Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

DOCUMENTO

“Breve Guida sulle Firme Elettroniche”

Roma, 18 gennaio 2018

A cura del Gruppo di Lavoro Firma Digitale - Area Innovazione e organizzazione degli Studi Professionali

CONSIGLIERE DELEGATO
Maurizio Giuseppe Grosso

COORDINATORE
Fabrizio Scossa Lodovico

COMPONENTI
Salvatore Crapanzano
Giuliano Ravasio
Gaia Campione Taddei

RICERCATORE
Angela Fichera

Con la collaborazione del
Circolo Giuristi Telematici

Indice

Premessa

L'ampio processo di innovazione e digitalizzazione dei processi che va affermandosi con crescente velocità, impatta inevitabilmente anche sulle modalità di svolgimento dell'attività professionale dei commercialisti italiani. Al professionista viene richiesto l'utilizzo quotidiano di strumenti informatici sempre più complessi. Conoscerli in maniera approfondita è la precondizione per un loro uso più consapevole e, dunque, più fruttuoso.

Uno di questi strumenti è la firma elettronica nelle sue varie accezioni: l'esperienza italiana dell'utilizzo della firma digitale ha generato notevoli risultati nella gestione informatica di rapporti nei confronti di enti, quali CCIAA e Agenzia delle Entrate; risultati positivi si sono registrati anche con riferimento all'utilizzo di questa modalità di sottoscrizione nella cessione di quote di srl.

Per questa ragione, come già avvenuto in precedenza con il "Vademecum sull'utilizzo della PEC", si è ritenuta utile la predisposizione di un documento relativo alle firme elettroniche. L'elaborato è di tipo divulgativo e non scientifico e vuole fornire al collega sintetiche informazioni sulle diverse tipologie di firme presenti, indicazioni sul corretto utilizzo delle stesse ed efficacia probatoria; in chiusura, è stato inserito un elenco riportante le best practices suggerite sull'argomento. Segnalo inoltre che nella stesura finale l'elaborato ha tenuto in considerazione le concomitanti modifiche ed integrazioni intervenute sull'articolato del CAD, introdotte dal D. Lgs. 13 dicembre 2017, n. 217 cd. "decreto correttivo" ed entrate in vigore il 27 gennaio 2018, pur non potendone valutare, per ovvie ragioni di tempo, l'impatto reale nei casi concreti di utilizzo da parte del professionista.

Ringrazio i colleghi componenti il Gruppo di Lavoro costituito dal CNDCEC per la predisposizione del presente elaborato, gli avvocati Giorgio Battaglini e Paolo Lessio che, in qualità di Presidente e Tesoriere del Circolo dei Giuristi Telematici, hanno fornito importanti e autorevoli contributi in tema di efficacia probatoria e Angela Fichera per il notevole apporto fornito.

Come indicato in premessa, i commercialisti hanno sempre avuto uno stretto rapporto con la tecnologia informatica e, quindi, saranno pronti alla sfida per utilizzare al meglio anche eventuali nuovi impieghi degli attuali o futuri dispositivi di firma che tendano alla certezza nei rapporti tra cittadini e PA, consentano una gestione più agevole e strutturata dei dati posseduti dai soggetti riceventi migliorandone l'efficienza, e garantiscano la facilità di reperimento degli stessi.

Il Consigliere CNDCEC
delegato per l'Area Innovazione e Organizzazione degli Studi Professionali
Maurizio Giuseppe Grosso

1. Le Firme Elettroniche

1.1. 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 sulla nozione di documento informatico e 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 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.

1.2. 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".* 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.

1.3. 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.

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.

1.3.1. La Firma Grafometrica

Una 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.

1.3.2. 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).

1.4. Cenni sul Sigillo Elettronico

Il **Sigillo Elettronico** è uno strumento introdotto dal Regolamento eIDAS che, all'art. 3, n. 25, lo definisce come un insieme di "*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*". A differenza della firma elettronica, il sigillo consente di provare l'emissione di un documento elettronico da parte di una determinata persona giuridica, fornendo la certezza dell'origine e dell'integrità del documento stesso ma, naturalmente, non sostituisce la firma del rappresentante legale.
Anche i sigilli elettronici, come le firme, possono essere anche avanzati o qualificati.
Il **Sigillo Elettronico Avanzato** soddisfa i seguenti requisiti: 1) è connesso esclusivamente al creatore del sigillo; 2) è idoneo ad identificare il creatore; 3) è prodotto mediante dati per la creazione di un sigillo elettronico di esclusivo controllo del titolare; 4) è collegato ai dati a cui è stato apposto per garantirne l'originalità e l'integrità.
Il **Sigillo Elettronico Qualificato** è un sigillo elettronico avanzato prodotto con dispositivi dotati di certificato qualificato, per il quale ai sensi dell'art. 35, comma 2 del Regolamento sussiste una "*presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato*".
Alla luce di tali considerazioni, emerge come il sigillo elettronico sia uno strumento idoneo ad assicurare autenticità ed integrità dei dati trasmessi, con interessanti ed importanti risvolti in ambito applicativo: ad esempio con riguardo alla trasmissione di dati relativi ai corrispettivi dei registratori di cassa o alla fatturazione elettronica delle persone giuridiche (in questo caso l'uso del sigillo apposto dal servizio dell'Agenzia delle Entrate è un'alternativa per coloro che non sono dotati di firma digitale e garantisce l'immodificabilità delle fatture elettroniche se trasmesse tramite SDI, o inviate al servizio di conservazione messo a disposizione dall'Agenzia delle Entrate).

2. La Firma Digitale

La Firma Digitale è l'unica espressamente definita all'interno del CAD (art. 1, comma 1, lett. s); è un tipo particolare di firma qualificata "*basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*". In altre parole, 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 sotto forma di smart card (da collegare ad un apposito lettore) o di chiavetta USB ed è necessario possedere un software di firma rilasciato da un'Autorità di certificazione. Se il Certificatore è accreditato eIDAS (i servizi certificati eIDAS sono solitamente contrassegnati con il logo del lucchetto blu con le stelle degli stati europei), i suoi servizi rispettano gli standard di interoperabilità fissati in ambito comunitario.

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

Il documento sottoscritto con firma digitale 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 riconosciuto come valido in fase di verifica da parte della CA 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 disconoscere il documento sottoscritto con la propria firma digitale

2.1. Acquisto del dispositivo di firma

Per dotarsi di firma digitale è necessario rivolgersi ad un R.A.O. (Registration Authority Office): un RAO è un certificatore accreditato AGID ovvero un soggetto (società di servizi, ordine professionale…) autorizzato al rilascio, previa identificazione, del dispositivo smart card o token USB per la firma digitale. Per l'acquirente è sufficiente aver compiuto 18 anni, possedere il codice fiscale e un documento di identità in corso di validità.

Completato il processo di verifica dell'identità del richiedente, il RAO rilascia un PIN identificativo generato mediante doppie chiavi asimmetriche: quella privata, che rimane segreta, e quella pubblica, da fornire ai destinatari dei documenti

sottoscritti digitalmente, per verificare l'autenticità della firma utilizzata e consegna il supporto scelto (smart card o chiavetta USB).

2.2. Utilizzo della firma digitale

Per applicare la firma digitale occorre utilizzare il software messo a disposizione dal soggetto certificatore e le operazioni da compiersi, pur potendo variare lievemente in base all'applicazione utilizzata, sono sostanzialmente le seguenti:

1) si seleziona il file da sottoscrivere utilizzando il software di firma e si inserisce la smart card nel lettore o la chiavetta nella porta USB;
2) si seleziona il certificato di firma da utilizzare, qualora fossero presenti nel dispositivo più di un certificato di sottoscrizione;
3) si inserisce il codice PIN e si seleziona la cartella in cui salvare il documento sottoscritto, così come richiesto dal software;
4) si sceglie la tipologia di busta crittografica (PAdES, CAdES, XAdES rispettivamente caratterizzate dalle estensioni pdf per PAdES, p7m per CAdES e .xml per XAdES) tra quelle ottenibili in relazione al formato del file da firmare (es. PDF, XML, o altri);
5) nel caso di firma PAdES, è possibile selezionare la firma invisibile o firma grafica, che è utilizzabile per firmare PDF in precisi punti del documento (ad esempio, per la sottoscrizione delle clausole vessatorie);
6) infine, occorre procedere alla visualizzazione e confermare la lettura del documento, premendo sul tasto "Firma".

Il documento ottenuto sarà "imbustato" nel formato precedentemente selezionato e la busta conterrà al suo interno il documento originario, i dati dell'ente certificatore, il certificato qualificato del sottoscrittore e la firma digitale (calcolata sull'impronta hash[1] del documento).

2.3. 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. Per utilizzare tale funzione può essere utilizzato il software distribuito dal proprio fornitore di firma digitale, anche se alcune funzioni evolute sono disponibili solo con le versioni a pagamento dello stesso.

[1] L'impronta hash è una sequenza di lettere e cifre, solitamente 64 caratteri, ottenuta applicando un algoritmo alla sequenza di bit che formano il file. La sua principale caratteristica è quella di non permettere di risalire al testo originario o al contenuto del file. L'impronta può essere calcolata su qualsiasi contenuto digitale (testo, immagine, filmato, ecc.).

3. Le buste telematiche – 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?

3.1. 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 grafiche 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 sempre il formato PAdES BES.

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).

3.2 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.

3.3 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.

4. 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, così come modificata dalla Determinazione Commissariale 69/2010, n.69; 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 il sottoscrittore successivo al primo, firma solo i 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 di 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 bilancio o della relazione al bilancio da parte dei vari componenti del consiglio di amministrazione, oppure la firma della relazione del collegio sindacale da parte dei tre sindaci, o ancora 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 da un altro sottoscrittore col proprio software di firma. 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.

5. Le firme digitali locali e remote

5.1. 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[2].

All'interno dei dispositivi per la firma digitale, oltre il certificato di firma locale, possono essere inseriti altri servizi quali **il certificato CNS (Carta Nazionale dei Servizi)** utilizzabile per accedere ai servizi online della Pubblica Amministrazione su tutto il territorio nazionale, ai servizi telematici dell'Agenzia delle Entrate e, previa richiesta di attivazione, al punto d'accesso del Processo Tributario Telematico, **il certificato di ruolo, i certificati qualificati di firma digitale (FD) o firma elettronica qualificata (FEQ),** che sono solitamente utilizzati per indicare l'appartenenza del possessore ad una specifica organizzazione.

5.2. 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] 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"

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).

5.2.1. 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.

6. 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.

7. 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[3].

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

[3] 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.

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"[4].

8. Timbro digitale

Il timbro digitale consente di mantenere valida la catena del valore legale di un documento informatico firmato digitalmente quando il documento viene stampato su carta.

In pratica, si tratta dell'apposizione di un codice a barre/contrassegno (generato sulla base dei criteri definiti con linee guida dell'AgID) sulla copia cartacea del documento, con lo scopo di consentire la verifica della conformità al documento informatico da cui ha origine.

Utilizzando uno scanner e l'apposito software gratuito, generalmente reso disponibile sul sito internet del soggetto emittente (solitamente una PA), è possibile riacquisire dal timbro il documento informatico sottoscritto con firma digitale e salvarne copia informatica (p7m).

È una soluzione particolarmente indicata per le pubbliche amministrazioni: esempi concreti sono il DURC e la Gazzetta Ufficiale, che recano nella parte bassa del foglio il codice bidimensionale.

9. Documento informatico - valore legale

9.1. Documento informatico privo di sottoscrizione e sottoscritto con firma elettronica semplice

L'art. 20 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 (si vedrà però in seguito che, con riferimento alla disciplina del regolamento eIDAS vi è anche una scala di valore tra documento non sottoscritto e documento sottoscritto con firma semplice).

Nella pratica e in assenza di firma elettronica, il formato più comunemente accettato in giudizio e ben accolto anche dalla Pubblica Amministrazione è il formato Pdf/A[6], che garantisce facilità di visualizzazione, anche a distanza di tempo e utilizzando software diversi.

---

[4] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche

[5] 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.

[6] 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.*)

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

L'articolo 20 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*". Come si può vedere, il legislatore considera diversamente il valore giuridico e probatorio 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 (art. 21, comma 2). 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.

10. 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.

10.1. 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.

10.2. 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.

10.3. 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 "*Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi e' 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 prodotto in giudizio e non venga disconosciuto farà piena prova fino a querela di falso.

In caso di disconoscimento della sottoscrizione apposta con firma elettronica qualificata o digitale però il regime di c.d. verificazione (che in relazione ai documenti cartacei obbliga il soggetto che ha prodotto il documento sottoscritto a dare corso ad un vero e proprio giudizio tendenzialmente basato su una CTU calligrafica), subisce una inversione poiché è lo stesso soggetto che contesta l'apposizione della firma digitale a dover dare prova del fatto che la firma in questione non è stata da sé apposta: infatti Il comma 1-ter del medesimo articolo 20 del CAD dispone che *"L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che* ***questi*** *dia prova contraria".*

In sostanza, a differenza di quanto normalmente accade con i documenti cartacei, il documento firmato digitalmente può essere certamente contestato da chi appare il sottoscrittore apparente (cioè il titolare del certificato di firma che garantisce la chiave di sottoscrizione) a condizione però che contestualmente venga data dallo stesso sottoscrittore apparente la dimostrazione che la firma in questione non è stata da sé apposta (tramite, ad esempio, prove testimoniali o altro).

Sul punto però bisogna tenere presente, e la circostanza è certamente assai rilevante, che per disposizione normativa *"Il titolare del certificato di firma e' 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; e' altresi' tenuto ad utilizzare personalmente il dispositivo di firma".*

Ne consegue che nel caso in cui il soggetto titolare della firma riesca a dimostrare di non aver utilizzato personalmente il dispositivo di firma in questione, starà verosimilmente dimostrando anche di non aver garantito con tutta la diligenza necessaria la custodia dello stesso, diventando dunque responsabile dell'atto sottoscritto non più in ragione della sottoscrizione, bensì per negligenza nella corretta gestione del dispositivo di firma.

Il corollario di tale ricostruzione giuridica consiste, in sostanza, nell'impossibilità di cedere a terzi (salvo assumersene la relativa responsabilità) i meccanismi (fisici o remoti) legati alla propria firma digitale.

10.4. La validità temporale delle firme digitali: profili probatori

Come noto, tutti i certificati legati alle firme digitali sono generalmente dotati di una scadenza (di norma durano tre anni).

La necessaria validità temporale limitata delle firme deriva dal fatto che gli algoritmi di firma tendono, con il passare del tempo e l'aumento della potenza di calcolo degli strumenti hardware, tendono a diventare vulnerabili, cosicché sorge l'esigenza di "far scadere" periodicamente la validità delle firme, affinché vengano sostituite con firme basate su algoritmi e protocolli più sicuri.

Sul punto è quindi bene tenere presente che la scadenza delle firme costituisce elemento molto sensibile, considerato che il CAD prevede che *"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"* e ancora 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".*

La conseguenza maggiormente rilevante che dipende dalle valutazioni sopra indicate, consiste essenzialmente nel fatto che qualunque documento firmato digitalmente, a seguito di scadenza della relativa sottoscrizione perderà la propria efficacia, salvo che non sia versato in un sistema di conservazione a norma.

BEST PRACTICES

1) Chi intende richiedere il rilascio di un certificato di firma digitale, deve preliminarmente:
   - valutare le caratteristiche necessarie del certificato di firma, ad esempio se con o senza "attestazione di ruolo". L'inserimento di una attestazione di ruolo può essere importante per le firme degli iscritti negli Albi professionali, ma può essere importante indicare una qualifica anche all'interno di una struttura decisionale aziendale (esempio "responsabile ufficio acquisti ZZZ spa"). Il certificato di ruolo deve essere revocato tempestivamente in caso di cessazione dello stesso.
   - valutare l'opportunità di possedere più di una firma digitale per l'utilizzo in ambiti diversi;
   - valutare quale modalità di utilizzo del certificato di firma risponde alle proprie necessità:
     - ✓ firma con dispositivo su supporto;
     - ✓ firma remota con dispositivo di OTP su chiavetta, oppure su smartphone che genera un PIN monouso simile a quello solitamente richiesto dai circuiti bancari;
     - ✓ firma singola (una firma su ogni documento da sottoscrivere), oppure firma massiva che consente di firmare una pluralità di documenti con una sola operazione.

2) Chi ha ottenuto un certificato di firma digitale, dovrà poi:
   - custodire personalmente il dispositivo di firma, assicurandosi che nessuno possa essere in grado di utilizzarlo;
   - verificare la tipologia di sottoscrizione elettronica richiesta per il singolo documento che si deve sottoscrivere: elettronica semplice, avanzata, qualificata (digitale);
   - scegliere, di volta in volta, il formato di firma digitale da utilizzarsi in relazione allo scopo e alle finalità del documento: CAdES, PAdES, XAdES;
   - acquisire le competenze tecniche necessarie per il corretto utilizzo del dispositivo prescelto, non è escluso che in sede di contestazione all'intestatario possa essere richiesto di dar dimostrazione della capacità di utilizzo del dispositivo;
   - tenere presente la data di scadenza del certificato di firma, al fine di valutare se non far scadere il certificato e quindi rinnovarlo prima della sua naturale scadenza, oppure attendere la cessazione dello stesso per poi ottenerne uno nuovo, con caratteristiche uguali o diverse rispetto al precedente;
   - valutare la necessità o l'opportunità di associare alla firma digitale la marca temporale, al fine di garantire la validità del documento anche dopo la scadenza del certificato di firma.