COMUNE DI
GUSPINI

SERVIZIO SEGRETERIA, AFFARI GENERALI

INNOVAZIONE TECNOLOGICA – SERVIZIO SISTEMI INFORMATIVI, E-GOVERNMENT E COMUNICAZIONE

MANUALE DI GESTIONE

PROTOCOLLO, DOCUMENTI ED ARCHIVIO

AI SENSI DEL D.P.C.M. 3 DICEMBRE 2013

ALLEGATO 04 – FIRMA DIGITALE E FIRME ELETTRONICHE

INDICE

FONTI NORMATIVE

Il DPCM 22 febbraio 2013, come previsto dagli artt. 24, 25 comma 4, 27, 28, 29, 32, 33 35 comma 2 e 36 del Codice dell'Amministrazione Digitale (CAD), stabilice, le regole tecniche per la generazione, apposizione e verifica della firma elettronica avanzata, qualifica e digitale, per la validazione temporale, e per lo svolgimento delle attività dei certificatori qualificati.

Il CAD (D.Lgs. 82/2005) all'art. 1 comma 1 e il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio all'art. 3, richiamato dal CAD all'art. 1 comma 1-bis prevede quattro tipologie di firma:

- **Firma elettronica.** (art. 3 Punto 10 del Regolamento UE n. 910/2014) definita come "*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*";

  Il valore giuridico di questa tipologia viene dal punto di vista probatorio risulta liberamente valutabile dal giudice in fase di giudizio, che valuterà le caratteristiche oggettive di qualità e sicurezza.

- **Firma elettronica avanzata** (art. 3 Punto 10 del Regolamento UE n. 910/2014) definita come "*una firma elettronica che soddisfi i requisiti di cui all'articolo 26*";

  L'art. 26 del Regolamento UE n. 910/2014, recita: considera "Una firma elettronica avanzata soddisfa i seguenti requisisti:
  a) è connessa unicamente al firmatario;
  b) è idonea a identificare il firmatario;
  c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
  d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati."

  In questo caso il valore giuridico attribuito ad un documento informatico sottoscritto con questa tipologia di firma, se formato nel rispetto delle regole tecniche, è valido fino a querela di falso; ciò comporta l'inversione dell'onere della prova per il suo disconoscimento. L'utilizzo di questa tipologia di firma consente, di formare in modalità informatica gli atti che per legge devono essere redatti in forma scritta, salvo i casi in cui la legge richiede l'utilizzo della firma digitale o della firma elettronica qualifica.

- **Firma elettronica qualificata** (art. 3 Punto 10 del Regolamento UE n. 910/2014) definita come "*una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche*"

- **Firma digitale** (art. 1 lett. s) definita dal CAD come "*un particolare tipo di firma qualificata avanzata 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*"

  Il valore giuridico di queste ultime due tipologie di firma digitale, quanto formato nel rispetto delle regole tecniche, viene riconosciuto valido a tutti gli effetti di legge, soddisfa il requisito della forma scritta. Con questi strumenti è possibile creare in modalità informatica tutti gli atti cui la legge

richiede che sia utilizzata la forma scritta. Per alcuni particolari tipi di atti (individuati nel Codice Civile all'art. 1350, ai punti da 1 a 12 quali atti di compravendita di beni immobili o mobili registrati, costituzione di società ecc.) viene richiesta esclusivamente l'utilizzo di una di queste due firme, mentre le altre non sono ritenute valide.

Il CAD, all'art. 21, inserisce un riferimento alla firma elettronica avanzata poiché a tale tipologia di firma digitale viene dato una rilevanza giuridica, sancendo che il valore probatorio di un documento informatico sottoscritto da una firma elettronica, è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Quando ci si riferisce al titolare si intende la persona fisica cui è attribuita la firma elettronica/digitale e che ha accesso al dispositivo che consente di apporre la firma.

Va sottolineato che i documenti informatici e i messaggi trasmessi tramite posta ordinaria e/o certificata con accesso protetto da nome utente (userid) e password si intendono sottoscritti con firma elettronica del mittente titolare della casella. I documenti così trasmessi sono da considerarsi validi a soddisfare il requisito della forma scritta e agli effetti di legge validi e rilevanti (vengono in pratica considerati sottoscritti con una delle prime due tipologie di firme.

Possono sottoscrivere documenti informatici con firma digitale e/o elettronica qualificata gli amministratori e i dipendenti comunali titolari di apposito dispositivo (anche firma digitale remota).

I dispositivi di firma e le relative credenziali per l'utilizzo sono strettamente personali e non devono essere mai affidati o rivelati a terzi.

AMBITO DI UTILIZZO DELLA FIRMA ELETTRONICA

I documenti trasmessi mediante posta elettronica avente validità di firma elettronica è utilizzabile in generale per i documenti non sottoposti a registrazione obbligatoria di protocollo, e in particolare nelle comunicazioni interne ed esterne che abbiano ad oggetto inviti, partecipazioni, ringraziamenti, auguri ecc., nonché per tutti gli atti che per loro natura non rivesto rilevanza giuridico-amministrativa quali informative, appunti, memorie informali e similari.

L'art. 61 del DPCM 22 febbraio 2013 dispone che "*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."*

Quando espressamente consentito dalla legge, in alternativa alla firma digitale, si possono utilizzare altre firme elettroniche (esempio il Adobe EchoSign®)

AMBITO DI UTILIZZO DELLA FIRMA DIGITALE

Per la sottoscrizione di documenti facenti parte di processi o provvedimenti amministrativi completamente informatizzati, la sottoscrizione di atti appartenenti a categorie che l'Amministrazione ha deciso di digitalizzare (esclusi i casi previsti dalla legge) deve essere utilizzata la firma digitale.

La firma digitale dovrà inoltre essere utilizzata (se non disposto diversamente):

- nei rapporti con cittadini, imprese o altre pubbliche amministrazioni;
- Nelle comunicazioni con pubbliche amministrazioni per gli atti non facenti parte di procedimenti amministrativi, o appartenenti a procedimenti o processi informatizzati;
- Per ogni tipologia di documento a cui si desidera assegnare una particolare valenza o rilevanza dal punto di vista giuridico-amministrativa.

TRASMISSIONE DEI DOCUMENTI SOTTOSCRITTI CON FIRMA DIGITALE

Di norma i documenti che vengono sottoscritti con firma digitale vengono trasmessi tramite posta elettronica certificata.

GESTIONE DEGLI ALLEGATI

Un allegato viene inteso come un documento unito ad altro documenti o ad una pratica che abbia la funzione di comprovare, chiarire o integrare notizie.

Ai fini di una corretta utilizzazione dei documenti dal punto di vista giuridico sarà buona norma inserire nel documento il numero degli allegati e la loro descrizione sintetica.

La registrazione di protocollo di documenti informatici ricevuti tramite posta elettronica (ordinaria o certificata) viene effettuata in modo da far corrispondere al singolo messaggio una registrazione, riferita sia al corpo del messaggio sia a uno o più file allegati al messaggio come previsto dall'art. 18 commi 1 e 2 del DPCM 31 dicembre 2013.

Il calcolo dell'impronta, come previsto dall'art. 19, comma 1, DPCM 13 dicembre 2013, previsto nell'operazione di registrazione di protocollo è effettuato per ogni singolo allegato al messaggio di posta elettronica ricevuto.

Normalmente non si ritiene necessario (così come avviene per gli allegati ai documenti cartacei), la firma degli allegati uniti ai singoli documenti, in quanto sufficiente l'apposizione della stessa al documento principale.

Gli allegati verranno descritti nella registrazione di protocollo e associati al programma Gestionale di Protocollo.

MODALITÀ DI APPOSIZIONE DELLA FIRMA DIGITALE

Per l'apposizione della firma digitale occorre utilizzare dispositivi che rientrino tra quelli classificabili "Secure Signature Creation Device" come stabilito dall'allegato II del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio.

Si tratta di dispositivi fisici che contengono le chiavi private, pubbliche e certificati digitali, attraverso i quali sono eseguite le operazioni di crittografia per l'apposizione della firma. Tra gli strumenti disponibili allo stato attuale ricordiamo le Smart Card, i Token USB e i dispositivi di firma remota (HSM).

Il file una volta firmato verrà salvato e se si utilizza la tecnologia CAdES (specifiche ETSI TS 01 733) avrà l'estensione .P7M, mentre se si utilizzerà la tecnologia PAdES il file firmato generato avrà estensione .PDF. La tecnologia PAdES è utilizzabile solo a partire da un file .PDF, mentre la CAdES può essere utilizzata con tutte le tipologie di files.

I file generati con tecnologia CAdES necessitano di software di verifica appositi, mentre i file generati con tecnologia PAdES sono verificabili direttamente dal reader dei file .PDF (Acrobat Reader e similari).

L'APPOSIZIONE DELLE FIRME E INFORMAZIONI SUI DOCUMENTI FIRMATI

Un documento sottoscritto con firma digitale ha piena efficacia giuridica se dopo l'apposizione della firma non sia modificato. Per questo motivo occorre esaminare e chiarire gli le caratteristiche dei formati di firma CAdES e PAdES (rispettivamente estenzione .P7M e .PDF) e la loro capacità di contenere più firme e informazioni disponibili solo dopo la generazione delle firme digitali come ad esempio le informazioni relative alla segnatura di protocollo prevista dall'art. 55 del DPR 28 dicembre 2000 n. 445 (TUDA).

In termini semplici, all'atto della firma digitale il file che viene creato sarà costituito da una sorta di busta digitale (denominata "busta crittografica"), al cui interno è contenuto il documento originale, l'evidenza informatica della firma e la chiave per la verifica della firma stessa, la quale a sua volta è contenuta nel certificato emesso a nome del sottoscrittore. L'autenticità della firma è garantita da un'Autorità di certificazione e nello specifico ai sensi dell'art. 29 del CAD, dai certificatori accreditati.

Analizziamo meglio i formati di firma:

- La firma CAdES

  La busta crittografica è un file con estensione .P7M. Il contenuto di questo file è visualizzabile con specifici software, rendendo meno agevole la visualizzazione del documento in essa contenuta, ma ha il vantaggio di consentire la firma di qualsiasi tipo di file.

  Con questa tipologia di firma l'apposizione di più firme può essere effettuata in modi differenti, la prima consiste nel "reimbustare", e cioè firmare il file firmato creando la cosiddetta "firma matrioska", quindi avremmo un file .p7m che contiene un altro file .p7m che conterrà il documento originale, oppure aggiungendo alla prima busta ulteriori firme, accompagnate dai relativi certificati, usando il metodo delle firme congiunte (che deve essere possibile tramite software adatti).

  In entrambi le soluzioni è presente un'unica versione del documento, il quale può quindi accogliere ulteriori firme senza subire alcuna modificazione del contenuto.

  Con questa tipologia di firma quindi non è possibile gestire diverse versioni del documento all'interno della busta crittografica è quindi se fosse necessario aggiungere al documento delle annotazioni successive alla sottoscrizione, occorrerà provvedere ad esportare il documento originario, e apportarvi le annotazioni. Così facendo il documento perderebbe le firme e di conseguenza si avrebbero due documenti uno firmato e l'altro con le informazioni ma privo di firma digitale del sottoscrittore.

  Questo è il limite principale di questa tipologia di firma.

- La firma PAdES

  Nel formato PAdES la firma è un file con estensione .PDF, leggibile con i comuni lettori di file .pdf. Tale formato prevede diverse modalità di apposizione della firma, asseconda che il file sia stato predisposto per accogliere le firme previste e eventuali informazioni aggiuntive (quali la segnatura di protocollo). Produce documenti quindi più accessibili il suo utilizzo è limitato ai file .pdf.

Il formato .pdf consente il "versioning" cioè la gestione di diverse versioni dello stesso documento senza invalidare le firme digitali apposte. Inoltre, questa tipologia di firme include l'importante caratteristica di consentire di collocare fisicamente la firma digitale in un punto preciso del documento (ed eventualmente aggiungere anche una firma autografa scannerizzata). Questa caratteristica è interessante perché consente la sottoscrizione per esempio di clausole vessatorie, e quindi posizionando la firma specificamente al di sotto di tale clausola o comunque in una collocazione specifica che dia una particolare valenza ad una firma.

Qualora il documento non sia stato predisposto per l'apposizione di firme multiple è comunque possibile apporre ulteriori firme, senza che le precedenti vengano invalidate. Con la funzione di "versioning" infatti ogni versione è successiva alla prima contiene la versione integrale, non modificata, del documento precedente incluse le firme apposte.

Questa caratteristica rende questa tipologia di firma idoneo ad apportare modifiche al documento dopo averlo sottoscritto, ad esempio per riportarvi le annotazioni, es. segnatura di protocollo disponibile solo successivamente alla sottoscrizione del documento.

Non bisogna farsi fuorviare dai messaggi che i lettori di .pdf mostrano, tipo "almeno una delle firme non è valida" o "Il documento dopo la firma è stato modificato o si è danneggiato" infatti è comunque possibile accedere alla versione del documento correttamente sottoscritta che mantiene la sua validità e piena efficacia giuridica secondo quanto previsto dalla regole tecniche di cui al DPCM del 22 febbraio 2013.

- firma XadES XML Advanced Electronic Signatures ancora poco diffusa, il file mantiene l'estensione xml e contiene al suo interno i dati di certificazione con struttura aderente alla specifica pubblica ETSI TS 101 903 versione 1.4.1,

VERIFICA DELLE FIRME ELETTRONICHE QUALIFICATE E DIGITALI

La verifica delle firme elettroniche qualificate e digitali è trattato dal DPCM 22 febbraio 2013 all'art. 14 che recita:

"*Art. 14. Verifica delle firme elettroniche qualificate e digitali*

1. *I certificatori che rilasciano certificati qualificati forniscono ovvero indicano almeno un sistema che consenta di effettuare la verifica delle firme elettroniche qualificate e delle firme digitali, conforme a quanto stabilito con i provvedimenti di cui all'art. 4, comma 2.*
2. *Il sistema di verifica delle firme elettroniche qualificate e digitali deve quantomeno:*
   a) *presentare, almeno sinteticamente, lo stato di aggiornamento delle informazioni di validità dei certificati di certificazione presenti nell'elenco pubblico;*
   b) *visualizzare le informazioni presenti nel certificato qualificato, in attuazione di quanto stabilito nell'art. 28, comma 3, del Codice, nonché le estensioni obbligatorie nel certificato qualificato (qcStatements), indicate nei provvedimenti di cui all'art. 4, comma 2;*
   c) *consentire l'aggiornamento, per via telematica, delle informazioni pubblicate nell'elenco pubblico dei certificatori;*

d) in caso di firme multiple, visualizzare l'eventuale dipendenza tra queste;

e) visualizzare chiaramente l'esito della verifica dello stato dei certificati qualificati e di eventuali certificati di attributo secondo le modalità indicate nei provvedimenti di cui all'art. 4, comma 2;

f) evidenziare l'eventuale modifica del documento informatico dopo la sottoscrizione dello stesso;

g) consentire di salvare il risultato dell'operazione di verifica su un documento informatico

h) rendere evidente la circostanza di cui all'art. 19, comma 7.

3. *L'Agenzia, ai sensi dell'art. 31 del Codice, accerta la conformità dei sistemi di verifica di cui al comma 1 alle norme del Codice e alle presenti regole tecniche.*

4. *L'Agenzia, al fine di fornire garanzie di attendibilità nelle operazioni di verifica e di rendere effettivamente interoperabili le firme elettroniche qualificate e le firme digitali, anche in base all'evoluzione delle normative europee ed all'evoluzione degli standard tecnici, può elaborare Linee Guida utili per la verifica della firma elettronica qualificata e della firma digitale apposte a documenti informatici cui i certificatori accreditati hanno l'obbligo di attenersi.*"

MARCA TEMPORALE

Lo strumento preposto ad assegnare valore giuridico probatorio ai documenti dell'Amministrazione è il protocollo informatico. È infatti la registrazione di protocollo che certifica l'autenticità di un documento, e cioè è possibile attribuire allo stesso la certezza della provenienza e della data.

La marca temporale è una sequenza di caratteri, e tale sequenza contiene una data e un orario preciso e viene generata da un'autorità terza fidata (Time Stamping Authority – TSA).

Un file marcato temporalmente ha estensione .m7m e al suo interno contiene il documento al quale è stata effettuata la validazione temporale.

Con la marcatura temporale è consentito di stabilire in maniera certa la data di un documento rendendolo opponibile a terzi.

Alcune tipologie di documenti (es. contratti redatti nella forma pubblica amministrativa) pur registrati nel protocollo informatico possono richiedere l'apposizione della marca temporale.

L'argomento è trattato dal DPCM 22 febbraio 2013 al titolo IV.