

La Firma Digitale

Dicembre 2009

Agenda

- > Introduzione
- > La normativa
- > La tecnologia:
 - la crittografia, il certificatore, i dispositivi
- > Validità nel tempo
- > I vantaggi



Introduzione

La firma digitale è un sistema che consente:

- > **Autore:** rendere manifesta l'**autenticità** di un documento informatico, analogamente a quanto avviene apponendo la firma autografa su un documento cartaceo
- > **Destinatario:** verificare l'**integrità** e la **provenienza** del documento informatico

La firma digitale si può definire come l'equivalente elettronico di una tradizionale firma autografa con il medesimo valore legale

Normativa di riferimento

Legge n. 59 del 15.03.1997 > Legge c.d. “Bassanini 1”

D. Lgs. n.82 del 07.03.2005 > Codice dell’ Amministrazione Digitale

D. lgs. n. 159 del 04.04.2006 > Disposizioni integrative e correttive del Codice dell’Amministrazione Digitale

Decreto del Presidente del Consiglio dei Ministri del 30.03.2009 > Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici
(sostituisce DPCM 13/01/04)

Normativa

Legge n. 59 del 15.03.1997

Stabilisce 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**

Normativa

D. Lgs 82/2005 – Codice dell'Amministrazione Digitale

D. lgs. n. 159 del 04.04.2006

- > Disposizioni concernenti documenti informatici, firme elettroniche, nonché formazione, gestione, conservazione e trasmissione di documenti informatici
- > Obiettivo: **assicurare, da parte delle PP.AA. centrali e locali, la disponibilità, la gestione e la fruibilità dell'informazione in modalità digitale**
- > Il Codice dell'Amministrazione Digitale prevede l'applicazione del DPCM 13/01/04 (Regolamento tecnico) ora sostituito dal DPCM 30/03/09

Normativa

D. Lgs 82/2005 – Codice dell'Amministrazione Digitale

Definizione di “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 (*art.1, lettera s*)
- > per la generazione della **firma digitale** deve adoperarsi un **certificato qualificato** che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso (*art. 24*)

Normativa

D. Lgs 82/2005 – Codice dell'Amministrazione Digitale

Requisito di “forma scritta”:

- > Il **documento informatico** sottoscritto con firma elettronica qualificata o con **firma digitale**, formato nel rispetto delle regole tecniche [...], che garantiscano **l'identificabilità** dell'autore, **l'integrità** e **l'immodificabilità** del documento, si presume riconducibile al titolare del dispositivo di firma [...], **e soddisfa comunque il requisito della forma scritta**, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, 1°co., numeri da 1 a 12 del codice civile (*art. 20*)

Normativa

D. Lgs 82/2005 – Codice dell'Amministrazione Digitale

Valore probatorio del documento informatico sottoscritto:

- > 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 (*art. 21*)

** Art. 2712. Riproduzioni meccaniche. — Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.*

Normativa

D. Lgs 82/2005 – Codice dell'Amministrazione Digitale

Valore probatorio del documento informatico:

- > Il **documento informatico** ha l'efficacia probatoria prevista dall'art. 2712* del c.c., riguardo ai fatti ed alle cose rappresentate. Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate (art. 23)

* Art. 2712. Riproduzioni meccaniche. — Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

Normativa

D. Lgs 1182/2005 – Codice dell'Amministrazione Digitale

Disconoscimento della Firma Digitale:

- > **Prima** del Codice dell'Amministrazione Digitale: **il documento con firma digitale** faceva “piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l’ha sottoscritto”. **Era perciò equiparato ad un documento cartaceo con firma autografa autenticata da pubblico ufficiale**. La firma non era disconoscibile, e il documento era impugnabile solo con lo strumento della querela di falso.
- > **Ora: il documento ha l’efficacia prevista dall’ art. 2702 c.c.**, “fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l’ha sottoscritto, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è **legalmente considerata riconosciuta**”. Il documento ora è **impugnabile** non solo con lo strumento della querela di falso: infatti **la firma è disconoscibile**, se viene fornita prova che l’utilizzo del dispositivo di firma non è riconducibile al titolare

Normativa

DPCM 30/03/2009 – Nuove Regole Tecniche

Le novità principali:

- > Il **Titolare** può avere in uso esclusivo una sola delle due chiavi **della firma digitale (chiave privata e PIN)**
- > La **marca temporale** deve essere conservata dal Certificatore per almeno **20 anni**
- > Un **documento** firmato digitalmente può essere **valido** anche oltre la **scadenza del certificato** purché venga associato ad un **riferimento temporale certo** prima della scadenza (p.e. Marca temporale).

La tecnologia – Crittografia a chiave pubblica

- > La **Firma Digitale** si basa su una particolare forma di crittografia definita “**asimmetrica**” o a “chiave pubblica”
- > Il dispositivo di firma viene utilizzato per generare una **coppia di chiavi “asimmetriche”** biunivocamente associate
- > La chiave privata è **segreta** e non **può essere esportata** dal dispositivo
- > La chiave pubblica viene **associata al certificato di firma digitale** in modo che chi lo riceve possa effettuare la verifica
- > La chiave privata “**firma**” (cifra) i documenti
- > La chiave pubblica “**verifica**” (decifra) i documenti

La tecnologia – Realizzazione della firma digitale

- > La **Firma Digitale** viene realizzata “**cifrando**” con la chiave privata l'impronta (**hash**) del documento
 - Cifrare tutto il documento potrebbe richiedere anche molto tempo
- > Successivamente il **documento originario** viene “**imbustato**” insieme **all'hash “cifrato”** ed al **certificato di firma digitale** che contiene la chiave pubblica
- > La “**busta crittografica**” assume, tipicamente, lo standard **.p7m**
- > Il **destinatario**, aprendo la busta, può **risalire al documento iniziale** ed ai suoi attributi (compresa la firma digitale).

La tecnologia – Il Certificatore

- > La **Firma Digitale (da sola)** garantisce l'integrità del documento ma non la reale identità del titolare
- > Il Certificatore ha il compito di:
 - **Accertare**, prima del rilascio, la reale **identità del titolare**
 - **Creare** il Certificato Digitale contenente le **informazioni sul Titolare** e la chiave pubblica
 - **Consentire l'accesso** al registro dei certificati delle **chiavi pubbliche**
 - **Mantenere una lista** dei certificati **sospesi e/o revocati** (CRL)

La tecnologia – I dispositivi

- > La **Firma Digitale** deve essere realizzata utilizzando **dispositivi sicuri** in grado di:
 - Generare e custodire la coppia di chiavi
 - Impedire l'esportazione della chiave privata
- > I **dispositivi sicuri** più utilizzati sono:
 - **Smart Card a microprocessore** (deve essere utilizzata con un apposito lettore)
 - **Token USB** (utilizzano lo stesso chip delle smart card e aggiungono anche lettore e software per la firma digitale)
 - **HSM (Hardware Security Module)** che può contenere molti certificati e ha elevate prestazioni

La validità nel tempo

- > La **Marca Temporale** è una tecnica che consente di attribuire data certa ad un documento informatico
- > La **Marca Temporale** utilizza la stessa tecnica della firma digitale con l'aggiunta di un riferimento temporale preciso e affidabile:
 - Viene **creato l'hash** del file da marcare
 - Viene **spedito l'hash** al servizio di marcatura del **Certificatore**
 - Il certificatore **cifra l'hash** con la propria chiave privata
 - Il certificatore aggiunge: un **identificativo** dell'emittente, il **numero di serie** della marca, il **riferimento temporale**
- > Il **riferimento temporale** emesso dal Certificatore è **opponibile a terzi**

I Vantaggi

- > **Economicità** dei sistemi di archiviazione
- > Certezza dell'**integrità** del dato sottoscritto
- > Certezza assoluta dell'**identità** del sottoscrittore (non servono periti!)
- > **Impossibile falsificare** firma o documento
- > Possibilità di fare molti "**originali**" a **costo zero**
- > Possibilità del **riuso** del contenuto digitale con procedure automatiche
- > **Velocità** di ricerca e reperimento di informazioni anche tra moli elevate di documenti
- > **Facilità e basso costo** per la trasmissione a distanza