POLIZZE FIDEIUSSORIE EMESSE CON FIRMA DIGITALE

PREMESSA

QUADRO NORMATIVO DI RIFERIMENTO

DOCUMENTO INFORMATICO

- **Il "contenuto" del documento informatico**
- **Le regole tecniche**

LE FIRME ELETTRONICHE

- **Nuove definizioni introdotte dal regolamento eIDAS**
- **La Firma Elettronica "Semplice"**
- **Firma Elettronica Avanzata**
    - La Firma Grafometrica
    - La Firma Elettronica Qualificata

LA FIRMA DIGITALE

- **Diversi formati di firme – definizione e formati**
    - La firma in Formato PAdES (PDF Advanced Electronic Signatures)
    - La firma in Formato CAdES (CMS Advanced Electronic Signatures)
    - Formato XAdES (XML Advanced Electronic Signatures)
- **Firme digitali multiple**
    - Le firme digitali locali e remote
    - La firma digitale locale
    - La firma digitale remota
        - Firma digitale remota massiva e firma automatica

ENTI CERTIFICATORI - PRESTATORI DI SERVIZI FIDUCIARI QUALIFICATI

VERIFICA DELLA FIRMA DIGITALE

- **Verifica dei poteri del sottoscrittore con particolare riguardo alla firma digitale**

CENNI SUL SIGILLO ELETTRONICO

- **Effetti giuridici dei sigilli elettronici**

VALIDITÀ TEMPORALE DELLA FIRMA DIGITALE

- **Marca temporale**

DOCUMENTO INFORMATICO - VALORE LEGALE

- **Documento informatico privo di sottoscrizione e sottoscritto con firma elettronica semplice**
- **Documento informatico sottoscritto con firma elettronica (avanzata, qualificata, digitale)**

EFFICACIA PROBATORIA DEL DOCUMENTO INFORMATICO

- **Tratti probatori di ciascuna firma**
- **Efficacia probatoria documenti sottoscritti con firma elettronica semplice**
- **Efficacia probatoria documenti sottoscritti con firma elettronica avanzata, qualificata o digitale**

DISCONOSCIMENTO DELLA FIRMA DIGITALE

- **Efficacia del documento sottoscritto con firma digitale - Possibilità e limiti del disconoscimento della firma digitale e onere probatorio**
- **La firma grafometrica**

AUTENTICAZIONE NOTARILE DELLA FIRMA DIGITALE

LA FIRMA DIGITALE E LA POLIZZA FIDEIUSSORIA

- **Modalità di emissione della polizza fideiussoria con firma digitale**
    - Richiesta di emissione della polizza e previsione contenuta nei bandi
    - Numero di firme digitali apposte dalla Compagnia
    - Verifica della polizza emessa con firma digitale
- **Modalità di perfezionamento della polizza fideiussoria con firma digitale**

OBBLIGO DI CONSERVAZIONE DEI DOCUMENTI CONTRATTUALI – POLIZZA E ALLEGATI – ARCHIVIO CARTACEO E DIGITALE

CLAUSOLE VESSATORIE NEI CONTRATTI ON LINE

ALCUNI CENNI E ARRESTI GIURISPRUDENZIALI CON RIFERIMENTO ALLA PRODUZIONE DELLA POLIZZA PROVVISORIA CON FIRMA DIGITALE

POLIZZE DIGITALI SENZA EFFETTO

PREMESSA

Oggetto di questa breve trattazione è l'emissione ed il perfezionamento di polizze fideiussorie in via informatica e con firma digitale.

Sembra opportuno svolgere in premessa alcune considerazioni di carattere più generale, e dunque non riferibili esclusivamente alle cosiddette polizze digitali ma idonee a meglio comprendere l'assetto normativo e quello tecnico regolamentare connessi ai diversi istituti del documento informatico e della sua sottoscrizione elettronica.

Ed infatti dovendo trattare di polizza fideiussoria emessa in formato digitale occorre tenere ben presente che si tratta di un "*documento informatico*" e che se occorre apporre una firma su tale documento informatico questa avrà natura di "*firma elettronica*".

Finalità infatti di questa trattazione vorrebbe essere quella di fornire un quadro d'insieme che aiuti a comprendere quali sono gli elementi necessari e sufficienti per giungere ad una corretta stipulazione della polizza in formato digitale, e anche per consentire dunque un corretto consapevole dialogo con quei soggetti – non più il tipografo, ma l'informatico – che dovranno predisporre nei termini materiali lo strumento polizza rispondente alle esigenze tecniche, e successivamente con gli intermediari – Agente e Broker – che nei contatti con la clientela e nel perfezionamento dei contratti dovranno rispettare le regole giuridiche e tecniche.

QUADRO NORMATIVO DI RIFERIMENTO

Il quadro di riferimento normativo è rappresentato dal Codice dell'Amministrazione Digitale – CAD regolato dal D.lgs. 7 marzo 2005, n. 82. A tale normativa di carattere generale sono state apportate alcune modifiche ed integrazioni con riferimento ai diversi aspetti in generale trattati dal CAD anche in attuazione della normativa europea[1].

Non si può poi trascurare il rilievo della disciplina dettata dall'Organo di Vigilanza del Settore – ISVAP / IVASS – alla quale si farà richiamo e riferimento nel corpo della presente trattazione in relazione ad alcuni specifici aspetti.

[1] Come è noto l'originario testo del d.lgs. n. 82/2005 ha subito nel tempo diverse modifiche ed integrazioni, da parte di numerosi interventi normativi: D. Lgs. 4 aprile 2006, n. 159, legge 24 dicembre 2007, n. 244, legge 28 gennaio 2009 n. 2, legge 18 giugno 2009, n. 69, legge 3 agosto 2009, n. 102, d.lgs. 30 dicembre 2010, n. 235, legge n. 221/2012 (recante i principi dell'Agenda Digitale), legge n. 98/2013 (decreto del fare), d.lgs. n. 179 del 26 agosto 2016 (riforma Madia), D.lgs. 13 dicembre 2017, n. 217.

DOCUMENTO INFORMATICO

Il concetto di documento informatico è il perno attorno a cui gravita l'intero impianto del diritto dell'informatica: esso rappresenta il *trait d'union* tra il diritto e l'informatica pura.

La definizione contenuta nell'art. 1, lett. p) del d.lgs 82/2005, definisce

- il documento informatico come « ……..la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»;
- il documento analogico: "la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti".

Istintivamente si è portati ad associare l'idea di documento informatico a quella di file, termine inglese file (traducibile come "archivio") che viene utilizzato in informatica per riferirsi a un contenitore di informazioni in formato digitale[2]. Ciò che contraddistingue il documento informatico rispetto al documento analogico è la sua immaterialità, vale a dire la sua forma elettronica.

La definizione contenuta nel Regolamento UE n. 910/2014 (eIDAS), all'art. 3, n. 35, laddove definisce il «"documento elettronico", qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva» nella formulazione più generica ha portato i primi commentatori ad affermare che il documento informatico fosse una species del più ampio genus dei documenti elettronici e che dalla definizione eIDAS discendesse un generalizzato obbligo di conservazione di tutti i documenti ed a carico della totalità dei consociati.

La definizione del regolamento eIDAS fa riferimento ad un "contenuto", che non può essere altro se non l'oggetto della rappresentazione documentale: ritenere che col termine stored "**conservato**" il regolamento 910/2014 abbia voluto riferirsi all'istituto della conservazione appare molto più che una forzatura, dovendocisi piuttosto riferire alla mera memorizzazione su supporto informatico vale a dire che nella definizione legislativa nazionale è privilegiata la funzione rappresentativa del documento ed in quella europea la "forma" elettronica.

Il "contenuto" del documento informatico: il concetto di copia e di duplicato

Il concetto di contenuto del documento informatico è poi ripreso in numerose norme del

[2] Cfr. Wikipedia, voce "File": nella comune accezione, questo termine inglese file (traducibile come "archivio") viene utilizzato in informatica per riferirsi a un contenitore di informazioni in formato digitale.

C.A.D.: ci si riferisce in particolare alle norme che disciplinano le copie di documenti, nelle quali il predetto termine è una costante[3]. Ciò accade come diretta ed immediata conseguenza del fatto che il contenuto costituisce proprio l'oggetto della rappresentazione (cfr. art. 1, lett. p d.lgs 82/2005, « ……..la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti»), ovvero il testo scritto, l'immagine o la riproduzione audiovisuale.

Conseguenza ulteriore è la creazione, puramente giuridica e nient'affatto informatica, del concetto di

- copia come inteso nel C.A.D., vale a dire di documenti che si caratterizzino per avere lo stesso identico contenuto ma un diverso "contenitore".
- "duplicato informatico"[4], che traduce in diritto il concetto di copia adoperato in informatica: in informatica un file presenta rispetto alla sua copia sia il contenitore che il contenuto esattamente identici, vale a dire che sono "composti" da una stessa identica sequenza di bit.

Le regole tecniche

Il documento informatico è quello formato con mezzi informatici nel rispetto delle regole tecniche ex art. 71 del CAD, ovvero una serie di disposizioni a carattere regolamentare, adottate con appositi Decreti ministeriali, funzionali a dare concreta attuazione alle norme del CAD.

Le regole tecniche sono state approvate con il dpcm 13.11.2014, entrate in vigore l'11 febbraio 2015 ma sono destinate ad una revisione che dovrebbe intervenire di qui a breve, allorché l'Agid varerà le Linee Guida previste dal novellato art. 71 CAD.

---

[3] Basterà aver riguardo alle definizioni di cui all'art. 1 del CAD, e segnatamente alle seguenti:

«*i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;*

i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari»

[4] Art. 1 lettera i-quinquies) CAD*: «duplicato informatico: il documento informatico ottenuto mediante la , memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario».*

Ai sensi dell'art. 65 co. 10 del d.lgs. 217/2017 «*le regole tecniche emanate ai sensi dell'articolo 71 del decreto legislativo n. 82 del 2005, nel testo vigente prima dell'entrata in vigore del presente decreto, restano efficaci fino all'eventuale modifica o abrogazione da parte delle Linee guida di cui al predetto articolo 71, come modificato dal presente decreto*».

La disciplina tecnica sui documenti rimarrà in larga misura immutata rispetto alle previsioni contenute nel dpcm 13.11.2014, salvo probabilmente un approccio meno rigoroso e più flessibile rispetto alle attuali previsioni.

Secondo le attuali regole tecniche (art. 3), quattro sono le modalità di formazione del documento elettronico:

a) redazione tramite l'utilizzo di appositi strumenti software: è il caso "classico" nel quale rientra, ad esempio, la stesura di un documento mediante software di trattamento dei testi;

b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico: nella seconda parte di tale previsione rientra la formazione di copie documentali, mentre lascia perplessi la prima parte nella quale col termine "acquisizione" parrebbe farsi riferimento non al trasferimento di meri contenuti – e quindi alle copie – ma indistintamente alla acquisizione di documenti già esistenti in una determinata struttura, per effetto di trasmissione telematica o di trasferimento "fisico" di un supporto informatico: in altri termini, tale parte della norma tecnica sembra riferirsi non tanto alla formazione in senso stretto dei documenti informatici, quanto alla relativa acquisizione ad un protocollo informatico o in un sistema di conservazione.

c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente: rientrano in tale novero i documenti log, i tracciati di processi informatici o i documenti formati attraverso la compilazione di campi-modulo esposti su siti internet o formulari;

d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti, interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica. Rientrano in tale novero i documenti formati grazie alla cooperazione applicativa di cui all'art. 1, lett. ee) CAD: per fare un esempio vicino agli operatori di giustizia, si pensi

alle comunicazioni e notificazioni di cancelleria che vengono generate attraverso dati e documenti che confluiscono in un documento in formato MIME (la p.e.c.) a sua volta integrata dalle informazioni relative agli indirizzi dei destinatari.

Le regole tecniche sul documento informatico non si preoccupano solo della formazione elettronica degli stessi, essendo ispirate a precostituire quel minimum che diventerà indispensabile ai fini della loro conservazione.

LE FIRME ELETTRONICHE

E' necessario fare una premessa al riguardo, considerando che nel linguaggio comune sono denominate "firme elettroniche o firme digitali" tutte le firme non apposte su carta, mentre invece esistono sostanziali differenze tra firme elettroniche, elettroniche avanzate, qualificate e digitali.

Nuove definizioni introdotte dal regolamento eIDAS

La normativa italiana in materia di firme elettroniche è stata recentemente riformata per realizzare l'adeguamento alle norme e ai principi contenuti nel 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, direttamente applicabile in tutti gli Stati membri dal 1° luglio 2016.

Il Regolamento Europeo, noto con l'acronimo eIDAS (Electronic IDentification Authentication and Signature), 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 come visto sia sulla nozione di documento informatico che sulla definizione delle tipologie di firme riconosciute in ambito europeo. Per questo motivo, nel D.lgs. 7 marzo 2005, n. 82 (CAD), sono state soppresse le precedenti definizioni di firma elettronica, firma elettronica avanzata e firma qualificata e l'art. 1 comma 1-bis del CAD rimanda alle definizioni contenute nell'art. 3 del Regolamento eIDAS, mentre rimane presente, leggermente corretta, la definizione di firma digitale, che costituisce una tipicità del nostro ordinamento interno.

La Firma Elettronica "Semplice"

L'art. 3, n.10 del Regolamento definisce la firma elettronica come "*l'insieme dei dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare".*

L'art. 3, n.10 Regolamento UE n. 910/2014	Art 1 comma 1 lett q) del CAD soppressa
l'insieme dei dati in forma elettronica,	"L'insieme dei dati in forma elettronica,

acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare	allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica”

Come si può notare, con la riforma la firma elettronica perde il valore di mezzo di identificazione informatica (di autenticazione) e assume il valore di strumento esclusivo di sottoscrizione.

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.

La Firma Elettronica Avanzata

L’art. 3, n. 11 del Regolamento definisce Firma Elettronica Avanzata quella che soddisfa i requisiti di cui all’art. 26:

1) è connessa unicamente al firmatario;

2) è idonea a identificare il firmatario;

3) 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;

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

L’art. 3, n.11 Regolamento UE n. 910/2014	Art 1 comma 1 lett q-bis) del CAD soppressa
Firma Elettronica Avanzata quella che soddisfa i requisiti di cui all’art. 26: *1) è connessa unicamente al firmatario; 2) è idonea a identificare il firmatario; 3) è*	**Firma Elettronica Avanzata** “ insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario

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; 4) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.	del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario puo' 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;"

La normativa eIDAS segue il principio di neutralità tecnologica: non individua specifici formati, ma solo standard tecnici di riferimento, ai quali possono ricondursi diverse soluzioni di firma.

La Firma Grafometrica

Una tipologia di firma elettronica avanzata diffusa è la **Firma Grafometrica**, che consiste in una firma apposta su un particolare tablet con uno speciale dispositivo (pen drive) che consente di memorizzare alcune caratteristiche biometriche del soggetto: velocità di scrittura, pressione della firma, accelerazione del movimento.

La firma grafometrica, rilevata previa identificazione del firmatario nel rispetto delle regole tecniche vigenti, soddisfa il requisito della connessione univoca e della identificazione certa del firmatario e del suo controllo esclusivo sullo strumento di firma.

La Firma Elettronica Qualificata

Secondo l'art. 3, n. 12 del Regolamento **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 partica, 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).

l'art. 3, n. 12 del Regolamento	**Art 1 comma 1 lett r) del CAD soppressa**
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"*	**Firma Elettronica Qualificata "**un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

LA FIRMA DIGITALE

La Firma Digitale è l'unica espressamente definita all'interno del CAD

Art 1 comma 1 lett s) del CAD in vigore
un particolare tipo di firma qualificata basata su un [~~certificato qualificato e~~] sistema di chiavi crittografiche[5], 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'integrita' 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.

Il dispositivo di firma si presenta abitualmente - tratteremo poi l'ipotesi di firma digitale remota, firma massiva e firma automatica - 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.

Il documento sottoscritto con firma digitale presenta le seguenti caratteristiche:

- integrità: il contenuto non può essere alterato e il documento non può essere modificato o manomesso successivamente all'apposizione della firma. Più specificatamente, la modifica del documento firmato determina la perdita delle caratteristiche tecniche che caratterizzano il file, che non potrà più essere

[5] **Cifratura e decifratura del documento informatico**
La cifratura è quella funzione applicata ad un documento informatico che permette la protezione del file stesso, trasformandolo in un documento non immediatamente intellegibile. In sostanza, aumenta il livello di sicurezza ad un documento informatico firmato digitalmente.
Una volta cifrato, il documento può essere aperto esclusivamente con l'uso della chiave pubblica (anche in caso di successiva scadenza del certificato) e visualizzato e decifrato solo ed esclusivamente dal destinatario/i indicato/i in fase di cifratura.

riconosciuto come valido in fase di verifica da parte della Certification Authority che ha rilasciato il dispositivo di firma;

- autenticità: è certa l'identità del firmatario, essendo certificata l'autenticità delle informazioni relative al sottoscrittore;
- provenienza: risulta verificata la provenienza del documento dal sottoscrittore;
- non ripudiabilità: il firmatario non può ripudiare il documento sottoscritto con la propria firma digitale se non in determinati limiti di contestazione e disconoscimento che verranno trattati nello specifico in seguito.

Diversi formati di firme – definizione e formati

La firma digitale consiste nella creazione di un file, definito "busta crittografica", che racchiude al suo interno il documento originale, l'evidenza informatica della firma e la chiave per la verifica della stessa, che è contenuta, a sua volta, nel certificato emesso a nome del sottoscrittore. Le buste crittografiche possono essere intese come dei contenitori che racchiudono al loro interno i documenti informatici firmati con firma digitale e i dati tecnici usati dal processo di firma. Il processo di sottoscrizione genera un file chiamato "busta crittografica", ovvero "contenitore di firma" che può essere di tre tipologie: PAdES, CAdES e XAdES.

Come si fa ad individuare il formato di busta più idoneo?

La firma in Formato PAdES (PDF Advanced Electronic Signatures)

La firma in **Formato PAdES (PDF Advanced Electronic Signatures),** chiamata comunemente "firma PDF", prevede svariate modalità per la sottoscrizione e può essere apposta esclusivamente ai file in formato PDF.

Il documento informatico firmato PDF può essere generato attraverso i software applicativi gratuiti (es. Dike, Arubasign, FirmaCerta, FirmaFacile..) messi a disposizione dai certificatori. In alternativa, è anche possibile utilizzare il software applicativo Acrobat Professional, oppure altri software - gratuiti o a pagamento - che permettono di apporre la firma digitale da parte di più utenti, nel rispetto delle regole tecniche vigenti.

L'uso del formato PAdES presenta alcuni vantaggi: il documento informatico già firmato può contenere dei campi di testo nei quali inserire ulteriori informazioni anche

successivamente alla firma già apposta, senza invalidarla. A scopo esemplificativo, si pensi all'aggiunta della segnatura di protocollo ex art. 55 del D.P.R. 28 dicembre 2000, n. 445 al documento già firmato, all'inserimento di ulteriori elementi grafici quali loghi o timbri, all'apposizione di firme in calce alle clausole vessatorie.

A differenza del formato CAdES, il formato PAdES ha un sistema di mantenimento delle versioni documentali (versioning), per il quale è sempre disponibile la versione integrale, non modificata, del documento informatico precedente (comprese le firme digitali apposte). In sintesi, si ritiene che la busta PAdES sia un formato particolarmente idoneo quando è necessario apporre una nuova firma al documento dopo la prima sottoscrizione digitale.

Alcuni software di firma richiedono di effettuare la scelta tra le due tipologie di firma Pades: la versione Basic e quella BES avanzata:

a) **PAdES Basic:** è la tradizionale firma PDF. È compatibile con tutte le versioni di Adobe Acrobat; è valida sul territorio nazionale italiano, ma non può essere utilizzata per il trattamento di documenti a livello europeo. La determinazione commissariale 28 luglio 2010, prevede che le firme digitali apposte con il formato PAdES Basic siano valide solo se apposte anteriormente al 30 giugno 2011, mentre dal 1° luglio 2011 è necessario utilizzare una firma digitale PAdES avanzata.

b) **PAdES BES avanzata**: tipo di firma PDF "avanzata" è sviluppata per essere conforme con le restrizioni della normativa europea; questa busta crittografica è riconosciuta solo dalla versione 10 del software Adobe Acrobat.

La Decisione della Commissione Europea 2011/130/EU, che stabilisce i requisiti minimi per il trattamento transfrontaliero dei documenti firmati elettronicamente nel mercato interno, impone il suo utilizzo in maniera diretta. Dunque, il consiglio è quello di utilizzare tra i due tipi di firma PADES sempre il formato PAdES BES (siamo dunque fuori dall'ipotesi in cui si debba necessariamente usare il sistema di firma CADES di si tratterà a breve, come ad esempio nel caso in cui il disciplinare della gara richieda tale formato.

In conclusione, la scelta del particolare "contenitore di firma" PAdES dipende:

1. dal formato del file da firmare, che deve essere esclusivamente PDF;

2. dall'utilizzo che si intende fare del file PDF firmato e dai destinatari dello stesso. La

firma PDF può essere facilmente verificata ed il file può essere semplicemente visualizzato, anche dopo la firma, utilizzando qualsiasi lettore PDF. Il più diffuso e gratuito è l'applicazione Adobe Acrobat Reader, disponibile per qualsiasi sistema operativo e architettura hardware (dispositivi mobile-tablet o PC-desktop);

3. dall'interesse al mantenimento anche in fase di stampa della medesima formattazione e struttura del documento visualizzato e firmato (PDF/A-b1 e PDF/A-a1);
4. dalla necessità di gestire documenti PDF redatti in lingue che utilizzano caratteri diversi o simboli speciali come nei casi di un contratto internazionale in cinese o russo;
5. dalla indisponibilità di un software applicativo specifico per l'apertura della busta crittografica CAdES (il file.p7m) che contiene il documento. Infatti, solo disponendo di un programma per la firma digitale è possibile visualizzare il contenuto di un documento firmato CAdES;
6. dalla necessità di aggiungere una firma grafica visibile su una parte spaziale specifica del documento informatico PDF;
7. dall'esigenza di firmare il file PDF in momenti successivi da parte di soggetti differenti come, ad esempio, nel caso di modifiche contrattuali. Infatti, come già sopra indicato, il PAdES implementa il sistema delle versioni del documento e ogni versione successiva alla prima, contiene la versione integrale, non modificata, del documento precedente (comprese le firme digitali);
8. dalle richieste e specifiche tecniche del sistema applicativo usato: nel processo telematico tributario è richiesta la firma CAdES, in quello amministrativo telematico per sottoscrivere il Modulo di deposito si utilizza esclusivamente il formato PAdES BES e nulla è indicato con riferimento al formato di firma digitale dei singoli atti processuali (sia deposito che notifica); infine, nel processo civile telematico sono previsti entrambi i formati (PAdES e CAdES).

La firma in Formato CAdES (CMS Advanced Electronic Signatures)

La firma CAdES può essere utilizzata per sottoscrivere digitalmente qualunque formato di file (es. Ms-Excel, Ms-Word, PDF, XML, audio mp3, video mp4, etc.).

Per visualizzare il contenuto della busta CAdES, che ha estensione.p7m, occorre utilizzare il software di firma (es. Dike, ArubaSign, FirmaCerta, FirmaFacile, etc) in grado di "sbustare", ovvero di visualizzare e gestire il documento informatico sottoscritto.

La scelta del formato CAdES dipende:

1. dal tipo di file da firmare, diverso da PDF o XML. Occorre precisare che, comunque, è sempre possibile "forzare" il software di firma alla creazione della busta crittografica CAdES (.p7m) anche per i file XML o PDF (es. specifiche tecniche dell'invio telematico Agenzia delle Entrate);
2. dalle richieste e dalle specifiche tecniche del sistema applicativo usato: ad esempio, il sistema telematico dell'Agenzia delle Entrate "Fatture e Corrispettivi", per l'invio delle "Fatture e della comunicazione IVA periodica con prospetto di liquidazione" richiede obbligatoriamente l'uso del formato CAdES-BES o il XAdES-BES;
3. dalla disponibilità del software necessario alla lettura del formato del file da firmare.

Formato XAdES (XML Advanced Electronic Signatures)

Il contenitore di firma (busta crittografica) XAdES è ottenuto firmando digitalmente un file XML.

Caratteristica dello XAdES è la possibilità di firmare singole parti del documento, peculiarità di particolare importanza nei documenti scritti da più persone, in cui ognuno deve firmare la propria parte.

La rappresentazione dei dati in un file XML permette la lettura tramite un semplice editor, ma risulta poco leggibile ed è quindi solitamente abbinato un file di presentazione, un visualizzatore o un foglio di stile, che determina la creazione del documento di facile leggibilità. Tale operazione potrebbe creare delle problematiche correlate alla diversa rappresentazione visiva dei dati di uno stesso file XML, ad esempio utilizzando due diversi file XSLT.

Come per il formato PDF, questa tipologia di busta crittografica non necessita della fase di imbustamento/sbustamento per poter visualizzare il documento. Pertanto è sempre possibile accedere ai "metadati" contenuti all'interno del documento stesso (informazioni contenute nei tag xml).

Il formato XAdES-BES è utilizzato per la firma delle fatture elettroniche nei confronti della Pubblica Amministrazione e in ambito sanitario.

Firme digitali multiple

Ad un documento informatico è possibile apporre più firme digitali: il medesimo file può essere firmato da più soggetti, in momenti diversi e con kit di firma digitale rilasciati anche da differenti certificatori. In tal caso, si tratta di "firme digitali multiple".

L'apposizione di firme multiple ad un documento informatico è normata dall'articolo 24 della Deliberazione CNIPA n.45/2009[6], così come modificata dalla Determinazione Commissariale 69/2010, n.69[7]; tale azione può avvenire anche in momenti differenti e ha come conseguenza che più soggetti si assumono la paternità e/o la responsabilità del documento (es. sottoscrizione di contratti, bilanci, ecc).

È possibile classificare le firme digitali apposte allo stesso documento da soggetti sottoscrittori differenti in:

1. ***firme "parallele" od "indipendenti"***: quando la sottoscrizione successiva alla prima viene apposta solo ai dati contenuti nella busta crittografica.

   Un documento con firme parallele produce un file di tipo "nomefile.p7m" (formato CAdES) oppure "nomefile.pdf" (formato PAdES). La firma di questo tipo aggiunge ulteriori firme "a fianco" della prima e ciascuna firma mantiene la sua indipendenza (ogni firmatario firma gli stessi dati che firmano gli altri). Questa operazione di firma digitale equivale ad apporre più firme, da parte da parte dello stesso soggetto o di

[6] Art. 24 (Regole per l'apposizione di firme multiple)
1. Una stessa busta crittografica può contenere più firme digitali. Queste ultime sono identificate in:
a) "Firme parallele", in tal caso il sottoscrittore, utilizzando la propria chiave privata, firma solo i dati contenuti nella busta stessa (OID: 1.2.840.113549.1.7.1);
b) "Controfirme", in tal caso il sottoscrittore utilizzando la propria chiave privata, firma una precedente firma (OID: 1.2.840.113549.1.9.6) apposta da altro sottoscrittore.
2. Il formato delle firme multiple definite nel presente articolo è conforme al documento ETSI TS 101733 nella modalità BES.
3. L'apposizione di firme multiple di cui al presente articolo non comporta l'applicazione di ulteriori estensione al nome del file contenente il documento firmato.

[7] Le norme contenute nella Deliberazione CNIPA n° 45/2009 sono ancora un punto di riferimento in fatto di firma digitale. Esse furono modificate con la Determinazione 69/2010, dando vita a un corpus tecnico che allinea la normativa italiana alle direttive della Commissione europea.
Con la Deliberazione CNIPA 45/2009 venne introdotto il formato di firma standard CAdES (CMS Advanced Electronic Signature, file con estensione .p7m), che andava a sostituire il formato fino ad allora accettato PKCS7. Oltre il formato .p7m, che risulta essere il formato di firma digitale più diffuso, la Deliberazione CNIPA 45/2009 fa riferimento anche al formato di firma PDF (il PAdES, PDF Advanced Electronic Signature) e al formato di firma XML (XAdES, XML Advanced Electronic Signature).
In tutti casi, le nuove norme introducono anche l'obbligo d'impiego di un nuovo algoritmo per la creazione del digest (l'impronta digitale crittografata del documento firmato): lo SHA-256.
La nuova normativa, così come definita dalla Deliberazione CNIPA n° 45/2009 e successive modifiche, è entrata in vigore dal 2010 con l'obbligo, da parte dei certificatori, di conformarsi alle nuove indicazioni tecniche per tutto ciò che riguardava gli adeguamenti software o a livello di dispositivi di firma digitale.

persone differenti, in calce al medesimo documento. Ipotizzando l'utilizzo del formato CAdES, il nome del file sarà caratterizzato da una sequenza di estensioni, una per ciascuna firma apposta, es. nomefile.p7m.p7m.p7m.

La firma multipla è apposta in modalità parallela, quando i sottoscrittori sono ad un livello paritetico e le firme sono congiunte. Questo avviene, tipicamente, quando diversi professionisti collaborano alla realizzazione dello stesso documento: è' il caso della firma di un atto da parte di due legali con incarico congiunto oppure la firma di una perizia da parte di un collegio di periti con incarico congiunto.

Per aggiungere una "firma parallela o indipendente" utilizzando un qualsiasi software di firma digitale è necessario richiamare la funzione di verifica del file già firmato digitalmente e cliccare sulla funzione "Aggiungi firma…". Nel caso specifico in cui si debba apporre la prima firma digitale, si deve cliccare su "Firma" e, successivamente, in fase di verifica, si potrà constatare attraverso il report che il documento effettivamente contenga le firme aggiunte;

2. **firme "nidificate" o "annidate" od "a matrioska"**: in questo caso ogni sottoscrittore successivo firma l'intera busta crittografica generata dalla sottoscrizione precedente. Il documento informatico è contenuto in un file con estensione.p7m (formato CAdES) e l'apposizione di firme annidate produce un file "nomefile.p7m.p7m" oppure, "nomefile.pdf.p7m", se il file era stato precedentemente firmato in PAdES.

   Operativamente, per effettuare una firma "annidata o matrioska", occorre utilizzare la funzione "Firma", selezionando il file già firmato ed il software proporrà firma multipla "a matrioska" o "Firma esterna". Sottoponendo il file al processo di verifica verranno visualizzati più livelli per il file.p7m firmato. La firma nidificata è utilizzata, ad esempio, per firmare documenti informatici il cui certificato di firma è scaduto, qualora si voglia produrre una copia, oppure quando la proprietà sottoscrive il progetto commissionato e redatto dal progettista e controfirmato da quest'ultimo;

3. **firme digitali dette "controfirme":** in questo caso il soggetto che deve controfirmare, sottoscrive solamente una precedente firma apposta da un altro soggetto e conserva il risultato (detto controfirma) all'interno della medesima busta. Un documento con controfirme produce un file di tipo "nomefile.p7m" in formato CAdES. Con questa firma multipla, il secondo firmatario "controfirma" esclusivamente la prima firma apposta. A sua volta, la seconda firma potrà essere firmata da una terza persona, e così via. Si ritiene utile precisare che con la controfirma il

sottoscrittore non si assume giuridicamente la responsabilità dell'atto, ma si tratta di una firma successiva c.d. "nidificata", strettamente collegata alla firma precedentemente apposta per controllare o convalidare la prima (es: firma apposta nei ricorsi per convalidare la firma di un cliente o "vera la firma". In questo caso, ad essere oggetto di validazione è una firma già presente sul documento. Con qualsiasi software di firma digitale, per aggiungere una controfirma, occorre avviare la funzione di verifica delle firme, selezionare il file già firmato con estensione.p7m e lanciare la funzione "Apponi controfirma".

In conclusione, le firme multiple possono essere ricondotte a due categorie:

- **firme indipendenti**: sono firme parallele e sono usate quando l'ordine temporale di apposizione delle firme non è importante;
- **firme incorporate**: sono apposte una dopo l'altra e sono usate quando l'ordine temporale di apposizione delle firme è importante.

Le firme digitali locali e remote

La firma digitale locale

La firma digitale "locale" è lo strumento di firma tradizionale che si basa sull'uso di un supporto hardware (es. smart card, chiavetta USB) in cui è conservato il certificato di firma rilasciato dall'ente certificatore. Per il suo uso non è necessaria una connessione internet.

Con la firma digitale locale la data e l'ora di sottoscrizione è quella locale che viene rilevata dall'applicazione di firma digitale interrogando direttamente l'orologio del sistema operativo utilizzato dal software di firma; in conseguenza di ciò, la data e l'ora non sono né certe, né precise.

Per garantire la certezza della data, e quindi l'opponibilità ai terzi, è necessaria l'apposizione di firma digitale con marca temporale.[8]"

[8] Secondo la definizione che ne dà il DPCM 22 febbraio 2013 la marca temporale è "il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo

La firma digitale remota

La firma digitale remota è una firma digitale che si basa sull'uso di servizi telematici remoti e non prevede l'uso di dispositivi quali smart card o chiavi USB. La procedura di firma remota può essere utilizzata su pc o dispositivo mobile (tablet o smartphone).

Le differenze tra firma locale e remota riguardano la modalità operativa e gli strumenti necessari, mentre le buste crittografiche ottenibili sono le medesime.

Materialmente, servono soltanto:

1) un pc, tablet o smartphone collegati alla rete internet;

2) un dispositivo OTP (One Time Password), che genera password attraverso un token o una app per smartphone. Le password dinamiche sono considerate il sistema più sicuro per l'accesso ai sistemi informatici, eliminando i rischi legati alla necessità di memorizzare una password statica.

3) un software di firma remota (es. ArubaSign, Firma digitale Remota di Infocert, etc), attraverso il quale è possibile selezionare il documento digitale da sottoporre a firma remota.

Con la firma remota si possono firmare digitalmente tutti i formati di file (PDF, MS-EXCEL, MS-WORD, audio, video) ed ottenere tutti i formati di busta telematica crittografica previsti dalla normativa europea per la firma elettronica avanzata (CAdES, PAdES e XAdES).

Firma digitale remota massiva e firma automatica

Utilizzando la modalità di firma remota massiva il sottoscrittore firma almeno due o più documenti informatici con formato uguale o diverso. Questo strumento rappresenta l'evoluzione tecnologica "server side" della firma digitale locale singola che ha il suo fondamento giuridico nel DPCM 22 febbraio 2013: la chiave privata del certificato di firma digitale non è più fisicamente custodita dal firmatario, ma memorizzata in modo sicuro su un dispositivo server – connesso in rete e di solito disponibile sulla rete internet - che viene interrogato da remoto mediante l'accesso ad una rete protetta.

Il servizio è acquistato separatamente, ha una durata temporale limitata e rinnovabile e permette di sottoscrivere digitalmente in assenza di presidio puntuale e continuo da parte

del firmatario: per questo, si ritiene che sia il servizio indicato per coloro che gestiscono flussi documentali di grande entità.

La firma digitale automatica è una tipologia di firma digitale remota massiva che risulta particolarmente utile per sottoscrivere documenti informatici dello stesso genere.

In questo caso, l'utente specifica le tipologie di documenti informatici per i quali automatizzare l'applicazione della firma, senza che il PIN sia richiesto per ogni sottoscrizione del singolo documento informatico. Il firmatario non ha l'onere di presenziare durante l'operazione e gli vengono notificati l'apposizione della firma con sistemi automatici e i certificati di notifica.

ENTI CERTIFICATORI - PRESTATORI DI SERVIZI FIDUCIARI QUALIFICATI

La firma digitale si ottiene dai **prestatori di servizi fiduciari** presenti in una serie di elenchi gestiti dai singoli Stati membri europei.

Il Regolamento europeo eIDAS, ha cambiato le regole per i **certificatori di firma qualificata**. In base alla normativa italiana (derivata dal recepimento della direttiva 1999/93/CE e contenuta nel Codice dell'amministrazione digitale) un soggetto che intende svolgere l'attività di certificatore di firma qualificata presenta domanda ad AgID allegando alla domanda una serie di documenti amministrativi e tecnici. AgID esamina la documentazione e se la ritiene conforme ai requisiti normativi nazionali iscrive il soggetto richiedente in un apposito elenco pubblico. Il Regolamento sopra citato che è "*in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno* e che abroga la direttiva 1999/93/CE" ha modificato le regole introducendo **i prestatori di servizi fiduciari** e, per essi, l'attributo di qualificato che sostituisce l'accreditamento.

Quali sono i servizi fiduciari?

I servizi fiduciari sono definiti nell'articolo 3, numero 16 dell'eIDAS. Essi sono " *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; oppure*

b) creazione, verifica e convalida di certificati di autenticazione di siti web;

c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi."

L'avviamento di un servizio fiduciario qualificato da parte del prestatore di servizi fiduciari non è obbligatorio, ma ad esempio per erogare servizi attinenti alla sottoscrizione elettronica, che abbiano effetti giuridici equivalenti a quelli di una firma autografa, questa deve essere una firma elettronica qualificata. Quindi il prestatore deve avviare un servizio qualificato sul tema se vuole offrire questo tipo di servizio.

La qualifica si ottiene trasmettendo una notifica all'organismo di vigilanza (in Italia è l'Agenzia per l'Italia Digitale – AgID) alla quale è allegata una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità[9]. AgID verifica

[9] La relazione allegata alla notifica inviata ad AgID è rilasciata da un organismo che è conforme all'articolo 2, punto 13 del Regolamento comunitario n. 765/2008 ed è accreditato, a norma di quest'ultimo Regolamento,

le informazioni fornite e se tutto è conforme alle regole eIDAS concede la qualifica richiesta. La pubblicità legale dell'ottenimento del requisito di qualificato per i servizi richiesti è attestata da specifici elenchi di fiducia presenti in tutti gli Stati membri.

L'elenco dei soggetti qualificati da AgID in Italia è reperibile sul sito AgID

(alcuni fra i più noti: Actalis, Aruba, Banca d'Italia, Consiglio Nazionale del Notariato, Infocert, Intesa, Lottomatica, Namirial, Poste Italiane, Zucchetti).

---

come accreditato a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati.
L'accreditamento è, in Italia, a carico di ACCREDIA è viene valutato in base ad uno standard europeo numerato come ETSI EN 319 403 .
Una volta definiti gli organismi in grado di rilasciare attestazioni di conformità, i prestatori di servizi fiduciari devono essere conformi agli specifici standard EN relativi alla qualifica che vogliono ottenere.

VERIFICA DELLA FIRMA DIGITALE

Il processo di verifica di un documento firmato digitalmente ha l'obiettivo di verificare la validità, l'autenticità e l'integrità del documento.

È possibile procedere al controllo (verifica) sul documento per accertare che non sia stato alterato; questa attività può essere effettuata utilizzando un qualsiasi servizio online, messo a disposizione gratuitamente da uno dei certificatori, o tramite l'apposita funzione presente nel software di firma utilizzato.

Si procede con la selezione del file firmato ricevuto, si lancia la funzione di verifica e, attraverso il rapporto di verifica, si può riscontrare da quale soggetto è stato firmato il documento informatico analizzato, la data di firma, la conformità al regolamento EU 910/2014 eIDAS, la tipologia di firma (es. busta formato CAdES), la validità del certificato di firma (se è scaduto) e l'integrità del documento.

L'operazione di verifica può essere effettuata anche da coloro che non possiedono una firma digitale, utilizzando uno dei software di verifica resi disponibili gratuitamente, presenti nell'apposito elenco AGID.

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 (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.

In pratica, chi riceve il messaggio firmato, lo apre e, con lo stesso software, acquisisce il certificato annesso al documento firmato, estraendo la chiave pubblica del mittente; con la chiave pubblica viene decifrata la stringa della firma digitale, ottenendo l'impronta del documento. Il destinatario poi, esegue la stessa operazione generando autonomamente

con la chiave pubblica l'impronta del documento. Se le due impronte, quella generata dal mittente estratta dalla firma digitale e l'altra, appena calcolata dal ricevente, saranno uguali, allora vuol dire che il messaggio originario non è stato in alcun modo alterato e la verifica ha avuto esito positivo.

Verifica dei poteri del sottoscrittore con particolare riguardo alla firma digitale

Quando parte del contratto non sia la persona fisica del sottoscrittore – nel nostro caso, il contraente di polizza o il coobbligato – ma l'ente collettivo da questo rappresentato, è evidentemente necessario che risulti con certezza:

- che parte del negozio, che ne assume le relative obbligazioni, non è la persona fisica del firmatario bensì l'ente e dunque che la firma sia stata apposta dal primo nella qualità di rappresentante dell'ente;
- che la persona fisica, che in tale qualità ha firmato abbia i poteri per stipulare il contratto e assumere le obbligazioni per conto dell'ente rappresentato.

È principio consolidato in giurisprudenza e in dottrina che anche nell'ipotesi di rappresentanza societaria, e dunque di immedesimazione organica, è necessaria la cd. contemplatio domini e conseguentemente la spendita del nome della società da parte del suo rappresentante perché il negozio concluso attraverso l'atto da lui sottoscritto spieghi i suoi effetti nei confronti della società.

Dottrina e giurisprudenza concordemente affermano che il dettato normativo di cui all'art. 1388 cod. civ., in tema di contratto concluso dal rappresentante, è applicabile anche con riferimento alla rappresentanza organica, configurabile appunto in relazione ai soggetti che rivestono la qualifica di organi rappresentativi di persone giuridiche.

Perché il contatto produca i propri effetti nei confronti dell'ente rappresentato dal sottoscrittore occorre dunque la ricorrenza di tre requisiti:

a) il conferimento del potere rappresentativo, che nelle società spetta agli amministratori per effetto dell'atto costituivo, dello statuto o delle delibere di nomina;
b) l'agire il rappresentante nei limiti dei propri poteri, limiti peraltro opponibili ai terzi

solo coi limiti previsti dagli artt. 2298, 2384 e 2475 bis cod. civ. (in breve, nel caso di società di persone i limiti risultanti dall'atto costitutivo o dalla procura sono opponibili ai terzi solo se sono iscritti nel registro delle imprese o se si fornisce la prova che i terzi ne hanno avuto conoscenza; nel caso di società di capitali i limiti risultanti dall'atto costitutivo o dall'atto di nomina non sono opponibili ai terzi anche se pubblicati salvo che si provi che i terzi abbiano intenzionalmente agito in danno della società);

c) la cd. *contemplatio domini* ossia la circostanza che venga manifestata la riferibilità del negozio al soggetto rappresentato dal sottoscrittore. Tale elemento assolve alla duplice funzione di esteriorizzare il rapporto di gestione rappresentativa e di imputare all'ente rappresentato gli effetti del contratto concluso con la sottoscrizione da parte del suo rappresentante.

Con riferimento alla polizza fideiussoria è dunque compito degli uffici della Compagnia o dell'Agente che provvedono al perfezionamento del contratto raccogliendo la firma – del contraente o del coobbligato - quando questi sottoscriva non in proprio ma quale amministratore-rappresentante di persona giuridica, accertarne i poteri, ed opportunamente gli eventuali limiti, con riferimento all'ente da lui rappresentato, e verificare che nel documento sia idoneamente palesata la spendita del nome del soggetto-ente rappresentato che è parte del negozio giuridico.

Tale manifestazione o se si vuole *contemplatio domini* avviene:

- innanzi tutto, elemento ovviamente necessario ma che può ritenersi non sempre sufficiente o tranquillizzante, attraverso l'indicazione, nella intestazione della polizza o dell'atto di coobbligazione dell'ente societario quale parte del negozio (contraente o coobbligato) con la precisazione del codice fiscale/partita IVA dell'ente;
- nella indicazione, nello spazio della firma (di contraente o coobbligato) a stampa o attraverso l'apposizione di timbro, dell'ente societario che è parte del contratto.

Quando la polizza è emessa in formato elettronico e la parte - contraente o coobbligato - appone la firma digitale, la situazione non è poi così differente, ma con alcuni accorgimenti.

Analoghe le verifiche da compiersi dagli uffici della Compagnia o dall'Agente circa i poteri

di firma e di rappresentanza in relazione alla società che assume la veste di contraente o di coobbligato.

Nella verifica della firma digitale, o meglio dello strumento di firma digitale rilasciato dall'Ente certificatore, sarà opportuno verificare chi sia il soggetto titolare della firma digitale, ovvero che la persona (fisica) titolare della firma digitale sia tale nella qualità di amministratore-rappresentante dell'ente societario per il quale e nel cui nome viene concluso il contratto con la sottoscrizione digitale.

In definitiva il certificato di firma digitale, nelle sue diverse forme, sarebbe auspicabile che contenesse – e questa sarà la verifica da attuare all'atto della raccolta della sottoscrizione digitale - la precisazione che è rilasciato alla persona fisica nella sua qualità di rappresentante (della società contraente o coobbligata) e anche l'attestazione dei relativi poteri da parte del certificatore -verifica che in ogni caso deve essere condotta con gli stessi strumenti utilizzati in passato, come la visura camerale o l'acquisizione degli atti societari da cui risultano tali poteri in capo al soggetto firmatario.

CENNI SUL SIGILLO ELETTRONICO

Fra le novità introdotte dal Regolamento eIDAS, particolare rilievo assume il sigillo elettronico, che svolge per la persona giuridica lo stesso ruolo della firma elettronica per la persona fisica.

Il Regolamento eIDAS, all'art. 3, cc. 24-25 definisce:

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

E Creatore del sigillo: una persona giuridica che crea il sigillo

Esistono due tipi di sigilli: sigillo elettronico avanzato e sigillo elettronico qualificato

Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

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

Sigillo elettronico qualificato è creato da un dispositivo e certificato qualificato

(ad esempio rilasciato da un certificatore). (artt.35 e 36 Regolamento eIDAS)

Effetti giuridici dei sigilli elettronici

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

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

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

VALIDITÀ TEMPORALE DELLA FIRMA DIGITALE

Ai sensi dell'art. 24, comma 3 del CAD "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". Il comma 4 bis determina conseguentemente il valore legale del documento sottoscritto con certificato non più valido stabilendo che "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 è [...omissis...]". In altre parole, se il certificato di firma è scaduto, revocato o sospeso, non è possibile stabilire con certezza se il titolare ha firmato il documento quando il certificato era valido, e l'autenticità e l'integrità del documento non sono garantiti.

Al fine di rinnovare tempestivamente i certificati di firma, occorre tener conto che questi sono solitamente sottoposti a scadenza triennale.
Per mantenere la validità di un documento oltre la scadenza del certificato di firma le regole tecniche vigenti in materia firme elettroniche indicano diversi strumenti che certificano la data e l'ora del documento rendendoli opponibili ai terzi, quali la marca temporale, la posta elettronica certificata, la segnatura di protocollo e la conservazione a norma.[10]

Marca temporale

Nel caso specifico della marca temporale, si fa riferimento ad una procedura grazie alla quale la data impressa nel documento non è quella residente nel dispositivo di firma ma quella rilasciata da un ente certificatore appositamente accreditato (Time Stamping Authority - TSA), associata ad una data e ad un orario giuridicamente certi ed opponibili a terzi: "Nel caso di documenti su cui sia stata apposta una firma digitale, la presenza di una marca temporale consente di attestare che il documento aveva quella specifica forma in quel preciso momento temporale, pertanto anche se successivamente il certificato qualificato scadesse o fosse revocato, si potrebbe sempre dimostrare che la firma digitale è stata apposta durante il suo periodo di validità"[11].

[10] Si veda art. 41 DPCM 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.
http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche
[11] Articolo 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.

DOCUMENTO INFORMATICO - VALORE LEGALE

Documento informatico privo di sottoscrizione e sottoscritto con firma elettronica semplice

L'art. 20 comma 1bis secondo periodo del CAD, disciplina la "Validità ed efficacia probatoria dei documenti informatici" disponendo, con riferimento al documento informatico non sottoscritto ed al documento informatico sottoscritto con firma elettronica semplice, che *"[...omissis…] 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 sicurezza, integrità e immodificabilità*"5. 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): in questi casi sarà il giudice a valutare il valore del documento e 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.

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[12], che garantisce facilità di visualizzazione, anche a distanza di tempo e utilizzando software diversi.

Documento informatico sottoscritto con firma elettronica (avanzata, qualificata, digitale)

L'articolo 20 comma 1bis primo periodo del CAD determina poi il valore che ha un documento informatico sottoscritto con firma elettronica: *"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.*".

Come si può vedere, il legislatore considera diversamente il valore giuridico e probatorio

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

dei documenti sottoscritti con firme c.d. “forti” rispetto a quelli privi di sottoscrizione o sottoscritti con firma semplice. Infatti, il documento dotato di firma ”forte” mostra un’affidabilità più elevata in ordine alla paternità del documento, soddisfa sicuramente il requisito della forma scritta e, se sottoscritto con firma elettronica avanzata, qualificata o digitale ha valore di scrittura privata

A scopo esemplificativo di quanto riporta l’art. 20 nel suo complesso si pensi al diverso valore giuridico attribuito alle email dotate di firma elettronica semplice o debole o all’affidabilità di un messaggio di PEC, fino ad arrivare ad un file di testo sottoscritto con firma digitale.

EFFICACIA PROBATORIA DEL DOCUMENTO INFORMATICO

Lo spettro probatorio dei documenti informatici spazia dal documento informatico semplice (non firmato) al documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale.

Tratti probatori di ciascuna firma

Quanto ai documenti informatici non sottoscritti, è appena il caso di segnalare che questi non hanno, in sé considerati, alcun valore probatorio (né, tantomeno, costituiscono prova scritta), proprio per la natura dematerializzata degli stessi e la sostanziale impossibilità di riferire in maniera concreta un documento privo di sottoscrizione (intesa come applicazione di un algoritmo informatico, quale che sia) ad un estensore. Si consideri, tanto per fare un esempio, che ad un documento informatico recante la mera scansione di una firma non potrà essere conferito alcun valore probatorio, cosicché la semplice produzione in giudizio di un documento così formato non potrà essere considerata una prova (né un indizio).

Solo la concorrenza di tale produzione con altri elementi probatori (primo tra tutti, la mancata contestazione di un tale documento) potrà contribuire a far diventare il documento un indizio (difficilmente una vera e propria prova) utilizzabile in sede di decisione.

Ciò premesso per brevità, in questa sede, verranno analizzati solo i documenti sottoscritti.

Efficacia probatoria documenti sottoscritti con firma elettronica semplice

Il criterio di base per valutare l'efficacia probatoria di un documento informatico sottoscritto è disciplinato dal combinato disposto dell'art. 25 di eIDAS e dall'art. 20 del CAD. Sulla disciplina italiana si è già detto, quanto ad eIDAS invece dispone 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".*

In sostanza, la lettera della legge, dopo aver disposto il principio di non discriminazione del documento firmato con firma elettronica semplice, precisa che qualunque documento elaborato per il tramite di un meccanismo di firma elettronica è certamente dotato del requisito di forma scritta (e può dunque essere validamente usato per la conclusione di negozi giuridici che prevedano tale forma per la loro stipula) e, dal punto di vista probatorio deve essere valutato dal giudice in relazione all'attitudine che la firma apposta possiede, di rendere tale documento immodificabile e riferibile all'estensore apparente.

In proposito, e a titolo esemplificativo, si osserva come un filone giurisprudenziale che affonda le sue radici nella prima versione del CAD e che, dopo l'avvento di eIDAS, sta conoscendo un deciso consolidamento (si consideri ad esempio che la prima pronuncia di merito successiva all'entrata in vigore del Regolamento Europeo sulle firme elettroniche è stata la n. 11402/2016 del Tribunale di Milano, est. Consolandi), ha ridisegnato i confini della posta elettronica semplice facendo si che, nella sostanza, una mail tradizionale venga utilizzata nell'ambito della valutazione delle prove in sede giurisdizionale, come fonte di prova documentale paragonabile al documento firmato con firma elettronica semplice.
Si potrebbe dire dunque che, al di là della necessità di integrare una mail con ulteriori elementi (scambio di mail da e verso gli stessi indirizzi, mancata contestazione, conferma testimoniale,), la mail costituisce di per sé un indizio di prova (in forma scritta) idoneo ad indirizzare il convincimento di un Giudice.

Efficacia probatoria documenti sottoscritti con firma elettronica avanzata, qualificata o digitale

Anche in questo caso la disamina degli effetti probatori derivanti dall'applicazione, ad un file digitale, di una firma avanzata, qualificata o digitale deve partire dalle disposizioni del CAD il quale recita che "*II 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 […Omissis..]".*

Il citato articolo codicistico disciplina poi gli effetti probatori della firma autografa la quale, ove prodotta in giudizio può essere sempre contestata dal soggetto contro il quale sia

prodotta tramite una contestazione semplice.

Da un punto di vista di mero diritto dunque (e salvo quanto si dirà a breve circa l'inversione dell'onere probatorio in caso di sottoscrizione digitale) l'apposizione di una firma digitale, sul piano probatorio, ha gli stessi identici effetti della sigla vergata di pugno su un foglio di carta.
Dal punto di vista processuale, invece, il soggetto contro il quale sia prodotto un documento da lui sottoscritto (cartaceo o informatico che sia) può disconoscere la sottoscrizione negando che la firma sia stata da sé apposta.

Solo laddove il documento in questione venga riconosciuto o debba intendersi legalmente considerato come riconosciuto (ipotesi di autentica notarile) farà piena prova fino a querela di falso.

Trattiamo dunque il caso di disconoscimento della sottoscrizione della firma digitale.

DISCONOSCIMENTO DELLA FIRMA DIGITALE

Trattiamo ora i seguenti argomenti:

- efficacia del documento sottoscritto con firma digitale
- possibilità e limiti del disconoscimento della firma digitale e onere probatorio
- responsabilità derivante a carico del titolare della firma digitale
- la firma grafometrica

Efficacia del documento sottoscritto con firma digitale - Possibilità e limiti del disconoscimento della firma digitale e onere probatorio

L'art. 20 comma 1 bis del CAD nella sua attuale formulazione, riprendendo in sostanza e per quanto qui di interesse il disposto del precedente art. 21 comma 2 CAD ora abrogato, con riferimento all'efficacia del documento informatico sottoscritto con firma digitale, o altro tipo di firma elettronica qualificata o avanzata, dispone che:
"***soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'art 2702 del codice civile***".

Ancora **l'art. 20 comma 1 ter 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***".

Sulla scorta di una prima lettura delle norme del CAD e della valutazione circa la portata della firma digitale conseguente all'utilizzo dello strumento rilasciato al titolare della firma da Certificatore qualificato, si è da più parti ipotizzato che la pienezza della prova conferita al documento informatico sottoscritto con firma digitale, quanto alla sua provenienza dal firmatario, potesse essere messa in discussione solo attraverso la querela di falso e che la richiesta di autentica notarile rappresentasse un *plus* del tutto ultroneo.

A ben vedere, e pur sussistendo vivace contrasto in dottrina circa la maggiore o minore forza probatoria della firma digitale - alla luce della nuova formulazione dell'art. 20 del CAD -, non è proprio così.

Va premessa la considerazione, ovvia anche se non sempre scontata, che il documento

informatico con firma digitale è la semplice evoluzione biologica del documento cartaceo con firma autografa, e che quindi si tratta di sopperire con le regole tecniche dettate dal legislatore alla necessità di trasferire dal primo al secondo strumento (cartaceo e firma autografa – informatico e firma digitale) le idonee forme di garanzia circa la imputabilità e la verifica della sottoscrizione.

Come si è visto l'art, 20 del CAD si limita a riconoscere al documento informatico sottoscritto con firma digitale la stessa efficacia di cui all'**art. 2702 del codice civile**.

Orbene la norma del codice civile dispone che ***"la scrittura privata fa piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta"*** (ma solo) ***"se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta****".*

Questi essendo i limiti circa la piena prova, superabile con la querela di falso, dettati dall'art. 2702 cod. civ., e considerato anche che **l'art. 25 del CAD** prevede, nell'attuale testo, che *"**si ha per riconosciuta ai sensi dell'art. 2703 cod. civ. la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato**",* sembra potersi concludere nel senso che sia ammessa non solo la contestazione attraverso prova contraria dell'utilizzo della firma digitale, ma anche il disconoscimento della firma digitale in senso stretto, e cioè ai sensi dell'art. 214 del codice di procedura civile ("*Colui contro il quale è prodotta una scrittura privata, se intende disconoscerla, è tenuto a negare formalmente la propria sottoscrizione*").

In altre parole: il CAD non attribuisce al documento informatico con firma digitale una fede privilegiata rispetto a quello cartaceo con firma autografa, ma solo l'efficacia della scrittura privata con espresso rinvio alla previsione dell'art. 2702 cod. civ. e non piuttosto l'efficacia dell'atto pubblico con firma autenticata ai sensi dell'art. 2703 cod. civ...

Ed ancora il CAD prevede espressamente l'ipotesi di autenticazione di ogni tipo di firma elettronica avanzata (prima dell'ultima modifica la norma faceva peraltro riferimento alla firma elettronica "avanzata o digitale") da parte di notaio per i relativi effetti giuridici (compresa la trascrivibilità dell'atto) che non avrebbe alcun senso diversamente ragionando.

Fermo quanto precede è peraltro opportuno verificare il diverso atteggiarsi dell'onere della prova nelle due ipotesi di disconoscimento, della firma autografa e di quella digitale.

Nel primo caso (firma autografa), a fronte del disconoscimento a norma del richiamato art. 214 del codice di procedura civile, la parte che intende avvalersi della scrittura disconosciuta è tenuta a chiederne la verificazione, ai sensi dell'art. 216 cod. proc. civ., ed è onerata di proporre i mezzi di prova utili a tal fine, e la giurisprudenza di Cassazione ha chiarito come sia onere di chi subisce il disconoscimento della sottoscrizione esibire in giudizio l'originale del documento contenente la sottoscrizione per poter raggiungere attraverso C.T.U. calligrafica la prova circa la autenticità della firma contestata.

Nel secondo caso (firma digitale), è stato osservato come si porrà non tanto un problema di "falsità", quanto piuttosto di "attribuzione" della firma.

In ogni caso, in ipotesi (che si profila in verità rara) di contestazione circa la falsificazione della firma digitale, a fronte del disconoscimento, nella evidente impossibilità di dar corso ad una consulenza grafologica sulla firma contestata, si tratterà di chiederne una verificazione di tipo informatico cioè di controllo di tutte le fasi del procedimento per accertare che non ci siano state alterazioni del contenuto del documento.

La contestazione peraltro (almeno nella maggior parte dei casi) verterà non già sulla firma elettronica in sé, bensì sul suo eventualmente indebito utilizzo, ed anche in considerazione del dettato dell'art. 20 comma 1 ter del CAD (che riconduce con presunzione l'utilizzo del dispositivo di firma al titolare, salvo prova contraria) si può affermare che l'onere della prova è inverso, nel senso che sarà il soggetto che disconosce il documento, ovvero la sua firma digitale allo stesso, a dover provare di non avere apposto la firma digitale sul documento informatico.

In definitiva pare potersi concludere:

- che il disconoscimento della firma digitale si possa ritenere consentito senza necessità di fare ricorso alla querela di falso:
- che il disconoscimento, almeno nella generalità dei casi, verta non sulla sottoscrizione in sé ma sull'utilizzo dello strumento di firma digitale.

La giurisprudenza, assai scarsa, che si è occupata della problematica ha inteso consentire al soggetto disconoscente il ricorso ad ogni mezzo di idonea prova, utile a dimostrare l'indebito utilizzo del dispositivo dii firma elettronica, ed anche dunque alle prove orali attraverso testimoni, idonee a smentire la riconducibilità al titolare.[13]

A siffatte pittoresche ed in parte superficiali affermazioni giurisprudenziali, sembra doversi apportare un correttivo, sempre desumibile dalle norme del CAD.

Si è visto come il documento firmato digitalmente, a differenza del documento cartaceo, possa essere contestato dall'apparente sottoscrittore a condizione però che lo stesso dia dimostrazione che la firma (digitale) non è stata da lui apposta.

È dunque opportuno rammentare che l'**art. 32 comma 1 del CAD** dispone che:
*"**il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma**".*

Da tali previsioni normative deriva che nel caso in cui il titolare della firma digitale dia dimostrazione di non avere utilizzato personalmente il dispositivo di firma, e dia dimostrazione dell'utilizzo indebito da parte di terzi, dovrà comunque dare idonea dimostrazione anche di avere messo in atto tutte le cautele per la diligente custodia dello strumento di firma atte ad impedirne l'asserito illegittimo utilizzo da parte di terzi.

In mancanza di tale ulteriore prova, il titolare della firma digitale potrà ritenersi comunque responsabile dell'atto sottoscritto a suo nome, a seguito della negligenza nella corretta

[13] In tale senso si è espresso il Tribunale di Roma nella sentenza n. 1127/2017 del 23/1/2017. Nella fattispecie il Tribunale, pur affermando che ai sensi dell'art. 21 (ora art. 20) del CAD l'utilizzo del dispositivo di firma digitale si presume riconducibile al titolare, tenuto a dare prova contraria, con inversione dunque dell'onere probatorio, ha poi accolto la domanda di disconoscimento della sottoscrizione di un atto di cessione di quote con firma digitale, giudicando provato l'abusivo utilizzo del dispositivo di firma da parte di un terzo (tra l'altro successivo amministratore della medesima società) sulla scorta della produzione documentale della ricevuta di pagamento di un parcheggio situato presso l'abitazione di un'amica dell'attore disconoscente (circostanza all'evidenza di per sé priva di significato ai fini di dimostrare la non utilizzabilità del dispositivo di firma digitale da quella abitazione) e soprattutto sulla scorta delle dichiarazioni rese da tale conoscente dell'attore in sede di deposizione testimoniale (laddove la stessa ha dichiarato che l'attore, all'epoca suo fidanzato, aveva trascorso la notte nella sua abitazione lasciandola solo nella tarda mattinata successiva).

gestione del dispositivo di firma, e sarà responsabile, se non anche della validità dell'atto e dei suoi effetti, comunque del danno dalla sua condotta causato ai terzi che in buona fede abbiano fatto affidamento circa la validità ed efficacia dell'atto a lui apparentemente riconducibile e da lui apparentemente sottoscritto con la sua firma digitale.

La firma grafometrica

La **firma grafometrica o firma biometrica**, come già visto, rappresenta una tipologia di firma elettronica avanzata e come tale sembra indubbiamente rapportabile alla previsione dell'art. 20 comma 1bis del CAD, analogamente alla firma digitale, e dunque soddisfa il requisito della forma scritta e ha l'efficacia probatoria della scrittura privata ai sensi dell'art 2702 del c.c..

Conseguentemente con riferimento alla firma grafometrica si possono svolgere le medesime considerazioni sopra svolte con riguardo alla firma digitale quanto all'ipotesi di eventuale disconoscimento, ammissibile entro certi limiti.
Quali sono in sostanza le differenze?

Nel caso di **firma digitale** la riconducibilità della sottoscrizione all'autore è individuabile nella titolarità del dispositivo di firma rilasciato dall'ente certificatore che all'atto del rilascio ha identificato il soggetto e quindi, come già visto, il disconoscimento della firma digitale viene a risolversi, nella quasi totalità dei casi, nella contestazione circa l'indebito utilizzo dello strumento di firma, laddove peraltro la normativa del CAD prevede la presunzione di utilizzo da parte del titolare e conseguentemente l'inversione dell'onere probatorio.

Nel caso invece di **firma grafometrica** la riconducibilità della sottoscrizione all'autore non può che essere attestata dal soggetto (ad esempio l'agente della Compagnia o il funzionario della Banca), che raccoglie la firma grafometrica (del contraente o del coobbligato), verificandone l'identità.
In questo caso, in ipotesi di disconoscimento, all'atto della richiesta di verificazione del documento di cui ci si intende avvalere, non vi è inversione dell'onere della prova e sarà la Compagnia o la Banca a dover provare l'autenticità della firma attraverso una CTU grafologica che, ovviamente, dovrà svolgersi non con riguardo alla firma autografa

apposta sull'originale del documento cartaceo, ma sulla firma biometrica apposta su un documento informatico – file da esibire nel suo originale (ed il 'perito grafologico-informatico' dovrà accertare l'integrità del documento informatico e la firma biometrica nell'esame dei suoi elementi di forma, pressione e velocità del tratto grafico).

Questi sembrano essere gli evidenti limiti della firma grafometrica rispetto alla firma digitale (rapportabile la prima alla tipologia di firma elettronica avanzata, la seconda alla tipologia di firma elettronica qualificata).

Per contro, sembra altrettanto evidente la praticità della firma grafometrica nel momento in cui consente di raccogliere con semplicità ed immediatezza – ferma la necessità di identificazione del soggetto che appone la firma sul tablet – più firme del soggetto in calce a più files che gli vengono consecutivamente sottoposti (ad esempio per la sottoscrizione delle condizioni di contratto e poi delle clausole vessatorie).

Le Banche, come noto, da tempo hanno adottato questa tipologia di firma, proprio nell'ottica di acquisire la valida sottoscrizione con modalità semplici e veloci e, come ci è stato riferito, pur nella consapevolezza dei limiti sopra individuati che vengono accettati come contropartita della velocità e della semplicità dell'operazione di firma, in un'esperienza di contestazioni assai limitate rispetto alla miriade di negoziazioni.

Sempre con riferimento ai possibili limiti della firma grafometrica allorché si debba procedere alla prova circa l'autenticità della sottoscrizione, ci è stato riferito che al momento paiono porsi seri problemi dal punto di vista tecnologico per la esibizione processuale del documento informatico sottoscritto e per lo svolgimento della eventuale CTU "grafologica informatica".

AUTENTICAZIONE NOTARILE DELLA FIRMA DIGITALE

Si è già osservato come la richiesta di autentica notarile della firma digitale non sia da considerarsi formalità priva di significato, e si è richiamata la previsione **dell'art. 25 del CAD** che, nella sua interezza, dispone:

"***1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato***".

"***2. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico***".

"*3. L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2*".

"*4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5*".

Esaminiamo per quanto qui di interesse i primi due commi della norma.

Attraverso il procedimento di autenticazione della firma digitale , la scrittura privata contenuta nel documento informatico così sottoscritto acquista **l'efficacia di cui all'art. 2703 del codice civile** e dunque "**si ha per riconosciuta"**, con la conseguenza che essa "***fa piena prova della provenienza delle dichiarazioni da chi l'ha sottoscritta fino a querela di falso***".

Solo attraverso tale strumento dunque potrà essere contestata dal sottoscrittore e il procedimento di querela di falso non potrà che avvenire nei confronti del notaio che ha autenticato la firma, il quale avrà necessariamente identificato il soggetto firmatario, certificato che la firma è stata apposta in sua presenza e constatato la validità del certificato di firma, così venendo a rispondere del reato di falso ideologico ove dovesse

essere dimostrata la falsità di quanto da lui attestato.

Dal coordinamento tra il richiamato **art. 25 del CAD e l'art. 47 bis comma 2 Legge Notarile** risulta quanto segue:

a) la autenticazione della firma digitale consiste in una attestazione del notaio;

b) detta attestazione può essere contenuta nello stesso documento informatico o in un documento informatico ulteriore collegato con quello che reca le firme digitali delle parti;

c) per procedere alla attestazione il notaio deve previamente accertare:

- **1.** l'identità personale della parte che sottoscrive l'atto;
- **2.** la validità del certificato elettronico di firma utilizzato per la sottoscrizione;
- **3.** il fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico (cd. controllo di legalità);

d) quanto al contenuto della attestazione notarile, da essa devono risultare:

- **1.** la dichiarazione del notaio che la firma digitale della parte è stata apposta in sua presenza, e ciò al fine evidente di garantire che il dispositivo di firma è stato effettivamente utilizzato dal relativo titolare, e non da un terzo che lo detenga illegittimamente, previa verifica circa la validità del certificato elettronico di firma;
- **2.** l'indicazione della data e del luogo.

Più in generale può osservarsi che trovano applicazione nel procedimento di autenticazione della firma digitale tutte quelle disposizioni della legge notarile la cui ratio ha carattere generale e prescinde dal tipo di supporto utilizzato, cartaceo o informatico.

Se il notaio non attesta che la firma è stata apposta in sua presenza previo accertamento dell'identità personale del sottoscrittore, limitandosi ad attestare la verificata validità del certificato di firma, tale attività del notaio dovrebbe essere qualificata alla stregua di mera "verifica di firma", che poco aggiunge al documento perché il notaio ha semplicemente verificato i poteri di firma e quanto alla firma in sé ha fatto ciò che ciascuno può fare e cioè verificare l'esistenza della firma digitale; l'operazione può avere senso per certificare ad esempio la data certa dell'atto, ciò che potrebbe risultare utile anche allo scopo di verificare la apposizione della firma digitale nel termine di validità del relativo certificato.

Altra operazione è la "autentica di firma" che presuppone, e il notaio lo attesta, che la

firma è stata apposta in sua presenza, su documento, con firma cartacea o digitale, previa verifica dell'identità del sottoscrittore: in tal modo la firma fa piena prova fino a querela di falso come sottoscrizione proveniente dal titolare dello strumento di firma digitale.

È sempre necessaria, come detto, la menzione dell'accertamento circa la validità del certificato elettronico di firma, ciò che garantisce che le scritture private (contenute in un documento informatico con firma digitale) autenticate da notaio conservino validità anche qualora in futuro fosse impossibile verificare la validità e la vigenza del certificato di firma (problema al quale sembra potersi altrimenti ovviare, nella generalità dei casi, attraverso la apposizione al documento informatico della marca temporale).

Seppure non espressamente previsto, anche per l'autenticazione delle firme elettroniche o digitali deve ritenersi applicabile in via analogica quanto disposto dall'art. 52 bis Legge Notarile e pertanto deve ritenersi possibile l'autenticazione digitale della firma autografa, contenuta dunque su un documento non informatico ma cartaceo.

Infine, la previsione del terzo comma dell'art. 25 CAD sta a significare che l'apposizione della firma digitale del notaio (che produce gli effetti di cui all'art 24 secondo comma CAD) integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine prevista dalla normativa.

LA FIRMA DIGITALE E LA POLIZZA FIDEIUSSORIA

Esaminando le differenti modalità di emissione delle polizza fideiussorie attualmente adottate si può osservare che l'emissione della polizza in formato digitale è una modalità alternativa a quella di emissione in formato analogico[14] e cioè su supporto cartaceo e con firma autografa.

La prima costituisce evoluzione della seconda e si sostanzia nella produzione di un documento informatico[15] e deve rispettare le necessarie forme per la sua validità ed efficacia.

È dunque indispensabile il puntuale rispetto della normativa del CAD con riferimento ai documenti informatici per come normati all'interno dello stesso.
Esamineremo nel seguito le modalità di emissione della polizza con firma digitale da parte delle Compagnie vuoi della Direzione o dell'Agenzia, la trasmissione al Contraente e il perfezionamento del contratto da parte del contrente ed eventuali coobbligati.

Modalità di emissione della polizza fideiussoria con firma digitale

Richiesta di emissione della polizza e previsione contenuta nei bandi

Le principali modalità di emissione con firma digitale attualmente adottate dalle Compagnie si possono così individuare:

1. Emissione di un unico file polizza contenente la scheda-frontespizio di polizza, le condizioni di assicurazione, eventuali appendici, dichiarazioni del contraente.
2. Emissione di più file corrispondenti ai simpli della polizza (gli esemplari di pertinenza della Direzione della Agenzia del Beneficiario del Contrente) e per ciascuna parte gli eventuali ulteriori file contenenti ad esempio appendici di precisazione, dichiarazioni del contraente, atti di coobbligazione meglio descritti di seguito.

Simplo per il beneficiario contenente la scheda di polizza e le condizioni che regolano il

[14] CAD art 1: "documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti"
15 CAD art 1: "documento informatico: documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti";

rapporto tra beneficiario e garante, eventuali appendici [delle volte anche CGA tra garante e contraente (oltre ad eventuali dichiarazioni del contraente e la regolazione del premio e all'impegno ad esempio all'emissione della cauzione definitiva)]

Simplo per il contraente contenente più file relativi a scheda di polizza e le condizioni che regolano il rapporto tra garante e contraente, le clausole vessatorie (oltre ad eventuali dichiarazioni del contraente e la regolazione del premio) [delle volte anche CGA tra beneficiario e garante]

Simplo per la Compagnia contenente più file relativi alle condizioni che regolano il rapporto tra stazione appaltante e garante, tra garante e contraente (oltre ad eventuali dichiarazioni del contraente e la regolazione del premio), tra garante e coobbligati

atto di coobbligazione contenente più file relativi al file polizza per il coobbligato, l'atto di coobbligazione, le clausole vessatorie.

Firma digitale apposte dalla Compagnia

È necessario che la firma digitale apposta dalla Compagnia sul file contenente il documento informatico rappresentativo della polizza, ovvero sui singoli files contenenti i documenti informatici che compongono la polizza, sostituisce la firma autografa e ne segue la regolamentazione.

I primi commentatori della materia ritenevano che l'immagine digitale (un file bmp, gif, jpeg, ecc.) come la mera riproduzione all'interno del file della firma autografa (scanning della firma autografa) di un soggetto, inserita in un documento, dovesse considerarsi "firma elettronica".

In realtà, la riproduzione digitale di un segno grafico non può validare né i dati né l'identità del firmatario ma può solo essere considerata una "*pace per gli occhi*" laddove sia previsto ancora uno spazio fisico nel quale inserire una firma in un documento che è sottoscritto con firma digitale; la firma elettronica non va quindi confusa con la riproduzione a stampa del nome dell'autore dell'atto e neppure con la firma "digitalizzata" (o scannerizzata).

Una prima considerazione: si è osservato come la firma elettronica sia l'evoluzione della firma autografa e non abbia una diversa e maggiore valenza e dunque in linea di massima le sottoscrizioni digitali in un documento informatico non possono che essere tante quante sarebbero le sottoscrizioni analogiche in un documento cartaceo.

Si deve ritenere evidentemente necessaria una sottoscrizione, analogica o digitale che sia, in calce alle condizioni di contratto ed alle altre previsioni di polizza che debbano autonomamente essere sottoscritte.

La Compagnia dunque dovrà apporre tante firme digitali quante sono richieste nel file accorpando per semplicità quelle parti del contratto che non richiedono una sottoscrizione autonoma.

Un tempo si chiedeva ai tipografi di modificare l'aspetto del simplo polizza, oggi oltre all'aspetto grafico occorre coordinarsi con gli informatici.

A nostro parere nella stampa del simplo tanti spazi per la firma della Compagnia a fronte di un'unica sottoscrizione digitale potrebbero apparire contraddittori.

Verifica della polizza emessa con firma digitale

Può essere opportuno che contestualmente alla polizza venga redatta, all'interno del documento contrattuale o quale allegato a costituirne parte integrante, una dichiarazione che consenta al beneficiario di verificare l'esistenza e regolarità e l'eventuale conformità del documento cartaceo consegnato dal contraente alla polizza emessa e sottoscritta con firma digitale da soggetto munito dei poteri nel rispetto della normativa di riferimento.

Di seguito il testo che si è suggerito ad alcune imprese ed è stato inserito in calce alla polizza in apposito riquadro o quale allegato alla polizza a formarne parte integrante

La presente polizza è conforme alla polizza originata, emessa e conservata in via informatica, sottoscritta con firma digitale dalla …… Assicurazioni S.p.A. nella persona del Sig. ..... in qualità di ..... munito dei poteri in forza di .....

La polizza è stata emessa e sottoscritta dall'impresa garante digitalmente nel rispetto delle regole

per la formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione anche temporale dei documenti informatici, nonché in materia di generazione, apposizione e verifica della firma digitale, come stabilito dal CODICE DELL'AMMINISTRAZIONE DIGITALE (D.Lgs n. 82/2005 e succ. modd.) e dalle vigenti Regole Tecniche dettate con decreti ai sensi dell'art. 71 del CAD.

Il documento che sostanzia l'assunzione del nostro impegno di garanzia potrà essere visualizzato mediante la seguente chiave di accesso e seguendo la procedura appresso descritta:

1) connettersi via web al sito www._____.it

2) cliccare su area a Voi riservata denominata "consultazione e verifica emissione polizze digitali";

3) inserire nella "area download" il predetto codice corrispondente alla polizza da noi emessa, che potrà essere verificata nella sua validità , efficacia e sottoscrizione.

Per qualsiasi eventualità potrete rivolgerVi ai nostri Uffici Cauzioni al seguente numero di telefono:

_____

Modalità di perfezionamento della polizza fideiussoria con firma digitale

Una considerazione in premessa: sembra opportuno condividere il pensiero che le sottoscrizioni digitali di documenti informatici non possano che essere tante quante sono le sottoscrizioni analogiche richieste per il valido perfezionamento del negozio giuridico in un documento cartaceo.

La considerazione sopra svolta a maggior ragione deve applicarsi con riferimento alle modalità di perfezionamento della polizza fideiussoria con la firma digitale del contraente e dei coobbligati.

Si deve ritenere evidentemente necessaria una sottoscrizione digitale in calce:

- alle condizioni di contratto;
- alla approvazione specifica delle clausole vessatorie;
- eventuali condizioni particolari;
- presa visione di note informative;
- dichiarazioni in tema privacy.

Sotto questo ultimo specifico profilo (sottoscrizioni in tema privacy) dobbiamo segnalare l'esistenza di autorevole posizione secondo la quale le dichiarazioni da rendere con riferimento alla normativa sulla privacy debbono essere ciascuna di esse autonomamente

sottoscritta (cioè, tante dichiarazioni, tante sottoscrizioni).

Comprendiamo che quanto sopra espresso non sia di semplificazione del processo di firma e dei successivi controlli ma, specie in assenza di diversa e contraria previsione normativa, la circostanza che la sottoscrizione sia apposta in forma digitale su documento informatico, anziché analogica su documento cartaceo, non consente di attribuire, come già più volte detto, diversa e più estesa efficacia giuridica alla firma digitale.

ANNOTAZIONE GRAFICA O SEMPLICE INSERIMENTO DELLE MOTIVAZIONI

L'apposizione di più firme digitali, tante quante necessarie, può avvenire con diversi formati e diverse modalità.

Con il formato PADES è possibile inserire più firme e collocarle spazialmente all'interno di un unico file inserendo anche eventualmente una motivazione della firma digitale.

Con riferimento alle diverse corrette motivazioni occorrerà sintetizzare brevemente il motivo della firma:

- sottoscrizione della scheda di polizza contenente gli estremi della garanzia e delle condizioni generali di assicurazione;
- sottoscrizione dell'appendice n. …… (condizioni particolari o quant'altro);
- sottoscrizione specifica delle clausole vessatorie ai sensi degli artt. 1341-1342 c.c.;
- sottoscrizione della dichiarazione di ricezione della Nota informativa;
- sottoscrizione delle dichiarazioni in tema privacy;
- sottoscrizione per conoscenza dell'atto di coobbligazione.

Questa modalità di firma è indicata espressamente dalla AGID quale modalità preferibile per la sottoscrizione delle clausole vessatorie.

Con il formato CADES non è possibile né collocare spazialmente le firme all'interno del file né motivare le singole firme digitali: si tratterà dunque di creare più file ciascuno oggetto di sottoscrizione con firma digitale e "congiungerli" tra loro mediante le cosiddette firme a matrioska o più semplicemente un file .zip (operazione quanto mai opportuna per

collegare il file clausole vessatorie al file condizioni di polizza o) che dovrà a sua volta essere sottoscritto digitalmente.

OBBLIGO DI CONSERVAZIONE DEI DOCUMENTI CONTRATTUALI – POLIZZA E ALLEGATI – ARCHIVIO CARTACEO E DIGITALE

La problematica in tema di rispetto dell'obbligo di conservazione dei documenti contrattuali, con riferimento alle polizze emesse in formato digitale, si pone anche come conseguenza del fatto che tali polizze, le relative appendici ed eventuali coobbligazioni, saranno rappresentate, come ha dimostrato la pratica di questi anni, da:

- uno o più documenti informatici che contengono tra l'altro l'esemplare per il beneficiario da voi sottoscritto con firma digitale e trasmesso al contraente tramite l'agente o il broker con l'invio del relativo file e gli eventuali esemplari sottoscritta con firma digitale del contraente e dei coobbligati
- uno o più documenti cartacei anche questi sottoscritti dall'impresa e dagli altri soggetti – contraente ed eventuali coobbligati – sprovvisti di firma digitale che rappresentano la stampa di quei file ma che sono indispensabili per raccogliere la sottoscrizione autografa del contraente e degli eventuali coobbligati.

Da questo sistema complesso di formazione del contratto discendono i conseguenti oneri inerenti la conservazione ed archiviazione dei documenti (informatici ed analogici) nei quali si sostanzia la polizza.

La materia è regolata, tra l'altro, dagli artt. 8 del regolamento ISVAP numero 27 del 14/10/2008[16], regolamento modificato e integrato nel 2010 e nel 2016,

[16] Regolamento n. 27 del 14/10/2008 concernente la tenuta dei registri assicurativi di cui all'art.101 del D.Lgs. 7/9/2005 n. 209- codice delle assicurazioni private
Art. 8
(Modalità di conservazione dei documenti)
1. Le imprese conservano le proposte di assicurazione, i contratti di assicurazione, i trattati,i certificati medici, i fascicoli di sinistro, le comunicazioni delle imprese delegatarie, delle imprese cedenti e delle imprese gestionarie e, in genere, la documentazione di supporto
per le annotazioni nei registri assicurativi, per il termine di cui all'articolo 2220, comma 1, del codice civile. Le imprese conservano presso la sede legale o presso la sede secondaria nel territorio della Repubblica l'evidenza aggiornata dei luoghi di conservazione dei predetti documenti, secondo le disposizioni di cui all'articolo 5, commi 1 e 2.
2. Le imprese conservano, anche oltre il termine previsto dall'articolo 2220, comma 1, del codice civile:
a) gli originali dei contratti di assicurazione emessi e sottoscritti dal contraente e la documentazione connessa, per cinque anni dalla data in cui il contratto ha cessato di avere effetto;
b) i fascicoli di sinistro dei rami danni, per cinque anni dalla data della eliminazione senza pagamento di indennizzo o del pagamento di tutti gli importi dovuti a titolo di risarcimento e di spese dirette.
3. Le imprese possono effettuare la conservazione digitale sostitutiva dei documenti di cui al comma 1 secondo le disposizioni di cui all'articolo 2220 del codice civile, e per i contratti di assicurazione e i contratti generali di riassicurazione, nel rispetto delle regole stabilite per la conservazione dei documenti originali unici dal decreto

lasciando tuttavia inalterato il contenuto del citato art. 8 rubricato "modalità di conservazione dei documenti"; risulta inoltre regolata dall'art. 10 del regolamento IVASS n. 8 del 3/03/2015[17], e dall'art. 8 del regolamento IVASS numero 41 del 2/8/2018 rubricato "archiviazione e conservazione dei documenti"[18].

In estrema sintesi le imprese di assicurazione, debbono adempiere, oltre all'obbligo di tenuta dei registri assicurativi di cui al Codice delle Assicurazioni Private, alla conservazione, anche oltre il termine previsto dall'art. 2220 comma 1 cod. civ., degli originali dei contratti di assicurazione emessi, e sottoscritti dal contraente, e della documentazione connessa, per 5 anni da quando il contratto ha cessato ogni effetto.

Lo stesso articolo 8 del Regolamento 27/2008, nonché l'articolo 8 del Regolamento 41/2018 prevedono poi che le imprese adottino procedure interne di archiviazione e conservazione dei documenti, anche facendo ricorso a supporti informatici nel rispetto della normativa del CAD. Da quanto precede si rileva dunque la necessità di conservazione digitale dei documenti informatici nonché la possibilità di conservazione sostitutiva attraverso le dematerializzazione dei documenti cartacei.

---

legislativo 7 marzo 2005, n. 82, e dalle relative disposizioni di attuazione.
4. Le imprese adottano procedure idonee a documentare in modo certo la data di pervenimento presso l'impresa o altro soggetto legittimato a riceverli dei documenti rilevanti ai fini della tenuta dei registri assicurativi.
5. Le imprese autorizzate all'esercizio dell'attività assicurativa nei rami danni conservano, nel fascicolo di sinistro, i diari di trattazione relativi ai sinistri per i quali debba essere utilizzato il metodo dell'inventario ai sensi del Regolamento ISVAP n. 16 del 4 marzo 2008, secondo le istruzioni di cui all'allegato 1.

[17] Regolamento IVASS concernente la definizione delle misure di semplificazione delle procedure e degli adempimenti nei rapporti contrattuali tra imprese di assicurazioni, intermediari e clientela in attuazione dell'art. 22, comma 15 bis, del decreto legge 18 ottobre 2012, n. 179, convertito nella legge 17 dicembre 2012, n. 221.
Art. 10
(Conservazione dei documenti)
1. Le imprese italiane…….adottano procedure di conservazione dei documenti e delle comunicazioni previsti dai Capi II e III, ……nel rispetto delle disposizioni attuative del decreto legislativo 7 marzo 2005, n. 82 in materia di conservazione di documenti informatici.
2. Le procedure di cui al comma 1 devono consentire di mantenere evidenza della scelta operata dal contraente e garantire l'ordinata e sollecita gestione delle comunicazioni intercorse tra le parti.

[18] Regolamento IVASS recante disposizioni in materia di informativa, pubblicità e realizzazione dei prodotti assicurativi ai sensi del D.Lgs. 7/9/2005, n. 209 – codice delle assicurazioni provate
Art. 8
(Archiviazione e conservazione dei documenti)
1. L'impresa adotta procedure interne di archiviazione e conservazione dei documenti e dell'adempimento degli obblighi di consegna e di informativa di cui al presente regolamento, in coerenza con le modalità di cui al decreto legislativo 7 marzo 2005, n. 82.
2. Le procedure e le modalità di archiviazione e conservazione adottate devono essere idonee a garantire l'ordinata tenuta e gestione della documentazione di cui al comma 1.
3. Le imprese, al fine di ridurre gli oneri a carico dei contraenti, adottano modalità di gestione della documentazione idonee a evitare che venga richiesta, in fase di assunzione di nuovi contratti o gestione dei sinistri, documentazione non necessaria o di cui già dispongano,
avendola acquisita in occasione di precedenti rapporti con il medesimo contraente, e che risulti ancora in corso di validità.
4. La disposizione di cui al comma 3 si applica anche riguardo ai rapporti relativi ai contratti assicurativi collettivi.

Peraltro nella complessiva valutazione della materia non possono essere trascurati quegli aspetti di tutela della posizione giuridica della Compagnia che se non impongono, in senso assoluto, rendono comunque quanto mai opportuna la conservazione anche cartacea di quei documenti contrattuali formati in via analogica recanti la sottoscrizione autografa di quei soggetti (contraente ed eventuali coobbligati) che attraverso la sottoscrizione assumono precisi obblighi nei confronti dell'impresa garante.

Quanto meno allo stato dell'arte del processo civile risulta evidente la necessità di poter documentare in sede giudiziale e con semplicità la rituale assunzione degli obblighi da parte di contraente e coobbligati e di poter verificare l'autenticità della firma autografa, ove disconosciuta, eventualmente anche in sede di CTU (con l'esibizione dell'originale del documento cartaceo contenente la firma autografa).

Con riferimento poi alla cadenza del processo di conservazione dei documenti sembra potersi ritenere che la stessa debba essere "almeno" annuale ,che debbano essere rispettate le norme del Codice Civile, del Codice dell'Amministrazione Digitale, le relative Regole Tecniche e le norme tributarie riguardanti la corretta tenuta della contabilità.

Il processo di conservazione dei documenti informatici termina con l'apposizione di un riferimento temporale opponibile ai terzi sul pacchetto di archiviazione.

CLAUSOLE VESSATORIE NEI CONTRATTI ON-LINE

La problematica circa le formalità da osservare per la specifica approvazione, a norma di quanto disposto dall'**art. 1341 secondo comma cod. civ.**, delle clausole vessatorie nei contratti on line è sorta ed è stata affrontata da dottrina e giurisprudenza, peraltro con contrastanti visioni e conclusioni, con riferimento al commercio elettronico (cioè quelle ipotesi commerciali di offerta al pubblico e perfezionamento del contratto a distanza sul sito web dell'offerente) e non piuttosto con riferimento allo specifico settore delle polizze cauzionali in formato digitale.

Va peraltro considerato che la questione circa la possibilità di ricondurre l'emissione delle polizze alla fattispecie di contratti con collocamento a distanza è stata forse sottovalutata, anche nel sistema di emissione in formato analogico/cartaceo.

Ed infatti dalla lettura della disciplina dettata dall'ISVAP , in particolare con il **Regolamento n. 34 del 19/3/2010** contenente "Disposizioni in materia di promozione e collocamento a distanza di contratti di assicurazione", si evidenzia che per ***"contratto di assicurazione a distanza***" si intende (così l'art. 2 lettera d) ***"il contratto di assicurazione sulla vita o contro i danni stipulato tra un'impresa di assicurazione e un contraente nell'ambito di un sistema di vendita a distanza organizzato dall'impresa, che per tale contratto impiega esclusivamente una o più tecniche di comunicazione a distanza fino alla conclusione del contratto, compresa la conclusione del contratto stesso".***

Lo stesso Regolamento n. 34 del 2010 precisa (all'art. 2 lett o) che per ***"tecnica di comunicazione a distanza"*** si intende ***"qualunque mezzo che, senza la presenza fisica e simultanea dell'impresa e del contraente, possa impiegarsi per la conclusione del contratto tra le due parti".***

Ancora all'art.3 del citato Regolamento se ne ribadisce l'applicazione ai contratti di assicurazione contro i danni per la copertura di rischi ubicati nel territorio della Repubblica italiana, ed all'art.11 (nel testo come sostituito dall'art.13 del **Regolamento IVASS n. 8 del 3 marzo 2015**) si precisa che ***"la polizza può essere formata come***

documento informatico sottoscritto con firma elettronica avanzata, con firma elettronica qualificata o con firma digitale, nel rispetto delle disposizioni normative vigenti in materia"

Così delineata la fattispecie, sembra potersi concludere che il contratto di assicurazione possa intendersi collocato a distanza anche nell'ipotesi in cui la polizza in formato cartaceo venga inoltrata, per posta corriere, al contraente e da questo ritornata sottoscritta all'impresa con lo stesso mezzo, e che in definitiva il contratto si concluda "senza la simultanea presenza fisica delle parti".

In questa accezione non pare potersi escludere che la polizza fideiussoria in formato digitale, emessa dalla Compagnia e trasmessa in via informatica al Contraente, che ne curerà la trasmissione o la consegna al Beneficiario e ritornerà all'impresa garante, in via informatica o per posta, la copia da lui sottoscritta (rispettivamente con firma digitale o autografa), senza dunque quella "simultanea presenza fisica delle parti", sia riconducibile alla fattispecie di contratto concluso a distanza, e per l'ipotesi in cui tutta l'operazione avvenga in via informatica all'ipotesi di contratto on line concluso a distanza.

Non potendosi escludere che un qualche settore o tipologia dei contratti assicurativi cauzionali possa attuarsi attraverso una mera contrattazione on line a distanza, può essere interessante esaminare, sia pure in sintesi, le considerazioni della dottrina e della in verità ancora scarsissima giurisprudenza in tema di efficace approvazione delle clausole vessatorie.

Il nostro ordinamento giuridico si basa sul principio della libertà della forma per la conclusione dei contratti, con le eccezioni rappresentate dai casi in cui è espressamente richiesta la forma scritta, che sono quelli contemplati all'**art. 1350 cod. civ.** (ad esempio, i contratti di trasferimento della proprietà e costituzione di diritti reali su beni immobili, di locazione di immobili per durata superiore a nove anni). **L'ultimo comma dell'art. 1350**, come norma di chiusura, prevede la forma scritta per ***"gli altri atti specialmente indicati dalla legge"***

La contrattualistica on line, ed in particolare l'e-commerce attuato attraverso il cd. contratto *"point and click"* (cioè quel contratto concluso con l'accesso al sito web

dell'offerente ed il perfezionamento da parte del contraente con la manifestazione del consenso attraverso la compilazione dei campi elettronici proposti e la spunta sul pulsante negoziale virtuale) è riconosciuta come pienamente valida.

Il commercio elettronico non pare peraltro esonerato dal rispetto delle previsioni in tema di specifica approvazione delle clausole vessatorie, e la giurisprudenza maggioritaria non pare, almeno allo stato, orientata nel senso di riconoscere idoneità al sistema del "point and click" al fine di tale adeguata approvazione.

Nella prassi si è diffusa la previsione a tal fine di un "doppio click", ma la validità giuridica di una tale soluzione è discutibile e controversa.

Consolidato orientamento della giurisprudenza è quello di qualificare la specifica approvazione scritta ai sensi dell'art. 1341 cod. civ. come requisito di forma scritta *ad substantiam* in base alla previsione del richiamato ultimo comma dell'art. 1350 cod. civ.

Va poi considerato che l'art. 21 comma 2 bis del CAD prevede, nell'utilizzo dello strumento informatico, per i casi in cui sia richiesta la forma scritta, la necessità a pena di nullità della sottoscrizione con firma elettronica qualificata o con firma digitale.

Dispone infatti **l'art. 21 comma 2 bis del CAD**:

"Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350 primo comma numeri da 1 a 12 del codice civile, se fatte con strumento informatico, sono sottoscritte a pena di nullità con firma elettronica qualificata o con firma digitale"

"Gli atti di cui all'art. 1350 numero 13 del codice 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 1 bis primo periodo"

Tali considerazioni hanno condotto la prevalente dottrina a convergere circa la necessità della firma elettronica avanzata, qualificata o digitale, per la approvazione delle clausole vessatorie.

La giurisprudenza, come detto assai scarna, ha assunto una posizione analoga e restrittiva, ritenendo efficaci le clausole vessatorie in un contratto on line solo attraverso la loro specifica approvazione con la firma digitale. (Così il Tribunale di Catanzaro in una decisione peraltro risalente al 2012: *"Nei contratti telematici a forma libera il contratto si perfeziona mediante il tasto negoziale virtuale, ma le clausole vessatorie saranno efficaci e vincolanti solo se specificamente approvate con firma digitale").*

Un passo in avanti nel senso di consentire l'estensione della contrattualistica on line con l'utilizzo del metodo del "point and click", consentendo peraltro l'efficace inserimento di clausole vessatorie, può individuarsi, a parere di taluna dottrina, nella nuova formulazione (apportata con le modifiche al CAD del 2016) degli artt. 20 e 21 CAD, ove in qualche modo si prevede che soddisfa il requisito della forma scritta anche il documento informatico "formato con le ulteriori modalità ivi indicate" al quale si apposta una firma elettronica, anche oltre quello sottoscritto con firma elettronica qualificata, avanzata o digitale.

Secondo una interpretazione evolutiva, dunque, anche la modalità del "point and click" (o meglio del doppio "point and click") potrebbe essere considerata alla stregua di firma elettronica (debole) idonea a soddisfare la forma scritta, e così a consentire la valida approvazione delle clausole vessatorie.

In questo panorama in divenire si pone l'intervento della Cassazione a Sezioni Unite che con ordinanza del 19 settembre 2017 si è pronunciata circa la validità della clausola vessatoria di deroga pattizia alle norme in tema di competenza per territorio dell'autorità giudiziaria, contenuta nelle condizioni generali di un contratto stipulato a distanza e in forma telematica.

La Cassazione, richiamando un precedente della Corte di Giustizia UE (circa la ammissibilità di sottoscrizione mediante "click" delle condizioni generali di un contratto di vendita contenenti clausola attributiva della competenza giurisdizionale) ha in sostanza condiviso il principio espresso dall'art. 23 del Regolamento Bruxelles[19] per cui *"qualsiasi comunicazione elettronica che permetta una registrazione durevole della clausola deve*

[19] il Regolamento del Consiglio della UE n. 44/2001 del 22/12/2000 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale.

essere considerata comprendere la forma scritta".

Quanto deciso dalla Corte di Giustizia Europea e dalla Cassazione non può peraltro assurgere a regola di carattere generale, posto che per espressa ammissione della stessa Corte della UE le disposizioni del Regolamento Bruxelles hanno carattere speciale e non possono essere interpretate estensivamente.

In prospettiva sarebbe opportuno che il legislatore ripensasse l'intera disciplina delle clausole vessatorie nei contratti on line. Sino a tale momento non pare prudente trarre conclusioni affrettate, che potrebbero condurre a decisioni dei giudici contrarie al riconoscimento della efficacia delle clausole vessatorie non approvate nelle forme sicure, e dunque, in un contratto in formato digitale, attraverso la loro specifica sottoscrizione con firma digitale.

ALCUNI CENNI E ARRESTI GIURISPRUDENZIALI CON RIFERIMENTO ALLA PRODUZIONE DELLA POLIZZA PROVVISORIA CON FIRMA DIGITALE

Qualora, anche a prescindere da specifiche previsioni contenute nel bando di gara, l'impresa concorrente decida di presentare una garanzia provvisoria in formato digitale, e dunque una polizza provvisoria redatta su supporto informatico e con firma digitale, restando irrilevante che nel bando si preveda espressamente l'obbligo di produrre la garanzia provvisoria in originale o in un documento autenticato, resta comunque fermo che essa è tenuta all'osservanza di tutte le regole che stanno a presidio di tale modalità e che trovano disciplina nel CAD.

E nel rispetto di tali regole non può prescindersi da quella che consente di scegliere tra due opzioni fissate direttamente dalla legge:

a) la produzione del documento informatico, registrato dunque su supporto informatico (art. 20 CAD) nel rispetto delle regole tecniche per la formazione, conservazione, trasmissione stabilite con le Linee Guida;

b) la produzione di copia su supporto cartaceo del documento informatico, quantunque sottoscritto con firma digitale, che sostituisce ad ogni effetto l'originale informatico ma solo se la sua conformità all'originale in tutte le sue componenti è attestata da pubblico ufficiale a ciò autorizzato (art. 23 CAD).

Dispone infatti **l'art. 23 comma 1 del CAD**:

"***le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato***".

In tale seconda ipotesi – produzione di copia su supporto cartaceo del documento cartaceo sottoscritto con firma digitale – la giurisprudenza amministrativa ha ritenuto non idonea la presentazione di semplice copia cartacea della polizza generata in formato digitale sprovvista di autenticazione, e neppure surrogabile con altre modalità ivi compresa la apposizione di firma autografa (del rappresentante della Compagnia e/o del contraente) sul documento cartaceo che costituisce copia dell'originale informatico.

L'orientamento almeno in un primo momento maggioritario della giustizia amministrativa si è espresso dunque nel senso di affermare la necessità del rispetto, a pena di esclusione, delle formalità degli artt. 20 e 23 del CAD (Così: TAR Sicilia 12/4/2010, 5/7/2012; TAR Lazio 20/12/2012; Consiglio di Stato, Sez. VI, 29/1/2015).[20]

La giurisprudenza amministrativa ha ancora affermato il principio per cui la mancanza della attestazione di conformità all'originale da parte di pubblico ufficiale a ciò autorizzato e conseguentemente "la non conformità ai presupposti richiesti dalla legge non può essere superata dalla affermazione di un potere-dovere della Commissione di gara di riscontrare dall'esterno l'autenticità della polizza o della firma digitale ricorrendo a controlli complessi" (Così: TAR Calabria 6/6/2012).

Non mancano, come sempre accade, pronunce di segno contrario (TAR Toscana 18/3/2015; Consiglio di Stato, Sez. V, 23/3/2018)[21].

Ancora la giurisprudenza amministrativa ha osservato che qualora il bando preveda la presentazione di una copia autenticata della polizza assicurativa (nella specie polizza di assicurazione della responsabilità civile) non può ritenersi sufficiente una copia semplice corredata di dichiarazione sostitutiva di atto di notorietà contenente "attestazione di autenticità" del documento, giudicando essere concessa dalla legge la possibilità di fare ricorso alla dichiarazione sostitutiva dell'atto di notorietà purché si tratti di atti o documenti conservati o rilasciati da una pubblica amministrazione, e non anche di un documento contrattuale con soggetto privato terzo, quale è la polizza assicurativa.

[20] Il Consiglio di Stato sezione VI nella decisione del 29/1/2015, giudicando in tema di cauzione provvisoria, ha statuito che la produzione da parte dell'impresa concorrente di una semplice copia cartacea della polizza fideiussoria, mancante dunque della attestazione di conformità all'originale e della sottoscrizione dell'agente della Compagnia, debba valutarsi alla stregua di documento privo di validità e non comprovante la costituzione della garanzia.
Il Consiglio di Stato non ha dunque ritenuto sufficiente la allegazione di un documento cartaceo riproduttivo del documento informatico seppure comprensivo degli elementi atti a reperire il documento originale, in particolare facendo richiamo al disciplinare di gara ove si prevedeva a pena di esclusione la produzione di documento comprovante la costituzione di garanzia ed osservando ancora la mancanza del rispetto della piena garanzia per l'Amministrazione, soddisfatta soltanto con la certezza della provenienza della fideiussione.

[21] Il Consiglio di Stato sezione V, nella decisione del 23/3/2018, in termini in qualche modo non conformi al principio dettato nella sentenza della sezione VI del gennaio 2015, ha affermato:
- che la mancata presentazione della cauzione provvisoria ovvero la presentazione di una cauzione provvisoria invalida non costituisce causa di esclusione dalla procedura di aggiudicazione ma irregolarità sanabile attraverso l'istituto del soccorso istruttorio (in senso conforme: Consiglio di Stato 23/11/2017 e 27/10/2016);
- che la presentazione di una cauzione provvisoria falsa costituisce fattispecie diversa e non assimilabile a quella della cauzione provvisoria mancante, incompleta o irregolare, e che dunque alla presentazione a corredo dell'offerta di documentazione falsa, tra cui evidentemente anche la cauzione provvisoria, consegue l'esclusione dell'impresa.

In altre parole ha ritenuto il giudice amministrativo che se il bando espressamente prevede la presentazione della polizza in originale o in copia autentica, tale previsione vale ad escludere la possibilità di presentare una copia semplice corredata da attestazione di autenticità, nella forma di dichiarazione sostitutiva di atto di notorietà.

La ragione di tale assunto è stata rinvenuta nella "*importanza determinante, ai fini dell'esclusione, delle prescrizioni formali del bando di gara, anche per il valore sostanziale dell'adempimento in questione, trattandosi di documentare l'esistenza della copertura assicurativa che viene a toccare interessi vitali di soggetti estranei potenzialmente esposti a subire danni in seguito all'esecuzione del servizio*".

Sempre in argomento sono ancora interessanti due Delibere dell'ANAC.
La prima Delibera del 17/1/2018 ha ritenuto legittima la richiesta di integrazione della documentazione di gara in sede di soccorso istruttorio da parte della stazione appaltante, con il pagamento di sanzione pecuniaria, per la regolarizzazione del formato della polizza fideiussoria non conforme alle disposizioni della *lex specialis* (ovvero il disciplinare di gara che impone la stretta osservanza delle relative prescrizioni anche alla stessa amministrazione) laddove il bando prevedeva la presentazione della polizza in originale con firma autenticata o in copia autenticata, mentre il concorrente aveva prodotto copia analogica, cioè cartacea, della polizza provvisoria redatta e firmata dalla Compagnia garante in formato digitale (più precisamente si trattava di polizza sottoscritta dall'agente sul supporto informatico con firma digitale e dal contraente sul supporto cartaceo con firma autografa e recante nel frontespizio il codice di controllo per la verifica accedendo ad apposito link del file originale della polizza e della firma digitale).

La seconda Delibera ANAC n. 276 del 3/4/2019 ha chiarito che è illegittima l'esclusione dalla gara del concorrente che, anziché presentare la documentazione di gara sottoscritta come richiesto in ogni pagina, ha inviato il documento in forma di file in formato PDF e sottoscritto digitalmente.
In particolare il concorrente alla gara di appalto aveva fatto presente all'ANAC di essere stato escluso all'esito delle integrazioni documentali presentate in sede di soccorso istruttorio, per aver trasmesso la copia del Protocollo di Integrità senza rispettare le disposizioni del disciplinare di gara, che prevedeva che il documento fosse "debitamente

sottoscritto e timbrato su ogni pagina dal legale rappresentante", mentre il documento era stato inviato in formato PDF sottoscritto digitalmente, da ritenersi equivalente alla firma autografa.

L'ANAC ha ricordato la giurisprudenza del TAR per la quale la firma digitale equivale alla firma autografa apposta su un documento cartaceo e che la sottoscrizione del relativo file ".p7m", regolarmente effettuata secondo lo standard CAdES, è da ritenersi pienamente idonea ad assolvere alla funzione di attestare la provenienza dell'atto in capo al suo autore.

Ha dunque considerato che: (i) nel caso di specie la procedura è stata svolta sulla piattaforma telematica MePA; (ii) ai sensi dell'art. 24, comma 2 CAD, l'apposizione della firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente; (iii) nel rispetto del principio della tassatività delle cause di esclusione, sancito dalla normativa del Codice dei contratti, nonché dei princìpi della massima partecipazione, di non aggravamento del procedimento e di proporzionalità, non è legittima la richiesta della lex specialis di gara che preveda - pena l'esclusione - la sottoscrizione per esteso di ogni pagina dell'offerta.

Per tale motivo, ANAC ha ritenuto illegittima l'esclusione del concorrente dalla procedura di gara.

POLIZZE DIGITALI SENZA EFFETTO

Il problema relativo alla definitiva "eliminazione" delle polizze stornate dopo l'emissione, in quanto senza effetto perché ad esempio non perfezionate o non consegnate al beneficiario, così da scongiurare l'eventualità che quei contratti ed i relativi rischi possano invece avere un seguito, è problema che in realtà non si pone solo ora come conseguenza della emissione in via informatica e con firma digitale, ma si poneva già in passato con l'emissione in forma cartacea.

La differenza sta nel fatto che in tale ultima ipotesi era possibile conseguire in restituzione tutti gli esemplari di polizza, ed in particolare l'originale per il beneficiario (escludendo l'ipotesi di emissione fraudolenta), mentre nel caso delle polizze digitali non si può escludere che il cliente utilizzi una ulteriore stampa cartacea della polizza o ancor peggio abbia conservato il file sottoscritto digitalmente e ricevuto in via informatica e di tale file faccia uso con il beneficiario.

Quello che può e deve fare la Compagnia in caso di annullamento senza effetto della polizza digitale è, in buona sostanza, comportamento nel risultato non così dissimile da quello per le polizze in formato analogico: acquisire, in luogo della restituzione di tutti gli esemplari cartacei, una autocertificazione attestante la mancata consegna o il mancato utilizzo del file, e conseguentemente procedere all'annullamento della polizza nel sistema informatico.

Nel caso di polizze digitali l'operazione di storno a sistema informatico è di evidente maggior rilievo considerato che proprio in questa ipotesi il beneficiario potrebbe e dovrebbe verificare, eventualmente attraverso il codice/chiave crittografica indicata in polizza, la rituale emissione e sottoscrizione digitale della polizza.

Resta per contro evidente che in caso di utilizzo illecito del contratto senza effetto si sarebbe comunque creato nel beneficiario un legittimo affidamento.
È dunque importante seguire con attenzione la procedura di storno anche attraverso la dichiarazione (del cliente o dell'agente) in merito al mancato seguito della polizza.

In questo senso sono già state ipotizzate e predisposte da diverse Compagnie

dichiarazioni di autocertificazione, che possono essere modulate in base al momento nel quale si dichiara che la polizza deve ritenersi priva di effetto.

Esaminiamo le diverse ipotesi:

a) File Polizza inviato all'Agente e non al Contraente

Indipendentemente dal fatto che la polizza sia stata emessa dalla Direzione e trasmessa all'Agenzia o emessa direttamente da quest'ultima, nell'ipotesi che la stessa resti priva di effetto prima che sia consegnata o inviata telematicamente al cliente, in questo caso alla autocertificazione deve provvedere l'Agente, ovviamente nella persona del soggetto che ha i poteri di firma per l'Agenzia.

b) File Polizza inviato al Contraente

Analoghe le premesse, in questo caso alla autocertificazione deve provvedere il cliente ed in questo caso sembra che sia onere dell'Agenzia partecipare alla operazione di storno con la trasmissione dell'autocertificazione del Cliente e con la propria contestuale dichiarazione (alla Direzione) circa il mancato incasso del premio o l'intervenuta restituzione dello stesso al Contraente.

c) File Polizza inviato dall'Agente ad un intermediario

Quest'ipotesi di scinde in due casi:

c1) File consegnato al cliente: autocertificazione del Cliente e analoghe dichiarazioni di Broker ed Agente, sempre ed ovviamente rilasciate dal soggetto che ha i poteri di firma per l'Agenzia o per l'intermediario.

c2) File non ancora consegnato al Cliente: autocertificazione del Broker e dichiarazione dell'Agente.

È forse superfluo osservare che se tali dichiarazioni appaiono sicuramente opportune, per non dire necessarie, meno significativa pare un'eventuale previsione, da alcune Compagnie ipotizzata, circa il fatto che resta comunque fermo il diritto di rivalsa in caso di utilizzo della polizza dichiarata priva di effetto: in questo caso infatti ci si troverebbe, specie sussistendo l'autocertificazione, in ipotesi di utilizzo illecito (e fraudolento) del documento contrattuale, per cui appare in qualche modo contraddittorio prevedere l'esistenza del diritto di regresso del fideiussore con riferimento ad una polizza che gli è stata prospettata come priva di effetto.