEO e Nicola MAZZOCCA, elaborò, nell'ormai lontana estate del 1999, una soluzione che fu comunicata, attraverso i canali ufficiali, alla Presidenza del Consiglio dei Ministri, all'A.I.P.A., ai Ministeri dell'Industria, della Giustizia e delle Finanze, nonché ad INFOCAMERE. Tale soluzione prevedeva l'adozione del cosiddetto "certificato di attributo". In poche parole l'idea era questa: ciascun Notaio si sarebbe rivolto ad uno qualsiasi dei certificatori ufficiali iscritti all'A.I.P.A. il quale avrebbe certificato l'identità del Notaio e la veridicità della firma, mentre la funzione sarebbe stata certificata dal Consiglio Nazionale del Notariato attraverso un collegamento con tutti i Consigli Notarili d'Italia.

Tale soluzione, certamente la più adeguata e la più logica dal punto di vista teorico, è risultata, però, impraticabile per vari ordini di motivi che in questa sede non è il caso di esaminare. Basti dire, però, che in nessuna parte del mondo si è avuta un'applicazione pratica sufficientemente soddisfacente del cosiddetto "certificato di attributo".

Andava quindi ricercata un'altra soluzione di più facile ed effettiva applicazione ed esecuzione.

Aderendo all'associazione "ASSOCERTIFICATORI" (che riunisce la maggior parte dei certificatori iscritti all'A.I.P.A. ed il cui statuto consente la partecipazione degli ordini professionali), il Consiglio Nazionale del Notariato ha potuto far sentire la propria voce e studiare, proprio con i diretti interessati, la soluzione più idonea.

Ebbene proprio lo studio della fattispecie ha convinto la Commissione Informatica che l'unica soluzione praticabile e assolutamente certa (e la legislazione che man mano si è sviluppata ne è la dimostrazione), fosse quella di fare assumere la qualifica di certificatore al Consiglio Nazionale del Notariato. E' stata una decisione sofferta ma che il Consiglio ha assunto all'unanimità, senza esitazioni, nella consapevolezza che i tempi, non solo erano maturi, ma indifferibili e che il Notariato non doveva essere a rimorchio di nessuno, ma anzi doveva essere all'avanguardia nell'attuazione di questa "rivoluzione".

Presa la decisione bisognava attuarla. E questa fase è stata forse la più difficile. Predisporre il Manuale Operativo, prevedere tutte le ipotesi (e tralascio tutto il resto), è stata un'attività particolarmente faticosa ed impegnativa. E' quindi giusto che un ringraziamento vada a tutti i componenti il Gruppo di lavoro "firma digitale" composto oltre che dagli indicati coordinatore e consulenti, dai colleghi Gea ARCELLA, Ugo BECHINI, Sabrina CHIBBARO, Marco DOLZANI, Egidio LORENZI, Enrico MACCARONE, Raimondo ZAGAMI.

Un particolare ringraziamento, infine, deve essere rivolto all'*equipe* della NOTARTEL ed in particolare agli Ingg. Guglielmo IACONO, Pasquale STARACE e Luigi D'ARDIA che sono i veri realizzatori del progetto.

Infine l'ultima difficoltà: la gara. Complessa sia nella scelta del tipo, sia nella materiale esecuzione. Ma anche essa è andata a buon fine ed il partner vincitore (la B.N.L. MULTISERVIZI S.p.A.) è il certificatore che in *outsourcing* affiancherà il Consiglio Nazionale del Notariato nella materiale esecuzione del progetto.

Ho iniziato questo mio intervento con la frase "ebbene ci siamo". Ci siamo perché abbiamo lo strumento, ma sono assolutamente consapevole che questo è solo l'inizio, oserei dire il più semplice.

Adesso bisogna applicare la firma digitale. E questa, forse, è la parte più difficile.

L'EVOLUZIONE DELLA POLITICA INFORMATICA DEL NOTARIATO

di Paolo Piccoli

Mi si chiede di scrivere sull'argomento in occasione del Congresso di Milano, sia come delegato del Presidente per i rapporti, nel settore, con le Istituzioni, sia come detentore di una certa memoria storica, avendo avuto la responsabilità del Settore Informatico prima di Enrico Santangelo.

Il titolo assegnatomi potrebbe suonare un po' pretenzioso, se non si valuta che in realtà, negli ultimi cinque o sei anni molti sono stati i cambiamenti.

Non tutti i possibili obiettivi sono stati affrontati e raggiunti (essendo inevitabili scelte tra diverse priorità), ma certo se un collega ritornasse oggi da una lunga assenza, rimarrebbe colpito dalle trasformazioni avvenute in così pochi anni, meno avvertibili in chi quotidianamente le ha viste delinearsi a poco a poco.

Non sarà inutile dunque ripercorrere un po' di storia recente per avere un'idea complessiva dell'impegno del Consiglio Nazionale nel settore.

La consiliatura 1995-1998 aveva visto inizialmente la Commissione Informatica fortemente impegnata nella riflessione sulla fattibilità di un programma di gestione dello studio notarile. Il dibattito, durato circa un anno di lavoro, affiancato da serrati confronti tecnici, si concluse con la decisione negativa del Consiglio Nazionale, motivata sia dalla eterogeneità delle esigenze dei singoli notai, sia dalla impossibilità di organizzare una efficiente rete di assistenza.

Si era nel contempo avviata, per iniziativa precipua del Consigliere Vincenzo Ciancico, una trasmissione di dati via etere mediante il sistema Televideo della RAI, che ebbe il pregio di evidenziare, sia pure con i limiti tecnici del mezzo (unidirezionalità, scarsità di dati trasmissibili, necessità di trasmettere in una

finestra di tempo prefissata, difficoltà di ricezione), l'intuizione positiva di un invio di dati a distanza in forma non cartacea.

Ma il punto di svolta fu costituito dal Congresso di Stresa, nell'autunno del 1996. Tra le mozioni, ne fu presentata una (primi firmatari Santangelo e Nastri) che impegnava il Consiglio Nazionale a realizzare una rete intranet sfruttando la tecnologia internet che, si noti, a quel tempo era ancora lontana dall'essere considerata parte integrante della nostra vita quotidiana.

Quell'intuizione felice segnò l'evoluzione della politica del Consiglio Nazionale nel settore, rendendolo protagonista attivo della rivoluzione che si annunciava anche nei rapporti con la Pubblica Amministrazione.

La Commissione Informatica, fino ad allora presieduta da Andrea Pastore, che lasciò l'incarico a causa dei suoi impegni parlamentari, venne affidata il 13 dicembre 1996 a chi scrive.

La sera stessa, con la collaborazione di Guido Roveda, fu inviato - utilizzando la *mailing list* "Sigillo", nata da un'idea lungimirante di Enrico Maccarone - il primo numero di "CNN Notizie", che dai primi timidi passi nelle informazioni di dottrina e giurisprudenza, che via via ha sostituito tutta la comunicazione cartacea prodotta dal Consiglio Nazionale (comprese le mitiche schede di "Strumenti" curate da Enrico Marmocchi e Carlo Bordieri) ed è divenuto strumento di trasparenza sempre più prezioso con la pubblicazione dei resoconti delle sedute degli organi istituzionali e degli incontri di categoria.

L'obiettivo cui puntò la maggior parte del lavoro (continuando ovviamente ad occuparsi di rapporti con le case di *software*, di alfabetizzazione, di rapporti con i ministeri per le questioni correnti) fu la realizzazione di quella che sarebbe diventata le Rete Unitaria del Notariato, nome scelto per collegarci idealmente alla futura Rete Unitaria della Pubblica Amministrazione, sia perché l'acronimo RUN ha, in inglese, un significato legato alla velocità.

Dopo un complesso dibattito in Consiglio Nazionale, conclusosi con due soli voti di margine, nel quale fu determinante

la convinzione, tra gli altri, di Giancarlo Laurini, Paolo Pedrazzoli, Mario Miccoli, Gennaro Mariconda, Vincenzo Ciancico, Gianfranco Condò, Alberto Fornari, costituimmo Notartel S.p.A..

Nei primi mesi, oltre ad affrontare difficili scelte tecniche e rilevanti problemi economico-organizzativi, si dovette superare un certo scetticismo per un'impresa che non sembrava avere immediate ricadute e la mia personale responsabilità dovette munirsi di tenacia, fiducia e convinzione del tutto particolari.

La scommessa fu vinta grazie al lavoro dei componenti della Commissione informatica, all'assistenza tecnica dei consulenti Proff. Antonino Mazzeo e Nicola Mazzocca ed all'impegno del personale di Notartel, allora meno numeroso delle dita di una mano.

Nella consiliatura 1998-2001 il rafforzamento tecnologico fu posto tra i tre obiettivi principali, accanto alla formazione culturale ed ai rapporti internazionali. Il testimone del settore fu raccolto da Enrico Santangelo. Il suo lavoro e l'impegno di tutti i collaboratori hanno consentito non solo di raggiungere, entro i primi tre anni di attività di Notartel, l'equilibrio di bilancio nonostante gli ingenti investimenti effettuati, ma ancor più straordinari risultati nel riempire di contenuti la Rete stessa, in un incessante e a tratti snervante confronto con le istituzioni e la Pubblica Amministrazione.

Che cosa oggi la Rete Unitaria consenta è noto a tutti: servizi di base della rete (internet, posta elettronica, consultazione delle e-mail anche da internet, archiviazione automatica dei contenuti della lista "Sigillo", *firewall* di protezione da intrusioni), servizi di consultazione (Banca Dati Notarile con motore di ricerca e ricerca tramite *thesaurus*, Notarlex, Poligrafico dello Stato, Giuffrè, CED della Cassazione), servizi di visura e spedizione telematica adempimenti (Catasto, Conservatorie *online* e *offline*, Modello Unico, Registro Imprese, verifica banca dati protesti e interdetti, ACI, pubblicazione convocazione Assemblee in Gazzetta Ufficiale), monitoraggio rete e servizi, *help desk*.

Tutto questo a costi tanto contenuti quanto inimmaginabili al momento in cui muovemmo i primi passi.

Ma ciò di cui il Notariato deve andare orgoglioso (al di là del conseguimento dei molti e sempre più efficaci servizi per lo svolgimento della professione), è la determinazione con cui si è dotato per primo in Italia di uno strumento unitario che ci ha consentito di rafforzare rapporti importanti con la Pubblica Amministrazione, che a sua volta, a grandi passi, procedeva all'informatizzazione ed alla progressiva sostituzione del cartaceo con il telematico.

In tempi di grandi mutazioni, l'essere pronti, anche sul piano tecnologico, agli appuntamenti decisivi, sarà determinante per una professione, come la nostra, che fa della preparazione giuridico-fiscale di eccellenza e della pubblica funzione la propria forza; forza che deve esprimersi anche nel saper padroneggiare i nuovi strumenti tecnologici destinati a governare la tenuta dei registri della pubblicità immobiliare e societaria, alla cui certezza e completezza è destinata una buona parte della nostra attività.

E' in questo quadro di riferimento che va sottolineato come la scelta del Consiglio Nazionale del Notariato di diventare Certificatore dei notai italiani (constatata l'impossibilità di perseguire la via del certificato di attributo) ponga le premesse per l'utilizzo a norma della firma digitale e dell'intervento diretto sui data base della Pubblica Amministrazione, via via che le norme civilistiche lo consentiranno.

Un punto di arrivo e di ripartenza allo stesso tempo, che, come è agevole vedere, costituisce un elemento di rafforzamento anche sul piano politico generale del notariato e una conferma della sua veste di protagonista e di garante nel processo di modernizzazione del paese.

Un obiettivo per il quale si è lavorato con determinazione e flessibilità, nella consapevolezza che tutte le realizzazioni fin qui compiute non costituivano che una accumulazione di capitale umano e tecnologico in preparazione del vero salto di qualità che la Rete Unitaria consente: il passaggio storico da fruitori telematici a fornitori di dati; da garanti mediati a garanti immediati.

Non è lontano il giorno in cui il cliente uscirà dallo studio con la nota di trascrizione ad acquisto concluso; e sarà un giorno importante.

L'ESPERIENZA DIRETTA

di Enrico Maccarone

Non è facile raccontare la propria esperienza nel campo dell'informatica notarile senza essere condizionati dal modo col quale tale esperienza è stata vissuta, facendo a meno di cadere nel mondo dei ricordi e dei sentimenti.

Ancora più difficile se si considera a posteriori quanto il proprio operato abbia influito (non dipende da me determinare in quale percentuale) sull'operare sia proprio sia altrui, sull'essere notai "moderni" al passo con le nuove tecnologie e soprattutto padroni di esse.

I miei primi contatti col mondo dell'informatica risalgono alla seconda metà degli anni '70: a quell'epoca vennero immessi sul mercato alcuni home computers (Sinclair Zx, Commodore 64, Atari) che, pur essendo dotati di capacità elaborativa oggi risibile, erano tra loro accomunati dalla possibilità di produrre suoni musicali. Per un appassionato musicista come me divenne imperativo impararne l'uso e la programmazione.

Questo il punto di partenza.

Nel 1995 il Consiglio Nazionale del Notariato affidò al consigliere Andrea Pastore la guida di una Commissione "per la informatizzazione degli studi notarili". Fu sufficiente dare uno sguardo all'esterno del notariato per capire, al termine di poche ma intense riunioni, che se qualcosa doveva farsi per la categoria non era tanto la realizzazione di un programma di supporto per gli studi notarili quanto l'immediata realizzazione di una rete del notariato.

Occorreva "navigare in alto".

Si era agli inizi del 1996 e subito si cominciò a vivere il primo cambiamento: Andrea Pastore venne eletto Senatore, lasciando a Paolo Piccoli la guida della Commissione Informatica.

Altri colleghi vennero chiamati a condividere l'esperienza della Commissione; per avvenimenti del tutto fortuiti io venni

chiamato a rappresentare il Notariato (e subito dopo, con me, Mario Miccoli) presso l'Autorità per l'Informatica; alcune amministrazioni (Finanze e Giustizia in particolare) iniziarono a vedere nel Notariato un interlocutore attento, preparato e pressoché insostituibile.

Gli anni dal 1996 al 1998 (sembra storia lontana, ma è solo ieri!) furono caratterizzati da una frenetica attività diretta alla creazione della rete del notariato, all'acculturamento informatico della categoria ed al miglioramento dei rapporti con la Pubblica Amministrazione, con al centro – quasi sempre - i temi del documento informatico e dell'interscambio documentale.

Non ho vissuto l'esperienza del Registro delle Imprese, ma i colleghi che hanno partecipato alla redazione delle relative norme regolamentari raccontano di una esperienza ben diversa rispetto a quella vissuta dai componenti della Commissione Informatica: in quel caso il notariato venne "sentito", mentre dal 1996 in poi abbiamo sempre "partecipato".

Sul piano internazionale rivestono particolare importanza i lavori della Commissione Informatica della UINL (all'epoca presieduta da Mario Miccoli), tendenti a stabilire una normativa internazionalmente valida ed un quadro giuridico univoco sul tema del documento informatico e della firma digitale; analoga importanza, ma da risvolti più politici, deve riconoscersi al lavoro fatto da Giancarlo Laurini durante la sua presidenza della CNUE (lavori rivelatisi di importanza fondamentale per la redazione di alcuni passi della direttiva comunitaria sulle firme elettroniche).

Non è un caso se all'interno del trattato internazionale (Lisbona/Vienna 2000) sull'interscambio documentale tra gli uffici di stato civile dei paesi aderenti alla CIEC (circa 20 paesi dell'area mediterranea) l'istituzione notarile di modello italiano viene vista come l'unico "certificatore" capace di garantire la validità ed autenticità delle informazioni scambiate.

Ed è certo merito delle nostre commissioni internazionali il fondamentale contributo che ancora oggi viene fornito alle emergenti democrazie dell'est europeo sui temi di nostra competenza, e non solo.

Ma torniamo al 1996: nascevano il sito web del Notariato e le prime *mailing-lists*; prendeva corpo l'istanza di creare una rete del notariato (oggetto di specifica comunicazione al Convegno di Stresa, firmata da Enrico Santangelo); si facevano i primi passi "a braccio" della Pubblica Amministrazione.

L'avvenuta costituzione, e soprattutto il buon funzionamento, della Commissione Informatica del C.N.N. convinsero l'allora Direttore Generale Imposte Indirette del Ministero Finanze, Ing. Carlo Vaccari, e con lui i suoi più diretti collaboratori Ing. Antonio De Santis e Dott. Aldo De Luca, che era giunto il momento di creare "insieme" una nuova forma di dialogo, tesa allo sveltimento delle procedure, alla eliminazione dell'accesso fisico alle Conservatorie ed agli uffici del Catasto, alla eliminazione – ultimo traguardo - della nota di trascrizione.

In un settore ben ristretto, si cominciava a vedere il nucleo di quello che adeguatamente ampliato e adattato a più recenti realtà oggi costituisce il piano internazionale sullo sviluppo dello E-Goverment.

Analoghe iniziative vennero intraprese in quel periodo con rappresentanti del Ministero della Giustizia: col Presidente Genghini, per la consultazione della Banca dati esistente presso il CED della Cassazione; con la Dott.ssa Floretta Rolleri, per l'interscambio documentale tra gli studi notarili e le cancellerie dei Tribunali.

Ma tutto ciò necessitava, e necessita, di garanzie. Non può scambiarsi telematicamente alcun dato o documento se non se ne garantisce l'autenticità, l'integrità, la non ripudiabilità.

In altre parole: firma digitale.

Se questa esigenza era sentita dalle poche persone che componevano quei gruppi ristretti, basta nulla per immaginare quanta importanza vi si dava, al contrario, da parte dell'Autorità per l'Informatica nella P.A. (AIPA), i cui sforzi erano in quel momento tesi alla realizzazione della RUPA-Rete Unitaria della P.A.

E fu proprio merito dell'allora Capo di Gabinetto dell'AIPA, Avv. Francesco Cocco, l'avere intuito quanta collaborazione e competenza il notariato avrebbe potuto offrire all'Autorità: una collaborazione che ancora oggi continua, pur se tra mille difficoltà politiche ed oggettive.

A mezzo dell'Avv. Cocco, l'AIPA lanciò una sfida, raccolta da me e Mario Miccoli: scrivere in tempi brevissimi un testo di legge sul documento informatico.

Ci riuscimmo: il testo venne consegnato all'AIPA a fine luglio 1996 ed i suoi esiti sono storia nota a tutti. Gratificante e per noi molto importante è il fatto che il nucleo "civilistico" di quel testo, pur fra tanti sconvolgimenti e rimaneggiamenti, costituisce ancora oggi il nucleo centrale della normativa italiana in materia.

La partecipazione alle diverse commissioni costituite presso l'AIPA (Firma digitale e documento informatico; Archiviazione ottica dei documenti; siti Internet della P.A.; Carta di identità elettronica; etc..) ha insegnato e reso evidenti tante cose, prima sfuggite o comunque non attentamente valutate.

Prima fra tutte una lezione "comportamentale": mai guardare al Notariato come unico portatore della "verità". L'esigenza di terzietà tipica della nostra professione porta alcuni di noi a guardare con disgustato distacco ed a volte con superiorità tutto ciò che in tema di certezza ed autenticità non è di provenienza notarile: atteggiamento ideale, questo, per uccidere una funzione ed una professione facendo i killer di se stessi.

Altro insegnamento avuto è che nulla può farsi ed ottenersi se non collaborando con i portatori di interessi anche contrapposti ai nostri: valga per tutti il lunghissimo braccio di ferro fatto in AIPA con gli esponenti dell'ABI sul tema delle responsabilità del certificatore e del titolare di un certificato di firma.

E' opportuno sottolineare infine un dato che ritengo di importanza fondamentale, quasi lapalissiana, e che nelle vicende parlamentari ha costituito a volte motivo di salvaguardia della normativa sul documento informatico: non puoi regolare una materia se non ne conosci almeno i principi fondamentali. Dal che la necessità di una collaborazione sempre più stretta col mondo scientifico ed universitario, per la giusta definizione dei confini tra "certezza giuridica" e "certezza strumentale o scientifica": il metodo ideale in questo senso è proprio quello fin qui seguito sia in AIPA sia dal C.N.N., e cioè far sedere sempre allo stesso tavolo tecnici e giuristi.

Alla lunga ci si capisce, si dialoga, si costruisce.

Sicuramente molto si è costruito fino ad oggi, ma siamo ancora alle fondamenta e tanto deve ancora farsi, mai isolandosi e credendo sempre più in un notariato al servizio della società e del cittadino, capace di dialogare affermando la propria professionalità e competenza, ma mai assumendo atteggiamenti di superiorità o supponenza.

IL CONTESTO NORMATIVO

Le norme che in Italia disciplinano la firma digitale o firma elettronica sono fondamentalmente contenute nel **D.P.R. 28 dicembre 2000, n. 445** (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), che ha incorporato, tra le altre, in modo quasi letterale, le disposizioni del precedente ed oggi abrogato **D.P.R. 10 novembre 1997, n. 513** (Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59).

I suddetti provvedimenti trovano la loro base giuridica **nell'art. 15 comma 2 della legge 15 marzo 1997, n. 59** (Delega al governo per il conferimento di funzioni e compiti alle regioni ed agli enti locali per la riforma della pubblica amministrazione e per la semplificazione amministrativa, c.d. legge Bassanini-uno), la prima norma che nell'ordinamento italiano ha affermato in termini ampi e generali, sia dal punto di vista oggettivo che soggettivo, il principio della piena validità e rilevanza della documentazione informatica, delegando il governo ad emanare specifici regolamenti per disciplinare i criteri e le modalità di applicazione.

Le disposizioni di carattere tecnico relative all'infrastruttura di certificazione sono state poi emanate col **D.P.C.M. 8 febbraio 1999** (Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513), sulla base di specifica delega prevista dal D.P.R. n. 513/1997 (art. 3) ed ancora oggi vigente, nonostante ne fosse prescritto l'adeguamento almeno biennale.

Tra gli altri provvedimenti tecnici si segnalano, in particolare, la **Circolare AIPA 19 giugno 2000, n. 24** (Art. 16,

comma 1, dell'allegato tecnico al Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999. Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513), che stabilisce un formato comune dei certificati al fine di consentire il loro reciproco riconoscimento tra tutti i certificatori; la **deliberazione AIPA 23 novembre 2000, n. 51** (Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513); nonché la **circolare AIPA 8 febbraio 2002, n. 39** (Art. 14, comma 2, del Decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999: codici identificativi idonei per la verifica del valore della chiave pubblica della coppia di chiavi del Presidente dell'Autorità per l'Informatica nella Pubblica Amministrazione), che pubblicata in Gazzetta Ufficiale indica le chiavi pubbliche di vertice per una verifica completa della cosiddetta "catena di certificazione".

Ponendosi sul piano dell'ordinamento della Comunità Europea, al fine dell'armonizzazione delle normative nazionali in materia, occorre tenere conto della **direttiva 13 dicembre 1999, n. 1999/93/CE** relativa ad un quadro comunitario per le firme elettroniche. La direttiva segue l'emanazione del primo regolamento (D.P.R. n. 513/1997) ed ha, quindi, richiesto l'adeguamento dell'ordinamento italiano in materia (poi trasfuso come si è detto nel D.P.R. n. 445/2000) sotto alcuni importanti profili. La normativa italiana è stata fin dall'inizio pensata con l'obiettivo dell'introduzione della sottoscrizione elettronica nei rapporti con la Pubblica Amministrazione e, quindi, ha disciplinato un tipo di documento informatico dotato delle massime garanzie di sicurezza al fine di una sua piena equiparazione giuridica al documento cartaceo; diversamente, la prospettiva della direttiva europea è più ampia, rivolta anche ad applicazioni che richiedono minori garanzie giuridiche (ad es. il commercio elettronico su grande scala) e, quindi, prevede, oltre a firme "avanzate" anche firme non avanzate, al limite dotate di una scarsa o nulla sicurezza e garanzia.

La direttiva comunitaria è stata recepita nell'ordinamento italiano con il **D.lgs. 23 gennaio 2002, n. 10** (Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche) che, strutturandosi in parte come provvedimento autonomo ed in parte come modificativo del D.P.R. n. 445/2000, ha introdotto la categoria della "firma elettronica" ed ha previsto un regime più liberale per lo svolgimento dell'attività di certificazione, senza peraltro eliminare la figura della "firma digitale", la cui efficacia probatoria viene peraltro espressa in termini differenti. A parte ciò, l'impianto normativo precedente rimane ancora vigente e, pertanto, per operare il coordinamento tra le disposizioni del D.P.R. n. 445/2000 e quelle recate dal decreto di recepimento della direttiva, è prevista l'emanazione di un regolamento ai sensi dell'art. 17 comma 2 della legge n. 400/1988, entro trenta giorni dall'entrata in vigore del decreto di recepimento della direttiva (cioè entro l'1 aprile 2002). Tale decreto dovrà, inoltre, fissare i requisiti necessari per lo svolgimento dell'attività di certificatore, sostituendo così le regole tecniche contenute nel D.P.C.M. 8 febbraio 1999 ancora vigente.

ELENCO DELLE DISPOSIZIONI RILEVANTI

Firma digitale - Firme elettroniche

- Art. 15, comma 2, legge 15 marzo 1997, n. 59 - Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa (G.U. 17 marzo 1997, n. 63 suppl. ord.)
- D.P.R. 10 novembre 1997, n. 513 - Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59 (G.U. 13 marzo 1998, n. 60)
- D.P.C.M. 8 febbraio 1999 - Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti

informatici ai sensi dell'art. 3, comma 1, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (G.U. 15 aprile 1999, n. 87)

- Autorità per l'Informatica nella Pubblica Amministrazione - Circolare 19 giugno 2000, n. 24 - Art. 16, comma 1, dell'allegato tecnico al Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999. Linee guida per l'interoperabilità tra i certificatori iscritti nell'elenco pubblico di cui all'articolo 8, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (G.U. 30 giugno 2000, n. 151)
- Autorità per l'Informatica nella Pubblica Amministrazione - Deliberazione 23 novembre 2000, n. 51 - Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (G.U. 14 dicembre 2000, n. 291)
- D.P.R. 28 dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (G.U. 20 febbraio 2001, n. 42 suppl. ord.)
- Autorità per l'Informatica nella Pubblica Amministrazione - Circolare 16 febbraio 2001, n. 27 - Art. 17 del Decreto del Presidente della Repubblica 10 novembre 1997, n. 513: utilizzo della firma digitale nelle pubbliche amministrazioni (G.U. 26 febbraio 2001, n. 47)
- D.P.C.M. 3 ottobre 2001 - Differimento del termine che autorizza l'autocertificazione della rispondenza ai requisiti di sicurezza nelle regole tecniche di cui al Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 (GU 6 ottobre 2001, n. 233)
- D.lgs. 23 gennaio 2002, n. 10 - Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche (G.U. 15 febbraio 2002, n. 39)
- Autorità per l'Informatica nella Pubblica Amministrazione - Circolare 8 febbraio 2002, n. 39 - Art. 14, comma 2, del Decreto del Presidente del Consiglio dei Ministri dell'8 febbraio 1999: codici identificativi idonei per la verifica del valore della chiave pubblica della coppia di chiavi del Presidente

dell'Autorità per l'Informatica nella Pubblica Amministrazione (G.U. 20 febbraio 2002, n. 43)

Unico

- Art. 1, D.lgs. 18 gennaio 2000, n. 9 - Disposizioni integrative e correttive dei decreti legislativi 18 dicembre 1997, n. 463, e n. 466, in materia, rispettivamente, di utilizzazione di procedure telematiche per la semplificazione degli adempimenti tributari in materia di atti immobiliari e di ulteriori interventi di riordino delle imposte personali sul reddito al fine di favorire la capitalizzazione delle imprese (G.U. 7 febbraio 2000, n. 30)
- D.P.R. 18 agosto 2000, n. 308 - Regolamento concernente l'utilizzazione di procedure telematiche per gli adempimenti tributari in materia di atti immobiliari (G.U. 30 ottobre 2000, n. 254)
- Ministero delle Finanze - Decreto 13 dicembre 2000 - Utilizzazione di procedure telematiche per gli adempimenti in materia di atti immobiliari: approvazione del modello unico informatico e delle modalità tecniche necessarie per la trasmissione dei dati (G.U. 29 dicembre 2000, n. 302)
- Agenzia del Territorio, Decreto 12 dicembre 2001 - Attivazione della trasmissione per via telematica del modello unico informatico per la registrazione, trascrizione e voltura degli atti relativi a diritti sugli immobili (G.U. 22 dicembre 2001, n. 297)
- Agenzia del Territorio, Decreto 1 agosto 2002 - Estensione, in regime di obbligatorietà, ad altri distretti notarili del modello unico informatico, relativamente agli atti di compravendita di immobili, e, in regime di facoltatività, a tutti i distretti notarili, relativamente ad altre tipologie di atti (G. U. 9 agosto 2002, n. 186)

Registro Imprese

- Art. 31, comma 2, legge 24 novembre 2000, n. 340 - Disposizioni per la delegificazione di norme e per la

semplificazione di procedimenti amministrativi - Legge di semplificazione 1999 (G.U. 24 novembre 2000, n. 275)

- Ministero dell'Industria del Commercio e dell'Artigianato - Decreto 21 marzo 2001 - Deposito dei bilanci per via telematica
- Ministero delle Attività Produttive - Decreto 12 novembre 2001 - Modalità per la presentazione per via telematica o su supporto informatico degli atti di conversione in euro del capitale delle società al fine del deposito per l'iscrizione nel registro delle imprese (G.U. 20 novembre 2001, n. 270)
- Art. 3 comma 13 legge 28 dicembre 2001, n. 448 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2002) (G.U. 29 dicembre 2001, n. 301, s.o. n. 385)
- Ministero delle Attività Produttive - Decreto dirigenziale 19 marzo 2002 - Proroga del decreto dirigenziale 21 marzo 2001 concernente il deposito per via telematica dei bilanci d'esercizio e situazioni patrimoniali
- Ministero dell'Economia - Decreto 17 maggio 2002, n. 127 - Regolamento recante disciplina delle modalità di pagamento dell'imposta di bollo dovuta sulle domande, le denunce e gli atti che le accompagnano, presentate all'Ufficio del registro delle imprese in via telematica, nonché la determinazione della nuova tariffa dell'imposta di bollo dovuta su tali atti (G.U. 2 luglio 2002, n. 153)

Comunità Europea

- Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche (Gazzetta ufficiale n. L 013 del 19/01/2000)
- Rettifica della direttiva 1999/93/CE del Parlamento Europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche (Gazzetta ufficiale delle Comunità europee L 13 del 19 gennaio 2000)

Archiviazione ottica

- Art. 2, comma 15, legge 24 dicembre 1993, n. 537 - Interventi correttivi di finanza pubblica (G.U. 28 dicembre 1993, n. 303)
- Autorità per l'Informatica nella Pubblica Amministrazione, Deliberazione 13 dicembre 2001, n. 42 - Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (G.U. 21 dicembre 2001, n. 296)

CERTIFICAZIONE DI FIRME ELETTRONICHE E PUBBLICA FUNZIONE

di Michele Nastri

La scelta del Consiglio Nazionale del Notariato di divenire Certificatore delle firme digitali dei notai italiani è funzionale ad una politica di valorizzazione della funzione del notaio, e di difesa dell'atto notarile quale documento munito di efficacia giuridica privilegiata, in virtù del preventivo controllo esercitato dal notaio circa i suoi attori ed i suoi oggetti, e soprattutto circa la sua conformità all'ordinamento giuridico. Il documento notarile – è ovvio, ma non inutile ribadirlo – fornisce infatti una sostanziale certezza di legittimità, ed è garanzia per i diretti interessati, ma anche e soprattutto per la sicurezza del commercio giuridico.

La presenza da protagonista del notariato nella storia, ancora embrionale, del documento informatico, è necessaria per lo svolgimento quotidiano dell'attività notarile e per far sì che il notariato sia parte attiva dei mutamenti in atto, ma soprattutto serve all'affermazione - ed alla evidenziazione - del ruolo sociale del notariato quale tutore dei traffici giuridici, a difesa di interessi che trascendono quelli dei singoli coinvolti nelle contrattazioni e sono più propriamente della società, come cercherò di dimostrare con queste note.

Anche nell'ambito del documento informatico è infatti interesse della collettività l'ottenimento di livelli di sicurezza delle contrattazioni che siano pari (o possibilmente superiori) a quelli forniti dal documento cartaceo. E' altrettanto importante che tali livelli di sicurezza siano ottenuti senza rinunciare ai risultati già acquisiti in ambito tradizionale, ma adeguando gli strumenti utilizzati alle caratteristiche del nuovo mezzo. L'esperienza del notariato, tradizionale produttore di documenti con altissimo grado di sicurezza giuridica, costituisce un patrimonio peculiare, e non comune a tutti coloro che si avvicinano ora, da utenti o attori del settore, al documento informatico con rilevanza giuridica.

Il documento informatico pone le stesse problematiche di carattere logico-giuridico di qualunque altro tipo di documento, ed in particolare quelle della autenticità e della integrità. Le firme elettroniche, e tra queste quella digitale in particolare, costituiscono mezzi normalmente sufficienti a risolvere tali problematiche, e come tali sono riconosciute dalla legislazione nazionale e comunitaria, pur con un incerto trattamento dei fenomeni patologici, che ha portato a modifiche sostanziali della disciplina nell'arco di pochissimi anni (cfr. art. 10 del D.P.R. 445/2000 nella versione originaria e nella novella di cui al D.Lgs. 10/2002), ed è sostanzialmente dovuto alla diversità intrinseca tra firma elettronica e modalità tradizionali di sottoscrizione.

La nozione tradizionale di documento comprende però un'ampia casistica, che si ripropone identica, dal punto di vista del valore giuridico, all'interno della categoria del documento informatico: nell'ambito dei documenti aventi rilevanza giuridica, ve ne sono infatti alcuni con efficacia privilegiata, dal punto di vista sostanziale e/o dal punto di vista probatorio. E' il caso, nel diritto nazionale italiano, dei documenti provenienti dalle Pubbliche Amministrazioni (inclusi i provvedimenti giurisdizionali), ed è anche il caso dell'atto notarile, pubblico o autenticato, stante l'efficacia probatoria qualificata che gli è riconosciuta e l'idoneità pressoché esclusiva a costituire titolo per la trascrizione o iscrizione nei registri della pubblicità immobiliare e commerciale di atti a contenuto negoziale o in genere interprivatistico. Tali documenti si distinguono:

- dal punto di vista formale-contenutistico per avere caratteristiche almeno in parte predeterminate (es. requisiti formali di sentenze e atti notarili);
- dal punto di vista della paternità per essere formati da un soggetto qualificato appartenente ad una pubblica amministrazione o munito comunque di un potere delegato dallo Stato.

La verifica dell'autenticità del documento e della sussistenza del potere in capo al suo autore può essere effettuata presso l'autorità da cui il potere deriva.

Nel mondo del documento cartaceo, simili documenti sono però riconoscibili anche per un insieme di caratteristiche esteriori, quali la carta intestata, la protocollazione, le modalità di redazione e datazione e, non da ultimo, l'apposizione di timbri, sigilli, punzoni che caratterizzano e qualificano il documento e presentano alcune sommarie caratteristiche di sicurezza, sufficienti a garantire un'accettabile tutela dei traffici giuridici, anche in ragione dell'estrema onerosità di un controllo generalizzato. Inoltre il trattamento del documento cartaceo è basato normalmente su contatti diretti e personali tra i soggetti interessati (presentazione e ritiro agli sportelli, richieste di chiarimenti, contatti tra pubbliche amministrazioni) che costituiscono mezzi impliciti di controllo dell'autenticità.

Nessuna di queste caratteristiche è presente nel documento informatico. Esso esclude per sua natura ogni contatto diretto tra autore e destinatari e non è suscettibile dell'apposizione di segni esteriori quali, ad esempio sigilli, timbri, punzoni. Pertanto la normativa di settore espressamente prevede che l'apposizione della firma digitale (ed ora elettronica) integra e sostituisce l'uso di tali sistemi (art. 24 comma 3, art. 25, comma 2, D.P.R. 445/2000). Ciò però rende necessario, al momento dell'utilizzazione, un controllo, quanto meno nel settore pubblico, della provenienza del documento da soggetto abilitato alla sua emissione, con la conseguente necessità di inserire all'interno del processo della firma digitale l'indicazione di funzioni, qualifiche, poteri, cariche. Gli usi cui tali documenti sono destinati rendono perciò necessario che la provenienza ed autenticità siano garantiti al terzo destinatario od utilizzatore, e quindi all'intera collettività (validità *erga omnes*).

Tali problematiche si pongono non solo per i documenti informatici aventi rilevanza pubblicistica, ma anche per qualunque tipo di documento nei quali un soggetto utilizzi un potere in qualche modo derivante da altro soggetto (è il caso della rappresentanza in materia civile e commerciale). La possibilità di indicare poteri, funzioni, o più genericamente, attributi del titolare, è peraltro legislativamente prevista all'art. 6, commi 3 e 4 della Direttiva 1999/93/CE, ed all'articolo 10 del D.P.R. 445/2000, come novellato dall'articolo 6 del D.Lgs. 10/2002. In molti casi poi, in cui

l'enunciazione di funzioni non costituisce un'esigenza irrinunciabile, essa appare utile per fornire adeguati livelli di sicurezza e per attivare procedure automatiche di verifica, che rendano, in ultima analisi, il sistema affidabile e conveniente agli occhi dell'utenza.

La normativa di settore mostra di avvertire il problema, ma detta solo criteri generali per la soluzione. Ciò si spiega con la novità del mezzo, con la mancanza di esperienze applicative, e con la scelta, prima del legislatore comunitario e poi anche di quello nazionale, di non intervenire normativamente nelle caratteristiche tecniche della firma elettronica. Non vi sono infatti norme specifiche in materia di rappresentanza volontaria od organica, e si devono ritenere applicabili i principi generali, e vi sono solo scarne indicazioni in materia di pubbliche amministrazioni e pubbliche funzioni.

Esaminiamo brevemente i dati normativi.

La **Direttiva 99/93/CE** definisce firmatario "… persona che detiene un dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta" (art.2, comma 3); nell'allegato 1, relativo ai requisiti prescritti per un certificato qualificato, è prevista all'interno di tale tipo di certificato l'indicazione di un attributo specifico del firmatario.

L'art.28, comma 2, del **D.P.R. 445/2000** (già art.9, comma 2, D.P.R. 513/97) tra gli obblighi del certificatore impone di "identificare con certezza la persona che fa richiesta della certificazione", di "specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza di poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite" e di "procedere tempestivamente alla revoca o sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo".

L'art. 29 del **D.P.R. 445/2000** (già art. 17 del D.P.R. 513/97) sancisce: "1. Le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla

generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza.

omissis

3. Le chiavi pubbliche dei pubblici ufficiali non appartenenti alla pubblica amministrazione sono certificate e pubblicate autonomamente in conformità alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'ambito dei rispettivi ordinamenti giuridici.

omissis".

Da ultimo, l'articolo 11, comma 3 del **D.P.C.M. 8 febbraio 1999** stabilisce che possono essere indicate nel certificato eventuali "limitazioni nell'uso della coppia di chiavi", "eventuali poteri di rappresentanza" ed "abilitazioni professionali".

E' il caso di rilevare che il decreto modificativo del D.P.R. 445/2000, previsto dal D.Lgs. 10/2002, ed in corso di emanazione al momento in cui si scrive, dovrebbe contenere, secondo le versioni provvisorie note, alcune modifiche relative alle modalità per documentare la sussistenza di funzioni, cariche e poteri, nel senso di una maggiore fluidità e libertà della loro certificazione, e demanderebbe ad un successivo decreto ministeriale le modalità di enunciazione della qualifica di pubblico ufficiale o di abilitazioni professionali, permanendo transitoriamente l'attuale disciplina fino all'emanazione di questo ultimo decreto.

Infine, solo per inciso, va detto che anche la normativa sul processo telematico prevede per l'accesso una modalità di verifica delle funzioni e delle abilitazioni (D.P.R. 123/2001).

La Pubblica Amministrazione provvede quindi al rilascio delle chiavi ai propri appartenenti, nel rispetto del proprio ordinamento e delle norme in materia di firma digitale. Anche per quanto riguarda i pubblici ufficiali non appartenenti alla Pubblica Amministrazione (e quindi i notai), l'impianto normativo che risulta dall'articolo 29, comma 3, del D.P.R. 445/2000, è un semplice rinvio all'ordinamento di settore (peraltro ribadito nelle bozze del nuovo D.P.R.). Ciò significa che il rilascio delle firme elettroniche dei notai è soggetto alle stesse regole che abilitano il notaio all'esercizio della professione secondo l'ordinamento professionale.

Pertanto così come il Presidente del Consiglio Notarile Distrettuale, ai sensi dell'art. 24 della legge 16 febbraio 1913 n. 89, ordina l'iscrizione nel Ruolo dei notai esercenti nel Distretto, e da tale momento il notaio è abilitato all'esercizio, sarà il Presidente del Consiglio Notarile a procedere al rilascio (o ad intervenire necessariamente nella fase di rilascio) della firma digitale relativa all'esercizio delle funzioni notarili. Analogamente le procedure di sospensione e revoca della firma saranno modulate sulle procedure relative alla interruzione o alla cessazione dall'esercizio delle funzioni notarili, e tali cause di sospensione e revoca si aggiungeranno a quelle proprie di qualunque firma elettronica (cfr. le apposite sezioni di questa pubblicazione).

Il sistema prevede quindi in modo esplicito per taluni soggetti che la firma digitale a questi rilasciata ne attesti le funzioni, sulla base delle modalità previste dagli ordinamenti di settore. Si disinteressa, in verità, del successivo ciclo di vita del certificato di firma, ed in particolare delle ipotesi di cessazione dalle funzioni, per le quali si deve ritenere non possa agirsi che simmetricamente, conferendo il potere di revoca anche all'organo che ne è titolare in ambito generale.

Soddisfatto questo requisito, che tuttavia comporta non pochi vincoli applicativi, la normativa lascia piena libertà circa le modalità di indicazione delle funzioni.

Ciò ha comportato non pochi problemi.

Allo stato infatti, con l'unica eccezione dell'Autorità di Certificazione del Consiglio Nazionale del Notariato, non è attivo alcun sistema che consenta la diretta verifica, all'interno del complessivo sistema della firma digitale, di funzioni, poteri, abilitazioni professionali di un soggetto. E' vero che esistono nella pratica casi di indicazione delle funzioni all'interno del certificato di firma digitale, ma le modalità di tali indicazioni sono tali da non garantire con certezza che queste appaiano al terzo fruitore di un documento firmato; inoltre, nei manuali operativi dei Certificatori che inseriscono tali indicazioni, sono spesso presenti limitazioni di responsabilità che rendono le stesse non impegnative.

Tale carenza di applicazioni è da imputarsi a motivi tecnici e giuridici. Dal punto di vista giuridico, l'estrema sinteticità delle norme non favorisce scelte univoche che garantiscano soluzioni con validità generale. Dal punto di vista tecnico, è possibile teoricamente agire in vari modi per l'attribuzione di funzioni o poteri, che possono essere così sintetizzati, con le rispettive caratteristiche ed inconvenienti:

- l'indicazione di poteri o funzioni direttamente nel Manuale Operativo, collegando così ad un Certificatore esclusivamente soggetti aventi una determinata funzione (es.: le firme digitali del Certificatore C.N.N. sono rilasciate esclusivamente a notai in esercizio, e ciò risulta dal Manuale Operativo); tale soluzione aggira le problematiche di carattere tecnico, ma, a causa dell'unicità del Manuale Operativo per ogni Certificatore, può adottarsi esclusivamente nei casi in cui la qualifica da attribuire sia unica, come per il Notariato e le altre professioni; non è quindi applicabile a tutte le strutture gerarchiche, come nel caso della Pubblica Amministrazione, e costituisce soluzione ad una limitata classe di problemi; essa è stata adottata dal Notariato in quanto, come si vedrà in prosieguo, era l'unica scelta immediatamente praticabile;
- l'inserimento nel certificato di firma digitale di un campo cd. di estensione che indichi i poteri; tale soluzione, presente nella normativa nazionale, e compatibile con quella comunitaria, appare la più facilmente realizzabile in un futuro prossimo, ma necessita di un processo di standardizzazione delle procedure tecniche ed organizzative, perché le indicazioni dei poteri risultino con certezza all'atto dell'utilizzazione della firma, come richiesto dalle norme che determinano le responsabilità del Certificatore (art. 28 bis D.P.R. 445/2000); in tale prospettiva è l'attività, ormai pressoché ultimata, del Gruppo di lavoro coordinato dal Consiglio Nazionale del Notariato nell'ambito dell'Assocertificatori (associazione di categoria cui aderiscono la maggioranza dei Certificatori

italiani della firma digitale) che propone le linee guida di uno standard tecnico e giuridico-organizzativo;

- il collegamento al certificato cd. di firma, che individua il titolare, di un secondo certificato cd. d'attributo, che ne individua le funzioni o, traducendo dall'inglese, le attribuzioni; anche questa modalità è teoricamente possibile, e presenta l'innegabile vantaggio di consentire una vita del certificato di firma distinta da quella del certificato di attributo, ed anche la certificazione dell'attributo da parte di Certificatore diverso dal Certificatore della firma, prospettiva questa particolarmente interessante per il Consiglio Nazionale del Notariato, che avrebbe potuto assumere tale funzione (cfr. CNN Notizie del 4 agosto 1999); tuttavia essa è risultata non praticabile per i ritardi nell'elaborazione di uno standard riconosciuto da tutte le applicazioni di firma digitale presenti sul mercato, con i conseguenti insormontabili problemi di interoperabilità. Allo stato sono in corso in particolare a livello europeo, studi per la standardizzazione del certificato di attributo e per l'individuazione delle applicazioni per le quali utilizzarlo.

Tutte tali ipotesi avrebbero quindi potute essere applicate al notariato. I Presidenti dei Consigli Notarili Distrettuali interverranno, sulla base dello schema normativo in precedenza esposto, nella fase di rilascio delle chiavi di firma dei notai, allo scopo di garantire la sussistenza della funzione notarile; successivamente controlleranno il ciclo di vita delle chiavi in relazione sempre alla sussistenza in capo al soggetto di tali funzioni. Ciò è realizzabile sia nell'ipotesi dell'autorità di certificazione autonoma del notariato, sia nelle ipotesi di utilizzazione del sistema basato sulle estensioni del certificato di sottoscrizione o sul certificato di attributo. Queste ultime ipotesi non sono ancora tuttavia di piena attualità applicativa.

La scelta del Notariato di porsi in autonomia come certificatore dei notai è quindi basata, da un punto di vista pratico, sulla constatazione della inesistenza, allo stato attuale, di una

soluzione alternativa che consenta, come richiesto dalla normativa, da una parte l'evidenza della funzione notarile all'atto dell'apposizione della firma, e dall'altra il controllo delle funzioni da parte dei Consigli Notarili per tutti i casi di cessazione o sospensione.

Ma vi è di più. Il panorama delle firme elettroniche, dopo la Direttiva 99/93/CE, ed il D.Lgs. 10/2002, si è ulteriormente articolato, per non dire complicato, in virtù delle nuove figure previste, quali la firma elettronica semplice distinta dalla firma elettronica avanzata, quest'ultima basata o meno su un certificato qualificato e creata eventualmente con un dispositivo sicuro per la creazione della firma, e rilasciata da un Certificatore che sia o meno accreditato. Senza voler entrare nel dedalo di ipotesi che ne derivano, va chiarito che la Direttiva ha ritenuto di dare cittadinanza e dignità di firma praticamente ad ogni sistema di imputazione ad un soggetto di un documento informatico, allo scopo di impedire che gli stati nazionali scoraggino normativamente l'utilizzo di firme elettroniche, e di soddisfare le diverse esigenze provenienti dai paesi membri. Ne è conseguenza però un generale alleggerimento del sistema originariamente previsto dal legislatore italiano, che equiparava la firma digitale alla sottoscrizione manuale solo se conforme a precisi requisiti tecnici. Basti pensare che non sussiste ormai, per nessun certificatore di firma digitale, l'obbligo di iscrizione a pubblici elenchi, che resta una mera facoltà.

Questa situazione, unita al continuo susseguirsi di modifiche normative più o meno importanti (ma spesso molto importanti) comporta l'assoluta priorità per il Notariato di una gestione autonoma dei propri documenti informatici e della loro sicurezza, per preservarne la qualità ed il valore sia dal punto di vista tecnico sia dal punto di vista giuridico, ma anche e soprattutto per porsi come attore principale di una vicenda che sta incidendo in modo irreversibile sulla natura e le funzioni del documento giuridico, e per fornire esperienze applicative che coniughino la sicurezza tecnologica e giuridica alla semplificazione delle procedure ed all'utilizzo di nuove tecnologie.

Il tutto in uno scenario molto variegato, in cui la competenza tecnologica non sempre va di pari passo con la cultura del documento giuridico, dei suoi usi e della sua

conservazione, e nel quale la mancanza di esperienze diffuse rende prevedibile che gli autori delle prime applicazioni di successo possano essere i capofila del processo di pratica del documento informatico.

Il notariato, con l'Adempimento Unico e la pubblicità commerciale telematici, la scrittura privata autenticata informatica, e soprattutto con la sua cultura del documento, può e deve avere questo ruolo.

IL MANUALE OPERATIVO, LA SUA FUNZIONE E STRUTTURA, RESPONSABILITÀ DEL CERTIFICATORE

di Sabrina Chibbaro

Il concetto di firma elettronica è abbastanza ampio: comprende tutti i sistemi che utilizzino dati in forma elettronica come metodo di autenticazione.

Altra cosa è quella che chiamiamo "firma digitale": essa non è un semplice metodo di autenticazione ma soddisfa altri requisiti e precisamente:

- essere connessa in maniera unica al firmatario;
- essere idonea ad identificare il firmatario;
- essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;
- essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati; (cfr. Art. 2 Direttiva 1999/93/CE).

La Direttiva Europea la definisce come "firma elettronica avanzata".

Il sistema di firma digitale (o firma elettronica avanzata) previsto dalla legislazione italiana si basa sulla crittografia a doppia chiave, in cui una delle due chiavi viene resa pubblica all'interno del certificato, mentre la seconda, univocamente correlata con la prima, rimane segreta, conosciuta solo dal titolare.

Punto critico di tutto il sistema della firma digitale è l'associazione della coppia di chiavi con il suo titolare.

Il ruolo dell'Autorità di certificazione (Certification Authority) è quello appunto di garante della corrispondenza tra l'identità del titolare del certificato e la coppia di chiavi (pubblica e privata) cui il certificato si riferisce.

Poiché la pubblicazione e la verifica delle chiavi si svolgono per via telematica, accedendo ad appositi elenchi, l'elemento più importante, per la certezza dell'identità del mittente, è l'affidabilità dei soggetti che quegli elenchi gestiscono.

Quindi l'attività di pubblicazione delle chiavi deve essere svolta da soggetti fidati, che certifichino l'attribuzione delle chiavi stesse, dopo aver compiuto le necessarie verifiche sull'identità di ciascun titolare.

Ma cosa determina il grado di affidabilità di un certificatore e, di conseguenza, del certificato da lui emesso? Come fa il terzo che riceve un documento firmato digitalmente a stabilire se può "fidarsi" e quindi accettare il documento firmato?

Proprio questa è la funzione del Manuale Operativo (Certification Practice Statement - CPS) della Certification Authority (CA): esso costituisce l'insieme delle regole a cui essa si attiene nella sua attività di certificazione di chiavi pubbliche.

Il Manuale Operativo deve essere pubblicato sul sito del Certificatore in modo che gli utenti possano comprendere il livello di sicurezza dei certificati rilasciati.

I Manuali Operativi delle CA hanno un contenuto, per così dire, "fisso", nel senso che si articolano in una serie di punti comuni, così che l'utente possa fare il raffronto fra le varie Autorità di Certificazione su diverse questioni.

Una delle prime specifiche del Manuale Operativo riguarda la *Tipologia delle utenze*: in essa viene specificato a quali soggetti può essere rilasciata la firma digitale e per quali scopi essa può essere utilizzata: nel caso del C.N.N. la limitazione è subito evidente.

Il C.N.N. certifica esclusivamente i notai nell'esercizio delle proprie funzioni (cfr. art. 3.3): la firma digitale in questo caso equivale alla corrispondente firma autografa con l'aggiunta del sigillo. Essa non è utilizzabile al di fuori dell'esercizio delle funzioni e, conseguentemente, il C.N.N. non assume responsabilità per un uso indebito (cfr. art. 5.1).

I capitoli 7, 8, 9 e 10 descrivono le procedure di identificazione, generazione delle chiavi di firma, emissione nonché di revoca e sospensione dei certificati: queste sono le sezioni del Manuale Operativo che si coordinano con le procedure previste dalla Legge Notarile per l'iscrizione a ruolo del notaio: poiché infatti la certificazione da parte del C.N.N. prevede che il notaio sia nell'esercizio delle funzioni, essa va in parallelo alla iscrizione a ruolo con consegna del sigillo.

Parte attiva della procedura è pertanto, oltre al notaio interessato, il Presidente del Consiglio Notarile, che effettua la materiale consegna della *smart-card*, ne cura l'attivazione da parte dell'utente-notaio e chiude il processo con la richiesta al C.N.N. di emissione del certificato.

Corrispondentemente la revoca e la sospensione ricorrono nei casi in cui il notaio è tenuto a riconsegnare il sigillo per un qualsiasi caso di interruzione dell'attività nel distretto di appartenenza.

Revoca e sospensione vanno inoltre richieste al Certificatore in tutti i casi in cui si abbia la sottrazione o lo smarrimento della *smart-card*, nonché anche il semplice sospetto di una compromissione delle chiavi.

Sia la revoca che la sospensione (che si differenziano per il fatto che la prima è una definitiva caducazione del certificato, mentre la seconda è solo temporanea) possono essere richieste dal notaio titolare del certificato, dal Presidente del Consiglio Notarile (quale terzo interessato) o dalla stessa Autorità di Certificazione nei casi previsti dal Manuale Operativo.

Il capitolo 4 fissa gli obblighi di ciascuna delle parti coinvolte nel processo di firma digitale: del Certificatore, che deve attenersi ai livelli di sicurezza previsti dalla legge o a quelli previsti dal Manuale Operativo; del Titolare, che deve custodire con diligenza la *smart-card* ed il relativo PIN evitando ogni possibile compromissione delle chiavi e che deve attivarsi con la massima sollecitudine per avvertire la CA di eventuali casi di revoca o sospensione; dei destinatari, che devono sempre verificare le firme apposte sui documenti che ricevono nonché prendere visione del Manuale Operativo per verificare eventuali limitazioni

all'uso della firma o alla responsabilità del Certificatore; del Presidente del Consiglio Notarile, che quale "terzo interessato" deve curare la tempestiva pubblicità di una eventuale revoca o sospensione dalle funzioni del notaio appartenente al suo distretto, con conseguente revoca o sospensione del relativo certificato.

L'elencazione degli obblighi fissa i limiti delle responsabilità per ciascuno dei soggetti considerati.

Il capitolo 5, in particolare, si occupa della responsabilità del Certificatore: è di tutta evidenza che quanto più la CA limita la sua responsabilità, tanto più diminuisce il "peso" e il valore delle firme da lei emesse.

E questo costituisce il punto cruciale del Manuale Operativo, sicuramente l'indice principale di affidabilità del Certificatore.

Tutti i Certificatori stabiliscono dei limiti alla propria responsabilità: basta scorrere i Manuali Operativi di tutte le CA iscritte all'elenco dell'AIPA; nel caso del C.N.N., che certifica i notai nell'esercizio delle funzioni, la responsabilità va commisurata al tipo di attività che tramite quei certificati di firma viene svolta.

Il Manuale Operativo si occupa poi del servizio di emissione di marche temporali (capitolo 12), che attribuiscono al documento firmato data ed ora certa.

L'apposizione ad un documento firmato digitalmente della marca temporale è di fondamentale importanza per stabilire se quando una certa firma è stata apposta essa era valida e non revocata o sospesa, controllo che si effettua tramite la consultazione delle Liste dei Certificati Revocati e dei Certificati Sospesi (CRL-CSL).

Tali liste sono consultabili sul sito del certificatore tramite specifici protocolli (LDAP) e sono periodicamente aggiornate: tanto più spesso il certificatore provvede a aggiornare tali liste, tanto più viene ridotta la possibilità che il terzo destinatario faccia incolpevole affidamento su un documento firmato con una chiave il cui certificato risulti poi revocato.

Il Manuale Operativo descrive infine tutte le procedure e specifiche tecniche di gestione del servizio di certificazione.

Per concludere, il Manuale Operativo si può considerare un documento di fondamentale importanza per ogni soggetto coinvolto nel processo di firma, il quale non può pertanto esimersi da un'attenta lettura al fine di un consapevole utilizzo dello strumento.

REVOCA E SOSPENSIONE DELLA FIRMA DIGITALE

di Marco Dolzani

Prima di esaminare in dettaglio le norme, contenute nel Manuale Operativo della P.K.I. del notariato, in tema di revoca e sospensione dei certificati di firma, occorre nuovamente riflettere sul concetto stesso di firma digitale abbinato alla funzione notarile.

Come ben puntualizzato nelle note curate da Ugo Bechini, "*La procedura di firma eseguita tramite la "smart card" rilasciata dal C.N.N. equivale alla apposizione sul documento, sia della firma del notaio che del suo sigillo*". E poiché ai sensi dell'art. 23 del D.P.R. 28 dicembre 2000 n. 445 "*l'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo*", tale modalità è di per sé idonea a far conseguire al documento informatico la medesima forma autentica propria degli atti notarili cartacei.

Tale risultato non può non suscitare inquietudini e preoccupazioni in soggetti, come i notai, abituati a siglare ogni atto, scrittura privata, copia autentica, estratto ecc..., direttamente ed esclusivamente mediante la propria sottoscrizione autografa.

I dubbi derivano non solo da un senso di insicurezza legata alla mancata padronanza dello strumento tecnologico adottato e dalle difficoltà, congenite alla figura propria dei notai, di utilizzo di meccanismi non direttamente controllabili, ma anche e soprattutto dagli interrogativi riguardanti la intrinseca pericolosità di tale invenzione; di fronte ad una prospettiva di massiccio utilizzo futuro della firma digitale, si profilano, accanto alle attuali possibilità di falsificazione dei documenti, nuovi orizzonti di abuso collegati ad episodi di incursione informatica e violazione dei sistemi di sicurezza che i rotocalchi di questi ultimi anni dimostrano essere tutt'altro che fantasiosi.

Compito immediato e primario di chi si appropria della tecnologia del secolo è pertanto quello di garantirne il buon funzionamento cercando di approntare tutti quegli strumenti

idonei ad escludere o limitare sul nascere ogni tentativo di abuso.

Il sistema della firma digitale infatti, non può dirsi completo e sicuro, se non dopo aver definito e collaudato un serio e funzionale apparato di controllo idoneo ad evitare ogni forma di abuso, falsificazione o manipolazione, che avrebbe effetti dirompenti per la sicurezza e la certezza dei documenti pubblici e conseguentemente del traffico giuridico in generale.

Le norme tecniche dettate dall'Autorità preposta, le procedure imposte per la sicurezza, gli algoritmi utilizzati per la creazione delle chiavi di firma, sono allo stato attuale delle conoscenze tecnologiche, certamente idonee ad escludere manipolazioni o falsificazioni dei dispositivi di firma.

La parte più vulnerabile del sistema riguarda invece la possibilità di un uso improprio della "smart card"; per esso deve intendersi sia quello effettuato da soggetti diversi dal titolare (in casi di smarrimento o furto), sia quello effettuato dal titolare stesso ove a quest'ultimo ne risulti inibito l'utilizzo (per legge o per disposizione delle autorità preposte).

Il Manuale Operativo dell'Autorità di certificazione costituisce, come già detto nei lavori che precedono, il primo strumento a disposizione degli utenti, per la verifica della "bontà" di un documento informatico munito di firma digitale.

Infatti solamente la firma digitale apposta secondo norma, cioè rilasciata ed utilizzata in conformità alle disposizioni in vigore cui il Manuale Operativo si deve attenere, è idonea a rispettare i requisiti di forma e probatori alla stessa assegnati dalla legge.

La "*smart card*" che contiene la firma digitale, ancorché rilasciata secondo le procedure di legge, non è strumento tecnico perpetuo, ma è destinato a "morire", sia per cause naturali quali il decorso del termine alla stessa irrevocabilmente assegnato nel momento in cui viene rilasciata, sia per altre vicende idonee a determinarne la sua revoca o la sospensione.

Va infatti ricordato come, "*l'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione*" (cfr. art. 23 del DPR 28 dicembre 2000 n. 445).

A tal fine assumono particolare rilevanza i capitoli 10 e 11 del Manuale Operativo.

Il Manuale contiene peraltro delle peculiarità proprie, non previste nei manuali predisposti dalle altre autorità di certificazione attualmente riconosciute.

Infatti, ai certificati di firma in parola (cioè quelli della PKI del notariato) risultano abbinate le funzioni notarili: di conseguenza le ipotesi di revoca o sospensione di tali certificati debbono essere definite tenendo presenti, sia l'aspetto tecnico e proprio del congegno utilizzato e l'idoneità astratta del medesimo ad essere oggetto di un uso improprio, sia l'aspetto che investe il notaio, vuoi come utente privato, vuoi quale pubblico ufficiale.

Il primo profilo comporta la necessità di impedire l'illegittimo uso della "*smart card*" da parte di soggetti diversi dal suo titolare, nei casi di perdita di controllo diretto da parte del notaio ad es. per furto o smarrimento.

Per quanto attiene invece la persona titolare della "*card*", le ipotesi di revoca e sospensione si riferiscono ai casi di intervenuta incapacità, anche solo temporanea, di agire, sia essa determinata da fattori soggettivi patologici che da impedimenti giuridici rilevanti (fallimento, incapacità naturale, interdizione, inabilitazione, ordine del giudice).

La peculiarità della "*smart card*" rilasciata ai notai da parte del C.N.N., comporta altresì la necessità di garantire i terzi, che l'uso della stessa sia effettuato nel rispetto della legge notarile. A tal fine il Manuale Operativo ha riproposto la casistica della sospensione e revoca come prevista dalla legge notarile e dalle altre leggi speciali, affidando conseguentemente ai soggetti da tali fonti legittimati, facoltà di procedere, autonomamente, a richiedere all'Autorità di certificazione di intervenire in conformità.

I casi di revoca riguardano in particolare tutte quelle ipotesi in cui si verifichino delle situazioni, sia ricollegabili direttamente allo strumento tecnico, sia riferibili al titolare del certificato, che ne inibiscono l'utilizzo; la revoca è un fatto definitivo, che comporta la cessazione anticipata della validità di un certificato di firma senza alcuna possibilità di sua riattivazione (art. 10.2, I comma del manuale).

La sospensione attiene invece ai casi in cui il certificato non possa essere "temporaneamente" utilizzato: essa comporta

"*l'interruzione temporanea della sua validità"* (art. 10.2, II comma).

Il Certificatore utilizza per la revoca e la sospensione la Lista dei certificati revocati (CRL) e la Lista dei certificati sospesi (CSL).

In ogni ipotesi di revoca o sospensione il Certificatore procede infatti a registrarla nel Giornale di Controllo ed a pubblicare la Lista (CRL o CSL) che la contiene; il momento della pubblicazione è provato mediante l'apposizione della marca temporale.

La revoca o la sospensione del certificato è attuata nel momento della pubblicazione della lista; essa assume una particolare rilevanza ai fini della conoscibilità nei confronti dei terzi e per la conseguente opponibilità: l'art. 23, V comma del D.P.R. 445/2000 precisa che revoca o sospensione "*hanno effetto dal momento della pubblicazione salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate"*.

Ciascuna lista deve essere aggiornata ogni quattro ore a cura del Certificatore; in casi di urgenza, determinati dalla compromissione, manomissione (anche solo sospette), o dalla perdita del possesso della chiave privata, il Certificatore è tenuto a procedere immediatamente all'inserimento nella lista di revoca ed alla conseguente pubblicazione.

Va ricordato ancora che il Certificatore che non procede tempestivamente alla revoca o alla sospensione, assume una specifica responsabilità "*nei confronti dei terzi che facciano ragionevole riferimento sul certificato stesso, dei danni provocati per effetto della mancata registrazione della revoca o sospensione del certificato, salvo che provi di aver agito senza colpa.".*

Il quadro normativo così delineato, sembra quindi porre a carico del destinatario terzo, un onere di particolare cautela ogni volta che sia destinatario, anche solo indiretto, di un documento firmato digitalmente: cautela consistente nell'obbligo di consultazione diretta (ove essa non avvenga con procedura automatica del sistema) dell'elenco dei certificati revocati o

sospesi pubblicati dall'Autorità di certificazione.

Il Certificatore è parallelamente assoggettato ad una forma di responsabilità oggettiva, collegata all'obbligo di diligenza nella tenuta delle liste di revoca e sospensione, al loro aggiornamento e alla tempestiva pubblicazione, responsabilità aggravata dall'inversione dell'onere della prova.

Infatti il Certificatore è responsabile verso terzi per i danni derivanti dalla mancata pubblicazione tempestiva degli aggiornamenti riguardanti le Liste di revoca o di sospensione; tale responsabilità sussiste in ogni caso, salvo che il Certificatore riesca a provare di aver agito senza colpa.

I Certificati possono essere revocati o sospesi su richiesta del notaio titolare, per iniziativa del Presidente del Consiglio notarile Distrettuale, da parte del Certificatore oppure per ordine dell'Autorità giudiziaria.

Qui esamineremo solamente i casi di revoca e sospensione dei certificati ad iniziativa del Notaio o del Presidente Distrettuale.

La nostra disamina non sarà altresì rivolta ai casi di revoca dei certificati relativi a chiavi di certificazione, né a quelli relativi a chiavi di marcatura temporale (previsti rispettivamente nei capitoli 10.3 e 10.4 del Manuale cui si rinvia).

Orbene, la richiesta di revoca su domanda del Notaio può essere facoltativa oppure obbligatoria.

Quest'ultima riguarda i casi di perdita del possesso del certificato (furto, smarrimento, distruzione), i casi in cui si verifichi un guasto o il cattivo funzionamento del dispositivo di firma, se vi sia il sospetto di abusi o falsificazioni e quando sia stata compromessa la segretezza della chiave privata.

Il Notaio ha poi la facoltà di domandare la revoca del certificato anche per ipotesi diverse da quelle sopra previste specificandone i motivi.

La richiesta di sospensione da parte del Notaio è invece sempre facoltativa e può essere richiesta in caso di concessione del periodo di assenza e limitatamente a quest'ultimo.

Al Presidente del Consiglio Distrettuale Notarile compete invece il potere-dovere di richiedere la revoca del certificato in

tutti quei casi in cui, in base alla legge notarile, si siano verificate delle ipotesi di interruzione delle funzioni nell'ambito del distretto di competenza.

In particolare egli dovrà procedere alla richiesta di revoca per avvenuta decadenza dalla nomina da notaio, per cessazione dall'attività a seguito di dispensa, rimozione, destituzione, per trasferimento del notaio ad altro distretto, negli altri casi di cessazione definitiva dalle funzioni, nonché in esecuzione di provvedimenti dell'Autorità giudiziaria comportanti la cessazione dalle funzioni notarili.

I casi di richiesta di sospensione del certificato su iniziativa del Presidente, comprendono, oltre all'ipotesi già analizzata e riguardante il periodo di assenza autorizzata al notaio titolare, anche i casi di sospensione temporanea del notaio, di cessazione temporanea dall'esercizio notarile, di temporanea interdizione o inabilitazione all'ufficio, nonché i casi in cui la richiesta promani da un provvedimento dell'Autorità giudiziaria (comportante la cessazione temporanea dalle funzioni).

Il Certificatore è invece obbligato di procedere alla revoca oltre che nei casi di richiesta da parte degli altri soggetti a ciò abilitati, anche qualora venga a conoscenza di cause limitative della capacità del titolare, di sospetti abusi e falsificazioni.

Quanto ai casi di sospensione il Certificatore vi procede d'ufficio oltre che nei casi richiesti dai soggetti abilitati, anche quando, ricevuta una domanda di revoca, non abbia la possibilità di verificare l'autenticità della richiesta. In tal caso il certificato resta sospeso fino alla verifica.

Prima di procedere alla revoca o alla sospensione del certificato e salvo i casi di urgenza per i quali deve procedere immediatamente, il Certificatore ne dà preventiva comunicazione al notaio titolare, con specificazione dei motivi, nonché della data e dell'ora a partire dalla quale il certificato non sarà più valido o sarà sospeso.

Il Manuale Operativo si occupa anche di stabilire in dettaglio le varie modalità pratiche per richiedere la revoca o la sostituzione di un certificato.

Vengono definite le procedure alternativamente adottabili

da parte del titolare o su iniziativa del Presidente del Consiglio Distrettuale Notarile, nonché su iniziativa del Certificatore, distinguendo fra ipotesi "normali" e casi di "emergenza".

In questa sede passiamo ad esaminare solo le ipotesi di iniziativa del notaio o del Presidente Distrettuale.

In entrambi i casi vengono individuate tre diverse modalità.

Mentre le prime due sono consentite sia in casi normali che urgenti, la modalità che prevede l'utilizzo del telefono è limitata ai soli casi di emergenza.

Le richieste non determinate dall'emergenza vanno presentate con almeno 2 giorni feriali di anticipo rispetto alla data di entrata in vigore.

La prima modalità comporta che il notaio proceda alla richiesta, con firma autografa resa su documento cartaceo presso il Presidente del Consiglio Distrettuale il quale procederà al suo inoltro al Certificatore.

Nella richiesta il titolare dovrà indicare i dati essenziali (nome, cognome, distretto), nonché il codice identificativo proprio attribuito a ciascun titolare al momento della consegna della *smart card*, i dati identificativi del certificato (numero seriale), la motivazione e decorrenza della revoca o sospensione, nonché ogni altro elemento idoneo a determinare ipotesi di urgenza o di emergenza.

La seconda modalità prevede l'inoltro della domanda direttamente al Certificatore con sottoscrizione digitale da apporsi sull'apposito modulo informatico (scaricabile direttamente *"on-line"*); la domanda deve contenere i medesimi dati sopra evidenziati (cfr. Modalità n. 1).

In questo caso il Certificatore deve provvedere immediatamente all'aggiornamento della lista ed alla sua pubblicazione.

In caso di emergenza è poi possibile procedere alla richiesta anche per via telefonica, utilizzando il codice riservato del notaio ed il codice identificativo (Contenuto nel campo Subject, AIPA\24). E' questa la terza delle modalità previste, che consente di procedere immediatamente a sospendere la validità di un certificato.

Il notaio titolare procede personalmente ad inoltrare, al centro telefonico predisposto dal Certificatore (che deve essere

attivo dal lunedì al sabato a partire dalle 8:30 fino le ore 20:00), la richiesta, facendosi identificare attraverso la comunicazione del proprio Codice riservato (CRN) e del Codice identificativo e deve fornire nome, cognome, sede e distretto di appartenenza, la motivazione e la decorrenza della revoca o sospensione, nonché gli elementi rilevanti a determinare l'emergenza.

In questo caso tuttavia il Certificatore provvede alla sola sospensione del certificato ed al suo inserimento nell'apposita Lista dei certificati sospesi (CSL), nonché alla pubblicazione della Lista nel registro dei certificati.

Affinché il certificato sia definitivamente revocato o sospeso occorre infatti che il titolare provveda entro i dieci giorni feriali successivi ad inoltrare la medesima richiesta o a chiedere la riattivazione secondo una delle due modalità precedentemente esaminate.

Il Presidente del Consiglio Distrettuale può procedere a propria volta ed autonomamente alla richiesta di revoca o sospensione.

Allo stesso sono riservate le medesime modalità sopra esaminate e concesse al titolare del certificato; per le relative procedure possiamo fare direttamente rinvio a quanto sopra evidenziato, anche per quanto attiene la casistica e le formalità di compilazione delle richieste. Naturalmente il Presidente Distrettuale dovrà altresì unire ai propri dati personali identificativi anche quelli del notaio del cui certificato viene richiesta la revoca o la sospensione.

L'UTILIZZO DEL SISTEMA

di Ugo Bechini

La procedura di firma eseguita tramite la *smart card* rilasciata dal C.N.N. equivale all'apposizione sul documento sia della firma del notaio che del suo sigillo. I documenti così sottoscritti hanno il medesimo valore di un originale notarile o di una copia autentica su carta. Questa è una caratteristica unica, che distingue i dispositivi di firma rilasciati dal C.N.N. da quelli emessi da ogni altro certificatore, e da cui dipendono le speciali cautele che circondano la vita del sistema in ogni sua fase.

Per questa ragione, ad esempio, la consegna di *smart card* e PIN avviene ad opera del Presidente Distrettuale, e cioè il Pubblico Ufficiale che consegna al notaio il sigillo metallico e ne raccoglie la firma autografa. In quest'ottica, appare evidente l'improponibilità di ogni tentativo di attribuire eguale valenza alla firma digitale emessa da altri certificatori e cioè, in concreto, dal non meglio qualificato impiegato o collaboratore esterno di un'azienda privata.

I dispositivi di firma rilasciati dal C.N.N. sono destinati ad essere utilizzati dai notai esclusivamente nell'esercizio delle loro funzioni. L'eventuale utilizzo per scopi diversi è ammesso solo se autorizzato espressamente dal C.N.N.. Va appena sottolineato che, anche se la procedura di firma viene eseguita in vista di un determinato adempimento, il documento elettronico firmato è documento autentico ad ogni effetto.

In linea generale qualunque file è suscettibile di firma. E' ad esempio possibile firmare digitalmente una copia autentica creata direttamente al computer attraverso il normale *word processor* di studio, oppure un file realizzato passando allo *scanner* una copia preparata su carta, od anche un file prodotto utilizzando promiscuamente le due tecniche (esempio: atto costitutivo e statuto direttamente da *word processor* e ricevuta dei tre decimi da *scanner*). In tutti questi casi, è comunque sufficiente firmare il file una sola volta.

La principale limitazione pratica deriva da una caratteristica intrinseca dei dati in forma digitale, e cioè la possibilità di riprodurli all'infinito in modo assolutamente indistinguibile dall'originale. Si usa anzi osservare che i concetti stessi di originale e di copia non hanno molto senso nel mondo informatico: si può parlare al più di duplicati identici. Al momento non è pertanto possibile impiegare la firma digitale in tutte quelle ipotesi in cui un determinato documento (in senso fisico) ha un peculiare valore giuridico. Il pensiero corre immediatamente ai titoli di credito e, per quel che concerne lo specifico notarile, alle copie in forma esecutiva, che al momento dovranno quindi essere prodotte in forma cartacea. La difficoltà potrà essere in futuro superata attraverso il ricorso a complesse infrastrutture di cui solo nei mesi scorsi sono iniziate negli USA le prime sperimentazioni.

In questa prima fase, appare conveniente pure astenersi cautelativamente dall'uso della firma digitale per la produzione di procure speciali, copie di procure a raccolta, e comunque documenti destinati all'allegazione ad atti notarili su carta. L'interesse pratico è evidente (Tizio rilascia una procura a Palermo e questa viene utilizzata pochi minuti dopo per un rogito a Trieste; la Banca X rilascia una nuova procura ai suoi funzionari che viene diffusa in tempo reale a tutte le Agenzie) ma vi sono almeno due punti bisognosi di ulteriore approfondimento:

- per i motivi appena accennati, una procura speciale per un solo atto potrebbe essere riprodotta in un numero indefinito di esemplari identici, tutti egualmente utilizzabili; l'ostacolo non pare insormontabile ma su alcune implicazioni non vi è ancora generale accordo;
- ciascun documento dovrà essere stampato in forma tradizionale, leggibile, per l'allegazione agli atti cartacei. E' ben vero che la firma digitale, come ogni altra sequenza di bit, è indifferente al supporto (in teoria potrebbe anche essere scolpita su pietra) ma è impossibile risalire in modo univoco dalla comune stampata al file firmato. Se ad esempio, una copia è prodotta in formato *pdf*, non c'è modo di ricreare con esattezza il file *pdf* a partire dalla stampata leggibile. Ciò impedisce, tra l'altro, di eseguire la

verifica standard della firma, ed una firma digitale non verificabile è, almeno in prima approssimazione, una *non firma*. Si tratta di problemi certamente superabili, ma con procedure innovative ancora allo studio.

L'assenza di regole certe per la produzione e conservazione in forma digitale dell'originale d'atto pubblico consiglia di attenersi a tal fine alla forma cartacea.

Il panorama tecnologico attuale ha sconsigliato l'adozione di tecnologie biometriche (ad esempio: riconoscimento dell'impronta digitale o della retina) che impediscano fisicamente l'uso della *smart card* a persone diverse dal notaio. La ragione non risiede nella relativa facilità con cui è possibile ingannare tali sistemi, emersa evidente dalle ricerche compiute soprattutto in Giappone e negli USA ed intensificatesi a partire dal settembre 2001: nel nostro caso si sarebbe trattato di un dispositivo di sicurezza aggiuntivo, e quindi un livello di inviolabilità non eccelso sarebbe in definitiva risultato accettabile. Più problematico sarebbe stato piuttosto il caso inverso, e cioè il mancato riconoscimento del vero avente diritto. Tali disfunzioni, tutt'altro che infrequenti, sono paradossalmente più tollerabili in contesti ad altissima sicurezza (accesso a sale di controllo di centrali nucleari o ad impianti militari) ove è immediatamente disponibile personale specializzato, oppure è possibile attivare metodi alternativi di identificazione, oppure ancora procedere alla sostituzione dell'addetto cui è negato un accesso: tutte soluzioni che ci sono precluse. Ma la difficoltà al momento pressoché insuperabile risiede nell'indisponibilità di protocolli standard che consentano di integrare i dati biometrici nella *smart card*. I dispositivi comunemente disponibili in commercio hanno tutt'altra funzione, giacché bloccano l'accesso a determinati computers od apparati, e non precluderebbero l'impiego della *smart card* su altri apparecchi.

Attualmente non è quindi fisicamente impossibile che persona diversa dal notaio utilizzi la *smart card* rilasciata dal C.N.N., se in possesso del codice numerico che ne consente l'attivazione (PIN). Lo stato d'elaborazione di simili questioni da parte della dottrina e della giurisprudenza, sia in campo civile che penale, è ancora assolutamente rudimentale, e sono poche le

affermazioni che in questo campo si possano compiere con ragionevole certezza. Non si può quindi che limitarsi ad affermazioni assolutamente generali.

Consegnare la propria *smart card* ad un terzo, collaboratore od altri, rivelandogli nel contempo il proprio PIN, significa porlo in condizione di produrre in totale autonomia, e senza controllo alcuno, atti autentici assolutamente indistinguibili da quelli posti in essere dal notaio. Ciò è sicuramente un illecito deontologico della massima gravità, e con ogni verosimiglianza il fatto ha rilevanza penalistica sia per il notaio che per il soggetto agente. E' inoltre praticamente impossibile al notaio dimostrare la sua mancata partecipazione alla formazione di un determinato documento, dal quale sarà quindi di fatto vincolato. Non si vede come, dinanzi ad una qualunque vicenda patologica, il notaio possa affermare la propria estraneità.

Nel mondo cartaceo la disponibilità fisica del sigillo metallico di per sé non permette alcunché, dacché manca la firma. Similmente, nel mondo telematico, la *smart card* di per sé non consente alcunché, se il suo detentore non è a conoscenza del PIN. Chi dispone di *smart card* e PIN riunisce invece in sé i poteri di documentazione che spettano al notaio. E' quindi sensato equiparare la cura riservata alla conservazione della *smart card* a quella sinora dedicata al sigillo, ma è lampante che a ciò deve necessariamente accompagnarsi la gelosa custodia del PIN da parte del notaio, personalmente.

E' ben vero che autorevole dottrina ha avvicinato la firma elettronica al sigillo: lo ha fatto però per evidenziare come la mancanza di *autografia*, l'assenza nella firma di parametri fisici irriproducibili (pressione, forma, direzione della penna) faccia sì che il risultato dell'operazione di firma sia indipendente dall'identità fisica dell'operatore, come accade per l'impronta del sigillo. E si può forse ammettere che il privato consegni *smart card* e PIN ad altro soggetto operando una valida delega *de facto* della propria firma digitale: la giurisprudenza ha anzi già lasciato intravedere esiti di tal fatta. Ma non occorre lungo discorso per dimostrare che ciò è sicuramente illecito in relazione all'esercizio di pubbliche funzioni.

L'uso concreto del sistema di firma è estremamente agevole, e non più complicato di un'operazione Bancomat. E' sufficiente introdurre la *smart card* nell'apposito dispositivo, lanciare il programma, digitare il proprio PIN e impartire il comando di firma.

La procedura di firma può svolgersi autonomamente, ed in tal caso è sufficiente scegliere il file da firmare, allo stesso modo in cui si sceglie un testo da stampare. Tale fase è rapidissima, ma non ne va sottovalutata l'importanza: l'erronea identificazione del documento da sottoporre alla procedura di firma, la sua incompletezza od inesattezza, può essere fonte di responsabilità non trascurabili.

Come già accennato, il formato del file è del tutto indifferente, qualunque file può essere firmato: persino un'immagine od una registrazione sonora, se lo si desidera. Le limitazioni derivano piuttosto dall'uso che si intende fare del file firmato: se ad esempio l'amministrazione destinataria accetta solo files di tipo *pdf*, occorrerà preventivamente produrre il file in tale formato avvalendosi di un programma idoneo. E' comunque prevedibile che le *software houses* integrino le funzioni di firma nei loro pacchetti; tendenzialmente ci si deve attendere che per firmare un determinato file sia sufficiente premere un pulsante identico a quelli che consentono di stampare o memorizzare il file medesimo.

Il file firmato può a questo punto essere memorizzato su qualunque supporto (anche un floppy, ad esempio) oppure inviato via posta elettronica, senza che il suo valore giuridico subisca variazioni: le caratteristiche intrinseche della firma elettronica rendono praticamente impossibile qualunque manipolazione anche da parte di chi abbia totale accesso al file firmato. Anche per quanto concerne la trasmissione un elevatissimo livello di automazione, specie per quanto riguarda gli adempimenti, sarà senz'altro la norma.

La firma digitale rilasciata dal C.N.N. appartiene esclusivamente al notaio: il coadiutore o delegato adopererà, ovviamente, la propria firma, menzionando la propria qualifica, con le formule abituali, in coda al documento firmato. All'uopo il Manuale Operativo ha previsto che i coadiutori non notai ricevano una loro *smart card*.

In caso di smarrimento o disfunzione del dispositivo di firma occorre immediatamente procedere alla revoca ed all'emissione di una nuova *smart card*. La tecnologia impiegata consente di prevenire, operando praticamente in tempo reale, la circolazione di firme prodotte abusivamente, a condizione però che la revoca sia tempestiva: la responsabilità di ogni ritardo (come di ogni violazione delle procedure fissate dal Manuale Operativo) ricade sul notaio.

Qualora nelle more (si parla di un intervallo comunque misurabile in ore) fosse indispensabile produrre copie digitali autentiche, allo stato della normativa non si vede alcuna soluzione di portata generale diversa dalla nomina di un delegato ai sensi della legge notarile.

LA MARCATURA TEMPORALE

di Raimondo Zagami

La sostituibilità agli effetti giuridici degli attuali documenti cartacei con i nuovi documenti informatici presuppone che questi ultimi offrano garanzie di sicurezza quantomeno equivalenti, se non anche superiori, ai primi. Tra i profili probatori del documento assume un'importanza fondamentale l'attribuzione della cosiddetta "data certa" e cioè la prova con validità *erga omnes* della formazione del documento in un certo arco temporale o, comunque, della sua esistenza anteriormente ad un dato evento (art. 2704 codice civile). Un documento informatico del quale non fosse riconoscibile il tempo della sua formazione avrebbe ben poca rilevanza dal punto di vista giuridico e non potrebbe servire a risolvere quelle soluzioni di conflitti che si ispirano al noto brocardo *prior in tempore potior in jure*. In definitiva, in mancanza di un sistema sicuro e pratico per attribuirne la data certa, il documento informatico non sarebbe utilizzabile per la stragrande maggioranza delle applicazioni aventi rilevanza giuridica, oggi già a regime, oppure in via sperimentale o ancora solo allo stadio di progetto.

Nel tradizionale sistema di documentazione cartacea, l'attribuzione della data certa deriva principalmente dal riscontro di un'attestazione fatta da un soggetto terzo ed imparziale depositario di pubbliche funzioni (ad es. notaio, ufficiale giudiziario, ufficio del registro, ecc.). Questa attestazione può essere espressa al momento della formazione del documento stesso (ad es. nell'atto pubblico notarile), oppure derivare dalla conservazione di un documento in un pubblico registro (ad es. per la storica funzione degli uffici del registro - ora delle entrate).

Il sistema italiano della infrastruttura a chiave pubblica, ponendosi l'ambizioso obiettivo di regolare il documento informatico quale sostitutivo del documento cartaceo nei rapporti con la pubblica amministrazione, non poteva ovviamente trascurare l'aspetto della attribuzione di "data certa" e, quindi,

basandosi sulla tecnologia oggi disponibile, ha offerto agli operatori un sistema sicuro, rapido, efficace ed economico per raggiungere anche questo importante risultato.

La stessa tecnologia informatica utilizzata per apporre firme digitali (la cifratura asimmetrica) consente l'apposizione di "marche temporali" (*digital time stamp*) che attestano la data e l'ora di un documento informatico (la cosiddetta "validazione temporale"). Come per la certificazione delle chiavi, occorre naturalmente l'intervento ancora una volta imprescindibile di una terza parte fidata ed imparziale che operi tale attestazione. Questa terza parte è normalmente lo stesso soggetto che opera la certificazione delle chiavi e, quindi, un soggetto privato, non necessariamente partecipe di pubbliche funzioni. L'apposizione di una marca temporale produce l'effetto giuridico di attribuire "ad uno o più documenti informatici una data ed un orario opponibili ai terzi" (art. 22 comma 1 lett. g D.P.R. n. 445/2000) e, dunque, non solo efficaci tra le parti. La veridicità ed esattezza di una marca temporale, come per i certificati delle chiavi pubbliche, dovrebbe presumersi fino a prova contraria, senza però la necessità di attivare la querela di falso perché non costituirebbe fede privilegiata.

In pratica, l'operazione per apporre una marca temporale ed ottenere così la validazione temporale di un documento informatico è molto semplice e si svolge in via telematica (ad es. tramite la R.U.N.) mediante una connessione tra l'elaboratore dell'utente e quello del Certificatore. Attraverso apposito programma, selezionato il documento su cui apporre la marcatura temporale, questo viene trasmesso al servizio di marcatura temporale che in automatico (senza diretto intervento umano) appone la marca temporale (data ed ora), la sottoscrive con firma digitale e restituisce il tutto all'utente. La marca temporale (similmente ad una firma digitale) consiste in un piccolo *file* informatico (un pacchetto di informazione digitale), contraddistinto da un titolo identificativo, che può essere conservato unitamente al documento cui si riferisce o anche in modo separato, dato che comunque è ad esso collegato inequivocabilmente.

Per essere più precisi, in realtà non viene trasmesso telematicamente il documento nella sua interezza, bensì soltanto

un suo estratto digitale (impronta) di dimensione fissa, che lo rappresenta in modo sintetico ed univoco, generato attraverso apposite funzioni matematiche (funzioni di *hash*). In tal modo si velocizzano le operazioni e si mantiene la riservatezza del documento, dato che il servizio di marcatura temporale dalla conoscenza dell'impronta non può risalire al contenuto del documento sottoposto. Il tutto si svolge in pochi secondi ed in modo trasparente per l'utente.

La successiva verifica della data di un documento informatico oggetto di validazione temporale può essere compiuta velocemente e facilmente da chiunque disponga del documento e della relativa marca temporale. In pratica occorrerà sempre un elaboratore elettronico con un apposito programma di verifica che, analogamente alla verifica di una firma digitale, in modo del tutto automatico e trasparente per l'utente, effettua le necessarie operazioni e restituisce all'utente l'informazione della data e dell'ora di apposizione della marca temporale.

Anche per la verifica occorre che il processo si svolga con l'interrogazione telematica dei registri dei certificatori allo scopo di evidenziare eventuali revoche o sospensioni che possano inficiare la persistente validità della validazione temporale. Infatti, dal punto di vista tecnico la marcatura temporale non è altro che un'attestazione di data ed ora effettuata in automatico da un elaboratore e firmata digitalmente dal certificatore che ne assume la responsabilità con una specifica chiave di marcatura temporale appositamente certificata. Di conseguenza, la verifica si svolge come la verifica di una qualsiasi firma digitale, attraverso la verifica del relativo certificato ed è soggetta agli stessi limiti e rischi (scadenza, revoca o sospensione del certificato).

La validazione temporale dei documenti informatici è uno strumento essenziale per la conservazione e gestione degli archivi di documenti informatici sottoscritti con firma digitale. Per il mantenimento dell'efficacia probatoria propria del documento informatico sottoscritto con firma digitale e, quindi, per consentire anche a distanza di anni la verifica di una firma digitale, non sarebbe sufficiente procedere ad una semplice archiviazione informatica del documento, ma occorre la manutenzione

dell'archivio con l'apposizione di marche temporali e la loro rinnovazione periodica.

Mentre una sottoscrizione su carta, con il trascorrere del tempo, mantiene in via di principio lo stesso valore probatorio, diversamente una firma digitale, invece, è fin dall'inizio destinata a perdere sicurezza in breve tempo a seguito della sua necessaria scadenza (predeterminata) o per eventuale revoca o sospensione anteriori alla scadenza. Il termine di scadenza di una chiave, infatti, non può essere superiore a 3 anni (art. 22 comma 1 lett. f D.P.R. n. 445/2000), in quanto si presume che nell'arco di tempo considerato, l'inarrestabile progresso nella potenza di calcolo degli elaboratori consentirebbe attacchi e frodi sui codici delle firme già apposte, potendosi perpetrare falsi non riconoscibili. Peraltro, anche prima della scadenza, la chiave di firma può essere compromessa (ad es. smarrita o sottratta) e, quindi, revocata o sospesa. In tutti questi casi, l'effetto della cessazione di validità della chiave (e del relativo certificato) si ripercuote direttamente sulle firme digitali successivamente apposte, per cui "L'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione" (art. 23 comma 5 D.P.R. n. 445/2000).

L'efficacia giuridica delle firme digitali apposte, invece, in un momento anteriore alla cessazione di validità della chiave è fatta salva, ma solo se la firma in considerazione è stata oggetto di validazione temporale (o di autentica notarile ai sensi dell'art. 24 del D.P.R. n. 445/2000). Occorre dimostrare che la firma è stata apposta in un momento anteriore alla cessazione di validità della relativa chiave. Una firma digitale di per sé non contiene alcuna connotazione di carattere temporale e, pertanto, una firma apposta dopo la scadenza (o revoca o sospensione) della chiave non sarebbe tecnicamente distinguibile da una firma apposta validamente in un momento anteriore. In questi termini, è stabilito che "la validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione, può essere estesa mediante l'associazione di una o più marche temporali" (art. 60 comma 1 Reg. tec.); con riferimento alla revoca o sospensione, "la presenza di una marca temporale valida associata ad un documento informatico ... garantisce la validità del documento anche in caso di

compromissione della chiave di sottoscrizione, purché la marca temporale sia stata generata antecedentemente a tale evento" (art. 60 comma 3 Reg. tec.). Si deduce *a contrario* che in mancanza di una marca temporale, la validità del documento non è garantita, né a seguito di scadenza, né di revoca o sospensione della chiave. Non potrebbe essere escluso il rischio che il documento sia stato falsificato o sottoscritto abusivamente (da chi ha decifrato chiavi non più sicure o si è impossessato di chiavi altrui); né, possono essere esclusi comportamenti fraudolenti di revoca della chiave (da parte dello stesso titolare), finalizzati al ripudio di precedenti firme digitali.

Pertanto, in pratica, il notaio che riceve in via telematica un documento informatico sottoscritto con firma digitale, potrà provvedere egli stesso all'apposizione della marcatura temporale, servendosi, tra gli altri, del servizio che sarà offerto dal C.N.N. quale Certificatore. In tal modo, ad es. documenti che giustificano l'esecuzione di un adempimento potranno dal notaio essere esibiti con piena efficacia probatoria, in caso di contestazioni, anche a distanza di anni per dimostrare la tempestiva esecuzione degli adempimenti posti a suo carico, mettendosi al riparo dalla naturale scadenza e da eventuali revoche delle chiavi. Per tali motivi è necessario che le ricevute di adempimenti telematici (come ad es. Unico informatico o Registro imprese) siano restituite all'utente con la firma digitale del soggetto ricevente, in modo del tutto analogo all'attuale ricevuta cartacea oggi consegnata. Documenti privi di firma digitale non è, invece, normalmente necessario che vengano sottoposti a validazione temporale, salvo casi particolari (ad es. opere dell'ingegno), dato che l'eventuale validazione temporale non potrebbe attribuire un'efficacia probatoria superiore a quella loro propria.

La marcatura temporale agli effetti giuridici, quindi, può essere facilmente apposta su qualunque tipo di documento informatico (testi, immagini, suoni, filmati, ecc.), dato che è del tutto avulsa dal contenuto; può essere apposta in qualunque momento, all'atto della formazione del documento o anche successivamente (purché prima della cessazione di validità della firma digitale); può essere richiesta senza formalità da chiunque,

autore del documento o estraneo ad esso; possono essere rapidamente apposte più marche temporali, da soggetti diversi ed in momenti diversi, essendo ogni marca verificabile autonomamente dalle altre; possono essere oggetto di marcatura temporale singoli documenti o nello stesso tempo gruppi di documenti, salvo in quest'ultimo caso operare una verifica congiunta sulla base del gruppo originariamente validato; le marche temporali possono essere conservate unitamente ai documenti cui si riferiscono o separatamente da essi, restando sempre valide e verificabili.

Nonostante quanto sopra rilevato, il testo unico e le regole tecniche, non stabiliscono come obbligatoria l'apposizione di una marca temporale. Nemmeno si prevede come obbligatoria la marcatura temporale della firma digitale del notaio autenticante *ex* art. 24 D.P.R. n. 445/2000. Si tratta, quindi, di un onere (in senso tecnico) a carico degli interessati che intendono tutelarsi - anche in relazione all'ammontare dei possibili danni - contro la scadenza della chiave o contro eventuali e future revoche. La validazione temporale, unitamente alla firma digitale è, invece, richiesta obbligatoriamente per la presentazione o il deposito di un documento per via telematica o su supporto informatico ad una pubblica amministrazione (art. 24 comma 6 D.P.R. n. 445/2000).

Si è detto che la validazione temporale risiede sull'efficacia di marche temporali, che consistono in un'attestazione garantita dalla firma digitale del soggetto emittente (il certificatore). Di conseguenza, le marche temporali sono esse stesse soggette a cessazione di validità per scadenza, revoca o sospensione, in modo del tutto analogo alle firme digitali. Quando cessa la validità di una marca temporale vengono meno i suoi effetti di attribuire "ad uno o più documenti informatici una data ed un orario opponibili ai terzi" (art. 22 comma 1 lett. g D.P.R. n. 445/2000). Inoltre, nel caso in cui la marcatura temporale garantiva la validità di una firma digitale dalla sua scadenza (o revoca o sospensione), logica conseguenza sarebbe la perdita di validità della stessa firma digitale garantita.

Pertanto, per mantenere l'efficacia di una validazione temporale e delle firme digitali da questa garantite, occorre procedere ad una periodica rinnovazione, da operare prima della

ultima scadenza. In tal senso è stabilito che "Prima della scadenza della marca temporale, il periodo di validità può essere ulteriormente esteso associando una nuova marca all'evidenza informatica costituita dal documento iniziale, dalla relativa firma e dalle marche temporali già ad esso associate" (art. 60 comma 2 Reg. tec.). Naturalmente, rinnovazione della marca temporale non significa rinnovazione del contratto o del rapporto giuridico documentato, dato che la rinnovazione della marca temporale serve solo a mantenere l'efficacia probatoria del documento originario.

Poiché al documento possono essere apposte più marche temporali (anche in tempi diversi e da soggetti diversi), la cessazione di validità di una di esse può essere compensata dalla persistente validità di un'altra. Anzi, per la conservazione di documenti particolarmente importanti è preferibile apporre più marche temporali, in modo che la revoca (per sua natura imprevedibile) di una delle marche non pregiudichi la validità del documento. L'importante è che la rinnovazione avvenga prima della scadenza (o, comunque, della cessazione di validità) dell'ultima delle marche temporali apposte.

La rinnovazione delle marche temporali può essere eseguita per singolo documento o per gruppi di documenti unitariamente considerati. Una sola marca temporale, in pochi secondi, potrebbe essere apposta all'archivio degli atti notarili e dei documenti di un intero anno. Peraltro, la rinnovazione potrebbe anche essere eseguita in automatico da appositi programmi che operano sulla base di orologi interni, selezionando i documenti in scadenza ed inviandoli telematicamente per la marcatura (rinnovo), senza che l'utente si accorga di nulla.

I documenti informatici con firma digitale autenticata da notaio ai sensi dell'art. 24 del D.P.R. n. 445/2000 e le copie informatiche dichiarate conformi dai notai ai sensi dell'art. 20 dello stesso D.P.R. n. 445/2000, in quanto provenienti da pubblico ufficiale, contengono già di per sé un'attestazione temporale avente efficacia giuridica *erga omnes*, senza la necessità della validazione temporale. Pertanto, una firma digitale autenticata da notaio mantiene la sua efficacia fino a che è valida la firma del notaio autenticante. Comunque, la marcatura temporale (ed il suo

rinnovo) sarebbe sempre necessaria per garantire il mantenimento dell'efficacia probatoria della firma del pubblico ufficiale oltre la sua naturale scadenza (o eventuale revoca o sospensione).

Il Manuale Operativo per il servizio di certificazione del C.N.N. regola espressamente in più punti il servizio di marcatura temporale, stabilendo che è riservato ai soli notai in esercizio titolari di un certificato di chiave pubblica emesso dallo stesso C.N.N. e che può avere per oggetto documenti informatici di qualunque specie, prodotti ed eventualmente sottoscritti, da un notaio o da altri soggetti.

L'IMPATTO DELLA PKI
SULLA ORGANIZZAZIONE DEGLI STUDI

di Egidio Lorenzi

Nella storia più recente (diciamo gli ultimi 50 anni) dell'organizzazione degli studi dal punto di vista pratico-operativo, ci sono alcune "tappe" importanti ed altre addirittura epocali.

Negli anni '50 ci fu l'avvento dei duplicatori ad alcool: per la prima volta si potevano ottenere più copie di uno stesso atto (fino a 20 o 30) battendo a macchina una volta sola e senza il limite delle 3 / 4 copie ottenibili con la carta carbone: fu una tappa importante.

Negli anni '60 fu la volta delle fotocopiatrici: le copie, volendolo, si potevano ottenere all'infinito direttamente dall'originale, senza neppure una ribattuta con la macchina da scrivere: fu una tappa epocale.

Negli anni '70 e '80 è stata la volta dei computer: inizialmente fu solo una tappa importante fintanto che il vantaggio è consistito nel poter correggere sul video l'originale infinite volte, rivederlo, variarlo e poi stamparlo; in seguito divenne una tappa senz'altro epocale quando hanno cominciato ad esistere dei veri e propri "sistemi informatici" capaci di costruire l'atto a partire da uno schema e poi di realizzare autonomamente i sottoprodotti e il repertorio.

Di mezzo, negli ultimi anni '80 e negli anni '90 e seguenti ci sono stati il fax, la cosiddetta "meccanizzazione" delle Conservatorie e dei Registri delle Imprese, internet, la posta elettronica e così via.

Ora la prossima tappa epocale è la piena realizzazione ed utilizzazione della firma digitale.

Per capire appieno perché questa novità costituisca un elemento davvero di svolta e non solo un parziale miglioramento dell'organizzazione degli studi, conviene forse "esagerare" ed immaginare lo scenario per così dire definitivo, quando l'utilizzo della firma digitale potrà dirsi completo e generalizzato: diciamo

fra 5 / 8 anni (ma forse non è improbabile che i tempi si accorcino fino a 3 / 4 anni).

Ecco allora che il personale di studio continuerà, probabilmente, a costruire l'atto notarile grosso modo come oggi con i diversi sistemi di composizione o di estrazione, partendo cioè da maschere o da schemi, immettendo i dati variabili ed ottenendo così l'originale.

Vogliamo immaginare che l'atto pubblico sia ancora redatto sulla carta e con metodi più o meno tradizionali o comunque molto simili a quelli attuali perché ci pare che quell'immaginato intervallo di tempo non basti a realizzare tutte le modifiche normative per poter costruire l'atto pubblico "elettronico", ma se quell'originale sarà una scrittura privata da autenticare cominceranno già le prime sostanziali differenze: non occorrerà stampare alcunché, le parti insieme al notaio controlleranno la scrittura sul video e poi estrarranno le loro *smart card* ed apporranno la loro firma digitale. A seguire il notaio autenticherà le firme apponendo la propria firma digitale. Se nello studio sarà presente una sola delle parti, il *file* viaggerà per posta elettronica fino al computer di un altro notaio, dove, allo stesso modo, verranno apposte le firme mancanti.

Da quel momento sarà il sistema stesso che ogni notaio avrà caricato sul proprio computer (e che probabilmente avrà scaricato gratuitamente da un sito di Notartel) a costruire automaticamente i sottoprodotti senza neppure quegli interventi manuali che oggi occorrono (come meglio si spiegherà in seguito) e poi una signorina (non serviranno più collaboratrici specializzate nel settore immobiliare o nel settore societario, almeno per i sottoprodotti perché appunto verranno realizzati automaticamente) manderà i vari sottoprodotti così realizzati in una cartella elettronica che potrebbe chiamarsi, per esempio, "firma".

Il notaio, fra un cliente e l'altro (speriamo che i clienti, almeno, ci siano ancora…) aprirà dal proprio computer quella cartella "firma": estrarrà dal portafoglio la propria "*smart card*", effettuerà probabilmente i controlli biometrici che allora esisteranno (tipo impronta digitale, iride od altro) e firmerà digitalmente i vari documenti.

A questo punto la stessa collaboratrice invierà per posta elettronica su canali privilegiati e sicuri i documenti all'ufficio pubblico prestabilito (anzi più probabilmente invierà tutti i documenti ad un unico ufficio il quale smisterà automaticamente le varie notizie a chi di dovere).

Il "fattorino" diventerà una figura storica, se ne ricorderanno i vecchi notai, i quali racconteranno di file lunghissime davanti agli sportelli pubblici con attese interminabili ed ai giovani sembrerà di sentir parlare della guerra e dei bombardamenti.

Anche le ispezioni, le visure presso i pubblici uffici, le richieste di certificazioni od altro, saranno un ricordo: tutto si effettuerà davanti al proprio computer con movimenti di documenti sicuri ed immodificabili perché firmati digitalmente e con movimenti di denaro altrettanto sicuri perché garantiti dallo stesso sistema.

La "macchina" più importante dello studio che è stata, via via nel tempo, prima la penna, poi la macchina da scrivere, poi la fotocopiatrice, poi il computer, diventerà il modem e quanto ad esso collegato o quel qualcosa di simile che esisterà allora.

Infatti il momento critico sarà appunto la trasmissione dei documenti e quindi sarà opportuno che in studio esistano almeno due, se non addirittura più sistemi di trasmissione che possano assicurare la utilizzabilità anche di fronte ad intoppi, a rotture e simili.

Ed il secondo momento critico, che costituirà l'ulteriore grande novità negli studi, sarà l'archiviazione dei documenti: non ci sarà più in giro la carta, finalmente, e si tratterà solamente di archiviare in maniera sicura e duratura nel tempo i *files* di testo ed i *files* immagine.

Anche questo aspetto aprirà problematiche e scenari nuovi, che non è il caso tuttavia di approfondire in questa sede.

Abbiamo immaginato il futuro, ma non crediate che si sia scritto di fantascienza. Per semplicità abbiamo immaginato un momento in cui tutto il meccanismo sia realizzato, completato e rodato. E per semplicità di comprensione anche da parte dei colleghi meno interessati ed attenti a questi argomenti abbiamo

generalizzato molto, usato termini tecnicamente non precisi e "saltato" dei momenti tecnicamente importanti (e di questo chiediamo scusa agli "informatici" più avveduti), ma, come si dice, "nel più ci sta il meno" e sia pure con qualche limitazione, con qualche necessità di verifica, con qualche intoppo di troppo, e così via, tuttavia gli scenari qui descritti cominceranno a realizzarsi molto presto ed i primi segni di quanto qui raccontato in certi casi si sono già cominciati a vedere e più generalmente si cominceranno a vedere già nei prossimi mesi.

I NUOVI LINGUAGGI DI *MARKUP* E L'ORGANIZZAZIONE DEGLI STUDI NOTARILI

di Gea Arcella

La differenza tra il contenuto e la struttura di un testo fa parte della esperienza di ognuno di noi, basta prendere in mano un libro ed andare all'indice: vi troveremo la materia trattata dal testo divisa in capitoli e paragrafi, e qualche volta anche in parti qualora l'argomento sia particolarmente esteso; l'esempio più pregnante che si possa fare per un giurista è l'indice del nostro codice civile con le sua partizioni in libri, titoli, capi, sezioni.

Proprio attraverso la lettura dell'indice abitualmente possiamo farci una sommaria idea di quanto aspettarci di trovare nel testo prescelto; infatti, dal punto di vista del contenuto a seconda che un determinato argomento sia oggetto di un paragrafo, di un capitolo, di una parte o dell'intera opera immediatamente avremo la percezione di quale sia la sua rilevanza dell'economia del testo, in un crescendo di importanza e soprattutto di ampiezza della trattazione.

Inoltre, anche a colpo d'occhio, e semplicemente scorrendo l'indice, ciascuno di noi è abituato a ritenere che un carattere più grande, come un allineamento più a sinistra, indichi un capitolo e un carattere minore, o un allineamento più a destra, un paragrafo – sempre riprendendo l'esempio or ora fatto dell'indice del codice civile anche in esso questo medesimo stile di formattazione viene rigorosamente rispettato.

In pratica l'indice di un libro riporta delle informazioni ordinate gerarchicamente e rappresentate secondo uno schema predefinito in modo da risultare funzionali alla loro fruizione, e questo a prescindere dalla casa editrice, dal colore della carta e dal tipo di carattere usato, ovvero a prescindere da quegli elementi rappresentativi meramente estetici, perché comunque saranno rispettate quelle modalità di formattazione che siamo abituati ad interpretare come divisione in capitoli e paragrafi.

Questo è un esempio molto evidente di come una tecnica di comunicazione, nel tempo, ha definito il rapporto fra la struttura gerarchica delle informazioni e la loro rappresentazione visiva.

Contenuto e struttura di un testo, infatti, non esauriscono gli elementi che entrano in gioco nella fruizione delle informazioni scritte, vi è un terzo livello, quello della rappresentazione, che ha una sua specifica valenza: un titolo, infatti, è un titolo a prescindere dal tipo di carattere usato in una particolare edizione o dal colore, lo stesso vale per i capitoli ed i paragrafi e per ogni elemento della struttura di un testo; fine della rappresentazione nell'edizione di un qualsiasi documento è proprio quello di favorirne la leggibilità, e soprattutto la percezione della struttura e del rapporto di questa con il contenuto. Certamente la rappresentazione serve anche a rendere un testo più accattivante di un altro, ma sempre fatti salvi alcuni limiti: infatti, se un editore invertisse i criteri che più sopra abbiamo indicato che differenziano la rappresentazione corrente dei capitoli e dei paragrafi – grandezza del font, spaziatura rispetto ai margini della pagina etc. - renderebbe di fatto illeggibile l'indice. Così come se tutti cominciassero ad utilizzare la grandezza dei caratteri e lo spazio, in una parola la formattazione del testo, con una valenza esclusivamente estetica, in breve si perderebbe la possibilità di capire, anche se a grandi linee, il contenuto di un qualsiasi documento scritto. Da ciò deriva che struttura e rappresentazione di un contenuto, anche se di fronte alla realizzazione di un testo possono sembrare confusi, sono due cose assolutamente separate.

Anche nei nostri atti avviene qualcosa di simile: in cima tutti ci aspettiamo di trovare il numero di repertorio e quello di raccolta, poi la natura, la dicitura REPUBBLICA ITALIANA, la data, il luogo di stipula, il nome e la sede del notaio, la comparsa delle parti, il dispositivo vero e proprio, la chiusa, le firme e il sigillo, ovvero tutto quanto è previsto dall'art. 51 Legge not. che rappresenta il nostro schema base per quanto riguarda la struttura dell'atto.

La stessa rappresentazione di queste informazioni è largamente condivisa – ad es. il fatto che a sinistra ci sia il numero

di repertorio e a destra quello di raccolta, o la suddivisione in articoli dell'atto - , ed in qualche caso anche prevista direttamente dall'art. cit. – pensiamo al maiuscolo per l'intestazione REPUBBLICA ITALIANA -, e comunque anche qualora non si adotti alcuna ripartizione del contratto, anche semplicemente con degli a capo o con la centratura di alcune parole cerchiamo di distinguere le varie parti del rogito individuando, magari con il grassetto, le informazioni che riteniamo più importanti e su cui vogliamo focalizzare l'attenzione del lettore.

Per quanto riguarda i testi elettronici il discorso è essenzialmente lo stesso: esiste un contenuto, la sua struttura e la rappresentazione di esso che di volta in volta si realizza, e la distinzione tra struttura e rappresentazione è fondamentale per garantire una buona fruizione delle informazioni.

Nei linguaggi di marcatura usati fin ora - ovvero quei linguaggi che permettono la visualizzazione dei testi a prescindere dal sistema utilizzato per la loro redazione, tra cui campeggia HTML che è a tutt'oggi il più diffuso sulla rete - questa netta distinzione tra struttura e rappresentazione si è andata via via perdendo, ed in questo modo si sono perse anche molte delle potenzialità dei motori di ricerca, costretti a fare ricerche su tutto il documento a parità di importanza, proprio nel momento in cui la mole dei testi accessibili attraverso la rete diventa tale da richiedere un meccanismo più puntuale - e' nell'esperienza di ognuno di noi l'effettuazione di ricerche che spesso restituiscono migliaia di documenti senza dire nulla della rilevanza del termine invocato come "parola chiave" all'interno della gerarchia logica di questi -.

Ma sotto i nostri occhi sta avvenendo un cambiamento radicale: attraverso l'adozione di un nuovo linguaggio di marcatura dei testi denominato XML (acronimo di *eXtesible Markup Language*), sarà finalmente possibile creare e/o accedere a documenti informatici che, tenendo distinti gli elementi di pura rappresentazione da quelli di struttura, forniscano le informazioni secondo un indice *rectius*, un albero che ne schematizzi il loro contenuto, di conseguenza sarà finalmente possibile effettuare delle ricerche mirate, poiché la "magica" parola chiave potrà

essere cercata solo tra gli elementi di struttura del documento e non necessariamente – come avviene oggi - in tutto il suo contenuto indistintamente; ciò renderà molto più agevole l'individuazione delle informazioni di cui abbiamo bisogno, tenuto conto che soprattutto in campo giuridico è essenziale poter distinguere se un determinato termine indichi l'argomento cui è dedicato il testo – o una sua parte – oppure compaia genericamente in esso.

Il linguaggio XML consente anche una ulteriore possibilità: attraverso l'adozione di un DTD (*Document Type Definition*), la cui composizione è libera seppure impostata secondo precise regole di sintassi informatica dettate dal formato XML, è possibile definire autonomamente una struttura o albero cui tutti i documenti di quel tipo dovranno conformarsi, creando in pratica un indice funzionale al tipo di informazioni che si vuole evidenziare in quell'insieme di testi.

Tra l'altro in questo modo la struttura del documento può essere definita, *rectius* dichiarata, non solo in un *file* esterno contenete il DTD, ma anche al suo interno, producendo così un testo già indicizzato che evidenzia dal resto le parti ritenute rilevanti e dichiarate preventivamente nel DTD.

Un documento in XML, inoltre, non deve necessariamente essere composto da un solo *file*, ma può assemblare al suo interno pezzi diversi chiamati "*entities*", entità.

Le entità permettono di creare dei riferimenti a dati esterni, ad altri documenti, o anche a porzioni di testo , a patto che ci sia una dichiarazione nel DTD in tal senso: esse possono essere sia interne che esterne a seconda di dove fisicamente si trovano i dati richiamati rispetto al documento indicizzato e soprattutto non vincolano ad un formato predefinito, sarà quindi possibile far riferimento a *file* di testo, in txt in pdf o rtf, o *file* di immagine o di suono.

Questo tipo di costruzione di un documento per mezzo di entità ha un grande vantaggio: una volta definitane la struttura nel DTD, si ha la possibilità di riempirlo con contenuti presi anche dall'esterno.

L'applicazione di questo nuovo linguaggio di marcatura dei testi – già adottato per l'Adempimento Unico - ai nostri atti

porterà una piccola rivoluzione sia per quanto riguarda la loro archiviazione che per quello che concerne la loro redazione al fine di ottenere i c.d. "sottoprodotti" con ricadute sulla stessa organizzazione degli studi.

Oggi, infatti, l'esistenza di formati proprietari tra loro diversi e incompatibili a seconda dei vari *word processor* utilizzati per la redazione informatica degli atti, non ne permette la loro archiviazione digitale su basi comuni ed eventualmente centralizzata.

L'adozione, invece, di un formato uniforme che contemporaneamente permetta l'esatta individuazione dei dati più salienti dell'atto - ad esempio che permetta di distinguere se il signor Mario Rossi è intervenuto in qualità di venditore in una compravendita, come semplice procuratore di un Terzo nella costituzione di una società, o se viene semplicemente menzionato come proprietario di un fondo confinante in un atto costitutivo di servitù - è il primo passo per dare il via ad un simile progetto, ovvero alla creazione di una banca dati informatica di tutti i rogiti notarili, che allo stato attuale della normativa potrebbe riguardare solo le copie informatiche degli originali cartacei conservati secondo le regole ordinarie, e che possa garantirne in primo luogo la loro corretta conservazione nel tempo sia dal punto di vista *hardware* – a questo scopo occorrono computer dotati di elevati sistemi di sicurezza tra l'altro posti in locali adeguati ed anch'essi rispondenti a requisiti severi sempre sul fronte della sicurezza – che *software* - poiché il susseguirsi delle diverse versioni di uno stesso programma di videoscrittura per la formazione di atto potrebbe comportare negli anni l'impossibilità di leggerlo nella sua versione informatica qualora non si disponga più di quella determinata *relise* -, ed in secondo luogo consenta la loro interrogazione per effettuare delle ricerche sugli stessi.

La possibilità poi di firmare digitalmente tali copie informatiche degli atti ne garantirebbe l'immutabilità da parte di terzi, ma soprattutto l'autenticità secondo gli stessi parametri che siamo abituati ad applicare a quelle cartacee.

L'adozione di questo standard comune avrà consistenti ricadute anche sulle nostre organizzazioni di studio: infatti, attraverso la creazione di un DTD notarile sarà possibile indicizzare già all'interno del rogito tutti gli elementi – numero di

repertorio e raccolta, data, luogo stipula, notaio rogante, parti, oggetto del contratto, corrispettivo etc. – necessari per compilare correttamente le varie formalità da esso scaturenti ed il repertorio in maniera sempre più automatica e semplificata, in tal modo l'atto notarile, attualmente creato attraverso finestre di composizione o interpretato dai vari *software* sempre e solo allo scopo di produrre in automatico i predetti adempimenti, riacquisterà tutta la sua centralità rispetto ai suoi "sottoprodotti".

Questo di fatto comporterà la progressiva sparizione dai nostri studi dello specialista in repertorio, in volture, quello in note di trascrizione, o in denuncie al Registro Imprese, o quello in registrazione e sempre più chi scriverà l'atto sarà responsabile, informaticamente parlando, di tutto quanto da esso scaturisce senza dover chiedere l'intervento di un altro soggetto che compili ulteriori modelli o adempimenti anche se di tipo informatico, in pratica la nostra organizzazione sarà meno settorializzata e quindi più orizzontale che non verticale.

Ma questo sistema, a parere di chi scrive, ha anche un ulteriore grande vantaggio: se attraverso il DTD e quindi attraverso l'indicizzazione delle informazioni essenziali, il formato XML fornisce alcuni dati dell'atto ritenuti rilevanti soprattutto a fini fiscali dall'Amministrazione Finanziaria – si pensi ai codici fiscali delle parti, ai dati catastali dell'immobile, al prezzo del bene negoziato – l'adozione di questo formato restituisce al giurista la possibilità, nel momento in cui lo redige, proprio attraverso le entità, di riempire a piacimento il suo contenuto anche con riferimenti esterni ad esso – ad esempio il testo di una procura già conservata nei rogiti del notaio rogante e quindi non allegata a quello specifico documento può così diventare fruibile anche nel suo testo esteso e non come mero riferimento -, e, nel momento in cui lo consulta, di avere a disposizione l'intero complesso delle pattuizioni, non necessariamente ridotte al loro "scheletro" funzionale essenzialmente per la redazione degli adempimenti e non certamente alla comprensione dell'intero contratto, e nella loro sistemazione originaria; ampliando ciò che abbiamo detto a proposito delle *entities* ed esemplificato con la procura conservata dal notaio rogante ma non allegata al documento, si può immaginare un sistema che laddove nell'atto sia citato un qualsiasi

altro rogito – ad esempio l'atto di provenienza in una vendita o una convenzione urbanistica rispetto alla vendita di area oggetto di lottizzazione – renda disponibile immediatamente questi testi e non il solo riferimento ad essi; la possibilità poi di utilizzare non solo file di testo ma anche di suono e di immagine apre ulteriormente il campo a scenari che oggi possiamo solo immaginare.

A questo punto il notaio, riappropriandosi della direzione della redazione dell'atto, si sarà automaticamente riappropriato anche dei suoi "sottoprodotti" e soprattutto potrà modellarne il contenuto sulle esigenze delle parti usando le nuove potenzialità offerte dall'informatica finalmente come mezzo e non come fine.

LA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

La gestione dei documenti informatici comporta l'esplorazione di un territorio in buona parte ignoto, che è quello della loro conservazione e archiviazione in sicurezza.

Non esistono infatti in Italia, con l'unica rilevante eccezione del Registro delle Imprese (che tuttavia si fonda su una norma speciale), esempi concreti di archivi di documenti informatici, aventi valore legale pari a quello dei documenti cartacei.

Anche a livello internazionale non constano particolari esempi (almeno nei paesi di *civil law*) di documenti informatici, o di archivi informatici di documenti aventi pieno valore legale. Costituisce una parziale eccezione l'Austria, paese nel quale i notai sono per legge tenuti, dal 1° gennaio 2000, a conservare con modalità prestabilite, copie in formato immagine dei propri atti, per le quali tuttavia non è al momento riconosciuta né prevista alcuna utilizzabilità.

Ciò è imputabile a fattori normativi, organizzativi e culturali.

Gli ostacoli normativi, o in genere attinenti la sfera giuridica, consistono nella imprecisione e lacunosità della normativa, e nella mancanza di precedenti giurisprudenziali, e quindi di casistica per i fenomeni patologici. Ciò rende evidentemente più rischiosa la pratica della conservazione del documento elettronico.

Le norme sulla conservazione dei documenti digitali sinora emanate, ed in particolare quelle sull'archiviazione ottica (da ultimo deliberazione AIPA n. 42 del 13 dicembre 2001, in G.U. 21 dicembre 2001 n. 296), non hanno infatti costituito una base solida per la realizzazione di tali archivi.

A parte le problematiche relative alla conservazione in sicurezza nel tempo, e quindi all'aggiornamento delle tecnologiche necessarie per preservarne l'integrità, per le quali si rinvia alla

parte dedicata alla marcatura temporale, va rilevata una oggettiva lacunosità della normativa in materia.

L'appiglio normativo su cui tali norme si fondano infatti è costituito dai primi due commi dell'articolo 6 del T.U. 445/2000, che consente a privati e pubbliche amministrazioni la sostituzione degli originali con copie fotografiche o con altro mezzo idoneo a garantire la conformità all'originale. I limiti di tale facoltà, le modalità tecniche e di autenticazione dovranno essere stabilite con un Decreto del Presidente del Consiglio dei Ministri, che non è stato ancora emanato. La situazione può quindi riassumersi come segue.

La norma dell'art. 6, primo comma, T.U. è formulata in modo tale da riferirsi alla sola sostituzione di originali cartacei con documenti informatici; non prende in esame espressamente l'ipotesi del documento informatico sin dall'origine.

Non è stato in ogni caso emanato il Decreto del Presidente del Consiglio dei Ministri che stabilisce i settori di applicazione di tale norma e le modalità.

E' stata emanata la deliberazione AIPA 42/2001 sull'archiviazione ottica che stabilisce modalità tecniche vincolanti per il caso di archiviazione ottica dei documenti, ma non affronta il problema dell'ambito applicativo della norma del primo comma dell'articolo 6 T.U.. Quest'ultima deliberazione, in verità, fornisce un appiglio interpretativo. Essa infatti prevede sia l'ipotesi dell'archivio di copie ottiche di documenti il cui formato nativo era cartaceo, sia l'ipotesi di archiviazione ottica di documenti originariamente informatici. Ciò sembra basato sul presupposto dell'inutilità di una norma apposita per consentire l'archiviazione ottica di documenti informatici. Tale presupposto però sembra tutt'altro che pacifico e generale: esistono infatti regole, in materia di conservazione del documento cartaceo che, se non espressamente derogate per il documento informatico, rischiano di renderne impossibile la pratica utilizzazione. E' il caso, per esempio, dell'atto notarile informatico che, indiscutibilmente, deve essere conservato per un tempo tendenzialmente illimitato come

l'atto formato su carta: ma se pure l'atto notarile informatico fosse ammissibile in astratto sulla base della normativa vigente (ed è discusso), la mancanza di una normativa che sostituisca le norme speciali sulla conservazione (tra le quali spicca l'articolo 72 della Legge notarile) previste dall'ordinamento del notariato e degli archivi notarili ne impedisce la pratica applicazione.

Esistono tuttavia documenti che possono essere conservati indipendentemente da modifiche normative, e sui quali occorre anzi sin da oggi interrogarsi: è il caso delle copie conformi degli atti notarili, utilizzate per gli adempimenti diretti alla Pubblica Amministrazione, o di documenti da quest'ultima provenienti, relativi ad adempimenti relativi alla pubblicità immobiliare o commerciale, o di carattere fiscale. La conservazione di tali documenti è necessaria esattamente come quella dei loro omologhi cartacei, ma presenta diverse problematiche.

Nella prima fase applicativa della firma digitale, la carenza di strumenti di conservazione definitiva non dovrebbe porre soverchi problemi pratici. Per quanto concerne le copie digitali inviate ai Pubblici Uffici la loro conservazione avverrà (come nell'esperienza cartacea) a cura delle competenti amministrazioni.

Il problema può semmai porsi per le ricevute e le altre comunicazioni provviste di firma digitale che pervengano al notaio. In linea di principio nulla impedisce che il notaio provveda sin d'ora alla loro periodica marcatura temporale, onde assicurarne a tempo indefinito il massimo grado di efficacia probatoria. Per i dati affluiti a pubblici registri la prova dell'avvenuta esecuzione delle formalità è però assicurata, sul lungo periodo, anche dal registro stesso in forma obiettiva e con ragionevole grado di sicurezza, onde l'esigenza di una conservazione a norma da parte del notaio appare non particolarmente pressante.

Sono, però, da una parte la visione prospettica della inevitabile migrazione dei pubblici archivi verso sistemi totalmente informatizzati, dall'altra l'inadeguatezza delle soluzioni sin qui disponibili, da cui deriva la carenza di esperienze rilevanti, a rendere l'argomento di interesse strategico il notariato.

La situazione di oggettiva difficoltà si rileva anche dall'evoluzione della normativa, che in precedenza tendeva ad imporre soluzioni obbligate dal punto di vista tecnico e organizzativo, ed è oggi sicuramente più liberale. Infatti la deliberazione AIPA 42/2001, modificando la precedente (24/1998) in senso meno vincolante, consente, sotto la responsabilità di chi effettua la conservazione, l'utilizzazione di ogni modalità che si ritenga sicura. Sono infatti dettate solo regole procedurali, finalizzate soprattutto alla definizione dei soggetti responsabili, senza vincoli tecnici.

Questo costituisce evidentemente allo stesso tempo un'occasione ed una responsabilità per chi si ponga come gestore di tali archivi.

Il Notariato, tradizionale custode di documenti, ha la competenza per impostare tali processi in modo corretto e sicuro, individuando i punti critici in cui si concentrano rischi e responsabilità.

Occorre pertanto impostare, seguire e utilizzare applicazioni di conservazione di documenti informatici con pieno valore legale. E' questa la prossima sfida dopo la firma digitale.

LE PROSPETTIVE DI FUTURE APPLICAZIONI

Ecco quindi la firma digitale.

Della firma digitale dei notai abbiamo cercato di dar conto in questo lavoro parlando di storia, ragioni, modalità d'uso, responsabilità. Abbiamo anche cercato di far comprendere come si inserirà nel nostro quotidiano.

La domanda successiva (o forse precedente, almeno per chi ha dovuto operare la scelta della Autorità di Certificazione) è: quali usi ne faremo?

Per i notai, che si pongono per loro natura quale tramite tra i privati, e tra questi e la Pubblica Amministrazione, la risposta è strettamente connessa al grado di diffusione (utilizzazione) delle applicazioni che utilizzano la firma digitale, da parte del settore pubblico e degli utenti privati.

Non poco influirà anche l'evoluzione normativa, sicuramente tumultuosa anche nei prossimi anni. L'atto notarile informatico richiede di sicuro qualche intervento, in parte già previsto.

Ma andiamo al concreto. Bisogna tenere conto che ciascuna utilizzazione della firma digitale per attività precedentemente svolta in modo tradizionale comporta lo sviluppo di un applicativo informatico specifico. E' anche necessario che tali applicativi siano pienamente integrati con i *software* degli studi notarili, e per far ciò il notariato deve continuare a partecipare alla loro elaborazione, come è successo negli ultimi anni, e non subirli semplicemente, come è successo in un passato meno recente. Molto spesso, inoltre, l'applicazione telematica, per essere funzionale, rende necessario il ricorso a modifiche normative.

Due applicazioni su tutte sono pronte per l'utilizzo (cominceremo ad utilizzare):

- La pubblicità commerciale, per la quale le Camere di Commercio sono pronte alla ricezione, ma mancava la certificazione delle funzioni notarili e manca ancora qualche tassello normativo (cfr. la convenzione C.N.N.-Unioncamere-Infocamere-Notartel dell'ottobre 2001, reperibile sulla R.U.N.) ed organizzativo (la restituzione di documenti firmati da parte del Registro Imprese, le modalità di apposizione delle firme degli amministratori di società in talune ipotesi); ma si tratta di particolari da sistemare in corso d'opera.

  Con la firma digitale del Notariato può partire il primo adempimento totalmente telematico nella Pubblica Amministrazione italiana.

- La seconda fase dell'Adempimento Unico: la normativa sull'Adempimento Unico prevede infatti un sistema misto telematico-cartaceo fino al pieno utilizzo della firma digitale, allo scopo di salvaguardare i principi in materia di pubblicità immobiliare. Dopo basterà la trasmissione di documenti firmati digitalmente, senza alcun deposito di documenti cartacei. Il Notariato è pronto a questa seconda fase. Il sistema della pubblicità immobiliare non ancora, per due ordini di ragioni: perché non è in grado di restituire documenti (ricevute, dupli) firmati a loro volta digitalmente, e perché non ha un sistema di archiviazione dei documenti informatici ovvero dei titoli in base ai quali attuare la pubblicità. L'obiettivo è la partecipazione attiva del notariato alla creazione e gestione di questi archivi, e della normativa che li riguarderà, essendo necessario un intervento sul sistema civilistico.

  Su richiesta dell'Amministrazione Finanziaria, sono già aperti tavoli di lavoro.

Vi sono poi alcune applicazioni apparentemente minori, ma che incidono tanto sul quotidiano e possono essere altrettanti cavalli di Troia per incominciare l'interazione in telematico con alcune pubbliche amministrazioni.

Ad esempio la trasmissione telematica degli elenchi alla questura relativi ad atti di cessione di aziende o di terreni, e l'eventuale trasmissione per conto dei cedenti, delle comunicazioni di cessione fabbricato: vi sono stati, e vi sono, contatti con il Ministero degli Interni, per lo sviluppo delle applicazioni; sembrano però necessari alcuni interventi normativi per rendere possibile la comunicazione non alle autorità locali di P.S., ma ad un sistema informativo centralizzato, e per consentire la comunicazione delle cessioni di fabbricati direttamente da parte dei notai in luogo dei cedenti.

Anche la trasmissione al Comune di atti relativi alla cessione di terreni inferiori a 10.000 mq., o più in generale, di tutti gli atti relativi ad immobili, rientra tra gli obiettivi prossimi; è infatti attivo un tavolo di lavoro con ANCI, ANCITEL, Ministero dell'Economia e Finanze; vi sono convenzioni pilota con i comuni di Palermo, Milano, Firenze (con interessanti contropartite quali l'accesso gratuito in via telematica ai registri informatici di stato civile). L'interesse dei Comuni è grande per la possibilità di aggiornamento automatico degli archivi ai fini ICI. L'interesse del notariato è quello di snellire attività dovute, di ottenere utili informazioni (ad es. atti di matrimonio con annotazioni) e di fornire ulteriori utilità alla P.A. ed ai cittadini (eliminazione della denuncia ICI) senza ulteriori aggravi (si pensa infatti ad una trasmissione in automatico estraendo i dati dal modello unico).

Questa applicazione potrebbe aprire la strada alla comunicazione in via telematica delle convenzioni matrimoniali per l'annotazione nei registri di stato civile, applicazione questa che richiederebbe in realtà solo posta elettronica, firma digitale e marcatura temporale, ma che necessita di una identica struttura presso i Comuni per la trasmissione delle ricevute. Si tratta di operare perché ciò avvenga, utilizzando le possibilità di esperienze pilota.

Le questioni di maggior rilievo riguardano però l'informatizzazione dell'intero processo dell'attività notarile.

Per fare ciò occorre innanzitutto che vi siano una serie di programmi interoperabili, e quindi il superamento definitivo delle

difficoltà di interazione tra i vari *software* utilizzati (non è tanto lontano il tempo in cui il cambiamento di *software* di studio comportava per molti la perdita di dati costituenti anni di lavoro).

Sono due i settori di azione:

- il primo è l'archiviazione di atti e documenti con valore giuridico: se ne è parlato specificamente in questo lavoro, e si sono spiegate le difficoltà normative e tecniche che ancora sussistono (per chiunque); è fondamentale che anche in questo settore il notariato si presenti come attore del processo, prima che come utente; in ciò sta la difesa della funzione, in un settore che peraltro costituisce prerogativa storica del notariato;
- il secondo è l'elaborazione di *software* o di regole per la loro elaborazione che costituiscano patrimonio comune dei notai e base per l'interazione con altri soggetti e la Pubblica Amministrazione.

Occorre qualche esemplificazione.

Per quanto riguarda i temi dell'archiviazione e della conservazione dei documenti informatici l'intervento deve essere di studio e sviluppo applicativo, da una parte, di interpretazione normativa, e possibilmente partecipazione alle indispensabili evoluzioni tecnico-normative, dall'altra. Ma questo è un discorso necessariamente fluttuante ed incompiuto, che non è possibile approfondire qui.

Più importante è definire gli scopi di tale impegno, che non potrà essere inferiore a quello profuso per la firma digitale:

1. in primo luogo la partecipazione al processo di creazione degli archivi pubblici informatici, con la possibilità di divenire compartecipi della loro gestione, od almeno arbitri della immissione di dati negli stessi con l'eliminazione di controlli anacronistici quali quelli dei conservatori;
2. in secondo luogo la gestione centralizzata da parte del notariato di un archivio degli atti notarili (per ora le copie),

e della relativa documentazione; un simile archivio, organizzato con corretti criteri di gestione dei dati, può portare nel tempo alla modifica di alcune modalità di interazione con la P.A. consentendo l'accesso ad archivi gestiti dal notariato, con valore legale, in luogo della trasmissione di atti a più archivi pubblici; inoltre il possesso e l'organizzazione ed una seria e approfondita rilevazione statistica dei dati riguardanti l'attività notarile può costituire, nella società dell'informazione, un patrimonio che oggi è ancora difficile quantificare (si pensi all'osservatorio privilegiato del settore immobiliare, ben migliore di quelli attualmente disponibili).

L'elaborazione di *software* o di regole comuni per *software*, costituisce poi il proseguimento del lavoro svolto da una parte con le case produttrici di *software* notarili, dall'altra per lo sviluppo dell'Adempimento Unico con il linguaggio XML.

Si sta procedendo, a cura della Commissione Informatica e di Notartel, allo sviluppo di un tracciato minimo comune da adottare per l'attività notarile da parte di tutte le case *software*, per realizzare una piena interoperabilità tra i vari *software*.

Da tale tracciato sarà possibile trarre elementi per la realizzazione del repertorio informatico, per il quale si attende, da parte del Ministero della Giustizia, l'emanazione delle regole per la tenuta informatica ai sensi dell'articolo 13 del D.P.R. 445/2000. La presenza di un principio di applicazione per il repertorio, di matrice notarile, potrà essere una base per l'emanazione di tali regole, e delle regole tutte per l'interazione telematica con il sistema degli archivi notarili (compreso il Registro Generale dei Testamenti).

Il tracciato potrà essere poi la base per applicazioni di maggiore respiro, a cominciare dall'integrazione diretta con gli altri programmi per gli adempimenti disponibili (Modello Unico, Fe.Dra., per il Registro Imprese) da utilizzarsi nel tempo con modalità ASP (*Application Service Provider*) vale a dire mediante utilizzazione di programmi residenti su server centrali da parte di utenti diffusi sul territorio. Proprio l'utilizzo di *software* in modalità ASP, resi oggi convenienti da connessioni telematiche veloci ed economiche, rappresenterà la più rilevante innovazione in tutti i sistemi di automazione ed organizzazione dello studio, spostando

l'accento dall'attuale impiego di risorse localizzate presso lo studio a nuove risorse distribuite su elaboratori geograficamente distanti e sfruttati in modo condiviso da più utenti contemporaneamente.

Manca ancora un tassello fondamentale al quadro del probabile futuro. L'atto notarile informatico in senso proprio. Sappiamo tutti che la scrittura privata autenticata è espressamente prevista (art. 24 D.P.R. 445/2000). Vi sono dubbi sull'ammissibilità dell'atto notarile pubblico, e soprattutto mancano regole specifiche per la sua conservazione.

Anche in questo caso quindi si tratta di attuare ciò che è espressamente consentito (non vi sono dubbi per esempio sulla possibilità di un consenso a cancellazione ipotecaria per scrittura privata autenticata, salve le già dette difficoltà per operare le formalità ipotecarie), e di operare per i necessari interventi.

Ed infine le nuove possibilità. Il documento informatico, il commercio elettronico, richiedono certezze, che non sono solo sicurezza delle transazioni e dei pagamenti, ma anche della solidità giuridica delle operazioni; questo comporta una serie di nuove domande anche per il notariato (basti pensare alla problematica delle copie delle pagine web, anche ai fini della paternità delle stesse) e soprattutto la possibilità di nuove prospettive e occasioni. Sarà senz'altro anche compito del notariato rispondere a queste richieste e rendersi parte attiva di tale sviluppo, anche oltre la pubblica funzione quale tradizionalmente riconosciuta, ma nella continuità della funzione sociale.