DPCM 12 ottobre 2007 Autodichiarazione dei certificatori

La Presidenza del Consiglio dei Ministri ha emanato - su proposta del CNIPA – un provvedimento che consente ai certificatori accreditati di autodichiarare la conformità dei dispositivi sicuri per la generazione della firma digitale con procedure automatiche, per un periodo di 24 mesi dall'entrata in vigore del DPCM.
Ciò consentirà di agevolare lo sviluppo di sistemi di conservazione documentale, di fatturazione elettronica o di gestione delle informazioni sanitarie.
Il decreto è stato pubblicato sulla Gazzetta Ufficiale n. 13 del 16 gennaio 2008.

INTRODUZIONE

La firma digitale costituisce uno dei cardini del processo di e-government. Per quanto riguarda la PA, l'obiettivo, abilitante allo sviluppo dei servizi on line, si sviluppa su tre principali linee di intervento:

*** diffusione della firma digitale all'interno delle amministrazioni, con distribuzione a dirigenti e funzionari con potere di firma, e relativa formazione;**
*** intervento su applicazioni e servizi, per renderli accessibili in sicurezza tramite la firma digitale;**
*** iniziative specifiche di stimolo all'utilizzo della firma da parte di gruppi specifici di utenti esterni all'amministrazione.**

Nell'ambito delle attività come certificatore, sono circa 50 le amministrazioni coinvolte, mentre i certificati di firma digitale emessi al primo semestre del 2006 sono circa 40 mila.

Elenco dei certificatori di firma digitale
IL QUADRO NORMATIVO

L'Italia si è posta all'avanguardia nell'uso legale della firma digitale, essendo il primo paese ad avere attribuito piena validità giuridica ai documenti elettronici.
Fin dal lontano 1997 l'articolo 15 della L. 59/97 stabilisce infatti che "gli atti, dati e documenti formati dalla Pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge".
In base a tale norma, un documento siglato con firma digitale ha lo stesso valore del suo omologo cartaceo.
Le implicazioni sono notevoli anche per il settore privato: dalla validità dei contratti on line alla possibilità di emettere fatture commerciali o ordini di acquisto.
La normativa pre-direttiva sulla firma digitale, la firma elettronica e la conservazione del documento elettronico, prevedeva un'unica tipologia di certificato, di certificatore e di firma digitale.
Con il recepimento della Direttiva 1999/93/CE e l'emanazione del D. lgs n. 10/02 e del DPR 7 aprile 2003 n. 137, il quadro normativo di riferimento ha subito una profonda trasformazione; in particolare, l'articolo 6 del decreto di recepimento ha modificato l'articolo 10 del DPR n. 445/00, stabilendo che il documento informatico (da intendersi, ai sensi del Testo unico del 2000, come la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti e, quindi, non recante alcuna sottoscrizione elettronica), ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile.
Con l'entrata in vigore del Codice dell'amministrazione digitale (gennaio 2006), attraverso il Decreto legislativo 7 marzo 2005, n. 82, il valore probatorio del documento informatico ha subito una ulteriore modifica, difatti con il comma 2 dell'articolo 21, come modificato dal D.Lgs. 4 aprile 2006, n. 159, è stabilito che

"Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile.
L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria. ".
Il citato decreto legislativo rivede anche le tipologie di firma elettronica previste contemplando tre tipologie di firma:

*** firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.**
*** firma elettronica qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.**
*****
firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Le norme continuano a contemplare due tipologie di certificato (qualificato e non qualificato) e tre di certificatore (che rilascia certificati qualificati: accreditato o notificato; che rilascia certificati non qualificati).
Istanze e dichiarazioni inviate per via telematica da e verso la PA sono valide se sottoscritte mediante firma digitale basata su un certificato qualificato rilasciato da un certificatore accreditato e generata mediante un dispositivo sicuro per la creazione di firme elettroniche.

IL CERTIFICATORE

Per garantire l'identità dei soggetti che utilizzano la firma digitale e per fornire protezione nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività di certificazione, le norme vigenti in materia richiedono che il soggetto certificatore sia in possesso di particolari requisiti tecnici, organizzativi e societari.
Tali soggetti che rilasciano certificati qualificati si distinguono, come precedentemente detto, in certificatori accreditati e notificati.
La differenza sostanziale fra le due tipologie è che il certificatore accreditato si sottopone volontariamente ad apposita preventiva istruttoria atta a verificarne il possesso dei requisiti di legge;
il certificatore notificato inizia ad operare contastualmente alla comunicazione di inizio attività al CNIPA.
Entrambe le tipologie sono soggette ad attività di vigilanza.
Documenti informatici sottoscritti con firma digitale possono essere scambiati con le pubbliche amministrazioni solo se le firme digitali sono basate su certificati qualificati emessi da certificatori qualificati.
Al termine dell'istruttoria, se positivamente conclusasi, i soggetti che intendono ottenere il riconoscimento dello status di "certificatore accreditato", sono inseriti in apposito elenco pubblico, consultabile telematicamente, predisposto, tenuto ed aggiornato a cura del CNIPA.

LE REGOLE TECNICHE

Con la pubblicazione del DPCM del 13 gennaio 2004 (G. U. 27 aprile 2004, n. 98) sono state emanate le regole tecniche per la formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione, anche temporale, dei documenti informatici.
Il provvedimento disciplina la formazione della documentazione amministrativa tramite il supporto informatico, con particolare attenzione per la generazione, apposizione e verifica delle firme digitali.
Viene quindi portato a compimento il recepimento della Direttiva europea 1999/93/CE.
Questo provvedimento delinea i requisiti tecnici ed organizzativi che i soggetti, pubblici e privati, che intendono emettere certificati qualificati devono possedere.
Prescrive inoltre le caratteristiche peculiari che devono essere possedute dai soggetti che intendono ottenere il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza.
Con l'entrata in vigore di queste regole tecniche viene abrogato il DPCM 8 febbraio 1999.
Sulla gazzetta ufficiale n. 51 del 3 marzo 2005 sono state infine pubblicate le "Regole per il riconoscimento e la verifica del documento informatico", attraverso la Deliberazione CNIPA n.4 del 17 febbraio 2005, emanate ai sensi del comma 4 dell'articolo 40 del DPCM 13 gennaio 2004.
Queste ulteriori regole sono fondamentali per garantire l'interoperabilità della firma digitale, cioè la possibilità di verificare qualunque firma digitale con qualsiasi software di verifica purché conformi alle medesime regole.
Per tale ragione il rispetto delle stesse è obbligatorio da parte dei certificatori accreditati.

L'UTILIZZO DELLA FIRMA DIGITALE

Il CNIPA ha predisposto un documento dal titolo "Le Linee guida per l'utilizzo della firma digitale" concepito per supportare gli utenti e le aziende circa l'utilizzo della firma digitale e organizzato in modo tale che gli interessati possano effettuare la sua consultazione in modo mirato, seguendo un percorso specifico secondo le proprie esigenze.
In tal modo, sarà possibile comprendere dove acquistare la firma digitale, come utilizzarla e soprattutto come verificare la sua validità legale mediante gli strumenti gratuiti segnalati dal CNIPA.