CITTÀ di PINEROLO

MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI (artt. 3 e 5 DPCM 3 dicembre 2013)

ALLEGATO N. 12

FIRMA DIGITALE E FIRME ELETTRONICHE INDICAZIONI

Cronologia revisioni			
Data	Versione	Provvedimento di approvazione	Descrizione

Sommario

1 *Premessa*

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.

Come è noto allo stato attuale il Codice dell'Amministrazione digitale (previste dall'art. 1) distingue tra quattro tipologie di firma e cioè:

- **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.

- **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.

- **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;

- **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 titolari delle credenziali di protezione.

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.

2 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.

3 Ambito di utilizzo della firma digitale

La firma digitale deve essere utilizzata per la sottoscrizione di documenti facenti parte di processi o procedimenti amministrativi completamente informatizzati, per le copie digitali di originali

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

4 Trasmissione dei documenti sottoscritti con firma digitale

I documenti sottoscritti con firma digitale sono trasmessi di norma tramite la posta elettronica certificata, se i documenti richiedono registrazione di protocollo dovrà essere utilizzata la PEC ufficiale abbinata alla AOO (in questo caso, dopo la protocollazione e automatico l'invio dei documenti).

5 Gestione degli allegati

Per allegato si intende un documento unito a un documento o a una pratica per prova, per chiarimento o integrazione di notizie, per memoria.

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).

In analogia con la gestione dei documenti cartacei in vigore presso questo Comune, che non prevede l'obbligo di firma degli allegati uniti ai singoli documenti e tenuto conto del valore accessorio degli stessi, si ritiene che non sia necessaria la firma digitale dei singoli allegati, ma sia sufficiente l'apposizione della stessa al documento principale.

Gli allegati andranno perciò gestiti mediante descrizione al protocollo ed eventualmente, ove disponibile il testo, associazione del file al programma gestionale.

6 Modalità di apposizione della firma digitale.

Per apporre la Firma Digitale possono essere utilizzati tutti quei dispositivi classificabili quali "*Secure Signature*" "*Creation Device*" ai sensi dell'Allegato III della Direttiva Europea sulle Firme Elettroniche (DIRETTIVA 1999/93/CE) e cioè dispositivi fisici che contengono oggetti (chiavi private, chiavi pubbliche e certificati digitali), attraverso i quali eseguono operazioni crittografiche.

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).

7 L'apposizione di firme e informazioni su documenti firmati

Il presente paragrafo si pone l'obiettivo di chiarire alcuni aspetti generali dei formati di firma CAdES (file con estensione p7m) e PAdES (file con estensione pdf) e la loro attitudine ad ospitare più firme e informazioni disponibili solo dopo la generazione della firma digitale quali, ad esempio, la segnatura di protocollo prevista dall'articolo 55 del D.P.R. 28 dicembre 2000, n. 445.

Come noto, un documento sottoscritto con firma digitale ha nel nostro ordinamento piena efficacia giuridica, a condizione che non sia modificato dopo l'apposizione della firma.

Con la diffusione dell'uso dei documenti informatici, sono sempre più numerose le richieste di chiarimento sul corretto utilizzo della firma digitale, con particolare riferimento ai casi in cui sia necessario apporre più firme su un medesimo documento o in cui si intenda aggiungere dei dati dopo la sottoscrizione, ad esempio, allo scopo di riportare gli estremi della segnatura di protocollo di un documento spedito o ricevuto da una pubblica amministrazione.

Senza entrare in dettagli tecnici, la firma digitale consiste nella creazione di un file, definito "busta crittografica", che racchiude al suo interno il documento originale, l'evidenza informatica della firma e la chiave per la verifica della stessa, che, a sua volta, è contenuta nel certificato emesso a nome del sottoscrittore. L'autenticità del certificato è garantita da un'Autorità di certificazione, in Italia, dai certificatori accreditati ai sensi dell'articolo 29 del CAD (D.Lgs. n. 82/2005).

Gli standard europei prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CAdES, PAdES e XAdES, modalità di sottoscrizione adottate anche in Italia. Ai fini del presente documento si tratteranno solo i primi due tipi.

7.1 La firma CAdES

La busta CAdES è un file con estensione .p7m, il cui contenuto è visualizzabile solo attraverso idonei software in grado di "sbustare" il documento sottoscritto. Tale formato permette di firmare qualsiasi tipo di file, ma presenta lo svantaggio di non consentire di visualizzare il documento oggetto della sottoscrizione in modo agevole. Infatti, è necessario utilizzare un'applicazione specifica.

Per il formato CAdES l'apposizione di due o più firme può essere effettuata in due modi:

- re-imbustando in una nuova busta CAdES la busta generata dalla sottoscrizione precedente (c.d. controfirma o "firma matrioska");
- aggiungendo nella busta ulteriori firme, accompagnate dai relativi certificati (c.d. firme congiunte).

In entrambi i casi è presente un'unica versione del documento, che pertanto può solo essere oggetto di ulteriori firme digitali senza modificarne il contenuto.

Nel caso di documenti sottoscritti in formato CAdES, come si è detto, non è possibile gestire diverse versioni di uno stesso documento all'interno della busta crittografica, pertanto, nell'ipotesi in cui si voglia riportare sul documento delle annotazioni successive alla sottoscrizione (ad esempio i

dati della segnatura di protocollo), sarà necessario esportare il documento nel formato originario, ossia non firmato, per apportarvi le annotazioni. Tali modifiche, infatti, sarebbero apportate nell'unica versione del documento presente all'interno della busta CAdES, operazione questa che renderebbe le firme invalide. E' evidente il limite di questa tipologia di firma. Nell'esempio fatto, si avrebbero due documenti: uno con la firma digitale del sottoscrittore del documento, l'altro con la segnatura di protocollo ma privo della firma digitale del sottoscrittore.

7.2 La firma PAdES

La firma digitale in formato PAdES è un file con estensione .pdf, leggibile con i comuni "*reader*" disponibili per questo formato. Questa tipologia di firma, nota come "firma PDF", prevede diverse modalità per l'apposizione della firma, a seconda che il documento sia stato predisposto o meno ad accogliere le firme previste ed eventuali ulteriori informazioni, rende il documento più facilmente accessibile, ma consente di firmare solo documenti di tipo PDF. Il formato PDF consente inoltre di gestire diverse versioni dello stesso documento senza invalidare le firme digitale apposte. Altra interessante caratteristica è che il documento in formato PDF consente di collocare fisicamente la firma digitale in un preciso punto del documento. Tale caratteristica è particolarmente utile nel caso di sottoscrizione di clausole vessatorie o, comunque, in ogni caso in cui la collocazione della firma abbia una qualche valenza.

Qualora il documento non fosse stato predisposto per tutte le firme necessarie, è comunque possibile apporre ulteriori firme senza invalidare le precedenti. A tale scopo, il formato PAdES implementa la funzione della gestione delle versioni (*versioning*): ogni versione successiva alla prima, contiene la versione integrale, non modificata, del documento precedente (comprese le firme digitali).

Ogni modifica al documento (ulteriore firma o aggiunta di testo o immagini) produce, infatti, una nuova versione che contiene la versione originale non modificata. Tale caratteristica della busta PAdES rende questo formato particolarmente idoneo anche nel caso in cui si renda necessario apportare delle modifiche al documento dopo averlo sottoscritto, ad esempio per riportarvi delle annotazioni, come i dati degli estremi di protocollo che sono disponibili solo successivamente alla sottoscrizione del documento stesso. Ad una prima analisi, un documento sottoscritto sul quale sono riportate tali annotazioni potrebbe apparire corrotto in quanto modificato dopo la firma, tuttavia nella busta PAdES è presente ed è accessibile anche la versione non modificata del documento, che pertanto conserva piena efficacia giuridica. Non devono, infatti trarre in inganno i messaggi mostrati dal "*reader*" del documento "Almeno una delle firme non è valida" e "Il documento dopo la firma è stato modificato o si è danneggiato", in quanto è comunque possibile accedere alla versione del documento correttamente sottoscritta, coerentemente con quanto previsto dalle regole tecniche di cui al D.P.C.M. del 22 febbraio 2013.

8 Verifica delle firme elettroniche qualificate e digitali

Vedasi l'art. 14 del DPCM 22 febbraio 2013.

9 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.