iRealtors

Il tuo ufficio, in tasca

Firma elettronica Avanzata (FEA)

Valenza giuridica

Ambiti applicativi

SOMMARIO

1. INTRODUZIONE

Da qualche anno la firma elettronica è entrata prepotentemente nell'ordinamento italiano e trova sempre più ambiti applicativi nei più svariati aspetti della contrattualistica, dopo che l'Italia infatti ha recepito le Direttive della Comunità Europea in materia, a far data dalla Direttiva 1999/93/CE del 13 dicembre 1999 pubblicata in Gazzetta Ufficiale delle Comunità Europee[1], finalizzata ad armonizzare tutto il territorio europeo su quelle che devono essere le caratteristiche che rendono la firma elettronica sicura e soprattutto attribuibile a un determinato soggetto, in modo tale da far sorgere una obbligazione e/o un diritto in capo al soggetto così individuato.

Il testo principe che regola la firma elettronica è il **Codice dell'Amministrazione digitale** (CAD, decreto legislativo 7 marzo 2005, n. 82 e successive modifiche) la cui ultima modifica in ordine di tempo è entrata vigore in data 27 gennaio 2018[2].

Tale ultima riforma si compone di 67 articoli, il cui intento è quello di procedere a integrare e modificare alcune disposizioni del CAD, in conformità a quanto previsto dalla legge delega, anche al fine di accelerare l'attuazione, a livello nazionale, dell'agenda digitale europea. L'obiettivo principale è quello di contribuire alla definizione di un quadro normativo idoneo ad abilitare e supportare le azioni di attuazione dell'agenda digitale dotando i cittadini, imprese ed amministrazioni di strumenti e servizi idonei a rendere effettivi i diritti di cittadinanza digitale che rappresentano il fulcro della legge delega e del decreto legislativo 179 del 2016.

Sulla base di quanto previsto dalla normativa europea e di conseguenza dal CAD, si definisce la firma elettronica come "*l'equivalente elettronico della tradizionale firma autografa su carta e deve essere associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'integrità, l'autenticità, la non ripudiabilità. Il documento così sottoscritto assume piena efficacia probatoria*".

Andiamo a vedere nel dettaglio come la firma elettronica opera nell'ambito del territorio italiano.

2. RIFERIMENTI NORMATIVI

Testo Unico - DPR 445/00 e successive modificazioni e integrazioni	Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*. Nel seguito indicato anche solo come *TU*.
DLGS 196/03 e successive modificazioni e integrazioni	Decreto Legislativo n. 196 del 30 giugno 2003 "*Codice in materia di protezione dei dati personali"*. Nel seguito indicato anche solo come *DLGS196/03*
CAD - DLGS 82/05 e successive modificazioni e integrazioni	Decreto Legislativo 7 marzo 2005, n. 82. "*Codice dell'amministrazione Digitale"*. Nel seguito indicato anche solo come *CAD*.
DELIBERAZIONE CNIPA n. 45 e successive modificazioni e integrazioni	Deliberazione CNIPA 21 maggio 2009, n. 45. *"Regole per il riconoscimento e la verifica del documento informatico"*. Nel seguito indicato anche solo come *DELIBERAZIONE*
DPCM 22/02/2013 *Nuove Regole Tecniche* e successive modificazioni e integrazioni	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lettera b), 35 comma 2, 36 comma 2, e 71" (del CAD, ndr).* Nel seguito indicato anche solo come *DPCM*
DPCM 19/07/2012 e successive modificazioni e integrazioni	Decreto del Presidente del Consiglio dei Ministri 19 luglio 2012 "*Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai*

[1] Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche, dove per la prima volta si è preso atto che le comunicazioni elettroniche e il commercio elettronico necessitano di firme elettroniche e dei servizi ad esse relativi, atti a consentire l'autenticazione dei dati.

[2] Decreto Legislativo 13 dicembre 2017, n. 217.

	requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma".
Regolamento (UE) N. 910/2014 (eIDAS) e successive modificazioni e integrazioni	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *eIDAS*

3. DEFINIZIONI & ACRONIMI

Termine o acronimo	***Significato***
AgID	Agenzia per l'Italia Digitale (già CNIPA e DigitPA): *www.agid.gov.it***.** D'ora in avanti anche solo *Agenzia*.
Certificato Qualificato	Attestato elettronico, che contiene un insieme di informazioni che creano una stretta e affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. È rilasciato da un Certificatore Accreditato.
TSP	Trust service provider – Prestatore di servizi fiduciari (già *Certificatore*). Persona fisica o giuridica abilitato a rilasciare certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Certificatore Accreditato	TSP presente nell'elenco pubblico dei Certificatori Accreditati tenuto da AgID. (nelle more del Regolamento (UE) N. 910/2014).
Chiave privata	E' la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica, ed è solo in possesso del Titolare che la utilizza per firmare digitalmente i documenti.
Chiave pubblica	E' la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata a una chiave privata ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica.
CIE	Carta di Identità Elettronica, è il documento di identificazione destinato a sostituire la Carta di Identità Cartacea sul territorio italiano.
CNIPA	Centro Nazionale per l'informatica nella Pubblica Amministrazione l'organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
CNS	Carta Nazionale dei Servizi
CP	Certificate Policy - Un insieme di norme, contraddistinto da un codice, che indica l'applicabilità di un certificato ad una particolare comunità e/o a una classe di applicazioni aventi comuni esigenze di sicurezza.
CPS	Certification Practice Statement - Una dichiarazione delle prassi seguite da un Certificatore / TSP nell'emettere e gestire certificati.
CRL	Certificate Revocation List - Un elenco firmato che riporta un insieme di certificati non più considerati validi dal Certificatore / TSP che li ha emessi prima della loro naturale scadenza. La revoca rende i certificati "non validi" definitivamente. La sospensione rende i certificati "non validi" per un tempo determinato.
CRS	Carta regionale dei servizi
CUC	E' il Codice Univoco certificato ed è indicato sulla Richiesta di Registrazione ed inserito nel certificato. Identifica in modo univoco il certificato emesso dal Certificatore.
CUT	E' il Codice Univoco Titolare ed è indicato sulla richiesta di Registrazione.
Destinatario	E' il soggetto a cui è destinato il documento e/o una evidenza informatica firmata digitalmente.
Documento informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento analogico	Rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
FEA	Firma elettronica Avanzata – ex Art.26 Reg. UE 910/2014 (eIDAS), la FEA soddisfa i segg. requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) 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; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
Firma Digitale	Particolare tipo di firma qualificata basata 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
Firma remota	Particolare procedura di firma qualificata o di firma digitale che consente di garantire il controllo esclusivo del dispositivo di firma;
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.
Giornale di controllo	Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche di Base.
Hash (o funzione di Hash)	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta 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.
Impronta (o impronta Hash)	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.
HSM (Dispositivo sicuro per la Creazione della Firma)	Hardware Security Module - 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
IUT	Identificativo Univoco del Titolare, diverso per ogni certificato emesso.
Manuale Operativo	E' il documento pubblico depositato presso AgID che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.
OID	Object Identifier - Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
OCSP	Onlice Certificate Status Protocol – è un protocollo che consente d verificare la validità di un certificato in tempo reale.
OTP	One Time Password – Codice numerico generato da un dispositivo fisico utilizzato per effettuare una autenticazione a due fattori.
PIN	Personal Identification Number – Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso.
PKI	Public Key Infrastructure - Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
CA	Certification Authority: Entità della PKI che rilascia i certificati.
RA Registration Authority	Autorità di Registrazione che su incarico del TSP esegue le registrazioni e le verifiche delle identità dei titolari dei certificati qualificati necessarie al TSP. In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del TSP.
Registro dei Certificati	E' la lista dei certificati emessi dal Certificatore. Nella lista sono inclusi i certificati revocati o sospesi, accessibili telematicamente.
Autorità per la marcatura temporale (Time-Stamping Authority)	E' il sistema software / hardware, gestito dal Certificatore, che eroga il servizio di marcatura temporale.
Validazione temporale	Informazione elettronica contenente la data e l'ora che viene associata ad un documento informatico, al fine di provare che quest'ultimo esisteva in quel momento .
Terzo Interessato	Il terzo interessato è il terzo dal quale derivino i poteri del Titolare medesimo.
Titolare	Persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica. Soggetto intestatario del certificato.
Token	E' il dispositivo fisico (smart card o chiave USB) che contiene la chiave privata del Titolare.
TSA	Time Stamping Authority - Autorità che rilascia marche temporali.

4. NORMATIVA DI RIFERIMENTO

Nel nostro ordinamento la firma digitale nonché le varie tipologie di firme elettroniche sono regolamentate dal D. Lgs. 82 del 7 marzo 2005, il cosiddetto CAD (Codice dell'Amministrazione Digitale).

Con l'emanazione e la successiva entrata in vigore del Regolamento Europeo 910/2014 (eIDAS - Electronic IDentification Authentication and Signature) a partire dal luglio 2016 sono intervenute delle rilevanti modifiche che riguardano la disciplina, anche tecnica, delle firme elettroniche.

Il Regolamento eIDAS fissa norme e procedure per le firme elettroniche, l'autenticazione web ed i servizi fiduciari per le transazioni elettroniche, definendo le condizioni per il riconoscimento reciproco e la piena

interoperabilità a livello comunitario. La riforma ha avuto un impatto rilevante sulla nozione di documento informatico e sulla definizione delle tipologie di firme riconosciute in ambito europeo.

Per questo motivo, nel CAD sono state soppresse (a mezzo D. Lgs. 179 del 26 agosto 2016) le precedenti definizioni presenti nei precedenti testi normativi di firma elettronica, firma elettronica avanzata e firma qualificata e l'art. 1 comma 1-bis rimanda alle definizioni contenute nell'art. 3 del Regolamento eIDAS, mentre rimane presente, leggermente corretta, la definizione di firma digitale, la quale costituisce una tipicità esclusiva del nostro ordinamento interno.

Il 27 gennaio 2018 un ulteriore decreto legislativo, il 217 del 13 dicembre 2017 (entrato in vigore appunto il 27 gennaio 2018) ha aggiornato quanto previsto dalla riforma del 2016, rendendo le firme elettroniche "italiane" riconoscibili e riconosciute a livello europeo.

5. TIPOLOGIE DI FIRME ELETTRONICHE

L'ordinamento italiano riconosce 4 tipologie di firma elettronica ciascuna con proprie caratteristiche peculiari. Vediamo nel dettaglio quali sono:

FIRMA ELETTRONICASEMPLICE (FES)

La firma elettronica semplice (Art. 3 comma 10 dell'eIDAS) è "**l'insieme dei dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare".**

Come si può notare, con la riforma, la firma elettronica perde il valore di mezzo di identificazione informatica e assume il valore di strumento esclusivo di sottoscrizione. La FES pertanto più che a una vera e propria firma dà vita a un processo di autenticazione cui sono riferibili minori requisiti di sicurezza rispetto alle altre tipologie di firma (avanzata e qualificata).

La firma elettronica semplice è detta anche "debole" o "leggera", perché costituisce la sottoscrizione meno sicura ed affidabile ma alla quale, per espressa previsione di legge, non possono essere negati effetti giuridici (principio di non discriminazione).

In sé, non è altro che un insieme di dati connessi attraverso un'associazione logica ad altri dati elettronici, vale a dire un'operazione informatica con la quale il sottoscrittore esprime la volontà di attribuirsi la titolarità di un documento. È quello che avviene, ad esempio, con la email tramite l'associazione di username e password

FIRMA ELETTRONICA AVANZATA (FEA)

L'art. 3 comma 11 eIDAS definisce la Firma Elettronica Avanzata come "**una firma elettronica che soddisfi i requisiti di cui all'articolo 26**" e pertanto (art. 26 eIDAS): "**Una firma elettronica avanzata soddisfa i seguenti requisiti:**

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) 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

d) **è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni**

IRealtors s.r.l. Società a Socio Unico Sede Legale e Amministrativa: Via C.R. Ceccardi 4/41 - 16121 Genova
C.F. e P.I.: 02469410993 - capitale sociale € 10.000 I.v. - REA: 488532
Email: info@irealtors.it – www.irealtors.it

successiva modifica di tali dati".

In altre parole la FEA è l'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.

In sostanza la FEA è una firma riferita ad un documento specifico che permette dal documento di identificare, in maniera certa, il firmatario e di rilevare anche se il documento stesso è stato modificato dopo la firma.

FIRMA ELETTRONICA QUALIFICATA (FEQ)

Secondo l'art. 3, n. 12 eIDAS la Firma Elettronica Qualificata è "**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**".

In aggiunta alle informazioni previste dal Regolamento, ai sensi dell'art. 28 del CAD, nel certificato di firma elettronica possono essere inseriti il codice fiscale, un codice identificativo univoco o anche altri dati pertinenti e non eccedenti rispetto alle finalità di firma come, ad esempio, l'appartenenza ad Ordini professionali, l'iscrizione in Albi, la qualifica di pubblico ufficiale. Si tratta, in pratica, di un attestato elettronico che collega i dati di una firma elettronica ad una persona fisica: ad esempio una SIM card con chip che contiene alcuni dati anagrafici e il codice fiscale (es: tessera sanitaria)

In sostanza siamo di fronte comunque ad una firma elettronica avanzata, ossia una firma che garantisce di poter risalire univocamente da un documento al suo sottoscrittore, ma stavolta ci sono due elementi addizionali:

- un certificato qualificato (che garantisce l'identificazione univoca del Titolare, rilasciato da Certificatori qualificati);
- un dispositivo fisico sicuro (ad esempio un Token USB) per la creazione della firma elettronica qualificata che soddisfa particolari requisiti di sicurezza.

FIRMA DIGITALE

La Firma Digitale è una esclusiva dell'ordinamento italiano, non essendo prevista a livello europeo, è espressamente definita all'interno del CAD (art. 1, comma 1, lett. s).

Essa è un tipo particolare 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**".

In altre parole, tale firma elettronica è associata stabilmente al documento elettronico sulla quale è apposta e ne attesta con certezza l'integrità, l'autenticità, e la non ripudiabilità.

Il dispositivo di firma si presenta sotto forma di smart card (da collegare ad un apposito lettore) o di chiavetta USB ed è necessario possedere un software di firma rilasciato da un'Autorità di certificazione. Se il Certificatore è accreditato eIDAS (i servizi certificati eIDAS sono solitamente contrassegnati con il logo del lucchetto blu con le stelle degli Stati

Europei), i suoi servizi rispettano gli standard di interoperabilità fissati in ambito comunitario. Un esempio particolare è costituito dalla firma digitale con certificato di ruolo rilasciata ai commercialisti dalla Certification Authority (CA) CNDCEC del Consiglio Nazionale, che qualifica il titolare come professionista iscritto all'Albo. Siccome la CA CNDCEC è certificata eIDAS ed è presente nella EU Trusted Lists, la firma di categoria è perfettamente valida e verificabile in tutto il territorio UE.

Il documento sottoscritto con firma digitale deve quindi presentare le caratteristiche di *integrità, autenticità del firmatario, provenienza, non ripudiabilità*.

La firma digitale è pertanto una particolare firma elettronica, rispetto alla firma elettronica qualificata è sempre presente il concetto di certificato qualificato, ma stavolta si fa riferimento ad un sistema di chiave pubblica e privata.

Senza entrare troppo nei concetti matematici di chiave pubblica e privata che avrebbero bisogno di una lunga premessa sui principi della crittografia, è sufficiente sapere che, in sostanza, ciascun soggetto firmatario di un documento deve disporre di:

- una chiave privata, nella disponibilità solo di colui che firma, che gli permette per l'appunto di firmare i documenti;
- una chiave pubblica, nota a tutti coloro che intendano leggere il documento e tramite la quale essi possono verificare che il documento sia stato effettivamente firmato dal soggetto in questione e non sia stato alterato nel tempo.

Potremmo quindi sintetizzare dicendo che la chiave privata serve a firmare il documento mentre la chiave pubblica serve a verificare l'identità del firmatario del documento, a mezzo di soggetti che potremmo definire "certificatori".

6. I CERTIFICATORI ACCREDITATI (TRUST SERVICE PROVIDER)

I Trust service provider sono coloro che prestano uno o più servizi fiduciari e solo coloro che sono presenti nell'elenco pubblico dei Certificatori Accreditati tenuto da AgID possono fregiarsi di tale titolo.

Possiamo quindi definire "certificatori" quei soggetti dotati di alta affidabilità che certificano e firmano un documento informatico contenente la chiave pubblica dei firmatari (soggetti fisici o giuridici).

A norma del CAD l'attività di certificazione è libera e non necessita di particolari autorizzazioni per essere eseguita. Tuttavia ci sono particolari soggetti ai quali l'AgID (per il territorio italiano) e eIDAS (per la Comunità Europea) ha riconosciuto particolari requisiti di affidabilità ed integrità morale, e, pertanto, ad essi sono attribuite grosse responsabilità, i cui certificati hanno un valore legale di maggior fede.

Questi certificatori vengono denominati dal CAD certificatori "accreditati" proprio perché hanno affrontato un processo di accreditamento presso l'AgID (o presso eIDAS per chi agisce sul territorio comunitario).

Potremmo dire che la differenza tra un certificatore qualunque ed uno certificatore accreditato è similare alla differenza sul piano della pubblica fede che intercorre tra un cittadino qualunque ed un notaio o un pubblico ufficiale.

7. TRUST SERVICE PROVIDER DI IREALTORS: NAMIRIAL SPA

Namirial è una società IT di software e servizi ed è un Qualified Trust Service Provider che fornisce Trust Services come Firme Elettroniche, Firme Elettroniche Avanzate (Grafometriche e con Strong Authentication), Firme Elettroniche Qualificate (anche Digitali), Posta Elettronica Certificata, Fatturazione Elettronica e Conservazione Sostitutiva a più di 500.000 utenti.

I gruppi di utenti serviti da Namirial si articolano in diversi settori, tra cui: Ordini Professionali di cui fanno parte Medici, Avvocati, Ingegneri, Consulenti del Lavoro, Dottori Commercialisti, Strutture Cooperative e Imprenditoriali tra cui la Media e Piccola Impresa, la Pubblica Amministrazione, i Trasporti, le Banche e le Assicurazioni e le aziende di classe enterprise.

La sede principale è a Senigallia con ulteriori uffici in Italia e sedi in Austria e Romania, da cui vengono serviti utenti situati in tutta l'Europa, gli Stati Uniti, il Medio Oriente e l'Africa.

Autorità di Certificazione accreditata presso AgID ed autorizzata all'emissione di certificati qualificati conformi alla Direttiva europea 1999/93/CE, certificati CNS e Marche Temporali;

Qualified Trust Service Provider eIDAS per l'emissione di validazioni temporali e certificati qualificati. In particolare Namirial ha conseguito il certificato n. IT269191 rilasciato da Bureu Veritas Italia SpA per l'emissione di validazioni temporali qualificate (marche temporali)

Gestore di PEC, accreditato presso AGID ed autorizzato alla gestione di caselle e domini di Posta Elettronica Certificata

Conservatore accreditato presso AgID per attività di conservazione dei documenti informatici di cui all'articolo 44- bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82

Certificata UNI EN ISO 9001:2008 Namirial ha conseguito il certificato n. 223776 rilasciato da Bureau Veritas Italia S.p.A.

Certificata ISO/IEC 27001:2013. Namirial ha conseguito il certificato n. IND15.0059U rilasciato da Bureau Veritas Italia S.p.A. e il certificato n.38271 rilasciato da CSQA

Certificata da Adobe. Da Giugno 2013 Namirial è membro dell'AATL (Adobe Approved Trust List

8. IL VALORE LEGALE DELLA FIRMA ELETTRONICA

L'art. 20 comma 1 – bis CAD (**validità ed efficacia probatoria dei documenti informatici**) testualmente recita: "*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 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. 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. La data e l'ora di formazione del documento informatico sono*

opponibili ai terzi se apposte in conformità alle Linee guida."

Inoltre, ai sensi del principio di non discriminazione del Regolamento eIDAS, è previsto che: "*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."*

"*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."

8.1 FIRMA ELETTRONICA SEMPLICE

Ne consegue che sulla base di quanto previsto all'art. 20 del CAD il documento informatico sottoscritto con firma elettronica semplice è, in astratto, un documento idoneo a soddisfare il requisito della forma scritta ma il suo valore probatorio è liberamente valutabile in un eventuale giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità (vedasi art. 1, comma 1 bis del D. Lgs. 7 marzo 2005, così come sostituito dall'art. 20, comma 1, lett. a) del D. Lgs. 13 dicembre 2017, n. 217). Ne consegue che i documenti sottoscritti tramite Firma Elettronica Semplice sono le forme più "deboli" di documento informatico, rappresentate ad esempio da un semplice file PDF non firmato o da un file formato con una firma "home made" (ad esempio PGP[3]): in questi casi sarà il giudice a valutare discrezionalmente il valore del documento, nonché la firma e la sua affidabilità giuridica nel caso concreto, considerando altri elementi quali i metadati del documento stesso o la provenienza dal computer di chi l'ha prodotto (con riferimento alla disciplina del regolamento eIDAS vi è anche una scala di valore tra documento non sottoscritto e documento sottoscritto con firma semplice). Nella pratica e in assenza di firma elettronica, il formato più comunemente accettato in giudizio e ben accolto anche dalla Pubblica Amministrazione è il formato Pdf/A[4] che garantisce facilità di visualizzazione, anche a distanza di tempo e utilizzando software diversi.

8.2 FIRMA ELETTRONICA AVANZATA (FEA)

Come poco sopra detto, l'art. 20 comma 1-bis del CAD attribuisce alla FEA l'efficacia prevista dall'articolo 2702 c.c. ovvero che "*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*." Ne consegue che la FEA ha acquisito un valore legale che la equipara alla firma digitale e alla firma elettronica qualificata e pertanto gli viene attribuito il medesimo valore della firma autografa scritta di pugno.

Ai fini del valore legale della firma elettronica avanzata (art. 20 comma 1-bis CAD così come novellato dal D.Lgs. 13 dicembre 2017, n. 217 entrato in vigore a gennaio 2018) si applica la presunzione di riconducibilità del dispositivo al titolare. Pertanto in un eventuale giudizio la persona alla quale viene attribuita una FEA può disconoscere tale firma e sarà onere della controparte provare che quella firma è stata in realtà apposta da chi la disconosce. A tal proposito si ricorda che è valida la FEA formata, 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).

[3] Pretty Good Privacy (PGP), creato da Phil Zimmermann, è un programma che può essere usato per proteggere la privacy, per aggiungere un filtro di sicurezza alle comunicazioni e per dare autenticità ai messaggi in formato elettronico.

[4] Il formato PDF/A è facilmente ottenibile con vari Software disponibili sul mercato anche in open source, trasformando i più diffusi formati testuali (.doc, .xls, .odt, ecc.)

IRealtors s.r.l. Società a Socio Unico Sede Legale e Amministrativa: Via C.R. Ceccardi 4/41 - 16121 Genova
C.F. e P.I.: 02469410993 - capitale sociale € 10.000 I.v. - REA: 488532
Email: info@irealtors.it – www.irealtors.it

La nozione di Firma elettronica avanzata era già presente nell'art. 2 della Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche, la quale definisce la firma elettronica avanzata come una firma elettronica che soddisfi i seguenti requisiti:

a) essere connessa in maniera unica al firmatario;

b) essere idonea ad identificare il firmatario;

c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;

d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

L'ordinamento italiano ha ripreso tale definizione, tanto è vero che i requisiti legali della FEA sono finalizzati a garantire che il documento informatico sottoscritto elettronicamente garantisca l'autenticità e l'integrità del documento sottoscritto, e più specificamente (cfr. art. 1 del CAD che a sua volta richiama art. 3 regolamento eIDAS): la firma elettronica deve soddisfare i requisiti di cui all'articolo 26 eIDAS:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) 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;

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Essendo quindi il documento informatico firmato con FEA equiparato alla scrittura privata, essa ha la stessa valenza probatoria di questa ultima, con la stessa forza in un eventuale giudizio.

8.3 IL VALORE LEGALE DELLA FIRMA ELETTRONICA QUALIFICATA (FEQ) E FIRMA DIGITALE

La Firma Elettronica Qualificata garantisce tutte le caratteristiche della Firma Elettronica Avanzata ed inoltre è basata su un certificato qualificato (rilasciato da un Certificatore accreditato dall'AgID). Nell'utilizzo della FEQ, il firmatario deve utilizzare un dispositivo sicuro con le caratteristiche identificate dalla norma.

La firma digitale, invece, è un particolare tipo di firma qualificata che esiste solo nell'ordinamento italiano ed è 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.

I documenti firmati attraverso FEQ o Firma Digitale sono pertanto documenti con un alto grado di validità, autenticità e integrità.

Un certificato qualificato (o digitale) si può ritenere valido se sono eseguiti e superati i seguenti controlli relativi a:

1. validità della firma digitale del certificatore che ha emesso il certificato;
2. validità del certificato di firma (la data di scadenza è presente all'interno del certificato);
3. non presenza del certificato nella lista dei certificati revocati/scaduti (CRL/CSL), emessa ed aggiornata dal certificatore.

Il superamento di questi controlli è prerequisito perché siano eseguite le successive verifiche di autenticità e di integrità del documento

Pertanto un documento sul quale è apposta un FEQ o una Firma Digitale fa piena prova laddove venga prodotto in un eventuale giudizio fino a querela di falso. Conseguentemente come nel caso di documento cartaceo in tali casi si dovrà procedere con apposita perizia grafometrica, in caso di documento elettronico dovrà procedersi a una apposita perizia, basata sulle chiavi crittografiche e lo stesso soggetto che contesta l'apposizione della firma digitale dovrà dare prova del fatto che la firma in questione non è stata da lui apposta: infatti Il comma 1-ter del medesimo articolo 20 del CAD dispone che "*L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria*".

9. AMBITI APPLICATIVI DELLA FEA

Sul piano applicativo e dei limiti di utilizzo della firma elettronica avanzata è lo stesso legislatore che esplicitamente elenca i documenti che possono essere firmati tramite FEA e quali tassativamente non possono essere firmati con questa modalità.

La FEA può essere impiegata in un ambito molto ampio, ma a differenza delle altre due tipologie di firme (quella digitale e qualificata), ai sensi dell'art. 21 comma 2-bis del CAD sono esclusi esplicitamente quei contratti che sono indicati nell'art. 1350, dal n. 1 al n. 12 del Codice Civile:

1) i contratti che trasferiscono la proprietà di beni immobili;

2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta;

3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti;

4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione;

5) gli atti di rinunzia ai diritti indicati dai numeri precedenti;

6) i contratti di affrancazione del fondo enfiteutico;

7) i contratti di anticresi;

8) i contratti di locazione di beni immobili per una durata superiore a nove anni;

9) i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato;

10) gli atti che costituiscono rendite perpetue o vitalizie salve le disposizioni relative alle rendite dello Stato;

11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari;

12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti.

Sempre ai sensi dell'art. 21 comma 2-bis del CAD "*gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, **a pena di nullità**, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1bis, primo periodo*"[5]. In altre parole possono essere sottoscritti con FEA, FEQ o Firma Digitale tutti i contratti che l'ordinamento italiano preveda debbano essere sottoscritti per scrittura privata, esclusi come detto quelli indicati nei numeri da 1 a 12 dell'art. 1350 c.c., che dovranno

[5] Comma così modificato dall' art. 21, comma 1, lett. c), D.Lgs. 13 dicembre 2017, n. 217.

IRealtors s.r.l. Società a Socio Unico Sede Legale e Amministrativa: Via C.R. Ceccardi 4/41 - 16121 Genova
C.F. e P.I.: 02469410993 - capitale sociale € 10.000 I.v. - REA: 488532
Email: info@irealtors.it – www.irealtors.it

necessariamente essere firmati, a pena di nullità, con FEQ o con firma digitale, in quanto trattasi di atti pubblici o scritture private autenticate.

Svolgendo un ulteriore passo in avanti, possono essere sottoscritti tramite FEA tutti quei documenti che qualora fossero cartacei necessiterebbero della firma autografa, con gli stessi ambiti applicativi e limiti che hanno i corrispondenti documenti analogici che assumono la forma della scrittura privata.

I documenti elettronici sottoscritti con FEA assumono conseguentemente la stessa forma giuridica della scrittura privata con firma autografa: per "scrittura privata" si intende un atto sottoscritto da una o più parti che assume un particolare valore legale giacché ai sensi dell'art. 2702 del codice civile "*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*".

Ne consegue che il documento informatico sottoscritto con FEA fa piena prova delle dichiarazioni in esso contenute, esattamente come accade per la scrittura privata in forma cartacea con firma autografa.

Complice, verosimilmente, la presenza nel nostro ordinamento di sempre più numerosi negozi giuridici che vanno ad aggiungersi a quelli più noti, la scrittura privata conosce oggi, nella sua applicazione pratica, molteplici e diverse sfaccettature: la si utilizza molto spesso per fare degli ordini di forniture, per sottoscrivere finanziamenti, contratti assicurativi, per i contratti preliminari di compravendita, per concludere una transazione, etc...

E' pertanto deducibile che nell'odierno mondo digitalizzato l'equivalente della scrittura privata, vale a dire il documento elettronico sottoscritto con FEA, trovi sempre più ambiti di applicazione, venendo applicata in ambiti sempre più ampi e con sempre maggior frequenza. Basti pensare alla sempre maggior diffusione dei documenti firmati con FEA in ambito bancario (ad esempio per la richiesta di carte di credito o aperture di finanziamenti) o nel mondo assicurativi, dove sta diventando la norma firmare le polizze in formato elettronico.

10.FEA: LA SCELTA DI IREALTORS PER LA CONTRATTUALISTICA DELL'AGENTE IMMOBILIARE

iRealtors si rivolge agli agenti immobiliari, essendo un utile e innovativo strumento per avere sempre a disposizione la numerosa contrattualistica che un tecnico del settore immobiliare si trova ogni giorno a maneggiare:

- compenso di mediazione;
- foglio di visita;
- incarico di mediazione per locazione;
- incarico di mediazione per vendita;
- proposta di acquisto;
- accettazione della proposta di acquisto;
- proposta di locazione;
- accettazione della proposta di locazione;
- contratto di locazione commerciale 6+6;
- contratto di locazione 3+2;
- contratto di locazione 4+4;

- contratto di locazione transitorio;
- preliminare di compravendita.

Tutti i sopra elencati atti, come poco sopra visto, se fossero analogici altro non sarebbero che scritture private, che necessitano solo della firma autografa delle parti.

iRealtors offre la possibilità di redigere tali atti in formato elettronico, utilizzando la Firma Elettronica Avanzata, che offre i vantaggi della semplicità di utilizzo, dell'immediatezza oltre a garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore, previa identificazione informatica, attraverso un processo avente i requisiti fissati dall'AgID. Altresì iRealtors permette, a differenza del documento cartacee, di attestare data e ora certa nella creazione del documento nonché dell'apposizione delle firme.

La piattaforma di iRealtors per il tramite del proprio partner Namirial Spa prevede due tipologie di FEA

A) *Firma Elettronica Avanzata Grafometrica*

La firma elettronica avanzata grafometrica generata da eSAW[6] è realizzata secondo un processo che prevede un meccanismo di document-binding estremamente robusto che si articola nelle seguenti macro-fasi:

A. Identificazione dell'utente sottoscrittore da parte di un operatore;
B. acquisizione del documento da firmare grafometricamente da parte di eSAW;
C. Caricamento del certificato di cifratura fornito dalla CA Namirial, integrato in eSAW;
D. Acquisizione protetta dei vettori grafometrici dal dispositivo di acquisizione grafometrica (tavoletta desktop o tablet);
E. Calcolo dell'impronta HASH SHA-256 del documento da sottoscrivere;
F. Creazione di una struttura dati contenente i vettori grafometrici in formato strutturato secondo le previsioni della normativa di settore;
G. Creazione di una busta crittografica cifrata con algoritmo AES e contenente la struttura dati predisposta allo step precedente. La cifratura avviene con il certificato Namirial.
H. Inserimento dei vettori grafometrici cifrati all'interno del documento;
I. Creazione di una firma elettronica avanzata in formato PAdES sul documento contenente I vettori grafometrici cifrati. La firma PAdES è basata su un certificato di firma elettronica avanzata di servizio installato all'interno della piattaforma eSAW.

Grazie al meccanismo software sopradescritto, mentre il firmatario appone la propria firma su un dispositivo, vengono rilevati tutti i dati biometrici della firma (coordinate, tempo, pressione, tratto in aria ecc).

Tutte queste informazioni, in combinazione con il tratto grafico della firma, sono inserite all'interno di documenti pdf contemporaneamente alla creazione di impronte HASH SHA-256 per assicurarne l'integrità.

I dati comportamentali non sono conservati all'interno di archivi separati per dei successivi confronti, ma vengono criptati ed "inglobati" nel documento stesso; solo nel caso in cui il documento dovesse essere disconosciuto, i dati grafometrici contenuti nel documento verranno decifrati per confrontarli con quelli presenti in altri documenti già verificati o con quelli raccolti al momento stesso dal perito "grafometrico" nominato dal giudice.

L'utilizzo di dati comportamentali legati al documento (mediante opportuni algoritmi di HASH) e l'utilizzo di

6 eSAW: piattaforma di firma integrata in iRealtors

IRealtors s.r.l. Società a Socio Unico Sede Legale e Amministrativa: Via C.R. Ceccardi 4/41 - 16121 Genova
C.F. e P.I.: 02469410993 - capitale sociale € 10.000 I.v. - REA: 488532
Email: info@irealtors.it – www.irealtors.it

una firma elettronica avanzata basata su un certificate emesso e gestito da CA Accreditata (c.d. terza parte fidata), permette di soddisfare pienamente i requisiti richiesti dalla normativa per la FEA, ovvero:

1. l'identificazione del firmatario del documento;
2. la connessione univoca della firma al firmatario;
3. il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
4. la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
5. la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
6. l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
7. l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
8. la connessione univoca della firma al documento sottoscritto.

B) Firma Elettronica Avanzata con SMS

La firma elettronica avanzata con SMS generata da eSAW è realizzata tramite un processo articolato secondo degli steps funzionali simili a quelli del punto A). Rispetto alla soluzione basata su grafometria, in questo processo il requisito di riconducibilità della firma al titolare viene garantita dal possesso del cellulare e dall'invio di un codice OTP[7] su tale numero.

Entrando nel dettaglio, il meccanismo si sviluppa secondo le seguenti macro-fasi:

A. Identificazione dell'utente sottoscrittore da parte di un operatore;
B. Acquisizione del documento da firmare da parte di eSAW;
C. Invio di un codice OTP al numero di cellullare del firmatario;
D. Login dell'utente su eSAW tramite l'inserimento del codice OTP ricevuto nel cellulare;
E. Registrazione dell'avvenuto login all'interno dell'audit log della piattaforma eSAW;
F. Visualizzazione del documento;;
G. Firma del firmatario tramite click su campo firma;
H. Calcolo dell'impronta HASH SHA-256 del documento da sottoscrivere;
I. Creazione di una firma elettronica avanzata in formato PAdES basata su un certificato di firma elettronica avanzata di servizio installato all'interno della piattaforma eSAW.

Grazie al processo sopradescritto, l'utente può apporre la propria firma solo se prima è riuscito ad autenticarsi tramite il codice OTP inviato sul suo cellullare.

L'informazione del login, in combinazione delle restanti informazioni collezionate dalla piattaforma eSAW sono inserite all'interno dell'Audit Trail (Log) che viene regolarmente firmato a garanzia dell'integrità.

Le informazioni contenute nell'Audit Trail possono essere successivamente prodotti in tribunale in caso di disconoscimento della firma da parte dell'utente.

[7] One Time Password

L'utilizzo di un codice OTP inviato tramite SMS al numero personale del titolare e l'utilizzo di una firma elettronica avanzata basata su un certificate emesso e gestito da CA Accreditata (c.d. terza parte fidata), permette di soddisfare pienamente i requisiti richiesti dalla normativa per la FEA, ovvero:

1. l'identificazione del firmatario del documento;
2. la connessione univoca della firma al firmatario;
3. il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
4. la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
5. la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
6. l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a);
7. l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
8. la connessione univoca della firma al documento sottoscritto.

Entrambe le tipologie di FEA (grafometrica e con SMS) rispondono alla normativa eIDAS, che – ad esempio – nel caso di firma OTP le operazioni eseguite vengono irrobustite nel fattore di autenticazione dall'invio della password al numero di cellulare univocamente collegabile al firmatario, in quanto deve essere intestato a quest'ultimo.

Nel caso di firma biometrica, la firma viene effettuata tramite appositi dispositivi di ultima generazione in grado di catturare un set strutturato di informazioni comportamentali relative allo stile di scrittura e alla grafia del sottoscrittore. Questi device, oltre a garantire una precisione molto elevata nella fase di acquisizione, realizzando anche canali di comunicazione per evitare che i dati sensibili in transito possano essere manomessi o intercettati.

Cliccando sul campo firma viene attivato il device di acquisizione del tratto utilizzato dal firmatario (pc, tablet o smartphone) e, in fase di firma, vengono registrate le informazioni sull'*habitus* di scrittura del sottoscrittore (aspetto, velocità, tempo, accelerazione, ritmo ecc). Queste informazioni vengono quindi connesse all'impronta del documento e l'intera struttura viene salvata in un contenitore cifrato congelato all'interno del documento.

In entrambi i casi (biometria e autenticazione tramite OTP) si dovrà procedere alla identificazione del firmatario in modo da rendere il processo ancora più robusto da un punto di vista della non ripudiabilità del documento sottoscritto.

Con la firma elettronica avanzata nel file viene utilizzato un certificato elettronico di servizio, integrato in piattaforma e rilasciata dal Certificatore qualificato. Il certificato è presente all'interno degli store Europei e del software di gestione dei PDF, Adobe, e serve a garantire l'integrità e immodificabilità del documento.