Firma Digitale

Cos'è, dove si ottiene, come si utilizza…..chi la richiede?

Normativa

Codice dell'amministrazione digitale
Decreto Legislativo 7 marzo 2005, n. 82

Art.24

https://docs.italia.it/italia/piano-triennale-ict/codice-amministrazione-digitale-docs/it/v2017-12-13/_rst/capo2_sezione2_art24.html

Cos'è la Firma Digitale e Remota?

Equivalgono alla tradizionale firma autografa apposta su carta, ed entrambe le tipologie di firma sono accomunate dalle stesse caratteristiche

…. in tecnico

La firma elettronica qualificata (FEQ) - o digitale - è il risultato di una procedura informatica, detta validazione, che garantisce l'autenticità, l'integrità e il non ripudio dei documenti informatici, è la rappresentazione informatica di atti, fatti o dati rilevanti giuridicamente (articolo 1, lettera "p" CAD).
Per avere valore legale e giuridico, il documento deve essere sottoscritto con firma digitale.
Si tratta di un dispositivo informatico che garantisce l'imputabilità di una certa rappresentazione (documento informatico) ad un soggetto specifico.
La firma elettronica assicura, insomma, il legame tra il firmatario e il documento informatico, così come la firma autografa assicura quello tra il firmatario e il documento cartaceo.

Cosa garantiscono

Validità legale
Il documento firmato digitalmente acquisisce pieno valore legale

Autenticità
L'identità del sottoscrittore è garantita

Integrità
L'inalterabilità del documento sottoscritto è assicurata

Non ripudio
Il documento firmato non può essere disconosciuto dal firmatario

A cosa servono

L'utilizzo della Firma Digitale snellisce e semplifica i rapporti tra **Pubbliche Amministrazioni, imprese e cittadini**, riduce l'utilizzo dei documenti in forma cartacea e rende quindi più dinamica, veloce ed ecosostenibile la gestione di pratiche e documentazioni.

Cosa si può firmare

Qualsiasi documento elettronico può essere sottoscritto digitalmente, come ad esempio fatture, documenti di bilancio, comunicazioni alle PA, visure camerali, contratti, ordini di acquisto e molti altri, nei formati pdf, word, excel, xml.

Chi la può avere e dove ottenerla

- Possono dotarsi di firma digitale tutte le persone fisiche: cittadini, amministratori e dipendenti di società e pubbliche amministrazioni. È possibile rivolgersi ai prestatori di servizi fiduciari qualificati autorizzati da AgID che garantiscono l'identità dei soggetti che utilizzano la firma digitale.
- https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia

Procedura per ottenere una firma digitale

Inserire i propri dati anagrafici

Avere un documento di riconoscimento da fornire per la registrazione

Procedere con il riconoscimento

QUADRO B1

Titolo[1] _____

Terzo interessato [2] _____

Sede/Indirizzo: _____

Codice fiscale/P. IVA: _____

Autorizzazione del Terzo Interessato
(Collegio/Ordine di appartenenza)

Il/la sottoscritto/a _____ in qualità di legale rappresentante dell'ordine/Collegio _____

in riferimento al Certificato richiesto per il/la Sig./Sig.ra _____ dichiara che il/la medesimo/a è regolarmente iscritto/a a questo Ordine/Collegio con matricola/ Numero di iscrizione _____

Settore _____ Sezione _____

Data iscrizione _____ Data abilitazione _____

Data _____

Firma e Timbro o Firma Digitale
del collegio/ordine di appartenenza

_____

QUADRO B2

Autorizzazione del Terzo Interessato
(Organizzazione di appartenenza)
da compilare a cura del legale rappresentante del Terzo Interessato

Il/la sottoscritto/a _____ in qualità di legale rappresentante dell'Azienda/Ente/Amm.ne _____

Sede/Indirizzo: _____

Codice fiscale/P. IVA: _____

in riferimento al Certificato richiesto dal Richiedente, dichiara che il/la medesimo/a è autorizzato all'utilizzo dei riferimenti dell'Organizzazione[3]

Allegare la documentazione comprovante la rappresentanza dell'organizzazione sopra indicata da parte del Terzo Interessato:

☐ Procura notarile (con data non superiore a 90 giorni prima); ☐ Estratto Notarile (con data non superiore a 90 giorni prima); ☐ Visura Camerale (con data non superiore a 90 giorni prima); ☐ Legge o Atto istitutivo (per la pubblica amministrazione) ☐ Procura generale o speciale

Carica ricoperta dal Richiedente (facoltativo)[4]

_____

Data _____

Firma e Timbro o Firma Digitale
Azienda/Ente/Amm.ne di appartenenza

_____

Modalità di riconoscimento

ONLINE

CON WEBCAM O APP MOBILE "ARUBA DE VISU"

COSA TI SERVE:

- documento di identità valido
- tessera sanitaria valida
- da smartphone - scaricare l'App "Aruba De Visu"

ONLINE

CON FIRMA DIGITALE O FIRMA DIGITALE REMOTA

COSA TI SERVE:

- Firma Digitale o Firma Remota attiva
- Lettore di smart card (in caso di Firma Digitale su smart card)
- **PIN** della smart card (in caso di Firma Digitale su smart card)

ONLINE

CON TESSERA SANITARIA O CARTA NAZIONALE DEI SERVIZI (CNS)

COSA TI SERVE:

- **TS-CNS** o **CNS** attiva
- Lettore di smart card
- **PIN** della TS-CNS o CNS

ONLINE

CON CARTA D'IDENTITÀ ELETTRONICA (CIE)

COSA TI SERVE:

- **CIE** (versione 3.0) attiva
- **Lettore NFC** contactless
- **PIN** della CIE

Cosa ho per avere una firma

Firma Digitale e Carta Nazionale Servizi

Firma Digitale Remota

FIRMA DIGITALE REMOTA

La soluzione più pratica per firmare digitalmente e in modo legale ogni tipo documento senza nessuna installazione hardware.

- Certificato di Firma Digitale virtuale
- One Time Password (OTP)
- Utilizzo multi device (PC, tablet e smartphone)
- Validità 3 anni

SPID e la firma digitale

- La firma digitale può essere ottenuta anche utilizzando lo SPID come sistema di riconoscimento. Tra i certificatori che hanno reso disponibile questa possibilità, sono attualmente attivi Infocert, Namirial (fornisce anche la possibilità di effettuare una sola firma (firma usa e getta)) e Intesi Group.
- I servizi prevedono l'accesso con credenziali SPID di livello 2, in questo modo il cittadino ha la possibilità di dimostrare con certezza la sua l'identità e ottenere la firma digitale.

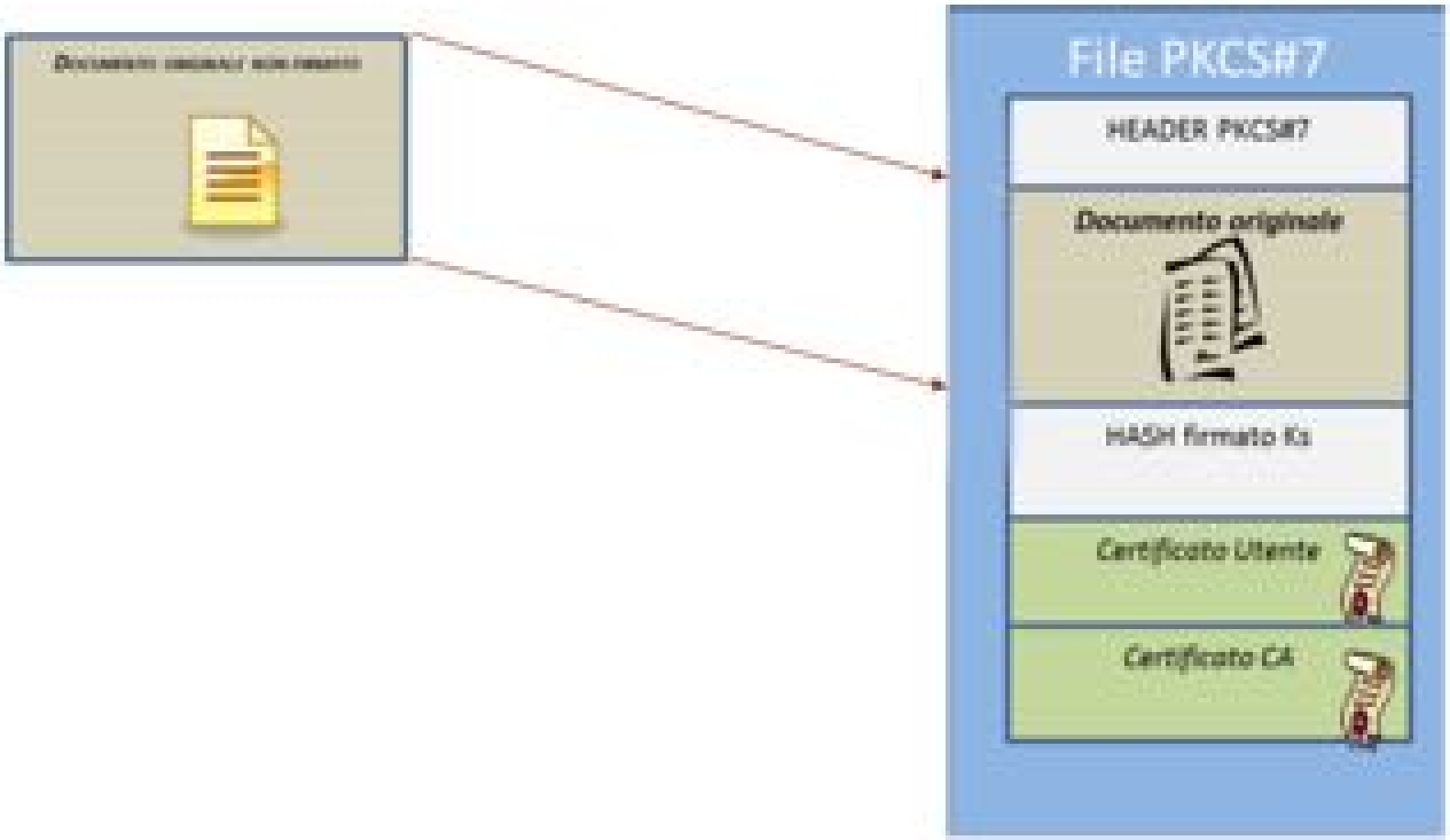
Programmi di firma e di verifica con programmi e online

https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/software-verifica

4-ter. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti previsti dal regolamento eIDAS ed è qualificato in uno Stato membro;
b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui al medesimo regolamento;
c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

Cosa accade quando si firma….



Firme elettroniche tipologie

La firma elettronica semplice
un esempio, sono il codice PIN o le credenziali di accesso ai siti web

Firma elettronica avanzata (FEA)
Un esempio di FEA è la c.d. **firma grafometrica**, che, per il tramite di un pennino, viene apposta su tablet ed è molto diffusa nel settore bancario e nel settore assicurativo

Firma elettronica qualificata (FEQ)
La firma elettronica qualificata, è una peculiare tipologia di firma avanzata, "creata da un dispositivo per la creazione di **una firma elettronica qualificata e basata su un certificato qualificato** per firme elettroniche" (art. 3, punto 1, n. 12, Regolamento eIDAS). La firma elettronica qualificata garantisce in modo univoco l'identificazione del titolare, e, dal punto di vista dell'efficacia giuridica, equivale ad una firma autografa, come statuito dall'art. 25 del Regolamento eIDAS

Firma Digitale (**Firma elettronica qualificata)**

La firma digitale è una **peculiare tipologia di firma elettronica qualificata**, prevista solamente a livello nazionale. L'art. 1, comma 1, lett. s del CAD la definisce come quel "particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una **pubblica** e una **privata**, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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".

Costituisce dunque **l'equivalente elettronico della tradizionale firma autografa su carta**, dal momento che attesta con certezza l'integrità, l'autenticità e la non ripudiabilità del documento informatico su cui è apposta

la firma remota

La firma remota è definita nel DPCM 22 febbraio 2013 (articolo 1, comma 1, lettera q) come *"particolare procedura di firma elettronica qualificata o firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse"*.

La firma remota è nata circa 10 anni fa per superare il problema dell'instabilità tecnologica nell'utilizzo tra PC, lettori di smart card e smart card e per il suo utilizzo sui nuovi dispositivi mobili quali Tablet e Telefoni mobili.

L'avvento dei microchip in formato SIM telefonica installati nei *token* USB ha mitigato questi problemi ma I dati forniti da **AgID** ci dicono che i certificati digitali rilasciati per la **firma remota sono l'82% del totale inoltre nel 2017** sono state generate 1.876.379.223 firme digitali remote.

Tipi di firma

La firma CAdES

Nel caso di una firma digitale apposta con modalità CAdES, il documento firmato e il file con la firma digitale vengono inseriti insieme in una busta. Tale busta, che contiene il documento e il file della firma, è anch'essa un file con estensione **.p7m**. Infatti, tutti i file firmati digitalmente con modalità CAdES hanno una seconda **estensione .p7m**.

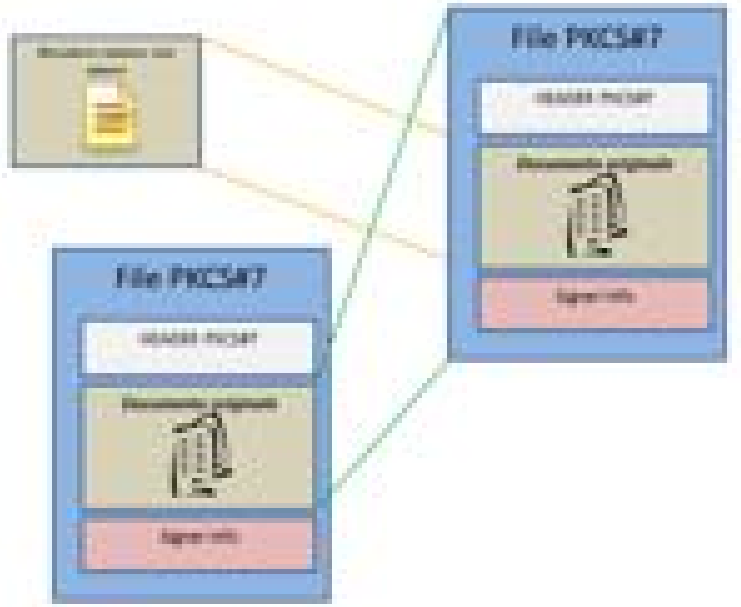
Vediamo le principali caratteristiche di questa modalità di firma:

- La modalità CAdES permette di **firmare qualsiasi tipo di documento** (docx, .xlsx, ecc.), anche se consigliamo comunque di firmare file in formato .pdf (vedi Validità di una firma digitale).
- Un documento, una volta firmato con modalità CAdES modifica il suo nome. Ad esempio un documento *Prova.docx*, una volta firmato digitalmente con modalità CAdES modificherà il suo nome in *Prova.docx.p7m*.
- Per verificare una firma digitale apposta con modalità CAdES e per visualizzare il documento firmato, occorre utilizzare uno degli **appositi software specifici** come Dike 6, ArubaSign, ecc.

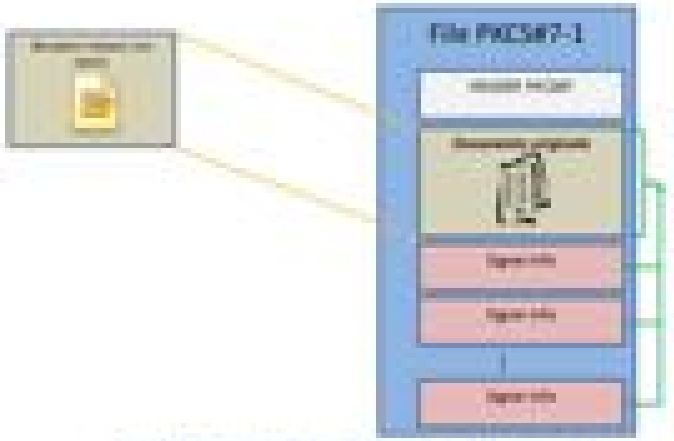
Tipi di firma La firma CAdES

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")



- oppure aggiungendo nella busta ulteriori firme, accompagnate dai relativi certificati (c.d. firme congiunte)



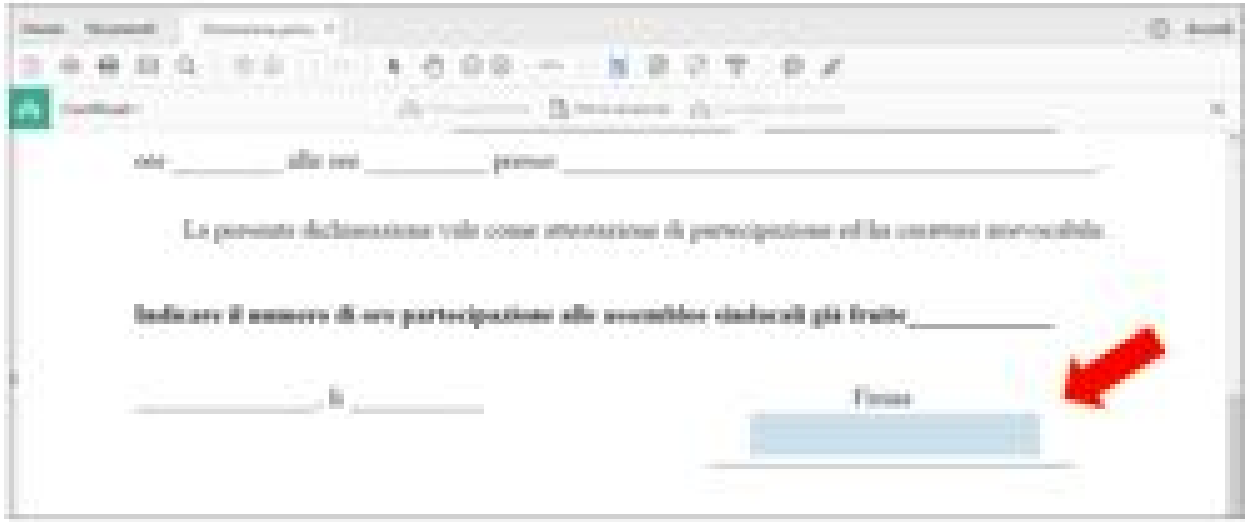
Tipi di firma La firma PAdES

Nel caso di firma digitale apposta con modalià PAdES, invece, vengono sfruttate le caratteristiche dei documenti in formato .pdf e il file contenente la firma digitale viene inglobato insieme al documento stesso.
Vediamo le principali caratteristiche di questa modalità di firma:

- La modalità PAdES permette di firmare **solo documenti in formato .pdf**
- Un documento, una volta firmato con modalità PAdES, mantiene il suo nome
- Per verificare una firma digitale apposta con modalità PAdES e per visualizzare il documento firmato, è possibile utilizzare un qualsiasi software per la lettura dei file .pdf come Acrobat Reader

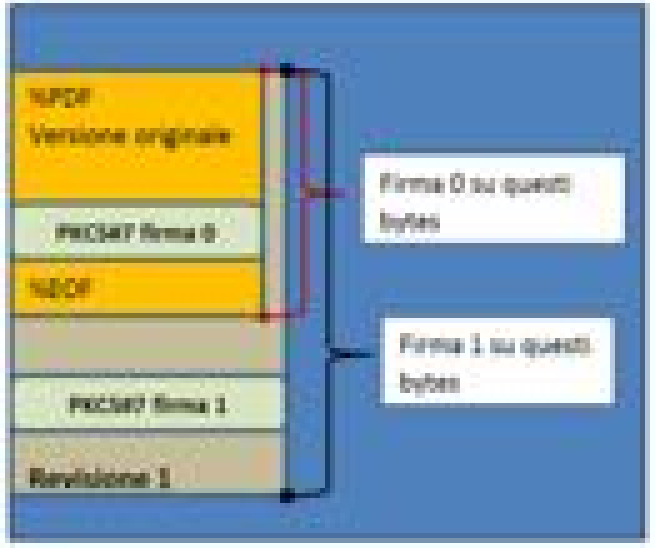
Tipi di firma La firma PAdES

Predisposizione del documento PDF Il documento può essere predisposto, attraverso la gestione dei "moduli" (disponibile con la versione professional di Acrobat e di altri prodotti conformi), alla firma digitale da parte di utenti che dispongono di un prodotto conforme allo standard PDF (ISO 32000), fra questi Acrobat Reader



Tipi di firma La firma PAdES

Molteplici firme nel documento PDF 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



Come si fa la firma in Cades imbustata e con firma aggiunta e quella in Pades

ESEMPIO PRATICO

Scadenza della firma o meglio quando è stata apposta la firma e per quanto tempo resta valida ai fini di legge

La scadenza dei certificati è un fattore alquanto delicato nel contesto della firma digitale dei documenti.

Nel contesto della firma digitale la scadenza ha ripercussioni gravi.

La firma non scade mai ma firmare oppure non poter mostrare che al momento della firma, il certificato non fosse scaduto, sospeso o revocato, rende (ovviamente) ogni firma digitale/qualificata basata su quel certificato non valida, ossia, **ai sensi dell'art. 24 comma 4-bis del CAD, il documento senza sottoscrizione**.

Un certificatore è in grado di verificare se un certificato ad una certa data fosse valido, **ma fornire una data (certa) in cui collocare temporalmente il documento è onere di chi produce il documento**

Tempo certo della firma

Per essere chiari: **un file firmato digitalmente privo di un riferimento temporale certo non serve**.

Ovviamente a livello tecnologico una soluzione standard è presente: **la marca temporale**.

Una marca temporale non è altro che un'altra "firma" dove all'impronta del documento è associata una data ed un'ora certificati da apposite autorità (TSA, time stamp authority).

Curiosamente, una marca temporale è essa stessa firmata con un certificato ma dura 20 anni, e lo fa perché è obbligo della TSA, conservare le marche emesse per tale periodo (art. 53 del DPCM 22 febbraio 2013, le regole tecniche sulla firma).

La marca temporale

La **Marca Temporale** è un servizio che permette di **associare data e ora certe e legalmente valide ad un documento informatico**, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005).

Il servizio di **Marcatura Temporale** può essere utilizzato anche su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida.

Inoltre apporre una **Marca Temporale** ad un documento firmato digitalmente, fa si che la Firma Digitale risulti sempre e comunque valida anche nel caso in cui il relativo Certificato risulti scaduto, sospeso o revocato, purché la Marca sia stata apposta in un momento precedente alla scadenza, revoca o sospensione del Certificato di Firma stessa.

Marca temporale serve, è utilizzata?

D'altronde per documenti informatici da conservare per lungo tempo non basterebbe più un riferimento temporale, ma sono necessari trattamenti ben più complessi in grado di mantenere il documento valido anche a fronte di problematiche specifiche del lungo periodo quali ad esempio l'obsolescenza dei formati.

Per questi documenti la soluzione è un'altra: **il deposito presso appositi sistemi pensati per la conservazione del lungo periodo**.

Ai tempi delle regole tecniche per la firma (l'ormai lontano 2013) la marca temporale **non era una soluzione sempre agevole** (serve essere online), e anche costosa.

Per questo vennero introdotte delle "alternative", quali la data riportata sulla segnatura di protocollo della PA, le PEC ed il riversamento nei sistemi di conservazione a norma.

Alternative alla marca temporale?

Per questo vennero introdotte delle "alternative", quali:

1. la data riportata sulla segnatura di protocollo della PA
2. le PEC
3. il riversamento nei sistemi di conservazione a norma.

Tutti metodi non pienamente convincenti:

il primo, valido solo per la PA

il secondo, quasi ridicolo, perché la PEC contiene sì all'interno una data valida, ma non in forma di marca temporale, come molti credono, bensì semplicemente **come testo riportato nella ricevuta**, firmata digitalmente dal gestore del servizio, e quindi anch'essa soggetta al problema della scadenza del certificato (che potrebbe scadere in teoria prima ancora di quello del documento trasmesso, salvo l'obbligo del gestore di conservare le ricevute per 3 anni);

il terzo, oltre che costoso, sembra davvero spropositato, specie per i documenti che richiedono periodi di conservazione (tipo quelli fiscali ad esempio) limitati.

Conservazione e scadenza certificato di firma

La conservazione

L'art. 34 del Regolamento eIDAS poi, detta la disciplina del **servizio di conservazione qualificato delle firme elettroniche qualificate**, individuato anch'esso quale servizio fiduciario, a norma dell'art. 3, punto 1, n. 16 del medesimo Regolamento. Tale servizio può essere svolto esclusivamente da prestatori di servizi fiduciari qualificati, che facciano uso di procedure e tecnologie in grado di estendere l'affidabilità della firma qualificata oltre il periodo di validità tecnologica.

Cos'è la Conservazione

La **conservazione digitale** è quel processo "disciplinato" che permette di conservare i documenti in formato digitale consentendo, nei casi previsti dalla norma, di distruggere l'originale cartaceo o di non procedere con la sua stampa. Serve a garantire ***autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti***.

Quali strumenti servono per conservare i documenti a norma?

"**Conservazione digitale**" significa quindi "sostituire i documenti cartacei, con lo stesso documento in formato digitale" la cui valenza legale di forma, contenuto e tempo è testimoniata con una firma digitale e una marca temporale.

Il processo di conservazione comprende automaticamente:

- la **firma digitale**, ossia quella firma elettronica che si applica ai documenti informatici, esattamente come la firma tradizionale (autografa) viene apposta sui documenti cartacei;
- la **marca temporale**, ossia una successione di caratteri che rappresentano una data e/o un orario per assodare l'effettivo avvenimento di un'attività/evento.

L'unione della firma digitale alla marca temporale consente di mantenere invariati nel tempo l'immodificabilità , l'autenticità , la reperibilità , il valore legale, la sicurezza, la leggibilità, l'integrità dei documenti conservati.

Ok abbiamo finito