▶ Servizi telematici al cittadino

Al varo la firma digitale europea

Come usare la via telematica per ridurre la mole dei documenti cartacei. Vediamo cos'è la firma elettronica e se è sicura

di Daniela Dirceo

Entro fine giugno scatterà per le aziende l'obbligo di inviare solo per via telematica gli atti societari al Registro delle Imprese delle Camere di Commercio: si tratta di un primo passo sancito per legge, volto a diffondere l'utilizzo della firma digitale. Di firma digitale se ne sente parlare da anni, per la precisione dal 1997, quando con la cosiddetta legge Bassanini, viene sancito che il documento informatico ha lo stesso valore legale di un documento cartaceo. La stessa legge introduce nel nostro ordinamento il concetto di **firma digitale**, che viene equiparata a tutti gli effetti alla firma autografa.

Pertanto, la corrispondenza, i contratti, gli ordini ed in generale i documenti inviati per via telematica su cui viene apposta la firma digitale hanno valore legale.

Per la legge, la firma digitale deve utilizzare un sistema di **crittografia a doppia chiave asimmetrica**, composta da una chiave pubblica e una privata, in quanto il sistema è in grado di garantire l'integrità e la provenienza dei documenti.

Abilitati a rilasciare la firma digitale, fino ad oggi, sono stati solo i tredici **certificatori accreditati (CA)** presso l'**AIPA (Autorità per l'Informatica nella Pubblica Amministrazione)** il cui elenco è pubblico e recuperabile all'indirizzo www.aipa.it.

Le "firme europee"

Così fino ad oggi. Più attuale è invece la notizia che a breve avremo a disposizione una firma digitale europea, o, per essere più precisi, più firme digitali.

Ma procediamo con ordine e vediamone i dettagli.

È dello scorso febbraio l'approvazione, da parte del Consiglio dei Ministri, del regolamento di attuazione della direttiva europea relativa al quadro comunitario per le firme elettroniche, messo a punto dal Ministro per l'Innovazione e le Tecnologie.

Ad oggi il provvedimento è all'esame della Corte dei Conti, ma diventerà, in breve tempo, definitivo con la sua pubblicazione sulla Gazzetta Ufficiale, dove si troveranno anche le "regole tecniche" (gli standard) sui documenti informatici che il ministero dell'Innovazione sta ultimando.

Cosa cambia rispetto al passato? "Per gli utenti non cambierà nulla" risponde Giovanni Manca, responsabile funzione certificazione AIPA "Il cittadino che avesse acquistato la firma digitale in passato presso uno dei certificatori accreditati potrà continuare a utilizzarla. Quello che cambia è il rapporto tra certificatori e istituzioni e che viene data una normazione ufficiale anche a quelle che gli addetti ai lavori hanno definito "firme deboli"".

Diciamo subito che la direttiva distingue la firma elettronica generica (definita dal secondo comma dell'artcolo 5 della direttiva e pertanto chiamata anche **"firma 5.2"**), strumento di autenticazione di dati elettronici, e che può essere realizzata con qualsiasi strumento (password, PIN, digitalizzazione delle firma autografa, tecniche biometriche e così via), da una firma elettronica avanzata (per lo stesso motivo definita anche **"firma 5.1"**), più sofisticata, che consente di identificare in modo univoco il firmatario, permettendo anche la scoperta di

Il parere dell'esperto

Ma la firma digitale è davvero a prova di frode? Lo abbiamo chiesto ad un vero esperto del settore, **Raoul Chiesa**, fondatore della società @Mediaservice.net, che si occupa di Web e sicurezza informatica (la Divisione Sicurezza Dati dispone di esperti che testano i sistemi informatici di difesa aziendali per scoprirne le vulnerabilità) e membro della Commissione per la Certificazione di sicurezza informatica del CLUSIT (Associazione Italiana per la Sicurezza Informatica) .

Il sistema utilizzato (a chiave pubblica) è davvero sicuro per gli utenti? E se ci fosse un tentativo di frode, come può avvenire?

Il sistema a chiave pubblica è – ovviamente anche in funzione dell'algoritmo di cifratura utilizzato – uno degli accorgimenti più sicuri ad oggi esistenti. Certo, molti sono i fattori di "contorno" che possono diminuire o innalzare questo "livello di sicurezza".

In primo luogo, è ovvio che, da qualche parte, le "chiavi private" dovranno essere custodite. Le custodisce la CA, la Certification Authority, ovverosia l'ente super partes che si fa "garante" dell'identità degli attori chiamati in causa. Risulta ovvio come – nel caso di CA non sufficientemente protette – questo elenco possa essere trafugato da persone non autorizzate, con tutte le ovvie conseguenze del caso: impersonificazione di terzi nelle transazioni, possibilità di non ripudio, e così via. In questo caso, tutti i punti di forza della firma digitale si potrebbero ritorcere proprio contro l'utilizzatore finale, l'utente, nel caso di abuso in seguito ad intrusione informatica. Quindi, un primo aspetto riguarda proprio la sicurezza intrinseca della CA: è opportuno sceglierne una che si sottoponga a security test (in gergo, Penetration Testings) di alto livello, simulando in tutto e per tutto le attività di attacco ed abuso che persone non autorizzate potrebbero lanciare contro l'infrastruttura.

Generalizzando, vediamo dove è possibile che avvengano "security incidents", relativi agli elementi toccati da processi di certificazione. In:

- Sistemi Operativi (bachi, falle, mancanza di security patch)
- Applicazioni (bachi, falle, mancanza di source auditing)
- Web Applications (bachi, falle, errori progettuali e/o implementativi)
- Procedure (Call Center, Helpdesk, e così via)
- Comportamenti umani (attacchi a Social Engineering, Insiders, Abusi dall'interno…)
- Sicurezza fisica (accessi fisici all'infrastruttura, security badges, trashing…)
- Old Technology (FAX, GSM, PSTN/ISDN, …)
- New Technology (SMS, GPRS, UMTS, …)
- Users Access (Smart Card, SMS, ….)
- Punti di contatto con l'esterno (IP, RAS, PBX, X.25, VPN, PtP)

Sottolineiamo che è probabile che proprio grazie agli "accessori di contorno", quali applicazioni Web ed SMS, in conseguenza delle falle già note di queste architetture, sia possibile effettuare attacchi ed abusi verso possessori di firme digitali.

Il consiglio dell'esperto, quindi?

Di affidarsi a CA note e con una storia alle spalle e non alle tante CA che spunteranno come funghi a seguito della liberalizzazione, ma che non avranno avuto ancora il modo di porsi i problemi che CA con maggiore esperienza hanno già affrontato.

Raoul Chiesa, *CTO di @Mediaservice*

modifiche all'oggetto firmato apportate dopo la sottoscrizione. Queste caratteristiche sono garantite dal certificatore.

Da qui il concetto di **"firma forte"** e **"firma debole"**, che non appare citato nella direttiva, ma che è stato introdotto dagli addetti ai lavori per semplicità di utilizzo. "In realtà" prosegue Giovanni Manca "si avranno due tipologie: una firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, le quali possono essere certificate da un certificatore accreditato o non accreditato, entrambe con lo stesso valore giuridico, con l'unica differenza che la PA accetta solo documenti digitali muniti di firma rilasciata da certificatori accreditati. Tutte le altre firme elettroniche rientreranno nella generica accezione di "firma debole" o "leggera"".

La scelta di utilizzare un tipo o l'altro di firma dipenderà esclusivamente dalle esigenze degli utenti. Se, ad esempio, un'azienda dovrà presentare atti societari al Registro delle Imprese della Camera di Commercio, necessiterà di una firma digitale "forte", nel caso in cui, invece, si vorrà mandare una e-mail, certificando proprio l'identità del mittente si potrà utilizzare una firma "debole".

Il ruolo dei certificatori

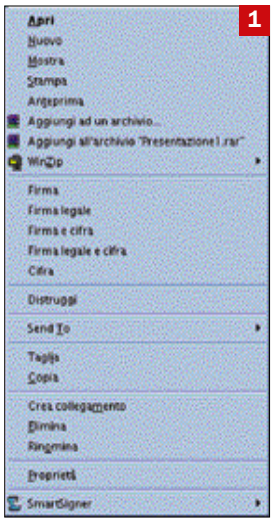
È chiaro, a questo punto, il ruolo chiave svolto dai **certificatori**, i veri erogatori del servizio. Fino ad oggi questi erano iscritti, come abbiamo visto, in un elenco pubblico tenuto dall'AIPA. "Tale elenco", afferma Libero Marconi, responsabile Dipartimento Consulting & Deliver Servizio di Certificazione di Trust Italia (affiliata italiana di VeriSign) provider di servizi per la sicurezza su Internet, dal 2001 CA presso AIPA "comprende la lista delle società che hanno superato l'istruttoria di accreditamento e sono abilitati ad operare come "terzi di fiducia", ossia come coloro che ufficialmente possono associare l'identità di una persona (il titolare della firma elettronica) ad una struttura dati riconosciuta da tutti (il certificato digitale di firma) nonché rendere tale informazione disponibile pubblicamente con tecnologia a prova di frode (infrastruttura a chiave pubblica, PKI)". Con la nuova normativa, i certificatori già iscritti nell'elenco, ora affidato al Dipartimento per l'innovazione e le tecnologie, saranno considerati **"certificatori accreditati"**, che verranno affiancati da **"certificatori notificati"**, che per esercitare non avranno bisogno di certificazione preventiva, ma saranno soggetti alla vigilanza del Dipartimento.

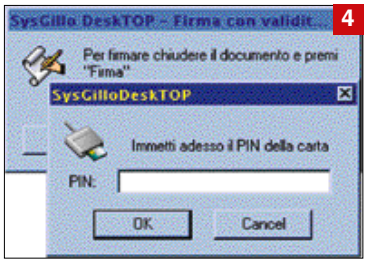
Una liberalizzazione, quindi, del settore, che potrebbe dare un colpo di acceleratore all'utilizzo della firma digitale, ma che per la sua più capillare diffusione avrà bisogno di importanti *killer application*, rivolte certo, al mondo delle imprese e dei professionisti, sicuramente in prima linea nell'adozione dello strumento, ma anche ai singoli cittadini, per agevolare il rapporto quotidiano con la PA. ■

Libero Marconi, *responsabile Dipartimento Consulting & Deliver Servizio di certificazione di Trust Italia*

Dalla teoria alla pratica: ottenere una firma debole e una forte

Utilizziamo Trust Italia, in quanto CA in grado di erogare entrambe le tipologie di certificati. E partiamo con un esempio che sta sotto gli occhi di tutti: se utilizzate Outlook o Outlook Express siete già in possesso di un sistema di firma digitale "debole". Il client di posta, infatti, può creare dei messaggi di posta firmati digitalmente. La procedura è semplice. Dal menu *Nuovo Messaggio, File* si seleziona *Proprietà* e quindi *Protezione*. Qui appare una finestra: basterà selezionare la voce *Aggiungi firma digitale al messaggio* e il gioco è fatto. Nel caso non foste ancora possessori di una ID digitale Outlook rimanda automaticamente all'area risorse che elenca dove ottenerla. VeriSign offre gratuitamente agli utenti di Outlook una ID digitale di prova per due mesi che potrà essere confermata allo scadere del periodo con normali pratiche commerciali. E passiamo alla "firma forte", e vediamo come si può ottenere. Il titolare deve contattare la CA e quindi rispettare una serie di obblighi di legge rappresentati nel "manuale operativo" della CA, al fine di documentare la sua identità. Al termine delle operazioni la persona che richiede il certificato di firma si ritrova in possesso di un **kit** composto da software, hardware e dal dispositivo di firma (smart card o chiave USB). Il primo problema sarà quello di installarlo nel suo PC. Quindi dovrà installare il software idoneo alla firma elettronica, perché senza di quello il certificato è perfettamente inutile. Alla fine il nostro titolare di certificato digitale di firma elettronica potrà creare delle **"envelope PKCS#7"** (file codificati con estensione **.p7m**, *vedi immagine*) che sono compatibili con null'altro che un software di firma simile usato nella funzione di verifica. Il costo è di circa 75 euro.





1 Selezione dal menù: *clic con il pulsante destro sul file da firmare*

2 La finestra di dialogo prima della firma: *da notare l'obbligo dell'esame*

3 La finestra di dialogo prima della firma: *Il pulsante "firma" adesso è disponibile, in quanto il documento è stato esaminato*

4 A questo punto si inserisce il PIN *per attivare la firma*

5 La firma è in corso*, da smart card, si impiega circa 20 secondi*

6 Ecco creato il nostro documento *con estensione .p7m. La firma è avvenuta*

Per competere siamo "condannati" ad innovare di Lucio Stanca*

***Lucio Stanca** Ministro per l'Innovazione e le Tecnologie*

L'Italia è la sesta potenza economica del mondo, ma nelle classifiche internazionali sulla competitività globale risulta essere al trentaduesimo posto.
Bisogna partire da questo dato per poter fare un'analisi corretta della situazione economica del nostro Paese e, quindi, poter ricercare nuove soluzioni, elaborare strategie che ci consentano di tornare ad essere competitivi. Premetto subito che non siamo in crisi o in declino, ma scontiamo il ritardo o, se si preferisce, il rallentamento in settori oggi più che mai strategici, quali la Ricerca e l'Innovazione, anelli fondamentali di quella che io definisco la "Catena del Valore": CONOSCENZA – RICERCA – INNOVAZIONE – MERCATO – SVILUPPO.
La conoscenza applicata all'ambito della ricerca crea innovazione, la quale a sua volta rende competitive le imprese nel mercato, creando così, sviluppo economico. In Italia il punto debole di questa catena è il passaggio dal secondo al terzo anello, vale a dire il trasferimento dalla Ricerca all'Innovazione. Abbiamo esempi significativi degli effetti di una catena del valore che funziona: le 4000 imprese fondate da studenti e ricercatori del MIT *(Massachussetts Institute of Technology)* occupano oltre 1 milione di persone e se aggregate rappresenterebbero il ventiquattresimo paese in termini di volume d'affari (circa 232 miliardi di dollari). In generale, negli Stati Uniti due terzi dei nuovi posti di lavoro creati negli ultimi 4 anni sono di imprese ad alta tecnologia, di cui la metà sono piccole medie imprese. Questo dato trova la sua giustificazione nel fatto che negli Usa il 61% delle imprese utilizza le nuove tecnologie, contro il 45% medio di Germania, Francia ed Inghilterra e, purtroppo, solo l'11,4% delle imprese italiane.
A questi dati si aggiunge anche quello relativo alla percentuale di brevetti ICT sul totale registrato, che ci vede fermi al 15%, contro il 27% dei tre Paesi europei citati prima e il 45% dei Paesi Nordici.
Le imprese italiane possono avere due approcci di fronte all'innovazione ICT: creare innovazione oppure semplicemente usarla nei processi produttivi (esistono Paesi, come l'Australia, che pur non producendo beni o servizi ICT sanno gestire bene l'innovazione ed essere competitivi). Un Paese che vuole essere moderno ed economicamente avanzato è, quindi, inesorabilmente costretto ad innovare per non perdere il passo, per non essere emarginato e schiacciato dai Paesi emergenti. Solo con una crescita basata sull'innovazione si ammoderna il Paese e si realizza nuova occupazione qualificata. In-fatti, l'innovazione tecnologica ed i suoi vari strumenti, come computer, Internet, posta elettronica e banda larga, non riducono l'occupazione ma, anzi, qualificano il posto di lavoro e gli stessi dipendenti.
Per questo è essenziale ed imprescindibile la necessità di spiegare in modo convincente ai dipendenti quali siano i reali vantaggi che l'innovazione tecnologica determina non solo per le aziende, ma anche per ogni lavoratore, di qualunque grado e posizione, pubblico o privato che sia, smentendo così il ricorrente pregiudizio "occupazionale" determinato dalla paura del nuovo e da abitudini che è difficile sovvertire. Nel nostro Paese l'ICT si è affermata più rapidamente nelle famiglie e nella vita quotidiana che nella trasformazione dei processi produttivi. Vi è un problema di cultura ICT nell'impresa. Una ricerca dell'Università Bocconi dello scorso ottobre indica che il 70% delle aziende italiane non ha adottato applicazioni in rete perché le ritiene "inutili". Un'altra ricerca, a cura di Federcomin ha messo in evidenza che i comparti dell'industria e della distribuzione sono quelli con la minore conoscenza della Larga Banda.
Il Governo italiano ha posto come 'priorità' la modernizzazione del Paese e la diffusione delle tecnologie digitali, contribuendo a creare quella "cultura digitale" che oggi è condizione necessaria per lo sviluppo economico. In tal senso, abbiamo posto in essere una serie di iniziative a sostegno delle imprese, come ad esempio, l'apertura dei **138 progetti digitali per portare in rete ben 80 servizi pubblici 'prioritari'**; oppure, penso agli enormi progressi ottenuti per la **firma digitale**, che dà valore legale ai documenti telematici, permettendo anche l'invio elettronico degli atti delle aziende al Registro delle imprese, con un risparmio di 260 milioni di euro l'anno tra minori consumi di carta, riduzione dei costi di archiviazione e l'annullamento delle spese di spedizione. A tal proposito, ricordo che l'Italia ha la più alta diffusione di questo strumento in Europa con oltre 500 mila firme digitali emesse. Un altro importante settore a cui stiamo dedicando particolare attenzione è quello dell'**e-commerce**. Le imprese sfruttano ancora troppo poco le potenzialità offerte da Internet, visto che solo il 10% dei consumatori italiani acquista in Rete, rispetto alla media europea del 23%. Per incentivare l'e-commerce il Governo ha approvato un pacchetto di 110 milioni di euro, con particolare attenzione ai collegamenti telema-tici nel tessile, nell'abbigliamento e nelle calzature. Uno dei maggiori problemi delle imprese è quello del **Fisco**, inteso non solo come pressione ma anche come vincolo, come complesso di "lacci" burocratici.
La riforma che stiamo attuando in Italia consentirà di **snellire enormemente certe lungaggini amministrative e** renderà più semplice per gli imprenditori compiere tutta una serie di adempimenti. Basti pensare che già nel 2002 le dichiarazioni fiscali presentate per via telematica sono state complessivamente 31,5 milioni a fronte di 29 milioni nel 2001, mentre le dichiarazioni di inizio, variazione e cessazione di attività ai fini IVA inviate in via telematica sono aumentate del 125% rispetto al 2001. Sempre nel 2002, inoltre, sono stati registrati telematicamente 35 mila contratti di locazione, contro i 16 mila del 2001, con un incremento del 120%. Infine, nell'ultimo periodo dello stesso anno oltre 800 mila aziende (pari a più del 50% del totale) ha effettuato denunce contributive mensili via Internet.
Attualmente sono allo studio **misure permanenti per le PMI che utilizzano l'innovazione tecnologica** per accrescere la loro competitività, ma c'è bisogno del coinvolgimento diretto di tutte le associazioni imprenditoriali per portare avanti questo indifferibile obiettivo. Non si tratta di sostenere la nostra industria, che ha potenziali rilevanti, in un momento congiunturale sfavorevole, quanto invece fornire impulso alle imprese che attualmente non innovano, per promuovere ed accelerare investimenti in ICT.
A questo punto la possibilità di far parte del gruppo di testa dei paesi europei dipende esclusivamente dalla nostra capacità di innovare e di investire nella Ricerca. Non abbiamo scelta: siamo 'condannati' all'innovazione. Sono ormai finite le armi che hanno portato al 'boom' economico e fatto crescere il nostro Paese: negli anni '50 e '60 era il costo del lavoro a favorirci; negli anni '80 era stata la competitività derivante dalla svalutazione. Ora, per essere concorrenziali ci resta solo l'innovazione. E, quindi, dobbiamo stimolarne la diffusione. A partire dalle piccole e medie imprese, che rappresentano la parte più rilevante del sistema produttivo nazionale. Infatti, il 95% delle imprese italiane ha meno di 20 occupati, dispone del 39% dei dipendenti totali del Paese ed ha un fatturato pari al 43% del totale nazionale.

**Ministro per l'Innovazione e le Tecnologie*

Il regolamento nei dettagli: la parola all'avvocato

Chi è abituato all'uso del computer conosce da tempo il documento elettronico e sa che questo può sostituire quello cartaceo. Tuttavia, gli effetti giuridici della formazione di un documento in formato elettronico, al posto del più tradizionale formato cartaceo, sono stati disciplinati e definiti solo in tempi più recenti: in primo luogo dalla Direttiva 1999/93/CE del Parlamento europeo, adottata il 13/12/99, che ha emanato norme di coordinamento comunitario in materia di firme elettroniche; in secondo luogo, dal D. Lgs. 23/1/02 n. 10, che ha finalmente dato attuazione, nel nostro Paese, a quella direttiva.

Il citato D. Lgs. contiene una norma fondamentale, che attribuisce al documento elettronico la medesima efficacia giuridica del documento cartaceo, purchè ricorrano determinate condizioni. A tale riguardo, l'art. 6 del D. Lgs. (che ha modificato l'art. 10 DPR 28/12/00 n. 445) prevede le seguenti ipotesi:

• **documento informatico privo di sottoscrizione.** In questo caso, il documento fa piena prova dei fatti o delle cose che rappresenta, a meno che colui contro il quale il documento informatico è prodotto non ne disconosca la conformità ai fatti o alle cose che rappresenta;

• **documento informatico sottoscritto con firma elettronica.** Questo tipo di documento soddisfa il requisito della forma scritta, quando richiesto dalla legge (in particolare, per espressa previsione della norma, questa ipotesi soddisfa l'obbligo dell'imprenditore di tenuta delle scritture contabili). Tuttavia, questo tipo di documento non ha un'efficacia probatoria assoluta, in quanto il giudice può valutarlo liberamente, in considerazione delle sue caratteristiche di qualità e sicurezza;

• **documento informatico sottoscritto con firma digitale avanzata,** basata su un certificato qualificato e generata mediante un dispositivo per la creazione di una firma sicura. In questo caso, l'equiparazione con il documento cartaceo è assoluta, in quanto questo tipo di documento fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

L'art. 13 del D. Lgs. ha invece disposto l'emanazione di un apposito regolamento che coordini con la Direttiva della UE sopra citata e con il D. Lgs. 10/02 le norme contenute nel DPR 445/00, che dispone in materia di documentazione amministrativa, alcune delle quali applicabili però anche ai privati. Questo regolamento, che dovrebbe chiarire i concetti sopra enunciati, non è ancora stato approvato; tuttavia, esiste uno schema di regolamento abbastanza rappresentativo di quella che dovrebbe essere la versione finale.

Lo schema di regolamento distingue tra firma elettronica e firma digitale. La prima consiste in un insieme di dati elettronici, connessi ad altri dati elettronici utilizzati per autenticare la firma. La firma digitale è invece un particolare tipo di firma elettronica, costituita da una chiave asimmetrica, di cui una privata (destinata ad essere conosciuta solo dal titolare, mediante la quale si appone materialmente la firma digitale sul documento) e una pubblica che, associata alla prima, consente di accertare l'autenticità della firma.

La novità più importante dello schema di regolamento sta nella disciplina dei certificatori delle firme elettroniche. Costoro sono distinti in tre categorie: **i certificatori in genere, i certificatori qualificati** e i **certificatori accreditati:**

• i primi svolgono il servizio di certificare le firme elettroniche. Per svolgere questa attività non è necessaria alcuna formalità o autorizzazione preventiva. Solamente, è previsto che il certificatore possegga i requisiti di onorabilità richiesti a chi svolga funzione di amministrazione, direzione e controllo presso istituti di credito. Il successivo accertamento dell'inesistenza o del venir meno di questo requisito comporta il divieto di proseguire l'attività di certificazione (la vigilanza è affidata al Dipartimento dell'innovazione e delle tecnologie presso la Presidenza del Consiglio dei Ministri);

• **il certificatore qualificato,** invece, deve possedere i requisiti previsti dal regolamento (tra l'altro, dimostrare affidabilità organizzativa, tecnica e finanziaria; impiegare personale dotato di conoscenze, esperienze e competenze specifiche; utilizzare sistemi affidabili che garantiscano la sicurezza tecnica e crittografica dei procedimenti; adottare adeguate misure contro la contraffazione dei certificati) e, prima di iniziare l'attività, deve darne comunicazione al citato Dipartimento. Quest'ultimo può procedere, d'ufficio o su segnalazione, all'accertamento della sussistenza dei requisiti e, se del caso, dispone il divieto di prosecuzione dell'attività. Questa categoria di certificatori rilascia certificati qualificati, che devono contenere alcune informazioni obbligatorie, come ad esempio l'indicazione che si tratta – appunto – di un certificato qualificato, il suo numero di serie, l'identità del certificatore e del titolare del certificato, l'indicazione del termine iniziale e del termine finale di validità del certificato;

• **il certificatore accreditato** è colui che ha il più elevato riconoscimento del possesso di requisiti di qualità e sicurezza. Per essere accreditati, non è sufficiente possedere i requisiti del certificatore qualificato, ma bisogna anche presentare un'apposita domanda al già citato Dipartimento, allegando il profilo professionale del personale responsabile della generazione dei dati per la creazione e la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati. Altri requisiti sono previsti se il richiedente è un soggetto privato (tra l'altro, deve trattarsi di una società di capitali, con un capitale sociale non inferiore a quello necessario per le attività bancarie). La domanda si considera accolta se non è rigettata nel termine di novanta giorni; all'accoglimento consegue l'iscrizione del richiedente in un apposito elenco tenuto presso il Dipartimento. Naturalmente, la certificazione proveniente da un certificatore appartenente all'una o all'altra delle categorie sopra indicata presenta diversi gradi di sicurezza e, talvolta, è richiesto che la firma elettronica sia autenticata da un certificatore appartenente a una certa categoria. Per esempio, i contratti stipulati con strumenti informatici, per essere validi ad ogni effetto di legge, devono essere sottoscritti almeno con la firma elettronica autenticata con certificato qualificato. La necessità di un certificatore accreditato riguarda invece per lo più i rapporti con la pubblica amministrazione. Per esempio, questa, per la sottoscrizione di documenti informatici di rilevanza esterna, può rilasciare direttamente certificati qualificati, previo accreditamento con la procedura prevista per i certificatori accreditati (ma, in questo caso, il terzo può utilizzare il certificato solo nei confronti dell'Amministrazione certificante), oppure deve rivolgersi a certificatori accreditati. Inoltre, chi intende presentare istanze o dichiarazioni alla pubblica amministrazione per via telematica, e non disponga della carta d'identità elettronica, deve possedere una firma elettronica autenticata da un certificatore accreditato. ■

a cura di Stefano Chiusolo
avvocato in Milano