NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

Linea 2.5 "Rafforzamento della capacità di attuazione dei Fondi SIE da parte degli Enti Locali"

ASSESSORATO REGIONALE
DELLE AUTONOMIE LOCALI E DELLA FUNZIONE PUBBLICA
DIPARTIMENTO DELLE AUTONOMIE LOCALI

Ciclo "I Responsabili per la Transizione al Digitale e l'innovazione negli Enti Locali'

La firma elettronica: tipologie e opportunità per una gestione digitale dei servizi pubblici

dott.ssa Laura Aglio

Unione Europea
Repubblica Italiana
Regione Siciliana
FSE FONDO SOCIALE EUROPEO
SICILIA 2020
PROGRAMMA OPERATIVO
FormezPA

La firma elettronica: caratteristiche, tipologie e valore giuridico

LE TIPOLOGIE DI FIRMA

Il Syllabus: le competenze di base

SYLLABUS "Competenze digitali per la PA"

https://www.competenzedigitali.gov.it/

1.2. Produrre, valutare e gestire documenti informatici	
Produrre e riconoscere la validità di un documento informatico. Acquisire, gestire e conservare appropriatamente documenti informatici.	
Livello di padronanza **BASE**	1.2.1.1 Conoscere il significato di documento informatico e di documento elettronico; conoscere le diverse modalità di formazione del documento informatico e le sue caratteristiche; 1.2.1.2 Conoscere il valore legale del documento informatico; 1.2.1.3 Conoscere il valore legale della firma digitale e del timbro digitale; 1.2.1.4 Conoscere l'esistenza e le funzionalità principali dei sistemi di protocollo informatico.

Il principio guida

Art. 3 CAD - il **diritto all'uso** di soluzioni e **di tecnologie** per poter colloquiare in modalità digitale con le Amministrazioni

"Chiunque ha il diritto di usare le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2"

"La gestione dei procedimenti amministrativi è attuata dai soggetti di cui all'articolo 2, comma 2, in modo da consentire, mediante strumenti informatici, la possibilità per il cittadino di verificare anche con mezzi telematici i termini previsti ed effettivi per lo specifico procedimento"

CAD e documenti informatici

Il Codice dell'Amministrazione Digitale (CAD-DLgs 82/2005) contiene una serie di **disposizioni normative che regolano l'uso dell'informatica nel contesto dei rapporti tra pubblica amministrazione italiana e cittadini** e regolamentano **procedure e condizioni per disponibilità, gestione, accesso, trasmissione, conservazione di informazione e di documenti o atti con modalità digitale**, individuandone le tecnologie più adeguate sia nell'ambito della pubblica amministrazione, che in quelle tra essa ed i privati e tra i privati.

documento informatico
"rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"

VS

documento analogico
"rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti"

Il documento elettronico

Ammesso che esista una reale differenza tra documento informatico (CAD) e documento elettronico, quest'ultimo viene introdotto dal **Regolamento eIDAS n. 910/2014** (art. 3, punto 35) che lo definisce come **"qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva"**.

Mentre il nostro **codice civile**, quindi, **si occupa di documento solo in modo indiretto**, ossia trattandone l'**efficacia probatoria agli artt. 2702 e 2712 c.c.**, rispettivamente relativi alla "scrittura privata" il primo ed alle "riproduzioni meccaniche" il secondo, il **D.LGS. n. 179/2016** ha recepito il Regolamento EIDAS e modificato il CAD definendo **il documento informatico** come: **"il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".**

Riferimenti normativi

Art. 1, lettera p) D.lgs. 82/2005 (C.A.D. Codice dell'Amministrazione Digitale)

"sono documenti **informatici** quei **file** che **contengano** una rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"

Art. 3 nr. 35 Regolamento UE n. 910/2014 (c.d. eIDAS)

"documento **elettronico**, **qualsiasi** contenuto **conservato** in forma **elettronica**, in particolare testo o registrazione sonora, visiva o audiovisiva"

Modalità per la realizzazione di un documento informatico a norma

- Registrazione nel Protocollo informatico
- **Apposizione di firma digitale**
- **Utilizzo di “marca temporale”**
- Riversamento in un sistema di conservazione “a norma”
- Trasmissione mediante PEC a terzi (modalità di ricevuta)

Validità dei documenti informatici

Art. 20 CAD - Validità ed efficacia probatoria dei Documenti informatici.

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

In tutti gli altri casi, 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 caratteristiche di qualità, sicurezza, integrità e immodificabilità.»

*art 2702 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.***

La sottoscrizione elettronica

La sottoscrizione elettronica non è semplicemente un'azione, si tratta piuttosto di un **processo informatico** che permette di **associare i dati utili a identificare il sottoscrittore al documento informatico**.
Il **processo di generazione della firma** costituisce **l'espressione della volontà di sottoscrivere il documento**.

Le diverse tipologie di firma elettronica consentono di raggiungere tale obiettivo in modo più o meno certo, fornendo contestualmente **effetti giuridici più o meno rilevanti**.

I documenti informatici sottoscritti elettronicamente possono essere distinti in **tre categorie**:

- documenti sottoscritti con firma elettronica ("semplice")
- documenti sottoscritti con firma elettronica avanzata
- documenti sottoscritti con firma elettronica qualificata (o firma digitale).

La firma elettronica: tipologie 1/2

Firma Elettronica (FE) - *Reg. eIDAS, articolo 3 comma 1 numero 10*
dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (c.d. **firma elettronica "semplice"**)

Firma Elettronica Avanzata (FEA) - *Reg. eIDAS, articolo 26; DPCM 22 febbraio 2013, articoli 55–61.*
insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono **l'identificazione del firmatario del documento** e garantiscono la **connessione univoca** al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

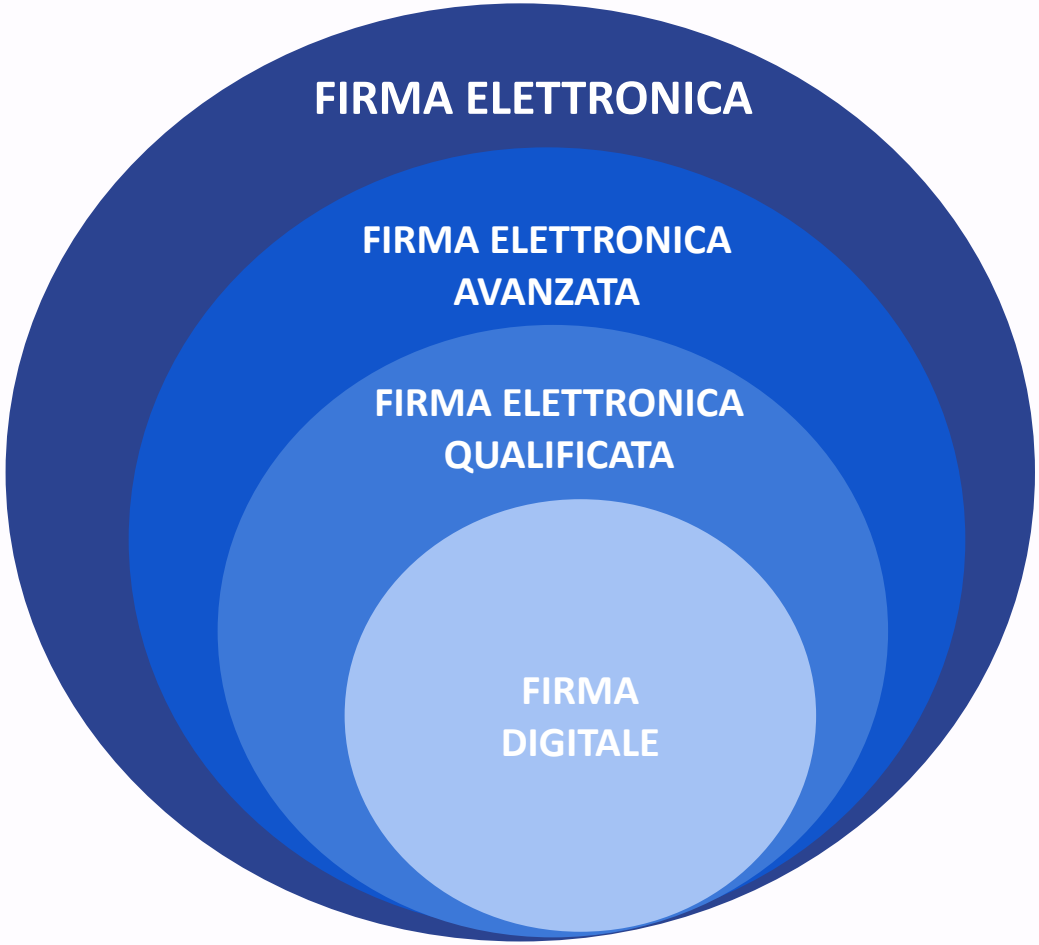
Firma Elettronica Qualificata (FEQ) - *Reg. eIDAS, articolo 3 comma 1 numero 12*
una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e **basata su un certificato qualificato per firme elettroniche.**

La firma elettronica: tipologie 2/2

Firma Digitale (FD) - *CAD, D.Lgs. N°82/2005, articolo 1 lettera s.*
un particolare tipo di firma elettronica 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.

Firma elettronica ex art. 20 - *CAD, D.Lgs. N°82/2005, articolo 20 comma 1-bis*
una **firma elettronica apposta su un documento informatico** formato previa identificazione informatica del suo autore attraverso un processo avente i requisiti fissati da AgID, con modalità tali da garantire la sicurezza, l'integrità e l'immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore **(c.d. "firma con SPID")**

La firma elettronica: le diverse tipologie



La firma digitale è – al momento – l'unica specie del genere "firma elettronica qualificata".

Le locuzioni "firma elettronica qualificata" (o FEQ) e "firma digitale" sono pertanto utilizzati come **sinonimi**.

Firma elettronica (semplice)

La firma elettronica cosiddetta **semplice** può essere costituita da molteplici elementi che consentono di **ricondurre degli atti o fatti giuridicamente rilevanti a una persona fisica**.
E' **un insieme di dati** che consentono l'identificazione univoca con dati informatici.

Un esempio è l'invio di **un messaggio di posta elettronica** che, in alcune circostanze, è stato considerato costituire prova in tribunale.
Altro esempio è **la firma a stampa** (il nome e cognome in calce a un documento).

È evidente che, per sua natura, non è adeguatamente robusta.

Firma elettronica avanzata (FEA)

E’ un **processo** – e non una tecnologia - **che associa una firma autografa ad un documento informatico** ed avente requisiti tali da garantirne l’identità. Fra i requisiti più importanti:

- l’**immodificabilità** del documento dopo la firma,
- la **riconducibilità** della firma ad una persona garantendo alla stessa l’uso esclusivo degli strumenti di firma.

Esempi sono diverse **implementazioni basate sulla cosiddetta firma “grafometrica”**, ovvero soluzioni di firma che raccolgono le caratteristiche comportamentali e tipiche della firma autografa (attraverso **l’uso di tavolette** molto evolute) quali la velocità, l’inclinazione, la pressione, l’accelerazione (e rallentamenti), i tratti aerei (legate in maniera certa al documento, consentono di raggiungere il risultato voluto).

Da notare che, ai sensi dell’art. 61 del DPCM 22 febbraio 2013, queste soluzioni possono essere **utilizzabili limitatamente per i rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che rende disponibile la soluzione**. Esempio la struttura ospedaliera che rende disponibile presso i propri sportelli soluzioni di firma elettronica avanzata ai fruitori delle prestazioni sanitarie.

Firma elettronica qualificata (FEQ)

Questa tipologia di firma elettronica è oggetto di normativa comunitaria, in particolare, del **Regolamento eIDAS** articolo 3 comma 1 numero 12 e della **Decisione di Esecuzione (UE) N°1506/2015 della Commissione dell'8 settembre 2015**.

Basate su un Certificato Elettronico Qualificato (emesso da un Ente Certification Authority) e su un sistema di chiavi crittografiche asimmetriche, queste firme sono **generabili esclusivamente con gli strumenti resi disponibili dai soggetti qualificati a tale scopo**.
L'elenco dei soggetti stabiliti in Italia è disponibile nell'apposita sezione del sito dell'Agenzia per L'Italia Digitale.

La Commissione Europea, ai sensi del Regolamento Europeo n. 910/2014, mette a disposizione un servizio che consente di conoscere tutti i prestatori di servizi fiduciari qualificati accreditati nell'Unione Europea - per brevità, "**certificatori accreditati**" - altrimenti indicati come QTSP- Qualified Trust Service Providers.

Firma elettronica qualificata (FEQ): Certificato di firma in corso di validità

Il certificato di firma ha una validità limitata nel tempo, e si ritiene che un eventuale malitenzionato non possa individuare la password necessaria per l'utilizzo del certificato prima della scadenza di quest'ultimo.

La firma digitale apposta su un documento utilizzando un certificato in corso di validità **non ha più alcun valore dopo la scadenza del certificato** stesso **a meno che al documento non venga apposta una marcatura temporale** (*time stamping*: associa data e ora certe e legalmente valide ad un documento informatico, dando una validazione temporale opponibile a terzi) prima della scadenza del certificato utilizzato per la firma.

Il caricamento di un documento firmato digitalmente all'interno di un sistema di protocollo a norma equivale a tutti gli effetti all'apposizione di una marcatura temporale e quindi, **i documenti firmati digitalmente regolarmente protocollati restano validi anche dopo la scadenza del certificato utilizzato per la firma**.

Firma elettronica qualificata (FEQ): documento non modificato dopo la firma

Il fatto che il documento non possa essere modificato dopo l'apposizione della firma digitale, comporta che **un documento con firma digitale valida è identico a quello all'atto della firma** (si parla di **integrità del documento**).

Dato che **una minima modifica** in qualsiasi punto del documento **comporterebbe l'invalidità della firma digitale**, in caso di documenti firmati digitalmente **non ha più senso l'atto di siglare le varie pagine di un documento** (*se vogliamo fare un parallelo con il cartaceo, possiamo considerare come se il documento digitale fosse scritto tutto su un unico foglio*).

Dato che i documenti firmati digitalmente non devono più essere modificati dopo l'apposizione della firma digitale, richiamiamo **la regola generale di firmare solo file in formato PDF** e, laddove possibile PDF/A.

I formati di firma digitale: CAdES, PAdES e XAdES

La firma digitale consiste sempre nella **creazione di un file ("busta crittografica"** *una sorta di "pacchetto" in cui sono racchiusi più oggetti: il documento originale, la firma e certificato di autenticità di quella firma rilasciata da un certificatore fiduciario*) **associato ad un documento**, creato dal software di firma in base al documento da firmare e al certificato del firmatario.

I formati di firma consentiti (file contenitore di firma) sono:

- CAdES ("Cryptographic message syntax")
- PAdES (PDF)
- XAdES (XML)

la differenza consiste nel modo in cui il nuovo file viene associato al documento.

Questi tre formati appartengono alla famiglia di formati di firme digitale chiamata **AdES**, acronimo di **Advanced Electronic Signatura**, cioè **firma elettronica avanzata.**

I formati di firma digitale: CAdES, PAdES e XAdES

Firma 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.

Firma PAdES: vengono sfruttate le caratteristiche dei documenti in formato **.pdf** e il file contenente la firma digitale viene inglobato insieme al documento stesso; è possibile aggiungere una firma grafica visibile sul documento, oltre quella digitale, potendo quindi essere inserita nel punto desiderato del documento

Firma XAdES: è lo standard per la sottoscrizione elettronica dei documenti in formato **XML,** di difficile lettura.

I formati di firma digitale: CAdES e PAdES

La **modalità CAdES permette di firmare qualsiasi tipo di documento** (docx, .xlsx, ecc.), *anche se è consigliato di firmare file in formato .pdf*

Per effettuare più firme sullo stesso documento è necessario re-imbustare in una nuova busta CAdES. 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** (es. Dike 6, ArubaSign, ecc.)

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** (es. Acrobat Reader)

La firma elettronica - ex art 20 del CAD

Il Codice dell'Amministrazione Digitale prescrive che il *«documento informatico soddisfa il requisito della forma scritta e ha **l'efficacia prevista dall'articolo 2702 del Codice Civile** quando […] è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con **modalità tali da garantire la sicurezza, integrità e immodificabilità** del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore»*.

La soluzione, prevede **l'utilizzo dell'identità digitale SPID** – quindi delle medesime credenziali – **per esprimere la volontà di sottoscrivere un documento** (Linee guida recanti Regole Tecniche per la sottoscrizione elettronica di documenti - ex art. 71 del CAD)

Si tratta di una nuova modalità per raggiungere il requisito della forma scritta e l'efficacia prevista dall'articolo 2702 del Codice Civile.

Firma elettronica semplice: effetti giuridici

Gli effetti giuridici di una firma elettronica sono riconducibili alla loro capacità di **soddisfare il requisito della forma scritta alla loro efficacia giuridica**, all'onere della prova (*all'individuazione del soggetto che, in caso di contestazione, deve fornire prove atte a dimostrare la validità o invalidità della firma oggetto di contestazione*).

Firma Elettronica (FE) - CAD, D.Lgs. N°82/2005, articolo 20 comma 1-bis paragrafo II
Per i documenti sottoscritti con firma elettronica "semplice", l'**idoneità** del documento informatico a soddisfare il requisito della forma scritta e il suo **valore probatorio** sono liberamente **valutabili in giudizio (a discrezione del giudice)**, in relazione alle **caratteristiche di sicurezza, integrità e immodificabilità**.

Firma elettronica avanzata: effetti giuridici

I documenti sottoscritti con firma elettronica avanzata soddisfano il **requisito della forma scritta** e hanno l'efficacia prevista dall'articolo 2702 del Codice Civile (CAD, D.Lgs. N°82/2005, articolo 20 comma 1-bis paragrafo II).

Il soggetto cui la firma elettronica avanzata afferisce può disconoscerla; è onere della parte che vuole avvalersi degli effetti giuridici di tale firma dimostrare la conformità con quanto prescritto al Titolo V del DPCM DPCM 22 febbraio 2013, articoli 55–61. **Il valore probatorio è certo**.

La firma elettronica avanzata è **utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che eroga la soluzione** di firma elettronica avanzata al fine di utilizzarla nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali (9 DPCM 22 febbraio 2013, articolo 60).

Firma elettronica qualificata: effetti giuridici 1/3

I documenti sottoscritti con firma elettronica qualificata (cd. firma digitale), soddisfano il **requisito della forma scritta** e hanno l'efficacia prevista dall'articolo 2702 del Codice Civile (CAD, D.Lgs. N°82/2005, articolo 20 comma 1-bis).

L'utilizzo del **dispositivo** di firma elettronica qualificata o digitale **si presume riconducibile al titolare** della firma elettronica, salvo che questi dia prova contraria (CAD, D.Lgs. N°82/2005, articolo 20 comma 1-ter). **Il valore probatorio è certo.**

Il fatto che la firma digitale sia apposta utilizzando un certificato di firma in corso di validità comporta che **il firmatario di un documento con firma digitale valida non possa disconoscere il documento da lui firmato**, salvo che non dia prova contraria (si parla di **non ripudio** del documento).

Pertanto, al fine del disconoscimento, è **l'apparente sottoscrittore** (il soggetto cui la firma afferisce) che **ha l'onere di dimostrare** che tale firma digitale non sia stata generata da lui.

Firma elettronica qualificata: effetti giuridici 2/3

Visto che il titolare della firma elettronica qualificata deve **assicurare la custodia del dispositivo di firma ed utilizzare personalmente il dispositivo** di firma (CAD, D.Lgs. N°82/2005, articolo 32 comma 1) considerato che:

• i dispositivi utilizzati (chiamati dispositivi sicuri per la generazione della firma, ovvero QSCD) sono utilizzabili esclusivamente **se si conoscono i codici segreti necessari**;
• **i codici segreti sono consegnati al titolare** della firma dal certificatore in modalità sicura

il titolare della firma che intende disconoscerla ha solo due alternative:

- dichiarare di *non aver mai richiesto la firma digitale* al certificatore accreditato (che conserva elementi utili a provare di aver rilasciato la firma al soggetto) o
- dimostrare che è *stato vittima di furto o sottrazione temporanea* del dispositivo e dei relativi codici per il suo utilizzo.

Firma elettronica qualificata: effetti giuridici 3/3

Il fatto che la firma digitale debba essere apposta utilizzando un certificato di firma rilasciato da un ente accreditato in grado di identificarne in modo certo il proprietario, comporta che **analizzando un documento con firma digitale valida è possibile verificare in modo certo l'identità di colui che lo ha firmato** (si parla di **autenticazione del firmatario**)

Un documento sottoscritto con firma digitale ha **piena efficacia giuridica** nel caso in cui siano rispettate le seguenti condizioni:

- la firma digitale sia apposta utilizzando **un certificato di firma** rilasciato da un ente accreditato in grado di identificarne in modo certo il proprietario
- la firma digitale sia apposta utilizzando un certificato di firma **in corso di validità**
- **il documento non sia modificato** dopo l'apposizione della firma

Nel caso in cui venga meno anche una di queste tre condizioni, la firma digitale NON è valida.

La certezza dell'autore

La certezza dell'autore è la **capacità di poter associare in maniera certa e permanente un soggetto ad un documento**.
Dalla normativa nazionale e unionale trattata, emerge che la certezza dell'autore è **garantita dall'utilizzo della firma elettronica qualificata (FEQ) e dal sigillo elettronico qualificato**.

La **firma elettronica avanzata** fornisce, ai sensi della sola normativa nazionale, la medesima presunzione giuridica, ma può essere messa in discussione, **non godendo dell'inversione dell'onere della prova**.

Possibile nullità degli atti

Il CAD prevede la nullità di specifici atti se non si utilizza una precisa tipologia di firma.

In particolare, prevede che gli atti elencati ai punti **da 1 a 12 dell'articolo 1350 del Codice Civile** (es. i contratti che trasferiscono la proprietà di beni immobili) debbano essere sottoscritti, a pena di nullità, con **firma elettronica qualificata o digitale**.

Gli atti di cui **al punto 13 dell'articolo 1350** del Codice Civile (es. atto costitutivo di associazione) possono essere sottoscritti anche con **firma elettronica avanzata e con la firma prevista dall'art. 20 del CAD**.

Quale firma scegliere?

Si è visto che le diverse tipologie di firma elettronica si differenziano per la loro **capacità di resistere al disconoscimento**.
Ne consegue che, nello scegliere la tipologia di firma elettronica adeguata allo specifico scopo, è bene **partire da un'analisi del rischio di disconoscimento**.

RISCHIO BASSO	sufficiente utilizzare la firma elettronica avanzata, specialmente nel caso in cui vi sono molti firmatari in un'unica postazione es. sportelli destinati al pubblico
RISCHIO RILEVANTE	preferibile utilizzare la firma elettronica qualificata

Per riassumere

Tipologie di Firme	Caratteristiche	Valore giuridico	Valore probatorio
Firma elettronica "semplice" (FE)	Sicurezza, integrità e immodificabilità.	Forma scritta.	Liberamente valutabile in giudizio dal giudice.
Firma elettronica avanzata (FEA)	FE + Art. 26 del Regolamento eIDAS e Titolo V del DPCM 22 febbraio 2013.	Forma scritta ex art. 2702 c.c. in ambito chiuso. Non può essere utilizzata per gli atti di cui ai punti da 1 a 12 dell'art. 1350 c.c.	Firma autografa riconducibile al titolare se la parte che vuole avvalersene ne dimostra la conformità con quanto prescritto al Titolo V del suddetto DPCM.
Firma elettronica qualificata (FEQ) e Firma digitale	FEA + dispositivo sicuro di firma + certificato qualificato	Forma scritta ex art. 2702 c.c.	Firma autografa legalmente riconosciuta. Presunzione firma autografa ex art. 25 del Regolamento eIDAS. Presunzione sull'utilizzo del dispositivo sicuro di firma ex art. 20, comma 1 ter, del CAD da parte del titolare.

Gli aspetti normativi: il CAD e il regolamento eIDAS

L'APPROCCIO EUROPEO ALLA FIRMA DIGITALE

NUOVI PERCORSI DI SVILUPPO
DELLA CAPACITÀ AMMINISTRATIVA
DELLA REGIONE SICILIANA

FormezPA

CAD - art. 24 Firma Digitale

1. 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.

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

3. Per la generazione della firma digitale **deve adoperarsi un certificato qualificato** che, **al momento della sottoscrizione, non risulti scaduto** di validità ovvero **non risulti revocato o sospeso.**

4. Attraverso **il certificato qualificato** si devono rilevare... la **validità del certificato** stesso, nonché gli **elementi identificativi del titolare di firma digitale e del certificatore e gli eventuali limiti d'uso.**

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**, salvo che lo stato di sospensione sia stato annullato… *omissis*

CAD - art. 65 Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica

Presentare istanze digitali alla Pubblica Amministrazione può richiedere che i documenti trasmessi siano sottoscritti con **una firma elettronica**, come prevede l'articolo 65 del Codice dell'Amministrazione Digitale.

I professionisti e i legali rappresentanti delle aziende sono sempre in possesso di una **Firma Elettronica Qualificata (o Firma Digitale).**

Tutti gli altri cittadini possono, invece, sottoscrivere i documenti usando la **Carta Nazionale dei Servizi (CNS) o la Carta d'Identità Elettronica (CIE)**, come prevede l'articolo 61 del Decreto del Presidente del Consiglio dei Ministri 22/02/2013: "*L'utilizzo della Carta d'Identità Elettronica, della Carta Nazionale dei Servizi, […] sostituisce, nei confronti della pubblica amministrazione,* ***la firma elettronica avanzata*** *ai sensi delle presenti regole tecniche per i servizi e le attività di cui agli articoli 64 e 65 del codice*"

Il Regolamento eIDAS n. 910/2014

Il Regolamento (UE) eIDAS (electronic IDentification Authentication and Signature) ha l'obiettivo di fornire **una base normativa a livello comunitario:**

- **per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri**
- per **interazioni elettroniche sicure fra cittadini, imprese e pubbliche amministrazioni** e incrementa **la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico** nell'Unione Europea

Il regolamento eIDAS è stato emanato il 23 luglio 2014 e ha **piena efficacia dal 1 luglio del 2016**.

Il Regolamento eIDAS n. 910/2014

- fissa le condizioni a cui gli Stati membri **riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche** che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro;
- stabilisce le norme relative ai **servizi fiduciari**, in particolare per le transazioni elettroniche;
- istituisce un **quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato e i servizi relativi ai certificati di autenticazione di siti web**.

Il Regolamento eIDAS n. 910/2014: novità

Tra le **novità** del Regolamento eIDAS stabilisce le norme per i servizi fiduciari:

"**servizio fiduciario**”: un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi :

a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi
b) creazione, verifica e convalida di certificati di autenticazione di siti web
c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi

"**servizio fiduciario qualificato**", un servizio fiduciario che soddisfa i requisiti del regolamento

Prestatore di servizi fiduciari: una persona fisica o giuridica che presta uno o più servizi fiduciari

Prestatore di servizi fiduciari qualificato: un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato.

Regolamento eIDAS vs CAD

Il Decreto Semplificazioni Art. 25, D.L. 76/2020 (art. 44 CAD)

prevede **semplificazioni al sistema di qualificazione dei prestatori di servizi fiduciari** e dei conservatori di documenti informatici.

Con riferimento ai servizi fiduciari, **si demanda l'individuazione dei requisiti in relazione alla specifica attività svolta, nel rispetto dell'art. 24 Regolamento eIDAS**, al decreto adottato dal Presidente del Consiglio dei ministri o dal ministro delegato per l'innovazione tecnologica, sentita l'AgID.

Il Regolamento eIDAS n. 910/2014: novità

Tra le **novità** del Regolamento eIDAS, inoltre è:

- introdotto il sigillo elettronico
- riconosciuta e introdotta la firma digitale remota
- riconosciuta e introdotta la validazione temporale
- introdotto il servizio di recapito certificato
- introdotti i certificati qualificati di autenticazione dei siti web

Il sigillo elettronico qualificato

Il sigillo elettronico qualificato è stato introdotto nel nostro ordinamento con l'emanazione del **Regolamento eIDAS**.

Sostanzialmente è **equivalente a una firma elettronica qualificata**, con la differenza che non **afferisce** a una persona fisica, bensì **a una persona giuridica**.

Mentre da una firma siamo in grado di individuare con certezza un soggetto attraverso il suo nome, cognome, codice fiscale ecc., **da un sigillo possiamo risalire con certezza ad una persona giuridica** attraverso la sua denominazione, partita IVA o codice fiscale, ma ***non abbiamo alcun riferimento alla persona fisica che ha materialmente utilizzato le credenziali per generare tale sigillo.***

La firma digitale remota

Mentre la firma digitale si basa su un sistema di chiavi crittografiche e prevede l'utilizzo di un supporto come la business key (una USB) o la smart card (una carta simile alla carta di credito), con la Firma Digitale Remota, invece, **non servono USB o smart card** (e relativi lettori): basta un computer collegato a rete internet, un software di firma per selezionare i testi da firmare e una One Time Password generata da token o applicazione.

A differenza della Firma Digitale tradizionale, con cui si ha a disposizione sia il certificato di firma digitale che il **certificato CNS** (Carta Nazionale dei Servizi), **la Firma Digitale Remota non gestisce** quest'ultimo, **pertanto, non è possibile accedere ai servizi online della Pubblica Amministrazione.**

Le marche temporali

La marca temporale, normata dagli articoli 41 e 42 del Regolamento eIDAS. è un servizio offerto da un Certificatore accreditato, che consente di **associare data e ora, certe e legalmente valide, a un documento informatico**, permettendo una **validazione temporale del documento opponibile a terzi.**

Il servizio di Marcatura Temporale può essere utilizzato anche su documenti non firmati digitalmente.

eIDAS introduce due definizioni:

- **validazione temporale elettronica**, 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 (a validazione temporale elettronica dà luogo a una presunzione legale relativa alla certezza della data e dell'ora);
- **validazione temporale elettronica qualificata**, una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42 del Regolamento eIDAS.

Il servizio di recapito certificato (Serc)

Il servizio elettronico di recapito certificato (SERC) è **uno dei servizi fiduciari di base** stabiliti nel Regolamento eIDAS (Regolamento UE 910/2014) e come tale **può essere erogato da un prestatore qualificato** secondo quanto stabilito nel Regolamento medesimo. Esso è **analogo all'emissione di certificati qualificati per la firma o di marche temporali**.

La nostra **Posta Elettronica Certificata è certamente un servizio elettronico di recapito certificato** e il Legislatore lo ha previsto nel CAD art. 1-ter. Ove la legge consente l'utilizzo della posta elettronica certificata è ammesso anche l'utilizzo di altro servizio elettronico di recapito certificato qualificato ai sensi degli articoli 3, numero 37), e 44 del Regolamento eIDAS.

"servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto danni o di modifiche non autorizzate"

Il Regolamento eIDAS n. 910/2014: obiettivi

- Instaurare **la fiducia online** per agevolare lo sviluppo economico e sociale
- Realizzare **una base comune per interazioni elettroniche sicure** fra imprese, cittadini e autorità pubbliche, in modo da migliorare l'efficacia dei servizi elettronici pubblici e privati, nonché dell'ebusiness e del commercio elettronico, nell'Unione europea
- **Eliminare gli ostacoli all'esercizio dei diritti dei cittadini** dell'Unione
- Consentire ai cittadini di **utilizzare la loro identificazione elettronica** per autenticarsi in un altro Stato membro
- **Responsabilità dello Stato membro notificante**, in merito ai sistemi di identificazione e autenticazione riconosciuti dallo stesso
- **Responsabilità di tutti i prestatori di servizi fiduciari** per i danni provocati a persone fisiche o giuridiche a causa del mancato rispetto degli obblighi previsti dal regolamento
- **Mutuo e pieno riconoscimento della firma digitale**
- **Individuare formati delle firme digitali europei**
- **Autenticazione dei siti web**

Il Regolamento eIDAS n. 910/2014: la firma

Il Regolamento eIDAS disciplina **tre tipologie di firme elettroniche**:

Firma Elettronica - dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare

Firma Elettronica Avanzata (FEA) - firma elettronica che soddisfi i seguenti 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;
- è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Firma Elettronica Qualificata (FEQ) – che in aggiunta a quelle di una firma elettronica avanzata possiede queste caratteristiche:

- è creata su un dispositivo qualificato per la creazione di una firma elettronica
- è basata su un certificato elettronico qualificato
- ha effetto giuridico equivalente a quello di una firma autografa.

Regolamento eIDAS vs CAD

Mentre nel **Codice dell'amministrazione digitale** (CAD - Decreto Legislativo 7 marzo 2005, n. 82) la firma elettronica viene definita come un **insieme di dati in forma elettronica utilizzati come metodo di identificazione informatica**, nel **Regolamento eIDAS**, al Capo I Art. 3, la firma elettronica è descritta come **dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare**.

La locuzione "utilizzati dal firmatario per firmare" ha una funzione prettamente identificativa, comportando **un rafforzamento della funzione dichiarativa** (cioè la manifesta adesione al contenuto del documento firmato) e **della funzione probatoria** (cfr. art. 21 del CAD).

Il Regolamento eIDAS n. 910/2014

Interoperabilità delle firme elettroniche (firma digitale) **e dei sistemi di validazione temporale** (marca temporale)

Il Regolamento (articolo 25, comma 3) prescrive che: "*Una firma elettronica qualificata basata su un* ***certificato qualificato*** *rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata* ***in tutti gli altri Stati membri***".

eIDAS vs CAD: L'efficacia giuridica delle firme elettroniche

	Firma elettronica	Firma elettronica avanzata,qualificata o digitale
CAD	Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità (art.21)	**Garantisce l'identità dell'autore, l'integrità e l'immodificabilità del documento**, ha l'efficacia prevista dall'art. 2702 del codice civile. L'utilizzo del dispositivo di firma qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria (art.21)
eIDAS	Non sono negati effetti giuridici per via della sua forma elettronica. Spetta al diritto nazionale dei singoli Paesi europei definire gli effetti giuridici delle firme elettroniche (art. 25)	**Ha un effetto giuridico equivalente a quello di una firma autografa.** Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri (**mutuo riconoscimento**).

Il Regolamento eIDAS n. 910/2014

I **formati** che queste firme elettroniche qualificate devono possedere sono definiti nella Decisione di esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015: fra quelli previsti, **anche il formato PDF**.

Per **verificare la validità delle firme elettroniche qualificate** basate su certificati rilasciati da tutti i soggetti autorizzati in Europa, la Commissione europea ha reso disponibile **un'applicazione open source, Il Digital Signature Service (DSS)**

Il Regolamento eIDAS n. 910/2014

L'**obbligo di riconoscere le firme elettroniche qualificate** introdotto nel Regolamento eIDAS (art. 25, comma 3) deve essere onorato, altrimenti, oltre a non consentire l'esercizio di un diritto dei cittadini dell'unione, si incorre in una procedura di infrazione.
Al fine di verificare che i propri sistemi di verifica delle firme elettroniche qualificate siano conformi alla normativa europea, si rende disponibili un documento di prova sottoscritto con una firma elettronica qualificata basata su un certificato qualificato rilasciato in Irlanda. Tale verifica deve andare a buon fine.

I concetti chiave

CAD e Regolamento eIDAS

Interoperabilità delle firme elettroniche

NORMATIVA

Sportello Unico Digitale

Una completa digitalizzazione dei servizi pubblici nel 2023

STRATEGIA

DIRITTO ALL'USO DELLE TECNOLOGIE

Documento informatico

Efficacia probatoria con apposizione di firma digitale

STRUMENTI

Tipologie di firme

La firma digitale come firma elettronica qualificata

STRUMENTI