

CONSIGLIO NAZIONALE DEL NOTARIATO

Commissione Informatica

Il fattore tempo: la marcatura temporale

Firme Elettroniche - Questioni ed esperienze di diritto privato , Milano, 2003

1. Premesse

Con riferimento ai documenti informatici ed alle sottoscrizioni elettroniche, il fattore temporale e della datazione assume rilevanza sotto due profili concettualmente distinti ma tecnicamente e giuridicamente connessi.

In primo luogo, rileva la data del documento intesa come collocazione temporale del momento formativo del documento stesso, con un'efficacia eventualmente opponibile ai terzi (la c.d. "data certa"). In caso di documenti provenienti da un pubblico ufficiale, costituirà "data certa", opponibile *erga omnes*, l'attestazione operata dal pubblico ufficiale stesso e contenuta nel documento, non contrastabile se non con la querela di falso.

In secondo luogo, la datazione del documento informatico, ed in particolare della sottoscrizione informatica, rileva quale strumento tecnico, complementare e funzionale al perfezionamento di un'efficacia probatoria stabile e duratura del documento informatico stesso, risolvendo i limiti connaturati alla "scadenza" delle firme elettroniche, secondo quanto si chiarirà appresso.

Evidentemente, la datazione finalizzata alla nuova esigenza della stabilità probatoria del documento informatico non potrà non ripercuotersi sulla datazione intesa nel senso tradizionale, quale data efficace tra le parti oppure opponibile ai terzi ed eventualmente attestata da un pubblico ufficiale.

2. La data certa

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 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 efficacemente utilizzabile per la stragrande maggioranza delle applicazioni aventi rilevanza giuridica **(1)**.

Nel tradizionale sistema di documentazione cartacea, l'attribuzione della data certa (efficace nei confronti dei terzi e non solo tra le parti) 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 (in un momento successivo alla sua formazione) di un documento in un pubblico registro (ad es. per la storica funzione degli uffici del registro - ora delle entrate). In mancanza di tale attestazione di carattere pubblicistico (autenticazione del pubblico ufficiale o registrazione), una "data certa" efficace nei confronti dei terzi è riscontrabile in presenza di "un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento", tra cui, l'art. 2704 c.c. indica, non in modo esclusivo, il "giorno della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta o dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici". L'art. 2704 c.c. indica una serie di ipotesi specifiche, ed una clausola generale che rendono "certa" (i.e. opponibile) la datazione nei confronti dei terzi. La semplice dichiarazione in ordine alla data contenuta in una scrittura privata non fa prova nei confronti dei terzi, ma solo tra le parti, nei limiti e con gli effetti delle altre dichiarazioni del documento.

Per il documento informatico, sottoscritto con firma elettronica, si pone il problema se la data certa possa essere desunta secondo i metodi previsti dall'art. 2704, comma 1, c.c. Quest'ultimo non sembra applicabile direttamente alla documentazione informatica in quanto manca un rinvio espresso a tale norma da parte delle disposizioni sul documento informatico, inoltre, il documento informatico con firma elettronica non è una scrittura privata, anche se ne possiede un'efficacia probatoria simile o addirittura superiore (art. 10, d.p.r. n. 445/2000, come modificato dal d.lgs. n. 10/2002).

Tuttavia, un'applicazione analogica dell'art. 2704, comma 1, c.c. alla documentazione informatica sembra possibile, in ragione della identità di *ratio* e similitudine di fattispecie. Pertanto, la data certa di un documento informatico potrebbe essere acquisita mediante le seguenti presunzioni poste dall'art. 2704, comma 1, c.c.: *a)* autenticazione della firma digitale (ex art. 24, d.p.r. n. 445/2000); *b)* registrazione fiscale (art. 18, d.p.r. n. 131/1986); *c)* giorno in cui il contenuto del documento informatico (con firma elettronica) è riprodotto in atti

pubblici; d) altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento **(2)**.

Si osserva che, nel caso di autenticazione, la data certa è opponibile fino a quando è valida la firma digitale del pubblico ufficiale autenticante, la quale può a suo volta essere garantita da una validazione temporale, secondo il sistema che verrà appresso esaminato, o dagli stessi sistemi previsti dall'art. 2704 c.c. Invece, nei casi di riproduzione del documento informatico in atto pubblico (cartaceo), la data certa è opponibile senza limiti temporali.

Pare difficilmente applicabile l'ipotesi "della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta", prevista sempre dall'art. 2704 c.c. Infatti, dato che l'apposizione della firma elettronica è riconducibile all'utilizzo di un mezzo tecnico, non è escluso che esso venga utilizzato anche dopo la morte del suo titolare da parte di persona diversa.

Quando l'apposizione di una firma elettronica è accompagnata da una timbratura marca ai sensi del d.p.r. n. 445/2000, si restringono, ma non si escludono del tutto, i margini operativi per l'applicazione analogica dell'art. 2704, comma 1, c.c., in quanto la data certa risulterebbe già dalla stessa marca temporale apposta alla firma **(3)**.

3. La validazione temporale dei documenti informatici

Il sistema italiano dell'infrastruttura a chiave pubblica, ponendosi l'ambizioso obiettivo di regolare il documento informatico quale sostitutivo del documento cartaceo nei rapporti con la pubblica amministrazione e tra i privati, non poteva ovviamente trascurare l'aspetto della attribuzione di "data certa" e, quindi, basandosi sulla tecnologia oggi disponibile e sui documenti internazionali in materia, ha offerto agli operatori un sistema sicuro, rapido, efficace ed economico per raggiungere anche questo importante risultato.

La marca temporale (*digital time stamp*) attesta l'esistenza di un documento informatico (o meglio di un *file* informatico) ad una determinata data ed ora ("validazione temporale"). 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, lettera 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 **(4)**.

Potrà essere oggetto di validazione temporale qualunque *file* informatico e, pertanto, non solo testi, ma anche immagini, suoni, filmati, *software*, ecc., con il solo limite delle informazioni digitalizzabili **(5)**.

Dal punto di vista tecnico, una marca temporale (similmente ad una firma digitale) a sua volta consiste in un piccolo *file* informatico **(6)** (un pacchetto di informazione digitale), contraddistinto da un titolo identificativo, che può essere conservato unitamente al documento

cui si riferisce (ad es. nella stessa cartella informatica) o anche in modo separato, dato che comunque è ad esso collegato univocamente **(7)**.

Elementi essenziali del contenuto di una marca temporale sono l'impronta identificativa del *file* cui si riferisce, la data ed ora, il tutto sottoscritto con la firma digitale del certificatore. In quanto si tratta di un'attestazione, ancorché automatica, ma sempre un'attestazione, 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. Il servizio è svolto, normalmente dallo stesso soggetto che certifica le chiavi pubbliche **(8)** e, quindi, nel sistema italiano, un soggetto privato, non necessariamente partecipa di pubbliche funzioni **(9)**.

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 normalmente in via telematica mediante una connessione tra l'elaboratore dell'utente e quello del certificatore **(10)**. Attraverso apposito programma, selezionato il documento su cui apporre la marcatura temporale, si genera apposita richiesta di validazione temporale **(11)**, la quale viene trasmessa al servizio di marcatura temporale che in automatico (senza diretto intervento umano) appone la marca temporale (data ed ora) **(12)**, la sottoscrive con firma digitale **(13)** e restituisce il relativo *file* all'utente **(14)**.

Per essere più precisi, in realtà non viene normalmente 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*) **(15)**. 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 **(16)**.

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 **(17)**.

Come per la verifica delle firme digitali, anche per la verifica della marca temporale 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).

4. La validazione temporale delle firme elettroniche

La datazione del documento informatico, ed in particolare della sottoscrizione informatica, è fondamentale per il mantenimento della sua efficacia probatoria, in ragione dei limiti connaturati al sistema delle firme elettroniche. Questo problema si pone in modo autonomo rispetto alla specifica esigenza di collocazione temporale del documento che, in molti casi, potrebbe anche non sussistere, oppure, comunque, risultare da una attestazione del pubblico ufficiale autore del documento.

Mentre una sottoscrizione su carta, con il trascorrere del tempo, mantiene in via di principio lo stesso valore probatorio **(18)**, diversamente una firma digitale, invece, è fin dall'inizio destinata a perdere sicurezza ed efficacia probatoria in breve tempo a seguito della sua necessaria scadenza (predeterminata) o per eventuale revoca o sospensione (anteriore alla scadenza).

Il termine di scadenza di una chiave di firma, infatti, non può essere superiore a tre anni (art. 22, comma 1, lettera 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 ed il maggior tempo a disposizione per i truffatori, consentirebbe attacchi e frodi sui codici delle firme già apposte, potendosi perpetrare falsi non riconoscibili. Tuttavia, anche prima della scadenza, la chiave di firma può essere compromessa (ad es. smarrita o sottratta) e, quindi, revocata o sospesa.

Innanzitutto, in tutti questi casi, l'effetto della cessazione di validità della chiave (e del relativo certificato) si ripercuote direttamente sulle firme digitali apposte successivamente, per cui è espressamente stabilito che "L'apposizione ad un documento informatico di una firma elettronica basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione" (nuovo art. 23, comma 3, d.p.r. n. 445/2000, come modificato dal d.p.r. n. 137/2003) **(19)**.

La perdita di validità della chiave e del certificato non investe però solo le firme apposte successivamente, come appare immediatamente logico, ma travolge anche le firme apposte anteriormente, con un meccanismo e delle conseguenze che sono estranee al tradizionale modo di intendere la documentazione cartacea e possono apparire sconcertanti a chi non abbia ben chiaro l'attuale meccanismo tecnico della sottoscrizione elettronica basata sulla cifratura asimmetrica dei dati ed i suoi connaturati limiti **(20)**.

Una firma elettronica, infatti, di per sé non contiene alcuna connotazione di carattere temporale opponibile **(21)** e, pertanto, una firma apposta dopo la scadenza (o revoca o sospensione) della chiave non sarebbe tecnicamente riconoscibile e distinguibile da una firma apposta validamente in un momento anteriore. Pertanto, a seguito della cessazione di validità

del certificato, per tutte le relative firme, indistintamente, scatta l'applicazione della disposizione prima citata dell'art. 23, comma 3, d.p.r. n. 445/2000. Inoltre, il nuovo art. 29 *quater* del d.p.r. n. 445/2000 (come introdotto dal recente d.p.r. n. 137/2003), prevede che "La firma elettronica, basata su un certificato qualificato scaduto, revocato o sospeso non costituisce valida sottoscrizione", senza distinguere tra firme apposte prima o dopo la perdita di validità del relativo certificato.

Per fare salva l'efficacia giuridica delle firme digitali apposte anteriormente alla cessazione di validità del relativo certificato, e di conseguenza mantenere l'efficacia probatoria del relativo documento, occorre che la firma in considerazione **(22)** sia stata oggetto di validazione temporale, in un momento anteriore rispetto alla scadenza o revoca (o al di fuori del periodo di sospensione) del relativo certificato **(23)**. In altri termini, occorre che la firma sia stata oggetto di una marcatura temporale apposta durante il periodo di validità (*operational period*) del relativo certificato **(24)**.

In applicazione di tali principi, è stabilito espressamente dalle regole tecniche 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, d.p.c.m. 8 febbraio 1999); 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, d.p.c.m. 8 febbraio 1999). 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.

Comunque, sembra che la marcatura temporale non rappresenti l'unico sistema utilizzabile agli effetti del mantenimento dell'efficacia probatoria del documento firmato. L'anteriorità dell'apposizione della firma elettronica rispetto alla scadenza o revoca, o la sua estraneità rispetto al periodo di sospensione, potranno essere provate anche con altri sistemi diversi dalla marcatura temporale.

In primo luogo, costituisce senza dubbio prova della collocazione temporale della firma elettronica, l'autenticazione notarile ai sensi dell'art. 24 d.p.r. n. 445/2000, dato che il notaio ha l'obbligo di accertare la validità della chiave utilizzata per apporre la firma da autenticare **(25)**. Pertanto, l'efficacia probatoria della firma autenticata da notaio non viene meno a seguito della successiva scadenza, revoca o sospensione del relativo certificato della parte autenticata. Tuttavia, questo vale fintantoché resti valida la firma digitale del notaio autenticante, la quale è allo stesso modo soggetta a scadenza, revoca e sospensione con

identiche conseguenze sulla sua efficacia. **(26)**. La firma digitale del notaio autenticante dovrebbe essere garantita da idonea marcatura temporale, che la preservi, unitamente alla firma oggetto di autenticazione ed al relativo documento firmato.

Si pone il problema del rapporto tra la data attestata dal pubblico ufficiale nella formula dell'autentica e la data risultante dalla marcatura temporale, quando tra loro non corrispondenti **(27)**. Nel caso in cui la marca temporale indica una data successiva a quella attestata dal notaio, sussiste una perfetta compatibilità tra le due risultanze, con una prevalenza della seconda: la marca temporale, infatti può essere anche apposta in un momento successivo alla firma del notaio **(28)**, la cui attestazione prova la data di formazione del documento **(29)**. Nel caso in cui, invece, la marca temporale indichi una data **(30)** anteriore rispetto a quella attestata dal notaio, si determina un contrasto incompatibile tra le due risultanze. In quest'ultima ipotesi, ci si trova inevitabilmente di fronte ad un errore od un falso, da attribuire ad una delle due risultanze che non possono coesistere in modo compatibile. Stabilire quale delle due risultanze prevale è questione di fatto, rimessa all'apprezzamento probatorio.

Mancando anche un'autenticazione notarile, oltre che mancando anche una marca temporale, la data della firma elettronica, ai fini del mantenimento della sua efficacia nel tempo, potrebbe essere dimostrata attraverso ogni mezzo, tra cui la riproduzione del documento in atto pubblico, oppure la sua conservazione presso un pubblico registro. Naturalmente, dopo l'autenticazione notarile, il sistema della marcatura temporale è senza dubbio quello di più semplice utilizzo e che garantisce un risultato sicuro. Tuttavia, la prova del fatto che la firma è stata apposta prima della perdita di validità (per scadenza, revoca o sospensione) della chiave resta una prova libera, che potrebbe essere fornita in qualunque modo (testimonianze, altri documenti, giuramento, ecc.), con l'onere a carico di chi produce il documento.

La validazione temporale dei documenti informatici rappresenta, dunque, uno strumento essenziale per la conservazione e gestione degli archivi di documenti informatici sottoscritti con firma elettronica. Per il mantenimento dell'efficacia probatoria propria dei documenti informatici sottoscritti con firma elettronica e, quindi, per consentire anche a distanza di anni la loro verifica, 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, come si chiarirà appresso **(31)**. Il risultato essenziale da raggiungere consiste nel consentire che una firma elettronica possenga la stessa efficacia, in modo univoco e certo, valida nel tempo, indipendentemente dal momento in cui venga effettuata la sua verifica, allo stesso modo come si è sempre intesa la verifica della sottoscrizione cartacea.

Se perde validità la firma elettronica, a causa della perdita di validità del relativo certificato, viene meno l'efficacia di piena prova attribuita al documento dall'art. 10, comma 3, d.p.r. n. 445/2000 (come modificato dal d.lgs. n. 10/2002) ed il documento degrada

all'efficacia *ex art.* 2712 c.c. (comma 1) **(32)**. Se perde validità la firma digitale del pubblico ufficiale autenticante *ex art.* 24 d.p.r. n. 445/2000, il documento degrada alla efficacia *ex art.* 10, comma 3, d.p.r. n. 445/2000 (come modificato dal d.lgs. n. 10/2002), purché siano ancora valide le firme digitali delle parti.

La perdita di efficacia della firma non inficia però la forma dell'atto, quale attività storicamente compiuta. Infatti, ciò che viene meno è solo la firma elettronica quale risultato dell'attività di documentazione, ma resta il fatto avvenuto del compimento dell'atto secondo la sua forma originaria. La perdita di validità della firma potrebbe intendersi come distruzione del documento.

La "distruzione non fa venire meno la dichiarazione che nel documento era stata rappresentata. Ciò che viene meno è infatti la rappresentazione materiale della dichiarazione, ma non l'esistenza della dichiarazione" **(33)**. Se la forma è richiesta *ad substantiam*, storicamente ciò non toglie che tale forma sia stata a suo tempo integrata. Il problema diventa allora quello della forma per la prova (forma *ad probationem*), o meglio la prova della forma. Tenendo conto di ciò, la legge ammette la prova per testimoni "quando il contraente ha senza sua colpa perduto il documento che gli forniva la prova" (art. 2724, n. 3, c.c.) e disciplina la ricostruzione di documenti andati distrutti (ad es. r.d.l. 15 novembre 1925, n. 2071).

Per tutti questi motivi, in pratica, il notaio (o altro soggetto) che riceve in via telematica un documento informatico sottoscritto con firma elettronica, potrà provvedere egli stesso all'apposizione della marcatura temporale, servendosi, tra gli altri, del servizio offerto dal CNN ente quale certificatore (o da altro 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 dimostrarne la tempestiva esecuzione, mettendosi al riparo dalla naturale scadenza e da eventuali revoche delle chiavi **(34)**. Documenti privi di firma elettroniche 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.

In definitiva, la marcatura temporale, come si è detto, 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 **(35)**; può essere richiesta senza formalità da chiunque, autore del documento o estraneo ad esso **(36)**; 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.

Secondo la vigente normativa in materia, non è stabilito che le firme elettroniche debbano essere obbligatoriamente sottoposte a marcatura temporale, né si prevede come obbligatoria la marcatura temporale della firma digitale del notaio autenticante ex art. 24 del 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 ed eventuali 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).

5. La rinnovazione della validazione temporale

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 dei relativi certificati, in modo del tutto analogo alle firme digitali, a seguito della cessazione di validità dei rispettivi certificati **(37)**.

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, lettera 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 **(38)**, riproponendosi la stessa situazione di una firma elettronica priva di marca temporale.

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 dell'ultima scadenza della marca temporale **(39)**. 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, d.p.c.m. 8 febbraio 1999).

Naturalmente, rinnovazione della marca temporale non significa anche 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, inteso quale mezzo di prova e non ripropone l'atto come fatto storicamente compiuto.

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, proprio 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

(40). 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 breve tempo, potrebbe essere apposta all'archivio degli atti notarili e dei documenti di un intero anno **(41)**. 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), in modo trasparente per l'utente.

Anche le firme digitali dei notai (ad es. in sede di autenticazione o di rilascio di copie), ancorché non espressamente richiesto obbligatoriamente, dovrebbero essere oggetto di marcatura temporale, periodicamente rinnovata, per garantire il mantenimento della loro efficacia probatoria oltre la naturale scadenza (o eventuale revoca o sospensione), secondo lo stesso meccanismo prima esposto. Naturalmente, anche a seguito della rinnovazione della marca temporale, resta fermo che la data del documento è quella attestata dal pubblico ufficiale e non quella risultante dalla marca temporale, secondo il rapporto di compatibilità prima esaminato.

Non si pone un problema di rinnovazione di marche temporali quando la data del documento può essere provata attraverso un sistema diverso dalla marcatura temporale, secondo quanto prima esposto (ad es. riproduzione del documento o della sua impronta in un atto pubblico o altro documento autentico cartaceo).

In aggiunta, ma non in alternativa, alla validazione temporale, è prevista, dietro richiesta del soggetto interessato, la conservazione di copia del documento informatico cui la marca temporale si riferisce, da parte del certificatore, con modalità di conservazione e procedure per la richiesta del servizio stabilite dal manuale operativo. Questa conservazione andrebbe effettuata al solo fine di assicurare l'associazione tra documento informatico e le relative marche temporali (art. 59, comma 1, d.p.c.m. 8 febbraio 1999). Per dare un senso a tale norma, sembrerebbe, dunque, che adottando questa procedura, anche in caso di scadenza - o altra causa di perdita di validità - della marca temporale, possa in tal modo mantenersi l'efficacia della data ed ora certa opponibile ai terzi (art. 22, comma 1, lettera g, d.p.r. n. 445/2000) **(42)**. Mentre, secondo la norma, pare che non sarebbe possibile richiedere al certificatore la conservazione del documento privo di una marca temporale.

6. La conservazione delle chiavi e dei certificati

Proprio per consentire la verifica di firme apposte con chiavi scadute o, comunque, non più valide (perché revocate), si stabilisce che le chiavi pubbliche siano conservate per almeno dieci anni dall'inizio della loro validità (art. 27, comma 2, d.p.r. n. 445/2000; art. 29 *bis*, comma 2, d.p.r. n. 445/2000, come introdotto dal d.p.r. n. 137/2003), nonostante che il

termine di scadenza massimo di una chiave e del relativo certificato non può essere superiore a tre anni (art. 22, comma 1, lettera f, d.p.r. n. 445/2000.).

L'esigenza di mantenere l'efficacia probatoria del documento per lunghi periodi di tempo si pone in particolare per gli atti aventi ad oggetto diritti reali immobiliari, per i quali occorre poter disporre della prova documentale, normalmente per il periodo ventennale, richiesto per il maturarsi dell'usucapione ordinaria in materia di beni immobili (art. 1158 c.c.) **(43)**.

Tuttavia, come si è detto, il termine di conservazione minimo delle chiavi da parte del certificatore è prescritto in solo dieci anni. Così potrebbe succedere che la validità della firma sia mantenuta (mediante apposizione e rinnovo di periodiche timbrature temporali) a seguito della sua scadenza, però, dopo dieci anni, non si potrebbe più verificarne la provenienza se il certificato non è più disponibile.

D'altra parte, non è esclusa l'emissione di certificati destinati ad essere, per contratto, conservati per un periodo superiore. La disposizione stabilisce, infatti, che i certificati sono custoditi per un periodo non inferiore a dieci anni, ma non pone un termine massimo di conservazione. Il manuale operativo del certificatore (art. 45 reg. tec.) potrebbe stabilire un termine maggiore **(44)**.

Raimondo Zagami

-
- (1)** Ad es. si pensi all'importanza di attribuire una data certa alle trasmissioni telematiche di atti e documenti nei rapporti con i pubblici uffici, quando si tratta di rispettare termini e scadenze o, comunque, delle priorità temporali.
 - (2)** La stessa procedura di validazione temporale prevista dal d.p.r. n. 445/2000 potrebbe già, di per sé, rientrare in questa clausola generale.
 - (3)** Ma non è escluso che la marca temporale sia apposta successivamente all'apposizione della firma (purché durante il periodo di validità della relativa chiave), e si voglia far valere una data certa *ex art. 2704 c.c.* anteriore alla detta marca temporale (ad es. riproduzione in un atto pubblico o registrazione fiscale).
 - (4)** I certificati delle chiavi pubbliche, come i certificati amministrativi, sono delle dichiarazioni di scienza, ma non provengono da pubbliche autorità. Sulla certificazione amministrativa vedi A. STOPPANI, *Certificazione*, in *Enc. dir.*, vol. VI, Milano, 1969, p. 793 ss.
 - (5)** Nelle regole tecniche (art. 52, comma 1, d.p.c.m. 8 febbraio 1999) si legge che oggetto della validazione temporale è una "evidenza informatica", intesa nel senso precisato dall'art. 1, lettera e), e non solo un documento informatico. L'ottenimento di una validazione temporale potrebbe costituire un'efficace prova nell'eventualità di controversie sulla spettanza di diritti d'autore e brevetti o, comunque, in ogni altro caso in cui è necessario dimostrare l'anteriorità temporale di un certo dato informatico.
La marca temporale può essere generata, sul *file* risultante dall'applicazione di una firma elettronica (documento + firma), precostituendo in tal modo la prova dell'esistenza di una firma elettronica anteriormente ad un certo momento temporale, agli effetti del mantenimento della sua efficacia probatoria secondo il meccanismo di cui appresso.
 - (6)** Concretamente la marca temporale consiste in un piccolo *file* informatico, identificato nel nome da apposita estensione, da conservare alla stregua di qualunque altra informazione digitale.

Poiché la marca temporale è generata sulla base dell'impronta del documento, ne deriva che il relativo *file* sarà sempre della stessa lunghezza, indipendentemente dalla lunghezza del documento oggetto di validazione temporale.

- (7) Una marca temporale deve contenere almeno le seguenti informazioni (art. 53, d.p.c.m. 8 febbraio 1999): a) identificativo dell'emittente; b) numero di serie della marca temporale; c) algoritmo di sottoscrizione della marca temporale; d) identificativo del certificato relativo alla chiave di verifica della marca; e) data ed ora di generazione della marca (con riferimento al Tempo Universale Coordinato UTC); f) identificatore dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale; g) valore dell'impronta dell'evidenza informatica. Tale struttura deve essere sottoscritta digitalmente da apposito sistema elettronico sicuro (art. 53, d.p.c.m. 8 febbraio 1999).

Non è invece, contenuta alcuna informazione circa il soggetto richiedente la validazione temporale, perché irrilevante. L'identificazione del richiedente potrebbe rilevare solo al momento della richiesta della marcatura, in relazione a profili di tariffazione del servizio.

La marca temporale può, inoltre, contenere un identificatore dell'oggetto a cui appartiene l'impronta sottoposta a validazione temporale, per poterlo più facilmente individuare (ad es. il titolo del *file*).

- (8) Si pone un problema di coordinamento tra la liberalizzazione dell'attività di certificazione disposta dal d.lgs. n. 10/2002, in attuazione della direttiva comunitaria del 13 dicembre 1999, n. 1999/93/CE, ed i requisiti che devono rivestire i soggetti che rilasciano marche temporali con effetti di opponibilità della data *erga omnes*. Non è, infatti, stabilito alcun collegamento tra i diversi livelli di certificatori (semplici, qualificati ed accreditati) ed il valore delle marche temporali da questi emesse. Non si distinguono, infatti marche temporali qualificate da marche non qualificate. Anzi, la direttiva comunitaria trascura totalmente il profilo della validazione temporale dei documenti: la validazione temporale rientrerebbe tra gli "altri servizi connessi alle firme elettroniche" che il certificatore può offrire (art. 2, n. 11 direttiva CE; nuovo art. 1, lettera n), d.p.r. n. 445/2000, come modificato dal d.p.r. n. 137/2003). Pertanto, sembra che il servizio di marcatura temporale potrebbe essere svolto da chiunque (certificatore qualificato o meno). Tuttavia, per il raggiungimento degli effetti probatori di opponibilità ai terzi, come previsto dal d.p.r. n. 445/2000, sembra difficile ammettere marche temporali provenienti da certificatori non qualificati o non accreditati, che operano secondo le regole tecniche di cui al d.p.c.m. 8 febbraio 1999. Peraltro, essendo le marche temporali basate su certificati e su firme elettroniche, valgono per esse le stesse regole della direttiva CE applicabili alle firme ed ai certificati in generale.

- (9) Nel sistema tradizionale codicistico, l'attestazione di data certa poteva provenire esclusivamente da un soggetto pubblico. Il fatto che un soggetto privato, quale un certificatore, possa operare un'attestazione opponibile *erga omnes* suscita qualche perplessità. D'altra parte non sono regolate eventuali ipotesi di conflitto di interessi in cui potrebbe trovarsi il soggetto che genera le marche temporali.

- (10) Le procedure per l'inoltro della richiesta di validazione temporale sono stabilite dal certificatore nel manuale operativo (art. 58, comma 1, d.p.c.m. 8 febbraio 1999). Ad es., secondo il manuale operativo del servizio di certificazione del Consiglio Nazionale del Notariato (CNN), la richiesta di validazione temporale è inviata telematicamente al CNN, via *World Wide Web* utilizzando il protocollo *http* o mediante *software client* distribuito dal CNN che supporta tale protocollo o mediante posta elettronica o altro metodo coerente con i dettami dello *standard* (punto 12.2); la marca temporale generata è trasmessa telematicamente al richiedente con comunicazione dell'avvenuta ricezione; l'eventuale esito negativo della richiesta è parimenti comunicato al richiedente con l'indicazione della motivazione (*Manuale operativo*, versione 1.0.1, punto 12.3).

- (11) Non è richiesto l'impiego di un sistema di comunicazione sicuro (in particolare quello previsto dall'art. 25, d.p.c.m. 8 febbraio 1999), dato che chiunque potrebbe richiedere una marca temporale, anche se non registrato presso il certificatore. D'altra parte, nella marca temporale non è richiesta l'indicazione del richiedente (art. 53, d.p.c.m. 8 febbraio 1999). L'autenticità della marca temporale trasmessa (in un sistema di comunicazione insicuro) è verificabile con la chiave pubblica di marcatura temporale (art. 4, comma 4, lettera c, d.p.c.m. 8 febbraio 1999).

Volendo limitare e controllare l'accesso al servizio, per ovvi motivi di tariffazione, si utilizzeranno sistemi di autenticazione con password o tramite sottoscrizione elettronica della richiesta. Ad es., in tal senso, il manuale operativo del servizio di certificazione del CNN prevede che la richiesta deve includere l'impronta del documento oggetto della validazione temporale e deve essere firmata digitalmente dal notaio richiedente utilizzando la chiave privata corrispondente alla chiave pubblica certificata dal CNN (punto 12.2), e di conseguenza, la procedura di generazione della marca temporale è subordinata alla verifica della firma digitale del richiedente (Manuale operativo, versione 1.0.1, punto 12.3).

- (12) Sono richiesti stringenti requisiti di sicurezza e precisione cronometrica dei sistemi di validazione temporale (artt. 55 e 56, d.p.c.m. 8 febbraio 1999).
- (13) La generazione (e la verifica) della marca temporale avviene applicando una specifica chiave di marcatura temporale, oggetto di specifica certificazione, e diversa dalle chiavi utilizzate per la certificazione delle chiavi di sottoscrizione (art. 4, comma 4, lett. c e art. 54, comma 3, d.p.c.m. 8 febbraio 1999), i cui requisiti e ciclo di vita sono oggetto di specifica disciplina (art. 6, comma 1, art. 54, comma 1 e art. 11, comma 5, d.p.c.m. 8 febbraio 1999).

Al fine di limitare il numero di marche temporali generate con la medesima coppia [e, quindi, ridurre i potenziali danni in caso di loro compromissione], le chiavi di marcatura temporale debbono essere sostituite dopo non più di un mese di utilizzazione, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato (art. 54, comma 2, d.p.c.m. 8 febbraio 1999).

- (14) Tutte le marche temporali emesse da un sistema di validazione debbono essere conservate in un apposito archivio digitale fino alla scadenza della chiave pubblica della coppia utilizzata per la loro generazione (art. 57, d.p.c.m. 8 febbraio 1999). A seguito di tale scadenza, la marca temporale non sarà più verificabile. Peraltro, la perdita di validità di una marca temporale può essere compensata da altre marche apposte sullo stesso documento (art. 58, comma 4, d.p.c.m. 8 febbraio 1999).

Si può così risalire a marche temporali non più custodite dagli interessati. L'identificatore dell'oggetto cui appartiene l'impronta (e, quindi, la marca) agevola il collegamento di marca temporale e documento (art. 53, comma 2, d.p.c.m. 8 febbraio 1999).

- (15) Allo stesso modo, anche la firma digitale non è generata sul documento nella sua interezza, bensì sulla sua impronta generata dalla funzione di hash.
- (16) Secondo le regole tecniche emanate con d.p.c.m. 8 febbraio 1999, la generazione delle marche temporali deve garantire un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo (art. 58).
- (17) In quanto la marca temporale è generata sulla base dell'impronta del documento, ne consegue che per la verifica occorre disporre di entrambi i *file* (marca temporale e documento nella sua interezza) per operare il relativo confronto, che presuppone la decifrazione della marca temporale (i.e. della firma digitale del certificatore) e la generazione dell'impronta del documento.
- (18) Anzi, con il trascorrere del tempo, dopo la morte del suo autore, una sottoscrizione viene assistita anche dalla "data certa" (art. 2704 c.c.).
- (19) Il comma 2 dello stesso art. 23 del d.p.r. n. 445/2000 (sempre come modificato dal d.p.r. n. 137/2003), con riferimento alle firme apposte successivamente alla perdita di validità del certificato, precisa ulteriormente che "Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica sia stata oggetto dell'emissione di un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso".
- (20) Sul problema della scadenza della firma vedi U. BECHINI, *Contiene atto notarile: per la data di scadenza vedere sul tappo*, in *Federnotizie*, maggio 2001.
- (21) Non può considerarsi di nessuna attendibilità l'indicazione della data riportata nelle proprietà del *file* di sistema del documento, in quanto connessa ad un orologio interno del *computer*, regolabile a piacimento dall'utente, in modo del tutto analogo alla data riportata in un messaggio *telex*.

Per lo stesso motivo, nemmeno sono attendibili ed utilizzabili ai fini dell'opponibilità, le indicazioni temporali riportate in appositi campi eventualmente inseriti nella struttura di dati della firma digitale. Tali indicazioni

strutturate, prescindendo dalla loro efficacia probatoria, potrebbero, peraltro, risultare utili ai fini del trattamento automatizzato dei documenti con riferimento al momento di apposizione della firma, in quanto la marca temporale è un *file* diverso ed ulteriore rispetto al relativo documento.

- (22) La validazione temporale, a tal fine, deve ovviamente avere ad oggetto il *file* comprensivo della firma elettronica e non soltanto il *file* del documento senza firma.
- (23) Si tratta, in sostanza di confrontare la marca temporale che attesta il momento di pubblicazione della revoca e della sospensione (artt. 29, comma 3 e 33, comma 2, d.p.c.m. 8 febbraio 1999), con la marca temporale apposta alla firma digitale; nonché quest'ultima marca temporale, con il momento della scadenza della chiave certificata (indicato nel certificato stesso).
- La marca temporale può essere apposta anche in un momento successivo all'apposizione della firma, anche distante di giorni, purché entro il periodo di validità del relativo certificato. Tuttavia, più si attende ad apporre la marca temporale, più si aumentano i rischi di compromissione della chiave.
- (24) Tale problema è stato presente fin dalle prime elaborazioni in materia. Sull'esigenza dell'apposizione di una marca temporale per mantenere nel tempo l'efficacia probatoria del documento informatico, vedi B. SCHNEIER, *Applied Cryptography*, U.S.A., 1994, p. 36 s.; ABA, *Digital Signature Guidelines*, 1996, § 1.33.2, § 3.12.3, § 4.4.2. L'esigenza della marcatura temporale per consentire la verifica della firma digitale è chiaramente espressa anche dalla *Model Law on Electronic Signatures* dell'UNCITRAL (*United Nations Commission on International Trade Law*), 2001, "A digital signature corresponding to a message, whether created by the signatory to authenticate a message or by a certification service provider to authenticate its certificate, should generally be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the "operational period" stated in the certificate, which is a condition of the verifiability of a digital signature." (punto 55).
- (25) Il notaio non potrà, quindi, autenticare firme digitali apposte con chiavi i cui certificati non siano regolarmente pubblicati, oppure siano scaduti, revocati o sospesi.
- (26) La perdita di efficacia della firma del notaio autenticante si ripercuote anche sulla firma oggetto di autenticazione, se il relativo certificato di quest'ultima è nel frattempo cessato di validità.
- (27) Come si è prima detto, rimane, comunque, irrilevante la data del *file* di sistema.
- (28) Purché durante il periodo di validità del relativo certificato.
- (29) Lo stesso problema del contrasto tra la data attestata dal notaio e la data risultante dalla marca temporale si potrebbe porre in sede di rilascio di copie autentiche.
- (30) Ovviamente si intende una marca temporale apposta non solo al documento privo di firma della parte, bensì apposta al documento munito delle firma della parte autenticata dal notaio.
- (31) Quando si tratta di archiviare documenti sottoscritti dalle parti, per i quali potrebbe essere richiesta una futura verifica delle sottoscrizioni, non è concepibile un'archiviazione informatica secondo modalità riproduttive che fanno venire meno le corrispondenti firme ed impediscono una verifica completa. Anche in caso di copie autentiche, l'art. 2716 c.c., stabilisce, infatti, che "In mancanza dell'originale scrittura privata, le copie di essa spedite in conformità dell'articolo 2715 fanno egualmente prova; ma se presentano cancellature, abrasioni, intercalazioni o altri difetti esteriori, è rimesso parimenti al giudice di apprezzarne l'efficacia probatoria. Resta in ogni caso salva la questione circa l'autenticità dell'originale mancante".
- (32) In caso di documenti sottoscritti con molteplici firme elettroniche (anche dello stesso soggetto), la perdita di validità solo di alcune di esse, non inficia anche la validità delle altre. Per questo motivo può essere opportuna la richiesta contestuale di più marche sullo stesso documento presso lo stesso certificatore o anche presso certificatori diversi.
- (33) S. PATTI, Documento, in *Dig. disc. priv.* – sez. civ., Torino, 1991, p. 7.
- (34) Per tali motivi è necessario che le ricevute di adempimenti telematici (come ad es. Unico informatico o Registro imprese) siano restituite al richiedente con la firma digitale del soggetto ricevente, in modo del tutto analogo all'attuale ricevuta cartacea oggi consegnata.

- (35) Per mantenere l'efficacia probatoria della firma elettronica, secondo quanto spiegato sopra, la marca temporale deve essere ovviamente apposta prima della cessazione di validità del relativo certificato cui si riferisce la firma oggetto di marcatura.
- (36) La facoltà di richiedere marche temporali per qualsiasi documento, anche se prodotto e firmato da persona diversa, è espressa bene dal manuale operativo del servizio di certificazione del CNN, dove si legge che possono essere oggetto di marcatura temporale i documenti informatici di qualunque specie, prodotti ed eventualmente sottoscritti, da un notaio o da altri soggetti (Manuale operativo, versione 1.0.1, punto 12.1).
- (37) Non sono però specificamente disciplinate dalle regole tecniche emanate con d.p.c.m. 8 febbraio 1999 le modalità di revoca delle chiavi di marcatura temporale compromesse, che possono essere disciplinate dal manuale operativo del certificatore. Ad es. in tal senso dispone il manuale operativo del servizio di certificazione del CNN (Manuale operativo, versione 1.0.1, punto 10.4)
- (38) Applicazione di tale principio è rinvenibile nell'art. 38, comma 4, d.p.c.m. 8 febbraio 1999, con riferimento ai certificati per i quali risulta compromessa sia la chiave di certificazione con cui sono stati sottoscritti, sia la chiave con cui è stata generata la marca temporale che ne ha attestato la pubblicazione nel registro dei certificati.
- (39) Vi è una certa analogia con la rinnovazione dell'ipoteca (art. 2847 c.c.), quale atto da compiere per mantenere certi effetti prima di una scadenza prestabilita, ferma restando la sua estinzione con l'estinguersi dell'obbligazione (art. 2878 n. 3 c.c.).
- (40) Se specificato nella richiesta, possono essere emesse anche più marche temporali per la stessa evidenza informatica, così che in caso di perdita di validità di una di esse restano valide le altre; evidentemente, in tal caso, le diverse marche temporali non possono essere generate con la stessa chiave (art. 58, comma 4, d.p.c.m. 8 febbraio 1999).
- (41) Come si è detto, le marche temporali possono essere generate non direttamente sui documenti ma sulle loro impronte. Inoltre, la rinnovazione della marca temporale dal punto di vista tecnico potrebbe avere ad oggetto il *file* della sola marca in prossimità di scadenza, indipendentemente dal relativo documento, dato che è comunque a quest'ultimo univocamente collegato. Tuttavia, forse per evitare il periodico rinnovo di marche temporali scollegate da documenti con cui diventerebbe difficile ricostituire un'associazione, le regole tecniche stabiliscono che il rinnovo deve avere ad oggetto una "evidenza informatica costituita dal documento iniziale, dalla relativa firma e dalle marche temporali già ad esso associate" (art. 60, comma 2, d.p.c.m. 8 febbraio 1999).
- (42) Il certificatore svolge così un servizio analogo alla registrazione degli atti tradizionalmente svolta dagli uffici del registro (art. 2704 c.c.; art. 18, d.p.r. 26 aprile 1986, n. 131). Come per gli uffici del registro, anche la procedura dell'art. 59, presuppone l'intervento diretto del certificatore per attestare la data ed ora certa (se la marca temporale è divenuta invalida).
- Restano, poi, i rischi legati alla riservatezza dei dati conservati dal certificatore, a meno che non si consenta la conservazione della sola impronta del documento.
- Comunque, resta fermo che tutte le marche temporali emesse da un sistema di validazione debbono essere conservate in un apposito archivio digitale fino alla scadenza della chiave pubblica della coppia utilizzata per la loro generazione (art. 57, d.p.c.m. 8 febbraio 1999).
- (43) Come è noto, al fine di evitare la cosiddetta *probatio* diabolica, il *dante causa* prova la sua titolarità unendo il proprio possesso a quello del suo autore (art. 1146 comma 2 e art. 1143 c.c.) e risalendo così ai titoli di provenienza fino al ventennio anteriore si può ritenere maturato l'usucapione.
- (44) La norma che prescrive l'allegazione del certificato alla firma digitale (art. 9 comma 2 reg. tec.), non esime dalla verifica *on-line* della sua persistente validità. Una tale verifica sarà possibile solo fino a quando il certificato è conservato nel registro dei certificati, unitamente alle liste dei certificati revocati e sospesi (art. 43 reg. tec.).

(Riproduzione riservata)