

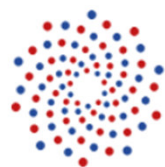


Città metropolitana
di Roma Capitale

Piano formativo

«OpenID Connect – PNRR 1.4.4»

Comuni Area metropolitana di Roma Capitale



CAPITALE LAVORO

società di  Città metropolitana
di Roma Capitale

Con il supporto tecnico di



LIVELLO NORMATIVO

LE FIRME ELETTRONICHE: prestatori di servizi – efficacia probata dei documenti informatici

Docente:

Dott. Rosario Carrisi

Consulente di management

Esperto di governance, e-government delle P.A



UD: CAD-007-01 - Edizione 05-2024

In questa unità didattica affronteremo i seguenti argomenti:

- **Approfondimento sui prestatori di servizi (certificatori);**
- **Valenza giuridico probatoria riconosciuta dalla normativa dei documenti sottoscritti con firme elettroniche**





**PRESTATORI DI SERVIZI FIDUCIARI
(IL CERTIFICATORE)**

Coloro che desiderano dotarsi di un dispositivo di firma digitale devono rivolgersi ai **prestatori di servizi fiduciari accreditati**, soggetti pubblici o privati che, sotto la vigilanza di AgID, emettono certificati qualificati (per la firma digitale) e certificati di autenticazione (per le carte nazionali dei servizi).

La firma digitale viene generata grazie ad una coppia di chiavi digitali asimmetriche attribuite in maniera univoca ad un soggetto, detto titolare:

- la **chiave privata** è conosciuta solo dal titolare ed è usata per generare la firma digitale da apporre al documento;
- la **chiave da rendere pubblica** è usata per verificare l'autenticità della firma.

Questo metodo è conosciuto come crittografia a doppia chiave e garantisce la piena sicurezza visto che la chiave pubblica non può essere utilizzata per ricostruire la chiave privata

- La certificazione della chiave pubblica costituisce il punto critico di tutto il sistema della firma digitale
- Il vantaggio dei sistemi a crittografia a chiave asimmetrica è la possibilità di rendere pubblica una delle due chiavi
- La pubblicazione e la verifica delle chiavi si svolgono per via telematica accedendo ad appositi **registri**

Art. 29 CAD - Qualificazione dei fornitori di servizi

[..]

6. A seguito dell'accoglimento della domanda, il AgID dispone l'iscrizione del richiedente in un apposito elenco di fiducia pubblico, tenuto dal AgID stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

- L'elemento più importante è l'affidabilità dei soggetti che gestiscono i registri
- E' indispensabile che i gestori di questi registri siano soggetti assolutamente scrupolosi e fidati (e a sua volta certificati)



- Identificare con certezza la persona che fa richiesta della certificazione;
- Rilasciare e rendere pubblico il certificato
- Specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite
- Procedere tempestivamente alla revoca od alla sospensione del certificato (richiesta da parte del titolare, terzo dal quale derivino i poteri, provvedimento dell'autorità)



- Sono soci di AssoCertificatori le società *ACTALIS, ARUBA, INFOCERT, I.T. TELECOM, LISIT, POSTECOM.*
È socio anche il CONSIGLIO NAZIONALE DEL NOTARIATO a garanzia del pieno utilizzo **della firma digitale da parte di tutti i notai italiani**

➤ **Validazione temporale**

Procedura informatica mediante la quale si attribuisce ai documenti informatici una data ed un orario opponibili ai terzi

➤ Determinare il momento di cui è stato sottoscritto

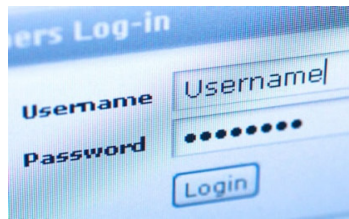
Nel documento informatico questo si ottiene attraverso la generazione di una **marca temporale** che viene applicata al documento ad opera di una terza parte fidata (*certificatore*)





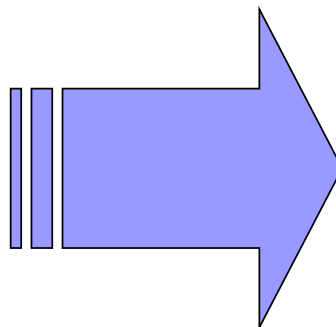
EFFICACIA PROBATORIA DEI DOCUMENTI SOTTOSCRITTI CON FIRMA ELETTRONICA

Art. 34 CAD:



- Atti interni possono essere firmati con firma elettronica
- Atti esternati devono essere firmati con firma digitale

**Documento
Informatico**



**Validità legale e giuridica
al documento**

A secondo del differente livello di sicurezza presentato dalle diverse tipologie di firme, differente sarà anche l'efficacia probatoria dei documenti informatici sottoscritti, nonché la loro capacità di soddisfare il requisito della forma scritta

- **a livello nazionale**, l'art. 20, comma 1-bis, del CAD, un *“documento informatico soddisfa il requisito della forma scritta e ha efficacia prevista dall' art. 2702 del c.c.”*, **se vi è apposta una tipologia di firma ritenuta univocamente sicura**, oppure se è stato formato attraverso un processo di identificazione informatica tale da soddisfare particolari requisiti.

Il verificarsi di tali circostanze fa sì che il documento informatico, assumerebbe l'efficacia di una scrittura privata, la quale *“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”* (art. 2720 c.c.).

- ❑ La sottoscrizione degli atti deve farsi per iscritto ai sensi dell' art. 1350 c.c., ma esiste una differenziazione tra le differenti tipologie di firme utilizzabili per sottoscrivere le varie categorie di atti.

- ❑ Nello specifico, *“salvo il **caso di sottoscrizione autentica**, le scritture private di cui all' art. 1350, primo comma, numeri da 1 a 12, del c.c., se fatte con documento informatico, sono sottoscritte a pena di nullità, **con firma elettronica qualificata o firma digitale**”, mentre maggiore libertà di azione è consentita per gli atti di cui all' art. 1350, primo comma, numero 13, del c.c., che *“redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale”**

Variabile a seconda della tipologia di firma elettronica adottata è anche la **ric conducibilità al titolare della firma dell'utilizzo del dispositivo utilizzato per apporla**.

Nel caso di utilizzo di firma elettronica qualificata o digitale, si determina un'inversione dell'onere della prova, e *“l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria”*.

D.lgs. 82/2005, art. 20, comm. 1-ter.

Data e ora di formazione del documento informatico

Per quel che riguarda la data e l'ora di formazione del documento informatico, queste sono opponibili ai terzi, esclusivamente se sono state apposte conformemente alle Linee guida di cui all'art. 71 del CAD

D.lgs. 82/2005, art. 20, comm. 1-bis

A livello comunitario, gli effetti giuridici delle firme elettroniche sono specificati nell' **art. 25 del Regolamento (UE) 910/2014**

- ❑ Indipendentemente dalla particolare firma elettronica considerata, a questa *“non possono essere negati gli effetti giuridici e l’ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate”*. art. 25,
paragrafo 1
- ❑ L’effetto giuridico ottenibile aumenta se si considera la firma elettronica qualificata, dato che questa *“ha effetti giuridici equivalenti a quelli di una firma autografa”*. art. 25,
paragrafo 2
- ❑ Se poi questa è anche basata su di un certificato qualificato che è stato rilasciato in uno Stato membro dell’ Unione europea, allora dovrà essere riconosciuta come firma elettronica qualificata anche in tutti gli altri Stati membri. art. 25,
paragrafo 3

Schema riassuntivo della valenza giuridica delle firme (1/2)

19

Tipo di firma	Italia (D.lgs. 82/2005)	Comunitaria (Reg. UE 910/2014)
Firma elettronica	<ul style="list-style-type: none">• Ammissibile come prova in procedimenti giudiziari, ma liberamente valutabile dal giudice	<ul style="list-style-type: none">• Ammissibile come prova in procedimenti giudiziari
Firma elettronica avanzata	<ul style="list-style-type: none">• Soddisfa il requisito della forma scritta e ha efficacia prevista dall'articolo 2702 del Codice Civile (ex art. 20, c.1-bis del CAD)• Utilizzabile per la sottoscrizione degli Atti di cui al Codice Civile, art. 1350, comma 13 (ex Art. 21, c.2-bis del CAD)	<ul style="list-style-type: none">• Ammissibile come prova in procedimenti giudiziari

Schema riassuntivo della valenza giuridica delle firme (2/2)

20

Tipo di firma	Italia (D.lgs. 82/2005)	Comunitaria (Reg. UE 910/2014)
Firma elettronica qualificata	<ul style="list-style-type: none"> • Soddisfa il requisito della forma scritta e ha efficacia prevista dall'articolo 2702 del Codice Civile (ex art. 20, c.1-bis del CAD) • Utilizzabile per la sottoscrizione degli Atti di cui al Codice Civile, art. 1350, comma 13 (ex Art. 21, c.2-bis del CAD) 	<ul style="list-style-type: none"> • Ha effetti giuridici equivalenti a quelli di una firma autografa
Firma digitale	<ul style="list-style-type: none"> • Si presume riconducibile al titolare della firma, salvo che questi dia prova contraria (inversione dell'onere della prova) – (ex art. 20, c.1-ter del CAD) 	<p>NON APPLICABILE <i>è un particolare tipo di firma elettronica qualificata presente esclusivamente nell'ordinamento italiano.</i></p>

	Definizione	Valore probatorio	Esempi
Firma Elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Efficacia probatoria valutabile dal giudice caso per caso	<i>Pin, firma biometrica</i>
Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e 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	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i> tranne che per i contratti immobiliari	<i>Firma su tablet</i>
Firma Elettronica Qualificata	Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i>	<i>Smart-card, token</i>
Firma Elettronica Digitale	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici	Efficacia probatoria della scrittura privata integra la forma scritta <i>ad substantiam</i>	<i>Smart-card, token</i>



EFFETTI GIURIDICI DEL SIGILLO ELETTRONICO

I sigilli elettronici nel nostro ordinamento non sono definiti direttamente, ma vengono recepiti dal diritto comunitario (Regolamento (UE) 910/2014).

Pertanto per comprendere e conoscere i loro effetti giuridici dobbiamo ricondurci alla normativa europea.

L'inserimento del comma 1-bis dell'art.1 CAD dal D.Lgs. 179/2016 dove si evidenzia come *“ai fini del presente Codice, valgono le definizioni di cui all' articolo 3 del regolamento eIDAS”* si legge esplicitamente il legame che lega il Codice dell' Amministrazione Digitale al Regolamento eIDAS. Dunque, le definizioni che valgono ai fini del CAD sono date dalla sommatoria di quelle presenti nel Regolamento eIDAS e di quelle contenute nel CAD stesso.

Gli effetti giuridici dei sigilli elettronici sono disciplinati nell' **art.35 del Regolamento (UE) 910/2014**.

Indipendentemente dal particolare sigillo elettronico considerato, a questo *“non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati”*.

Il livello di tutela sale se si considera il **sigillo elettronico qualificato**. Il quale, in aggiunta, *“gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato”*.

Se il sigillo, poi, si basa su di un **certificato qualificato** che è stato rilasciato in uno Stato membro dell' UE, questo sarà riconosciuto anche negli altri Stati membri.

Tipo di sigillo	Italia	UE
Sigillo elettronico	Tale strumento non direttamente presente nell'ordinamento italiano, di completa derivazione dal diritto comunitario	Ammissibile come prova in procedimenti giudiziari
Sigillo Elettronico avanzato	Tale strumento non direttamente presente nell'ordinamento italiano, di completa derivazione dal diritto comunitario	Ammissibile come prova in procedimenti giudiziari
Sigillo elettronico qualificato	Tale strumento non direttamente presente nell'ordinamento italiano, di completa derivazione dal diritto comunitario	Gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato

Fino a questo punto, sembra che il sigillo elettronico e la firma digitale possano essere considerati, di fatto, equivalenti (visto che, in sostanza, anche le due definizioni sono, di fatto, analoghe). In realtà, tra i due strumenti sussistono delle precise differenze. Differenze da conoscere bene per sapere quale dei due strumenti utilizzare a seconda di circostanze e necessità.

Sigillo elettronico	Firma digitale
Garantisce l'origine e l'integrità dei documenti digitali	Garantisce l'identità del firmatario di un documento digitale e conferisce piena validità legale a un documento digitale
Si riferisce a una persona giuridica (un organismo unitario composto da una pluralità di individui o un complesso di beni, al quale vengono riconosciuti diritti e doveri)	Si riferisce a una persona fisica (un soggetto di diritto, dotato di capacità giuridica, con degli obblighi e dei diritti fin dalla sua nascita)

In conclusione, si può dire che la firma digitale è uno strumento indicato per le persone, mentre il sigillo elettronico è a uso (quasi) esclusivo di enti o aziende.

La roadmap di eIDAS 2.0: a che punto siamo

Il 29 febbraio 2024 la revisione è stata ufficialmente approvata dal Parlamento Europeo ed è **stata pubblicata nella Gazzetta Ufficiale il 30 aprile 2024**. Successivamente, entro 12/24 mesi, dovranno essere pubblicati i cosiddetti “Implementing Acts” e il nuovo regolamento eIDAS entrerà ufficialmente in vigore.



«[] se non v'è dispiaciuta affatto, vogliatene bene a chi l'ha scritta, e anche un pochino a chi l'ha raccomandata. Ma se in vece fossimo riusciti ad annoiarvi, credete che non s'è fatto apposta.»

Cap. XXXVIII – I Promessi Sposi

Gratie

