

Scheda di approfondimento:

DALLA FIRMA AUTOGRAFA A QUELLA ELETTRONICA A QUELLA DIGITALE

Al momento che i documenti cartacei cominciarono ad essere sostituiti da quelli informatici nacque la necessità di trovare un metodo di firma che sostituisse la firma autografa, dandogli lo stesso valore giuridico di autenticità e immodificabilità.

LA FIRMA ELETTRONICA “SEMPLICE”

La **firma elettronica** rappresenta la più semplice fattispecie di sottoscrizione informatica.

Un esempio tipico è un messaggio di posta elettronica ordinaria: se riceviamo un messaggio dalla casella di posta di Mario Rossi possiamo presumere che la firma apposta Mario Rossi sia stata fatta proprio da lui.

E' definita nel Regolamento Europeo 910/2014 (eIDAS) al numero 10 dell'articolo 3 come *“l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica”*.

FIRMA ELETTRONICA AVANZATA (FEA)

Altro esempio tipico della firma elettronica è costituito dalla **firma grafometrica** utilizzata su tablet in molti contesti tra i quali le banche e le assicurazioni.

Questa tipologia viene anche detta dal Regolamento Europeo 910/2014 art. 3 n. 11 **firma elettronica avanzata** (FEA) in quanto aumenta le caratteristiche di capacità di identificazione unica del firmatario, è creata mediante dati che il firmatario può utilizzare sotto il proprio esclusivo controllo e può consentire di identificazione ogni eventuale modifica successiva.

FIRMA ELETTRONICA QUALIFICATA (FEQ)

Per potere attribuire alla firma informatica una valenza equivalente alla firma autografa in ogni contesto, soprattutto in quello giuridico, nasce l'esigenza di aumentare le garanzie di identificazione del soggetto firmatario .

Vengono, quindi, attivati dei meccanismi di sicurezza basati su un “certificato **qualificato**” che trasformano la firma elettronica avanzata (FEA) in **firma elettronica qualificata** (FEQ).

Il **certificato qualificato** può essere considerato come un documento elettronico che viene rilasciato da un autorità detta Certificatore sotto lo stretto controllo dell'AgID (Agenzia per l'Italia Digitale) che attesta in modo certo che una data persona è titolare dello strumento tecnologico utilizzato all'atto della sottoscrizione di un documento.

A partire dall'entrata in vigore, il 1° luglio 2016, del Regolamento europeo eIDAS (electronic IDentification Authentication and Signature) n. 910/2014 la firma elettronica qualificata (FEQ) ha valore europeo ed è interoperabile all'interno del mercato interno essendo le regole tecniche comuni a tutti gli Stati membri.

Le tipologie di FIRMA ELETTRONICA QUALIFICATA (FEQ)

1) FIRMA DIGITALE

Un particolare tipo di firma elettronica qualificata è la **firma digitale**, prevista in Italia dal Codice dell'amministrazione digitale (CAD) che è *“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”*.

In altre parole, è l'equivalente elettronico della tradizionale firma autografa su carta, in quanto è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'integrità, l'autenticità, e la non ripudiabilità.

Per dotarsi di firma digitale è necessario rivolgersi ad un O.D.R. cioè un Operatore della Registrazione che è un soggetto (società di servizi, ordine professionale...) autorizzato al rilascio da AGID l'agenzia pubblica per l'Identità Digitale, previa identificazione, del dispositivo smart card o token DNA per la firma digitale.

La Camera di Commercio di Firenze è un ODR e quindi è autorizzata a rilasciare dispositivi di firma Digitale (smart card e token wireless) certificati dal Certificatore Infocamere con all'interno la CNS (Carta Nazionale dei Servizi) che permette l'accesso ai siti dell'amministrazione pubblica.

2) LA FIRMA REMOTA

La firma remota è una **“particolare procedura di firma elettronica qualificata o firma digitale”** (art. 1 c. 1 lett. q DPCM 22 febbraio 2013). In pratica, attraverso una speciale tecnologia, è possibile firmare i documenti informatici, eliminando le problematiche connesse all'utilizzo dei dispositivi (Lettori, Smart Card e Token USB)

E' sufficiente una qualsiasi postazione dotata di collegamento ad internet e una OTP (One Time Password), o password dinamica, generata attraverso un apposito dispositivo che può essere anche lo smartphone, per firmare qualsiasi documento.

Le OTP sono considerate le password più sicure in quanto sono generate da un sistema informatico e distrutte direttamente dallo stesso pochi secondi dopo eliminando il principale difetto delle password statiche che devono essere memorizzate.

La firma remota rilasciata dalla Camera di Commercio di Firenze ha effetti analoghi alla firma digitale apposta tramite carta CNS.

3) LA FIRMA AUTOMATICA O MASSIVA

La **firma automatica o massiva** è un'altra **“particolare procedura di firma elettronica qualificata o firma digitale”** (art. 1 c. 1 lett. r DPCM 22 febbraio 2013) che viene *“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”*.

Nata per la sottoscrizione di documenti informatici che per loro natura non richiedono di essere presentati al titolare della firma prima dell'apposizione della stessa, come per fatture o atti di routine e utilizzata generalmente per quantità copiose di atti, ha intrinseco il suo difetto più grande cioè la possibilità di non essere usata con piena rispondenza ai suoi requisiti di legge ovvero al principio della consapevolezza della sottoscrizione da parte del titolare.

Il titolare cioè, non vedendo quello che sottoscrive, snatura la funzione dichiarativa della sottoscrizione, cioè l'assunzione della paternità e del consenso del documento.