

# ALLEGATO 3 - FIRMA DIGITALE E FIRME ELETTRONICHE

Il DPCM 22 febbraio 2013 stabilisce, ai sensi degli articoli 20, 24, comma 4, 27, 28, 29, 32, 33, 35, comma 2, e 36, del Codice dell'Amministrazione Digitale (CAD), le regole tecniche per la generazione, apposizione e verifica della firma elettronica avanzata, qualificata e digitale, per la validazione temporale, nonché per lo svolgimento delle attività dei certificatori qualificati.

Il Codice dell'Amministrazione digitale distingue tra quattro tipologie di firma e cioè:

**1. FIRMA ELETTRONICA SEMPLICE (lett. q)** - L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

Valore giuridico: Questo tipo di firma ha un valore probatorio liberamente valutabile dal giudice in fase di giudizio, in base a caratteristiche oggettive di qualità e sicurezza.

**2. FIRMA ELETTRONICA AVANZATA (lett. q-bis)** - Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

Valore giuridico: Il documento informatico sottoscritto con firma elettronica avanzata, formato nel rispetto delle regole tecniche, è valido fino a querela di falso; comporta l'inversione dell'onere della prova per il suo disconoscimento. L'utilizzo della firma elettronica avanzata permette, inoltre, di realizzare in modalità informatica gli atti che per legge devono essere realizzati in forma scritta, salvo i casi in cui la stessa legge richiede l'utilizzo della firma digitale o della firma elettronica qualificata.

**3. FIRMA ELETTRONICA QUALIFICATA (lett. r)** - Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

**4. FIRMA DIGITALE (lett. s)** - Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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.

Valore giuridico: Il documento informatico sottoscritto con firma elettronica qualificata o firma digitale, formato nel rispetto delle regole tecniche, è riconosciuto valido a tutti gli effetti di legge e soddisfa il requisito della forma scritta. In altre parole, questi strumenti permettono la valida realizzazione in modalità informatica di tutti gli atti per i quali la legge richiede che sia utilizzata la forma scritta. Inoltre, per la validità di alcuni atti, di particolare importanza (individuati dall'art. 1350 c.c., punti 1-12, come ad es. gli atti di compravendita di beni immobili o mobili registrati, le locazioni ultranovenali, le costituzione di società, ecc.) è necessario l'utilizzo di queste due tipologie di firma (mentre non è possibile utilizzare la firma elettronica avanzata).

L'art. 21 del CAD, ha introdotto al comma 1 un riferimento alla "firma elettronica avanzata" in conseguenza dell'attribuzione a tale tipologia di firma di nuova dignità e rilevanza giuridica.

Lo stesso art. 21 del CAD sancisce, dal punto di vista del valore probatorio, che il documento informatico, cui è apposta una firma elettronica, è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Il titolare è la persona fisica cui è attribuita la firma elettronica/digitale e che ha accesso al dispositivo per la creazione della firma digitale e/o elettronica.

Il documento informatico e i messaggi trasmessi mediante posta ordinaria e/o certificata con accesso protetto da user name e password personali s'intendono sottoscritti con firma elettronica

dal mittente titolare della casella e degli stessi user name e password.

Tali documenti sono idonei a soddisfare il requisito della forma scritta e sono validi e rilevanti agli effetti di legge nei limiti stabiliti dalle norme vigenti in materia.

Sono abilitati a sottoscrivere documenti informatici con firma digitale e/o elettronica qualificata gli amministratori e i dipendenti comunali titolari dell'apposito dispositivo (anche firma digitale remota). Il dispositivo di firma e i relativi codici sono strettamente personali e non possono essere affidati o rivelati a terzi.

#### Ambito di utilizzo della firma elettronica

La sottoscrizione di messaggi e documenti trasmessi mediante posta elettronica avente validità di firma elettronica è utilizzabile in generale per i documenti esclusi dalla registrazione obbligatoria di protocollo e in particolare nelle comunicazioni interne ed esterne riguardanti inviti, partecipazioni, ringraziamenti, auguri e simili, nonché per tutti gli atti che per loro natura non rivestono alcuna rilevanza giuridico-amministrativa quali informative, appunti memorie informali, e simili. Ai sensi dell'art. 61 del DPCM 22 febbraio 2013 "L'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera c -bis ) del Codice, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del decreto 2 novembre 2005 recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata» sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche."

E' consentito altresì utilizzare le firme elettroniche quando espressamente consentito dalla legge come alternativa alla firma digitale.

#### Ambito di utilizzo della firma digitale

La firma digitale dev'essere utilizzata per la sottoscrizione di documenti facenti parte di processi o procedimenti amministrativi completamente informatizzati, nonché per la sottoscrizione di atti appartenenti a categorie che l'Amministrazione ha deciso di digitalizzare fatto salvo quando espressamente prevista dalla legge.

Dovrà essere altresì utilizzata se non disposto diversamente:

- a) nei rapporti con cittadini, imprese o altre pubbliche amministrazioni;
- b) di norma nelle comunicazioni con pubbliche amministrazioni relativamente ad atti facenti parte di procedimenti amministrativi, ovvero appartenenti a procedimento o processi informatizzati;
- c) per tutti i documenti ai quali s'intende attribuire una valenza particolare o una rilevanza giuridico-amministrativa.

#### Trasmissione dei documenti sottoscritti con firma digitale

I documenti sottoscritti con firma digitale sono trasmessi di norma tramite la posta elettronica certificata.

La registrazione di protocollo dei documenti informatici ricevuti per posta elettronica PEO/PEC è effettuata in modo da far corrispondere ad ogni messaggio una registrazione, la quale si può riferire sia al corpo del messaggio e sia ad uno o più file ad esso allegati (Art. 18, commi 1 e 2, DPCM 31 dicembre 2013).

Il calcolo dell'impronta previsto nell'operazione di registrazione di protocollo è effettuato per tutti i file allegati al messaggio di posta elettronica ricevuto (Art. 19, comma 1, DPCM 31 dicembre 2013).

#### Modalità di apposizione della firma digitale

Per apporre la Firma Digitale possono essere utilizzati tutti quei dispositivi classificabili quali Secure Signature Creation Device

Ad oggi gli strumenti previsti sono le Smart Card, i Token USB e i dispositivi HSM (firma remota).

Il file firmato verrà salvato assumendo l'ulteriore estensione .p7m che costituisce il formato tradizionale utilizzato per la firma elettronica. Lo standard di riferimento è la specifica ETSI TS 101 733 nota anche come CadES. Tale formato consente di apporre tutte le tipologie di firma previste dalla normativa: singola, parallela, controfirma e enveloped. I file generati hanno una struttura

binaria (rigida), assumono l'estensione .p7m e sono leggibili solo dai software di verifica. Viene prevista inoltre la possibilità di generare file firmato in formato PDF che rappresenta il tipo di firma digitale definito all'interno della specifica PDF mantenuta da Adobe nota anche come PAdES (file con estensione pdf).

### **Marca temporale**

Il protocollo informatico è lo strumento per assegnare valore giuridico probatorio ai documenti dell'Amministrazione: la registrazione di protocollo certifica che un determinato documento è autentico, cioè è possibile attribuirgli una provenienza certa ed una data certa. La marca temporale è una sequenza di caratteri contenenti una data ed un orario preciso, generata da una Time Stamping Authority (TSA), terza parte fidata.

Un file marcato temporalmente ha estensione .m7m: al suo interno contiene il documento del quale si è chiesta la validazione temporale. La TSA è sincronizzata con il segnale emesso da un soggetto terzo.

La marcatura temporale consente di datare in modo certo un documento rendendo opponibile a terzi.

Viene prevista la possibilità di apporre a particolari fattispecie documentali (es. contratti redatti nella forma pubblica amministrativa) la marca temporale anche se registrata nel protocollo informatico.

Vedasi il Titolo IV del DPCM 22 febbraio 2013.