Il documento informatico e firme elettroniche

Dott.ssa Michela Rossi
michela.rossi@unibo.it
1 luglio 2020

1

La normativa di riferimento

- D.P.R. n. 445/2000 – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
- D.Lgs. 7 marzo 2005 n. 82 - **Codice dell'Amministrazione Digitale** (CAD)
- DPCM 13 novembre 2014 – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 10, 22, 23.bis, 23.ter, 40 comma 1, 41, 71, comma 1 del Codice dell'amministrazione digitale
- Circolare AgID 23 gennaio 2013 n. 60 – Formato e definizioni dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le pubbliche amministrazioni
- DPCM 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delel firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lett. b) 35 comma 2, 36 comma 2 e 71.
- Regolamento UE n. 910/2014 (electronic IDentification Authentication and Signature - **Regolamento eIDAS**) in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
- Regolamento UE n. 679/2916 – Regolamento generale sulla protezione dei dati (GDPR)

2

Il documento informatico

Dott.ssa Michela Rossi
michela.rossi@unibo.it
1 luglio 2020

3

Che cos'è un documento informatico?

UN FILE

Cioè una sequenza di bit che elaborata da un sistema informatico può essere resa visibile su uno schermo, stampata o inviata.

Principiali differenze rispetto al documento cartaceo:

- è **immateriale** (la sua esistenza è slegata dal supporto fisico nel quale può essere memorizzato)

- Non c'è distinzione tra **originale e duplicato** (i bit possono essere trasferiti, riprodotti e memorizzati su infiniti supporti senza perdere mai le proprie caratteristiche, senza subire degradazione o alterazione, con la conseguenza che è possibile avere una molteplicità di originali con lo stesso valore).

4

Com'è definito il documento informatico?

Art. 1. Definizioni.

lett. p) **documento informatico**: il **documento elettronico** che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

- **Documento elettronico**: qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (art. 3, comma 1, n. 35 Reg. eIDAS)
- Identificato come una sequenza di bit

lett. p-bis) **documento analogico**: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

.

5

Qual è il valore giuridico e probatorio del documento informatico?

Articolo 46 - Effetti giuridici dei documenti elettronici (**Reg. eIDAS**)

A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

Art. 20. Validità ed efficacia probatoria dei documenti informatici (**CAD**)

1-bis. […] l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

6

Il documento amministrativo informatico

Art. 23-ter CAD

Gli atti formati dalla pubblica amministrazione con strumenti informatici, nonché i dati e i documenti informatici **detenuti** dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per li usi consentiti dalla legge.

Art. 40 CAD

Le pubbliche amministrazioni formano gli originali dei propri documenti, inclusi quelli inerenti ad albi, elenchi e pubblici registri, con mezzi informatici secondo le disposizioni di cui al presente codice e le le Linee guida.

Art. 9 del DPCM 13-11-2014
Le pubbliche amministrazioni, ai sensi dell'art. 40 comma 1 del Codice formano gli originali dei propri documenti attraverso:
- Gli strumenti informatici riportati nel manuale di gestione
- Acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del codice.

7

Le firme

8

Esiste un equivalente della sottoscrizione autografa?

La sottoscrizione autografa consiste nella scrittura a mano del nome e del cognome in calce ad un documento.

Funzioni:

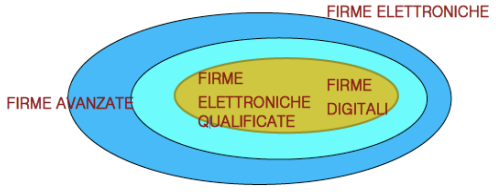
- **indicativa**: consiste nell'identificare l'autore del documento
- **dichiarativa**: prevede che la sottoscrizione imputi al titolare del nome la paternità del documento
- **probatoria**: la sottoscrizione è un mezzo di prova

9

Le firme elettroniche

La normativa prevede 4 tipi di firme elettroniche:

- Firma elettronica **(semplice)** – eIDAS
- Firma elettronica **avanzata** - eIDAS
- Firma elettronica **qualificata** - eIDAS
- Firma **digitale** - CAD



Titolare di firma elettronica: la **persona fisica** cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la sua creazione, nonché alle applicazioni per la sua apposizione. (art. 3 CAD)

10

La firma elettronica semplice

Art. 3. Definizioni – Regolamento eIDAS

10) **firma elettronica**: dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario **per firmare**;

Modificata rispetto alla versione precedente del CAD dove si definiva: "metodo di identificazione informatica"

11

Qual è il valore giuridico e probatorio del documento informatico sottoscritto con firma elettronica?

Art. 46. Effetti giuridici dei documenti elettronici (Reg. eIDAS)

A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica.

Art. 25. Effetti giuridici delle firme elettroniche (Reg. eIDAS)

A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.

Art. 20. Validità ed efficacia probatoria dei documenti informatici (CAD)

1-bis. […] l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

12

La firma elettronica avanzata (FEA)

Art. 3. Definizioni – Regolamento eIDAS

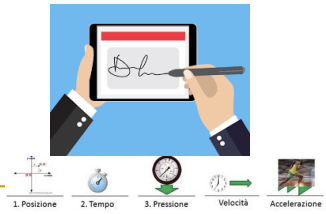
11) **firma elettronica avanzata**: una firma elettronica che soddisfi i requisiti di cui all'articolo 26.

Requisiti:

- è connessa unicamente al firmatario;
- è idonea a identificare il firmatario;
- 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; e
- è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

- possono variare da fornitore a fornitore
- alcune fea valgono solo fra le parti e non verso i terzi
- si può disconoscere

Art. 61 DPCM 22-2-2013



13

La firma elettronica qualificata

12) **firma elettronica qualificata:** 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.

Nell'allegato II del Reg. eIDAS sono elencati i requisiti che i dispositivi per la creazione di una firma elettronica qualificata devono soddisfare per essere considerati sicuri.

La conformità dei dispositivi per la creazione di una firma elettronica qualificata è certificata da appropriati organismi Pubblici o privati designati dagli Stati membri.

Il CAD assegna all'Organismo di Certificazione della Sicurezza Informatica (OCSI) il compito di accertare, sulla base di uno specifico schema di valutazione, la rispondenza dei sistemi di generazione delle firme ai requisiti e alle specifiche prescritti.

14

Le firma digitale

Art. 1 – Definizioni – CAD

lett. s) **firma digitale**: un 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.

paternità **immodificabilità**

15

Crittografia

È la tecnica alla base della firma digitale.

Essa permette, mediante l'uso di un algoritmo matematico, di trasformare un file di dati in un insieme di simboli privi di significato, quindi in una forma illeggibile da chiunque e decifrabile esclusivamente dal soggetto che possiede la chiave per decifrarli.

Crittografica → Simmetrica (a chiave segreta)
Crittografica → Asimmetrica (a chiave pubblica)

16

Crittografia asimmetrica

La crittografia asimmetrica contempla l'impiego di una coppia di chiavi, una privata e una pubblica.

Chiave: è una informazione usata come parametro in un algoritmo crittografico.

Chiave privata → l'elemento della coppia di chiavi asimmetriche, nota ed utilizzata solo dal soggetto titolare, **mediante il quale si appone la firma digitale** sul documento informatico.

Chiave pubblica → l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, avverrà la **verifica della firma** digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche

17

Crittografia asimmetrica

Ciascuna chiave può essere indifferentemente utilizzata per cifrare e decifrare un documento. La chiave utilizzata per cifrare il documento non può essere utilizzata anche per decifrare lo stesso documento. (**principio di correlazione**)

La conoscenza di una delle due chiavi non fornisce alcuna indicazione sull'altra. (**indipendenza delle chiavi**)

18

Funzione di hash

Funzione di hash: una funzione matematica che genera, a partire da una evidenza informatica, **una impronta (o digest)** in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti; (DPCM 22/2/2013)

La funzione di hash trasforma un documento, anche molto grande, in una stringa di caratteri di lunghezza fissa. L'hash cambia anche con un minimo cambiamento del testo, inclusi gli spazi.

Impronta di una sequenza di simboli binari è la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
IMPRONTA: **b89eaac7e61417341b710b727768294d0e6a277b**

19

Protezione della chiave privata

Ai sensi dell'art. 35 CAD
I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
- sia Riservata
- Non possa essere derivata e che la relativa firma sia protetta da contraffazioni
- Possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.

Art. 11 DPCM 22-2-2013
La **generazione delle firme** elettroniche qualificate e delle firme digitali avviene **all'interno di un dispositivo** sicuro per la generazione delle firme, in maniera tale che non sia possibile l'intercettazione della chiave privata utilizzata.
Il dispositivo sicuro per la generazione della firma elettronica qualificata o della firma digitale deve poter essere **attivato esclusivamente dal titolare** mediante sistemi di autenticazione ritenuti adeguati, secondo le rispettive competenze, dall'OCSI e dall'Agenzia, prima di procedere alla generazione della firma.

20

Protezione della chiave privata

Art. 8. - DPCM 22-2-2013

5. Il titolare della coppia di chiavi:

a) assicura la custodia del dispositivo sicuro per la generazione della firma in suo possesso e adotta le misure di sicurezza fornite dal certificatore al fine di adempiere agli obblighi di cui all'art. 32, comma 1, del Codice;

b) conserva le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave e segue le indicazioni fornite dal certificatore;

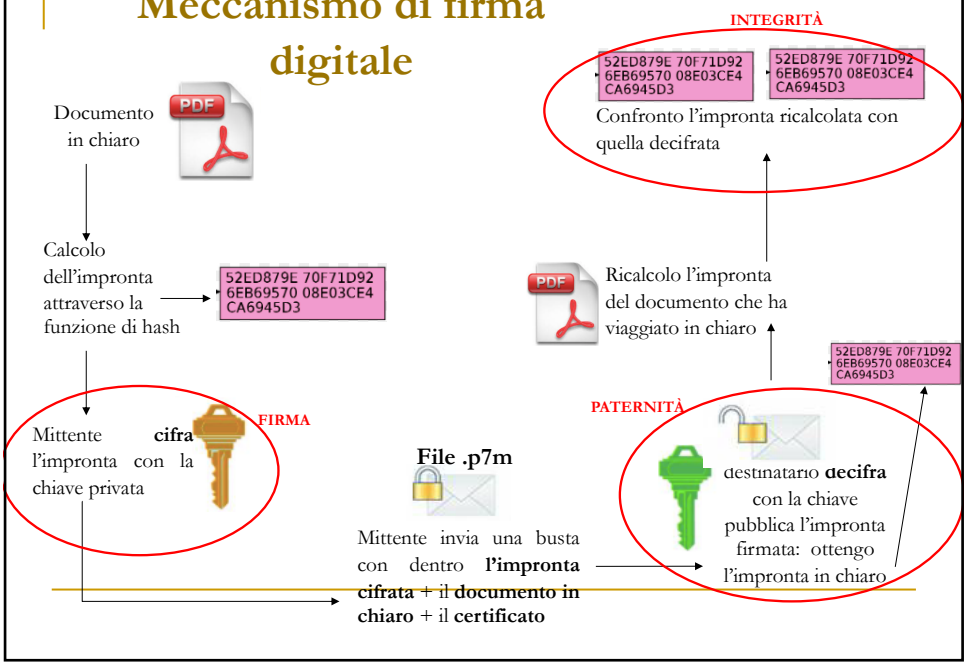
c) richiede immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale inutilizzabili o di cui abbia perduto il possesso o il controllo esclusivo;

d) salvo quanto previsto dai commi 3 e 4, mantiene in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma elettronica qualificata o digitale;

e) richiede immediatamente la **revoca** dei certificati qualificati relativi alle chiavi contenute in dispositivi sicuri per la generazione della firma elettronica qualificata o della firma digitale qualora abbia il ragionevole dubbio che essi possano essere usati da altri.

21

Meccanismo di firma digitale



22

Segretezza

Attraverso l'uso della crittografia asimmetrica è possibile garantire anche la **segretezza** del messaggio (mentre con la firma digitale garantisco solo la paternità e l'integrità).

Se voglio garantire **paternità, integrità e segretezza** → dopo aver firmato digitalmente l'impronta, il mittente cifrerà il documento con la chiave pubblica del destinatario in modo che solo quest'ultimo (attraverso la propria chiave privata, solo a lui nota) potrà decrifrarlo e quindi leggerne il contenuto.

Poi spedirà l'impronta, il documento cifrato e il certificato relativo alla propria firma al destinatario.

23

Il prestatore di servizio fiduciario

La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. Come fa la firma digitale a garantire la reale identità del firmatario? questi potrebbe usare il nome di un terzo o con un nome inventato.
Il sistema di crittografia asimmetrica e la funzione di hash non assicurano l'identificazione del soggetto che utilizza la coppia di chiavi.

Chi certifica la correlazione univoca tra firma e firmatario e lo attesta in un certificato?

↓

Il prestatore di servizio fiduciario

24

Il prestatore di servizio fiduciario (Reg. eIDAS – art. 3)

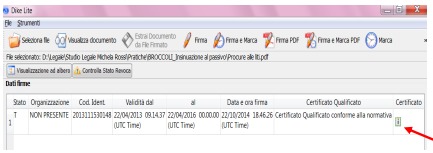
Prestatore di servizi fiduciari: è una persona fisica o giuridica che presta uno o più **servizi fiduciari**, o come prestatore di servizi fiduciari qualificato (qualifica assegnata dall'organismo di vigilanza) o come prestatore di servizi fiduciari non qualificato.

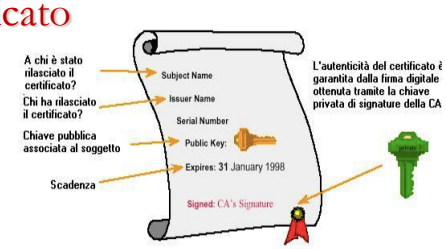
Il **servizio fiduciario**: è un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

- creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e **certificati** relativi a tali servizi; oppure
- creazione, verifica e convalida di certificati di autenticazione di siti web;
- conservazione di firme, sigilli o certificati elettronici relativi a tali servizi;

25

Certificato





Certificato di firma elettronica è **un attestato elettronico** che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona; (garantisce la connessione univoca tra chiave pubblica e il titolare di firma)

Attraverso il certificato si devono rilevare la validità del certificato stesso, nonché gli elementi identificativi del titolare (nome, cognome, codice fiscale) e del prestatore che l'ha emesso, nonché gli eventuali limiti d'uso.

26

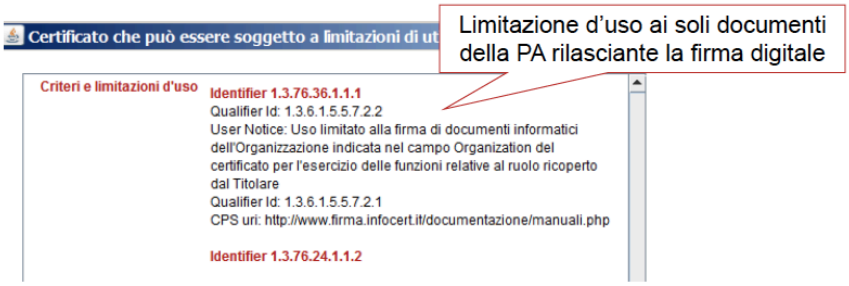
Contenuto dei certificati di firma elettronica qualificata

Art. 28. Certificati di firma elettronica qualificata (CAD)

2. In aggiunta alle **informazioni** previste nel Regolamento eIDAS **nel certificato di firma elettronica qualificata** può essere inserito il Codice fiscale […]
3. Il certificato di firma elettronica qualificata **può** contenere – se richiesto dal titolare di firma elettronica o dal terzo interessato – le seguenti informazioni […]:
   - **Qualifiche specifiche** del titolare di firma elettronica (appartenenza a ordini o collegi professionali, la qualifica di PU, l'iscrizione a albi, i poteri di rappresentanza, ecc)
   - I **limiti d'uso** del certificato
   - I **limiti del valor**e degli atti unilaterali e dei contratti per i quali il certificato può essere utilizzato
   - Uno pseudonimo.

27

Limiti d'uso



28

Obblighi per il prestatore di servizi

Art. 32. Obblighi del titolare e del prestatore di servizi di firma elettronica qualificata (CAD)

2. Il prestatore di servizi di firma elettronica qualificata è tenuto ad adottare tutte le **misure organizzative e tecniche idonee ad evitare danno a terzi**.

3. Il prestatore di servizi di firma elettronica qualificata che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:

- Provvedere con certezza alla **identificazione** della persona che fa richiesta della certificazione;
- **Rilasciare e rendere pubblico il certificato elettronico** […]
- Procedere alla tempestiva pubblicazione della **revoca** e della **sospensione** del certificato nei casi previsti dalla norma
- **Non copiare ne conservare le chiavi private** di firma del soggetto cui il prestatore ha fornito il servizio di certificazione;

4. Il prestatore di servizi di firma elettronica qualificata è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.

29

Revoca e sospensione del certificato

La revoca del certificato elettronico può definirsi come l'operazione con cui il certificatore annulla la validità del certificato.

La sospensione è, invece, l'operazione con cui il certificatore sospende la validità del certificato elettronico per un "determinato" periodo di tempo.

Art. 36. Revoca e sospensione dei certificati qualificati (CAD)

3.La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, **ha effetto** dal momento della **pubblicazione** della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

Art. 24 CAD

4-bis. L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a **mancata sottoscrizione**

30

La responsabilità dei prestatori di servizi fiduciari

Art. 13 Reg. eIDAS

[…] i prestatori di servizi fiduciari sono responsabili di danni causati con dolo e per negligenza a qualsiasi persona fisica e giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento.

- Per i prestatori di servizi non qualificato, l'onere della prova ricade su chi denuncia.
- Per i prestatori di servizi qualificati si presume il dolo e la negligenza pertanto devono dare prova di aver adottato tutte le misure idonee a evitare il danno.

Art. 30. Responsabilità dei prestatori di servizi fiduciari (CAD)

1. I prestatori di servizi fiduciari qualificati, […] che cagionano danno ad altri nello svolgimento della loro attività, sono tenuti al risarcimento, se non provano di avere adottato tutte le misure idonee a evitare il danno.

31

Qual è il valore giuridico e probatorio del documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale?

Art. 20. Validità ed efficacia probatoria dei documenti informatici (CAD)

1-bis. Il documento informatico soddisfa il requisito della **forma scritta** e ha **l'efficacia prevista dall'art. 2702 c.c**. quando vi è apposta una firma **digitale**, altro tipo di firma elettronica **qualificata** o una firma elettronica **avanzata** o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AGID ai sensi dell'art. 71 con modalità tali da garantire la sicurezza, l'integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

1-ter. L'utilizzo del dispositivo di firma elettronica qualificata o digitale **si presume riconducibile** al titolare di firma elettronica, salvo che questi dia prova contraria.

(Art. 2702 c.c. 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.)

32

Quale sottoscrizione per le scritture private di cui all'art. 1350 c.c.?

Art. 21. Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale. (CAD)

2-bis). Salvo il caso di sottoscrizione autenticata, le scritture private di cui **all'articolo 1350**, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, **a pena di nullità**, con firma **elettronica qualificata o con firma digitale**. Gli atti di cui all'art. 1350, numero 13, del Codice redatti su un documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale, […].

33

Busta crittografica

La firma digitale consiste nella creazione di un file, definito busta crittografica, con estensione p7m che racchiude al suo interno: il documento originale in chiaro, l'evidenza informatica della firma, il certificato qualificato.

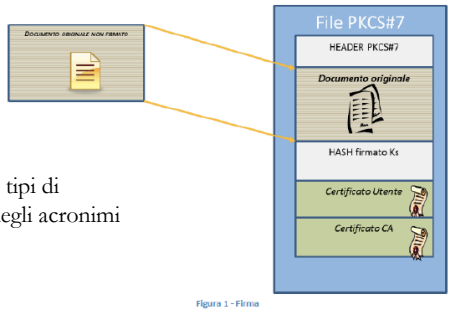


Figura 1 - Firma

Gli standard europei prevedono tre tipi di sottoscrizione digitale, identificati negli acronimi CAdES, PADES, XadES.

34

Firma digitale CAdES

Utilizzando il formato di firma digitale CAdES, l'apposizione di due o più firme può avvenire solo in due modi:

- Reimbustando in una nuova busta CAdES la busta generata dalla sottoscrizione precedente (**c.d. controfirma o firma matrioska**)
- Aggiungendo nella busta ulteriori firme, accompagnate dai diversi certificati (c.d. **firme congiunte o parallele**)

35

Controfirma o firma a matrioska

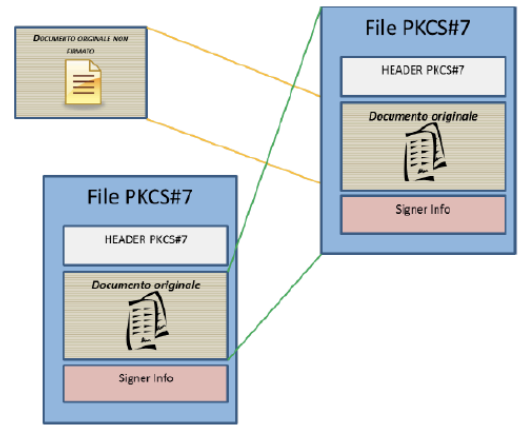


Figura 2 – Firma a matriosca – ogni firma afferisce al documento e alle firme precedenti formato CAdES

36

Firma congiunta o parallela

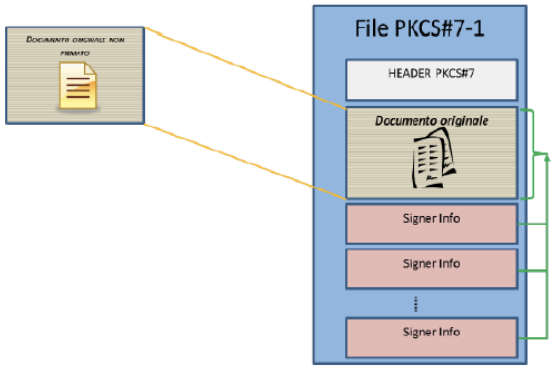


Figura 3 - Firme congiunte CAdES – ogni firma afferisce al documento

37

Quali sono gli accorgimenti tecnici da mettere in atto per la sottoscrizione delle clausole vessatorie presenti in un contratto stipulato in modalità elettronica?

- Soluzioni diverse a seconda che si usa la firma digitale nel formato CADES e nel formato PADES. In quest'ultimo caso non c'è problema in quanto tale tipologia di firma consente l'apposizione di due distinte sottoscrizioni (digitali) in due distinti punti di un documento informatico. Diverso il caso in cui si debba procedere alla sottoscrizione della clausole vessatorie con la firma CADES. Tale tipologia di firma, infatti, non permette di collocare la firma digitale in uno specifico punto del documento informatico, pertanto sarà necessario predisporre un distinto file, che diventerà un documento allegato al contratto, contenente le sole clausole vessatorie su cui la parte apporrà l'ulteriore – specifica – firma digitale. Occorrerà poi "unire" in modo inequivoco il file contenente le clausole vessatorie e la loro specifica sottoscrizione al contratto principale. In questo senso il DPCM 13 novembre 2014 prevede l'utilizzo dell'impronta del documento informatico che dovrà essere memorizzata in modo permanente sull'allegato in modo da garantire la riferibilità di quest'ultimo al contratto principale.

38

Firma PAdES

La firma digitale in formato PAdES, è un file con estensione pdf, consente di collocare fisicamente la firma digitale in un preciso punto del documento e anche di apportare modifiche al documento già sottoscritto. Questo grazie all'implementazione della funzione della gestione delle versioni del documento (versioning).

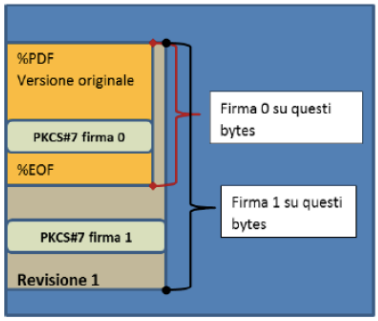


Figura 4 - busta formato PAdES – firme di versioni del documento firmato

39

Differenze giuridiche tra i due formati?

Cassazione Sez. Un. Civili, 27 Aprile 2018, n. 10266

«Tirando le fila sparse del discorso sin qui condotto, si deve escludere che le disposizioni tecniche tuttora vigenti (pure a livello di diritto dell'UE) comportino in via esclusiva l'uso della firma digitale in formato CAdES, rispetto alla firma digitale in formato PAdES. Nè sono ravvisabili elementi obiettivi, in dottrina e prassi, per poter ritenere che solo la firma in formato CAdES offra garanzie di autenticità, laddove il diritto dell'UE e la normativa interna certificano l'equivalenza delle due firme digitali, egualmente ammesse dall'ordinamento sia pure con le differenti estensioni ".p7m" e ".pdf". Addirittura, nel processo amministrativo telematico, per ragioni legate alla piattaforma interna, è stato adottato il solo standard PAdES (artt. 1, 5, 6, specifiche tecniche p.a.t., d.P.R. 16/02/2016, n. 40), mentre la giurisprudenza amministrativa riconosce la validità degli standards dell'UE tra i quali figurano, come già detto, sia quello CAdES, sia quello PAdES (Cons. Stato, n. 5504/2017, cit.)».

40

La firma automatica

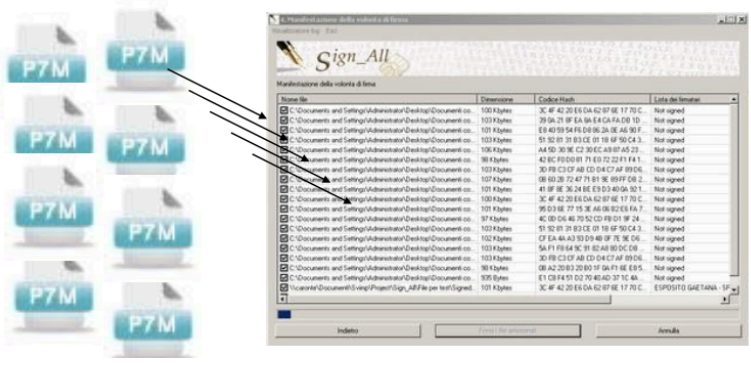
Art. 35 commi 2 e 3 CAD
2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quando previsto dalle Linee guida.
3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta **previo consenso** del titolare all'adozione della procedura medesima.

DPCM 22-2-2013
Firma automatica: particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita **previa autorizzazione** del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo.

41

La firma automatica

- **Il tool permette di selezionare tutti i documenti e di**
- **firmarli in automatico uno per uno**

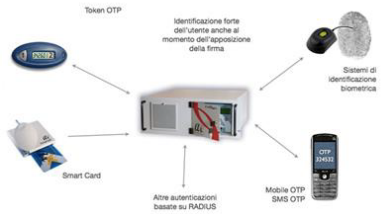


42

Firma remota

DPCM 22-2-2013
Firma remota: particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.

HSM: insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.



43

Firma remota

DPCM 22-2-2013

Art. 3 comma 4
La firma remota di cui all'art. 1 comma 1 lett. q è generata su un HSM custodito e gestito, sotto la responsabilità ,

- dal certificatore accreditato ovvero
- dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi
- ovvero dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi.

Il certificatore deve essere in grado, dato un certificato qualificato, di individuare agevolmente il dispositivo afferente la corrispondente chiave privata.

44

Firma remota

DPCM 22-2-2013

Art. 3 comma 5

Nel caso in cui il dispositivo di cui al comma 4 non sia custodito dal certificatore, egli deve:

a) indicare al soggetto che custodisce il dispositivo, le procedure operative, gestionali e le misure di sicurezza fisica e logica che tale soggetto è obbligato ad applicare;

b) effettuare verifiche periodiche sulla corretta applicazione delle indicazioni di cui alla lettera a) , che il soggetto che custodisce il dispositivo ha l'obbligo di consentire ed agevolare;

c) redigere i verbali dell'attività di verifica di cui alla lettera b) che potranno essere richiesti in copia dall'Agenzia ai fini dell'attività di cui all'art. 31 del Codice;

d) comunicare all'Agenzia il luogo in cui i medesimi dispositivi sono custoditi;

e) effettuare ulteriori verifiche su richiesta dell'Agenzia consentendo di partecipare anche ad incaricati dello stesso ente;

f) assicurare che il soggetto che custodisce il dispositivo si impegni a consentire le verifiche di cui alle lettere b) ed e).

45

Firma remota

DPCM 22-2-2013

Art. 3 comma 6 e 7

6. Nel caso in cui il certificatore venga a conoscenza dell'inosservanza di quanto previsto al comma 5, procede alla **revoca dei certificati** afferenti le chiavi private custodite sui dispositivi oggetto dell'inadempienza.

7. La firma remota di cui all'art. 1, comma 1, lettera q) , è realizzata con misure tecniche ed organizzative, esplicitamente approvate, per le rispettive competenze, dall'Agenzia, nell'ambito delle attività di cui agli articoli 29 e 31 del Codice, e dall' Organismo di Certificazione della Sicurezza Informatica, per quanto concerne la sicurezza del dispositivo ai sensi dell'art. 35 del Codice, **tali da garantire al titolare il controllo esclusivo della chiave privata.**

46

Il sigillo elettronico

Reg. eIDAS

creatore di un sigillo: una persona giuridica che crea un sigillo elettronico;

sigillo elettronico: dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;

sigillo elettronico avanzato: un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;

sigillo elettronico qualificato: un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;

47

Il sigillo elettronico

Reg. eIDAS

Art. 36 Requisiti dei sigilli elettronici avanzati

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

1. è connesso unicamente al creatore del sigillo;
2. è idoneo a identificare il creatore del sigillo;
3. è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e
4. è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Art. 35 Effetti giuridici dei sigilli elettronici

A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.

Un sigillo elettronico qualificato **gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati** a cui il sigillo elettronico qualificato è associato.

Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.

48

Validazione temporale

DPCM 22-2-2013

Art. 62 - **Valore delle firme elettroniche qualificate e digitali nel tempo**

1. Le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Reg. eIDAS

Validazione temporale: dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento.

49

Validazione temporale

Art. 20 comma 1-bis CAD

La data e l'ora di formazione di un documento informatico sono opponibili ai terzi se apposte in conformità alle previsioni delle Linee guida.

Linee guida contenenti le regole tecniche e raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate, pubblicate il 20/06/2019

Art. 41 del DPCM 22-2-2013

Riferimenti temporali opponibili ai terzi:

- Marca temporale
- Utilizzo di posta elettronica certificata
- Procedura di conservazione
- Segnatura di protocollo

50

Marca temporale

DPCM 22-3-2013

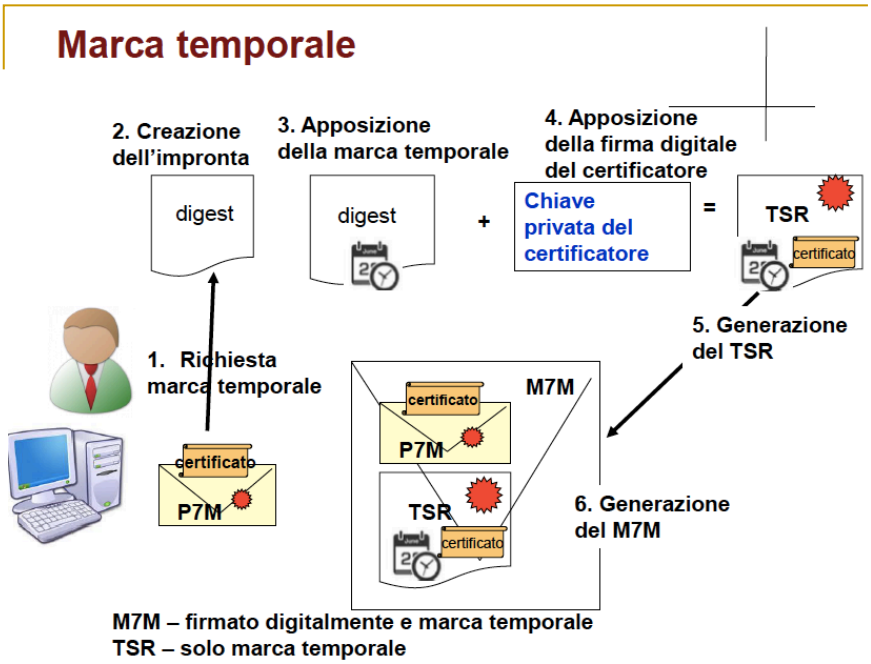
Marca temporale: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.
Riferimento temporale: evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.

La richiesta di marca temporale

- Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'invio della richiesta di marca temporale.
- La richiesta contiene l'evidenza informatica alla quale applicare la marca temporale.
- L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash scelte dal certificatore tra quelle stabilite ai sensi dell'art. 4, comma La generazione delle marche temporali garantisce un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo.

51

Marca temporale



52

Marca temporale

La marca temporale:

- Consente di stabilizzare la firma digitale nel tempo, indipendentemente dallo scadere del certificato di firma
- Viene apposta dal certificatore con un meccanismo di firma digitale
- Il riferimento temporale contenuto nella marca temporale è specificato con riferimento al Tempo Universale Coordinato (UTC)
- Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni, salvo richiesta di periodo maggiore da parte dell'interessato
- I riferimenti temporali realizzati dai certificatori accreditati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 20 comma 3 CAD.

53