CAMERA DI
COMMERCIO
MILANO

Dal 1786 l'istituzione al servizio del sistema produttivo di Milano.

La firma digitale

Come firmare i documenti informatici

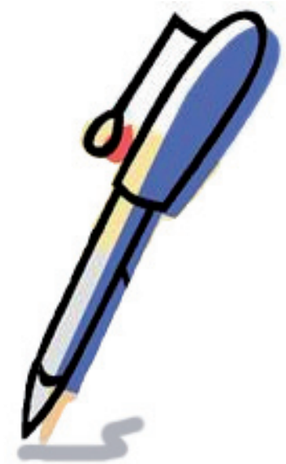
MANUALE

Sommario

Premessa

Questo breve manuale intende diffondere al personale e a tutti gli utenti della CCIAA l'utilizzo degli strumenti di firma digitale illustrando, in modo semplificato, i processi di acquisizione e le logiche di funzionamento.

L'autenticità dei dati di rilievo giuridico, in formato digitale, può essere tutelata in sicurezza solamente attraverso l'utilizzo di avanzate tecniche informatiche come la firma digitale.



Le firme elettroniche*

- **Firma elettronica:** strumento che consente l'identificazione informatica del mittente di un insieme di dati elettronici.

- **Firma elettronica avanzata:** insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e la connessione univoca del firmatario ai dati e l'integrità degli stessi.

- **Firma elettronica qualificata:** tipo di firma elettronica avanzata caratterizzata da una connessione univoca con il firmatario e la sua univoca identificazione basata sia su un certificato qualificato realizzato mediante un dispositivo sicuro per la creazione della firma.

- **Firma digitale:** tipo di firma elettronica avanzata basata su un certificato qualificato e un sistema di chiavi crittografiche, una pubblica e una privata, correlate fra loro. Questo sistema permette al titolare di rendere manifesta la provenienza del documento tramite una chiave privata e al destinatario di verificarne la provenienza e l'integrità.

*Art. 1 del d.Lgs n.82/2005 e successive modifiche

In sintesi

E’ possibile ritirare il dispositivo di firma presso gli sportelli RAO delle Camere di Commercio e i gestori accreditati.

Ottenuto il dispositivo è possibile apporre la firma sui documenti informatici.

1. La firma Digitale

La firma digitale è uno degli strumenti più utili e sicuri per firmare documenti informatici con la stessa validità giuridica di un documento firmato manualmente.

La firma digitale si può apporre su qualunque documento informatico: bilanci, atti societari, fatture, notifiche, moduli per l’iscrizione a pubblici registri, comunicazioni alla Pubblica Amministrazione.

Il documento firmato digitalmente integra e sostituisce l’apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

Perchè usare la firma digitale?

- **Autenticità**: attesta la volontà del titolare di sottoscrivere un documento informatico.
- **Paternità**: attesta l’identità di colui che ha firmato il documento.
- **Integrità**: rende noto se il documento viene modificato dopo l’apposizione della firma.
- **Non ripudio**: riconduce il documento firmato al titolare della firma.

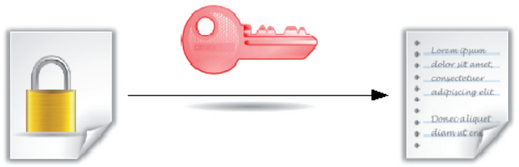
Quali sono i vantaggi di un documento firmato digitalmente?

1. **Eliminazione di documenti cartacei** - grazie all’archiviazione su supporti informatici, anche dei documenti firmati, da conservare in originale.
2. **Semplificazione e sicurezza dei rapporti tra aziende ed enti pubblici** - con la firma digitale si firma il documento attraverso dispositivi elettronici e lo si invia elettronicamente, senza stamparlo; si risparmia in costi di stampa, tempi di trasmissione e si garantisce l’inalterabilità dei contenuti.
3. **Economicità** - rende possibile la stipulazione di contratti anche a grandi distanze, senza necessità di spostamenti di persone o di spedizioni di materiale.
4. **Eliminazione di timbri e simili** – nei casi in cui hanno valore di firma, integra e sostituisce l’apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ove previsti per legge.

2. Come Funziona

La firma digitale si compone di una coppia di chiavi (pubblica e privata)

• La **chiave privata** è utilizzata dal titolare per apporre la firma digitale sul documento informatico. E' custodita all'interno di una **tessera magnetica** o **chiave USB** e protetta da un codice segreto conosciuto solo dal titolare.



• La **chiave pubblica** è lo strumento con il quale si verifica la paternità effettiva della firma apposta sul documento informatico.

La coppia di chiavi (pubblica e privata) per la creazione e la verifica della validità della firma può essere attribuita a **un solo titolare**.

- La firma viene rilasciata da un **Ente Certificatore**, ovvero da un soggetto iscritto in un apposito **elenco tenuto da DIGITPA** che rilascia un certificato elettronico qualificato.
- Il **certificato attesta la validità del documento**, gli elementi identificativi del titolare, i dati per la verifica della firma e del periodo di validità. E' prevista la possibilità di inserire nello stesso certificato elettronico le qualifiche specifiche del titolare (appartenenza ad ordini professionali, poteri di rappresentanza, limiti di firma ecc.).

1. E' **vietato duplicare** la chiave privata e i dispositivi che la contengono,
2. occorre **ben custodire il dispositivo di firma** (tessera elettronica, chiave USB); in caso di perdita o firma difettosa richiedere subito la revoca dei certificati qualificati relativi alle chiavi contenute nel dispositivo,
3. il **PIN** deve essere **conservato separatamente** dal dispositivo contenente la chiave,
4. la sottoscrizione di un documento informatico firmato con una firma digitale basata su un **certificato elettronico revocato**, scaduto o sospeso equivale a **mancata sottoscrizione**,
5. un documento cifrato dalla chiave privata della coppia può essere **decifrato** esclusivamente utilizzando la **chiave pubblica**, conoscendo solamente una delle due chiavi non c'è nessun modo di ricostruire l'altra.

L'HASH è una funzione matematica irreversibile che, applicata a un documento di qualsiasi dimensione, genera una sequenza alfanumerica (per esempio di 32 caratteri) che rappresenta una sorta di "impronta digitale" dei dati, e viene detta valore di hash. Se all'apertura del documento l'impronta risultante dalla decifratura con la chiave pubblica del mittente è uguale a quella che si ottiene applicando la funzione di hash, vuol dire che esso proviene da chi appare come il titolare della chiave pubblica e che non è stato alterato dopo l'apposizione della firma digitale.

3. Requisiti per la firma

Per il mittente che appone la firma al documento

Per utilizzare la firma digitale è necessario possedere alcuni requisiti minimi:

1. **dispositivo di firma** valido (tessera elettronica o chiave USB) con codice PIN rilasciato al momento dell'attivazione,
2. **computer** con connessione a Internet attiva,
3. **documento**, in formato **PDF**, da firmare.

Per il destinatario che riceve il documento firmato

Per poter visualizzare il documento ricevuto è necessario possedere alcuni requisiti minimi:

1. **computer** con connessione a Internet attiva,
2. **sotfware** in grado di aprire files in **PDF**,
3. **programma** in grado di **leggere la firma digitale del documento** (scaricabile gratuitamente da Internet) o in alternativa l'accesso a un sito di un Ente Certificatore che permetta di inviduare l'eventuale firma apposta.

4. Come si firma digitalmente

La procedura di firma è semplice:

Inserisco la tessera elettronica o la chiave USB → Scelgo il documento da firmare → Inserisco il codice PIN → Visualizzo il documento da firmare e firmo

Soggetto A

converte il documento in PDF

inserisce il dispositivo e appone la firma digitale.

Il soggetto A, tramite e-mail o Pec, invia il documento firmato.

Il soggetto B, che riceve il documento firmato, lo apre con la chiave pubblica e verifica l'integrità del documento e la validità della firma digitale.

5. Cosa sapere

SUI FORMATI DEI DOCUMENTI DA FIRMARE DIGITALMENTE

La firma digitale può supportare diversi formati (es. Xades, EDIFACT), ma è consigliato **firmare esclusivamente** files in formato **PDF**. Il formato PDF ha importanti vantaggi sia perché la firma apposta al file PDF **non modifica il formato** del documento, sia perché il formato PDF è **internazionalmente riconosciuto** e diffuso. I files che vengono generati con la firma digitale possono essere in formato PDF o "P7m".

SULLA CERTIFICAZIONE DIGITALE

- Certificato di autenticazione: è un file che permette di autenticarsi ai siti web delle PA in modalità sicura. Il certificato di autenticazione contiene i dati del titolare e riporta i dati dell'Ente Certificatore che lo ha rilasciato.

- Certificato di sottoscrizione: collega il titolare alla chiave pubblica ed è valido fino ad un massimo di tre anni (es. certificato contenuto nella chiave USB).

SULLA FIRMA AUTENTICATA

Ai sensi dell'art. 25 CAD*, viene riconosciuta la firma elettronica o altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale autorizzato. Con l'autenticazione il pubblico ufficiale attesta che la firma elettronica è stata apposta dal titolare in sua presenza dopo aver verificato l'identità personale del titolare della firma, la validità del certificato e la liceità del documento sottoscritto.

*D.Lgs n.82/2005 e successive modifiche.

6. Due firme a confronto

FIRMA AUTOGRAFA	FIRMA DIGITALE
• *Riconducibile direttamente al soggetto*	• *Riconducibile al soggetto solo attraverso il dispositivo di firma e il codice Pin*
• Legata al documento attraverso il supporto fisico	• *Legata indissolubilmente al contenuto del documento (impronta)*
• *Verifica diretta e soggettiva attraverso il documento*	• *Verifica diretta e oggettiva tramite una terza parte fidata (il Certificatore)*
• Falsificabile	• *Non falsificabile (in mancanza del Pin la firma non può essere apposta)*
• *In caso di disconoscimento, l'autenticità della firma deve essere dimostrata da terzi*	• *In caso di disconoscimento, è il titolare della firma a dovere dimostrare il mancato utilizzo del dispositivo di firma*
• Vale per tutta la vita del supporto cartaceo	• *È valida nel tempo, purché apposta durante il periodo di validità del certificato*
• Non è possibile l'automazione dei processi e servizi	• *E' possibile l'automazione dei processi e servizi*

7. Firme digitali in uso in Camera di commercio

I casi di utilizzo della firma digitale in CCIAA sono sempre più numerosi: si pensi, ad esempio, all'obbligo di trasmissione telematica delle pratiche societarie al Registro delle Imprese o alla dematerializzazione dei mandati di pagamento, delle determinazioni ecc. Ecco, quindi, che diviene sempre più indispensabile utilizzare i dispositivi di firma digitale.

Business key è uno strumento dotato di certificati di sottoscrizione e autenticazione, una cartella sicura dove salvare i documenti riservati, applicazioni professionali per l'ufficio, la posta elettronica, programmi di gestione delle password.

- È completa di applicazioni di sicurezza (Firma digitale, Autenticazione e cifratura) utilizzabili direttamente dal dispositivo senza necessità di alcuna installazione.
- Sempre aggiornata (update automatici dei programmi)
- Personalizzabile
- Subito pronta all'uso
- Pratica (un solo PIN per tutte le proprie password).

Business Key lite permette di firmare digitalmente e memorizzare le user e le password, senza dover installare alcun software. Non necessita di alcuna installazione, è portatile e permette di apporre la firma digitale su tutti i documenti, con lo stesso valore di una firma autografa su carta.
In più, permette di custodire tutte le password utilizzate per accedere ai diversi servizi su Internet con un unico PIN.

Carta Nazionale Dei Servizi (CNS) è un dispositivo elettronico (Smart Card o USB) che contiene un certificato di autenticazione personale grazie al quale è possibile accedere in modo sicuro ed identificato ai servizi telematici appositamente individuati dalle Pubbliche Amministrazioni.

Marca Temporale (time stamping) si definisce marca temporale il "segno" digitale apposto sul documento informatico il cui scopo è di rendere certa e opponibile a terzi la data e l'ora di formazione del documento. E' una sequenza di caratteri contenenti una data ed un orario preciso, generata da una Time Stamping Authority (TSA), terza parte fidata. E', quindi, una firma digitale di un Certificatore apposta a un documento informatico che contiene una serie di indicazioni, le più importanti delle quali sono la data, l'ora di generazione della marca stessa e l'impronta del documento. Le marche temporali sono utilizzate quando il processo richiede l'attestazione della data e dell'ora certa (Es. Documenti fiscali).

8. Normativa di riferimento

Dalle origini...

Legge 15 marzo n. 59 del 1997 (L.Bassanini)

Art. 15, comma 2: "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".

Dpr n. 445/2000
e successive modifiche

Art. 10, comma 1: "Il documento informatico sottoscritto con firma digitale soddisfa il requisito legale della forma scritta e ha efficacia probatoria".
Art. 25, comma 1: "In tutti i documenti informatici delle pubbliche amministrazioni la firma autografa o la firma, comunque prevista, è sostituita dalla firma digitale".
Art. 38, comma 1: "Tutte le istanze e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate anche per fax e via telematica."
comma 2: "Le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale".

...a oggi

Decreto del presidente del consiglio dei ministri del 13 gennaio 2004

a. Stabilisce che il documento informatico, sottoscritto con firma digitale o con altra firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 Codice civile, ai sensi del quale "La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".
b. Stabilisce che l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria;
c. Fa chiarezza e distingue tra firma elettronica, firma elettronica qualificata e firma digitale. Stabilisce che le istanze e dichiarazioni inviate per via telematica da e verso la CCIAA sono valide se sottoscritte mediante firma digitale basata su un certificato qualificato rilasciato da un Certificatore accreditato e generata mediante un dispositivo sicuro per la creazione di firme elettroniche.

Definisce le regole tecniche per la generazione, l'apposizione e la verifica delle firme digitali:

- Definisce le caratteristiche delle chiavi per la creazione e la verifica della firma.
- Distingue tra chiavi di sottoscrizione, certificazione e di marca temporale.
- Definisce le modalità di generazione e conservazione delle chiavi.
- Stabilisce l'onere per i Certificatori di indicare almeno un sistema che consenta di verificare le firme digitali.
- Identifica tutti i requisiti e gli obblighi dei Certificatori di firma digitale.

D.Lgs 7 marzo n. 82/2005
(Codice dell'Amministrazione Digitale) e successive modifiche relativamente alla firma digitale

Decreto del presidente del consiglio dei ministri del 30 marzo 2009 e successive modifiche

Prevede le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.

Adotta le regole per il riconoscimento e la verifica del documento informatico.

Deliberazione CNIPA n. 45 del 21 maggio 2009 e successive modifiche

Introduce rilevanti modifiche al Codice dell'Amministrazione Digitale del 2005, tra cui la reintroduzione della firma elettronica avanzata, l'obbligo per le pubbliche amministrazioni di comunicare con le imprese esclusivamente in modo telematico, la disciplina delle copie dei documenti informatici, ecc.

D.Lgs n. 235/2010

9. Breve glossario

Certificati elettronici: attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche.

Certificato di autenticazione: è un file che permette di autenticarsi ai siti web delle PA in modalità sicura. Il certificato di autenticazione contiene i dati del titolare e riporta i dati dell'Ente Certificatore che lo ha rilasciato (es. certificato contenuto nella CRS).

Certificato qualificato: certificato elettronico rilasciato da certificatori che abbiano i requisiti previsti dalla direttiva 1999/93/CE.

Certificatore: colui che effettua la procedura di certificazione: dopo aver rilasciato il certificato, lo pubblica unitamente alla chiave pubblica in uno specifico elenco liberamente accessibile per via telematica e, infine, aggiorna l'elenco dei certificati sospesi e revocati.

Chiave privata: chiave crittografica utilizzata dal soggetto titolare, mediante la quale si appone la firma digitale sul documento informatico.

Chiave pubblica: chiave crittografica destinata a essere resa pubblica, con la quale si verifica la firma digitale apposta sul documento informatico dal titolare della chiave privata.

Copia informatica di documento analogico: documento informatico avente contenuto identico a quello del documento cartaceo da cui è tratto.

Copia informatica di documento informatico: documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari (documento in formato .doc convertito in .pdf).

Dati per la creazione della firma: insieme dei codici personali utilizzati dal firmatario per creare la firma elettronica.

Copia per immagine su supporto informatico di documento analogico: documento informatico (es. "fotografia digitale di un documento cartaceo ad esempio in formato .JPG o .TIFF") avente contenuto e forma identici a quelli del documento analogico da cui è tratto.

Documento analogico: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (es. documento cartaceo).

Documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Duplicato informatico: documento informatico (ad es. file memorizzato nel disco del pc e copiato su chiavetta) ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.

Firma elettronica: insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

Firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e la connessione univoca del firmatario collegati ai dati a cui la firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

Firma elettronica qualificata: 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: un particolare tipo di firma elettronica qualificata 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.

Firme multiple: firme digitali apposte da soggetti diversi allo stesso documento. Si distinguono in:

- Firme parallele: questa funzione permette la firma di una busta PKCS#7 e consente ai firmatari successivi al primo di firmare il documento originale contenuto nella busta PKCS#7 prodotto dal firmatario precedente. L'estensione del file rimarrà con suffisso ".p7m".
- Firme "nidificate" o "annidate" o "a matrioska": in tal caso ogni sottoscrittore successivo al primo firma l'intera busta crittografica generata dal sottoscrittore precedente. Un documento con firme annidate produce un file "nomefile.p7m.p7m.p7m....".
- Controfirme: in questo caso il sottoscrittore firma una precedente firma apposta da un altro sottoscrittore. Un documento con controfirme produce un file di tipo"nomefile.p7m".

Identificazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo e univoco a un soggetto, che ne consentono l'individuazione nei sistemi informativi; è effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.

Impronta di una sequenza di simboli binari (bit): è la sequenza di simboli binari (bit) generata mediante l'applicazione alla prima di una opportuna funzione di hash.

Macroistruzione: è un singolo comando, composto da una sequenza di istruzioni, che fa compiere al computer una serie di operazioni ripetitive semplificandone l'uso.

PDF (Portable Document Format): formato documentale elettronico definito dallo standard internazionale ISO/IEC 32000.

Registro dei certificati: la combinazione di uno o più archivi informatici, tenuto dal certificatore, contenente tutti i certificati emessi.

Validazione temporale: il risultato della procedura informatica con cui si attribuiscono, a uno o più documenti informatici, una data e un'ora certa.

10. Domande frequenti

1) Che differenza c’è tra firma digitale e “digitalizzata”?

La firma digitalizzata, ad esempio la firma fatta con una penna particolare su un dispositivo con una tavoletta grafica, è la mera riproduzione informatica di un segno e nulla la collega a un documento. La firma digitale è il risultato di una procedura informatica che associa il documento e la chiave privata del firmatario.

2) Un documento firmato digitalmente può essere alterato?

Si può aprire un file cui è stata apposta una firma digitale, aggiungendo o eliminando le informazioni contenute. Il software di firma rileva le eventuali modifiche apportate dopo la firma e le segnala.

3) Nome utente e password possono sostituire la firma digitale?

Nome utente e password che, ad esempio, si utilizzano per accedere ad una casella di posta elettronica non possono sostituire la firma digitale perché non attestano la certezza sull’identità del mittente: qualcuno potrebbe aver libero accesso alla casella di posta elettronica di un’altra persona e mandare un messaggio al suo posto. La firma digitale che viene apposta su un documento attesta, invece, l’integrità del contenuto del testo e la sua provenienza. Il collegamento tra la chiave e chi la possiede è attestato dal certificato digitale, che viene emesso dopo la identificazione del richiedente.

4) Come riconosco una e-mail con firma digitale?

Generalmente nei programmi di posta elettronica più diffusi ogni messaggio firmato digitalmente è contrassegnato da una coccarda rossa: cliccandola è possibile visualizzare informazioni sul nome del titolare della firma, ente certificatore che l’ha emessa, periodo di validità della firma.

5) Quali documenti possono essere firmati digitalmente?

In linea di principio, qualunque documento può essere firmato digitalmente, diventando un vero e proprio documento informatico provvisto di un valore probatorio.

6) Che forma assume un documento firmato digitalmente?

Esistono diversi standard che permettono la rappresentazione di un documento informatico firmato digitalmente. Tuttavia l'attuale normativa italiana, per effetto di una Circolare di AIPA (Circolare 24/2000 aggiornata dalla Delib. CNIPA n. 4/2005), stabilisce che il formato raccomandato per questo tipo di documenti sia il PKCS#7. Questo formato contiene sia il documento digitale oggetto della firma, sia la firma o le firme digitali associate al documento, sia il certificato o i certificati di chiave pubblica corrispondenti all'autore o agli autori delle firme stesse. Il risultato è un file il cui nome viene modificato con l'apposizione di una ulteriore estensione ".p7m".

CAMERA DI
COMMERCIO
MILANO

Area Comunicazione
Ufficio Relazioni con il Pubblico
Camera Digitale

Via Meravigli 9/b 20123 Milano
urp@mi.camcom.it
www.mi.camcom.it