Www.carelladarcangelo.com

Firma Digitale - Principali novità:

Marca temporale. La marca temporale è il risultato di una procedura informatica che consente di attribuire a un documento informatico una data e un orario opponibile ai terzi ai sensi dell'articolo 20, comma 3, del Codice dell'amministrazione digitale (c.d. validazione temporale). Il servizio di marcatura temporale (*timestamping*) di un documento informatico consiste nella generazione, da parte di un soggetto terzo "certificatore", di una firma digitale del documento, cui è associata l'informazione relativa ad una data e ad un'ora certa. Concretamente, la marca temporale (*timestamp*), emessa dall'ente certificatore, consiste in una sequenza di caratteri che rappresentano una data e/o un orario per accertare l'effettivo avvenimento di un certo evento. La data è, di solito, presentata in un formato consistente, in modo che sia facile da comparare con un'altra per stabilirne l'ordine temporale. Esempi di marche temporali: *2005-10-30 T 10:45 UTC* ; *Sat Jul 23 02:16:57 2005.*

Novità sulla marca temporale. Il previgente quadro normativo prevedeva che le marche temporali fossero conservate dall'ente certificatore in un apposito archivio informatico non modificabile per un periodo non inferiore a 5 anni. Inoltre, subordinava la validità delle stesse al solo periodo di conservazione a cura del fornitore del servizio, vale a dire che, superati i 5 anni, i documenti "marcati temporalmente" rischiavano di non avere più la stessa rilevanza civilistica/fiscale. Il nuovo Dpcm (art. 49) risolve il problema, disponendo che tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio non modificabile per un periodo non inferiore a venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.

Firma digitale. "*La firma digitale è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una privata e una pubblica, 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*" (D.Lgs. 07/03/2005 n. 82 - Codice dell'Amministrazione Digitale). La firma digitale è l'equivalente elettronico di una tradizionale firma autografa apposta su carta. Attenzione: essa, però, non va confusa con la "firma elettronica", che è altra cosa. Il documento informatico sottoscritto con la firma digitale assume piena efficacia probatoria circa la data, l'ora e la paternità del documento. La firma digitale è, quindi, associata stabilmente al documento informatico (in pratica, è un suo allegato) e lo arricchisce di informazioni che ne attestano con certezza l'integrità, l'autenticità, la non ripudiabilità. Spiegare il funzionamento della firma digitale è assai complesso. Semplificando, si può dire che essa funziona sulla base di una coppia di "chiavi crittografiche", una "privata" ed una "pubblica", correlate tra loro. A quest'ultima si associa un "certificato qualificato di firma", che viene rilasciato da un "ente certificatore" (lo stesso delle marche temporali). Il certificato di firma, in pratica, è un file - generato seguendo precisi standard stabiliti per legge - che contiene informazioni sull'identità del titolare, sulla chiave pubblica attribuitagli al momento del rilascio, sul periodo di validità del certificato stesso. Nel certificato sono presenti anche i dati dell'ente certificatore. Quest'ultimo provvede alla tenuta di un elenco pubblico dei certificati di firma. Il certificato di firma garantisce la corrispondenza tra la chiave pubblica e l'identità del Titolare. Se un soggetto vuole creare una firma per un documento, procede nel modo seguente: a) mediante una una "funzione di *hash*" (= uno strumento che, dato un qualunque messaggio, di una qualunque lunghezza, ne produce un'impronta di lunghezza prefissata, di solito un file dell'ordine di 100-200 bit) ricava una impronta digitale del documento stesso (creazione dell'impronta digitale del documento informatico); b) dopodiché, utilizza la propria chiave privata per cifrare l'impronta digitale e di questa cifratura equivale alla firma (cifratura

dell'impronta digitale); c) a questo punto, la firma viene allegata al documento (allegazione al documento informatico); d) per verificare l'autenticità di un documento il destinatario decifra la firma del documento con la chiave pubblica del mittente, ottenendo l'impronta digitale del documento (decifratura dell'impronta digitale); e) infine, confronta quest'ultima con quella che si ottiene applicando la funzione di *hash* al documento ricevuto: se le due impronte sono uguali, l'autenticità e l'integrità del documento sono garantite (applicazione della funzione di *hash*).

Novità sulla firma digitale. Essendo la firma digitale subordinata alla validità di un certificato qualificato di firma, alla scadenza di quest'ultimo i documenti rischiavano di non essere più validi. Le nuove regole tecniche introducono nuovi termini e disciplinano più chiaramente il valore della firma digitale nel tempo. L'articolo 51 del Dpcm dispone, infatti, che la firma digitale, anche nel caso in cui sia scaduto, revocato o sospeso il certificato qualificato di firma a essa associato, è valida se a essa è associabile un riferimento temporale opponibile ai terzi che colloca la generazione della firma in un momento precedente alla scadenza, alla revoca o alla sospensione del certificato. I riferimenti temporali opponibili ai terzi sono costituiti, secondo il medesimo decreto, oltre che dalla marca temporale, dal riferimento contenuto nella segnatura di protocollo, dal riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti ad opera di un pubblico ufficiale o di una pubblica amministrazione, dal riferimento temporale ottenuto attraverso la posta elettronica certificata e dal riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica. A questi riferimenti specifici vanno aggiunti quelli dettati dai principi generali, come l'articolo 2704 del codice civile.