CAMILLO SACCHETTO*

DOCUMENTO INFORMATICO E FIRME ELETTRONICHE ALLA LUCE DELLE NUOVE REGOLE TECNICHE NEL DIRITTO TRIBUTARIO TELEMATICO

SOMMARIO: 1. *Firma digitale e firme elettroniche nell'ordinamento italiano* - 2. *Tipologie di firme elettroniche e valore probatorio della sottoscrizione digitale* - 3. *Profili tecnico-informatici della firma elettronica e disconoscibilità della firma digitale* - 4. *Dispositivi di firma e sicurezza: firme automatiche e firme da remoto*

1. *Firma digitale e firme elettroniche nell'ordinamento italiano*

Con l'art. 15, legge n. 59/1997 "*Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa*", è stato affermato il pieno valore giuridico dei documenti informatici, i quali sono validi e rilevanti a tutti gli effetti di legge.

Il principio generale affermato nell'art. 15, comma 2, legge n. 59/1997 è quindi stato attuato con il d.p.r. n. 513/1997, recante "*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, co. 2, della legge 15 marzo 1997, n. 59*" che ha introdotto la firma digitale nell'ordinamento italiano. Il d.p.r. n. 513/1997 è stato successivamente abrogato dal d.p.r. n. 445/2000, "*Disposizioni legislative in materia di documentazione amministrativa*", nel quale è sostanzialmente confluito, malgrado le disposizioni in materia di efficacia probatoria del documento informatico abbiano in tale sede subito modificazioni rilevanti[1].

---

* Avvocato

[1] La normativa sulle firme elettroniche è, invece, di derivazione comunitaria: la direttiva 1999/93/CE è stata attuata in Italia con il d.lgs. n. 10/2002, "*Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*", che ha riconosciuto il valore giuridico alle firme elettroniche, oltre che alla firma digitale. In seguito è stato emanato il d.p.r. n. 137/2003, "*Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10*", con lo scopo di coordinare le disposizioni della legislazione italiana in tema di documento informatico e di firma digitale e quelle di derivazione comunitaria sulla firma elettronica.

Il Codice dell'Amministrazione Digitale (di seguito denominato per semplicità "CAD"), di cui al d.lgs. 7 marzo 2005, n. 82, successivamente modificato dal d.lgs. 4 aprile 2006, n. 159, dal d.lgs. 30 dicembre 2010, n. 235 e dal d.l. 18 ottobre 2012, n. 179, recante "*Ulteriori misure urgenti per la crescita del Paese*", convertito in legge il 13 dicembre 2012, ha riordinato la normativa vigente, apportandovi anche alcune significative modifiche[2].

Il documento informatico, ai sensi dell'art. 1, comma 1, lett. *p*), del CAD, è la "*rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti*".Quest'ampia definizione fa sì che vengano compresi in questa nozione elementi di vario genere: da un filmato digitale a un tracciato EDI ai *log*, da una comunicazione *e-mail* ai *file* generati da una transazione commerciale su un sito *web*. Tali documenti però, al contrario di quelli cartacei, sono più facilmente soggetti a modifiche, falsificazioni e duplicazioni e pongono pertanto il serio problema della loro durevolezza nel tempo e della loro validità giuridica.

Secondo l'art. 20, comma 1 *bis*, del Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005, CAD) il documento informatico soddisfa i requisiti della forma scritta quando garantisce in modo oggettivo qualità, integrità, sicurezza e immodificabilità: in base alle medesime caratteristiche, il documento informatico fornito di firma elettronica "semplice" è, inoltre, liberamente valutabile in giudizio, secondo l'art. 21, comma 1, CAD. Se nel mondo analogico utilizziamo il documento scritto e sottoscritto per avere una documentazione certa che mantenga traccia delle nostre azioni e possa essere utilizzata ed esibita in caso di contestazione, per ottenere le medesime garanzie nel mondo digitale dobbiamo utilizzare dei processi informatici che possano allo stesso modo garantire la paternità di un documento e preservarne l'integrità e l'autenticità.

Emerge quindi l'importanza assunta dalle tecnologie scelte per salvaguardare il documento informatico e, tra queste, rientra sicuramente la

[2] Il quadro normativo è stato recentemente completato dal D.p.c.m. 22 febbraio 2013, contenente le "R*egole in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, co. 3, 24, co. 4, 28, co. 3, 32, co. 3, lettera b), 35, co. 2, 36, co. 2, e 71*" e dal D.p.c.m. 13 Novembre 2014 "R*egole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonche' di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*" (di seguito denominato per semplicità "regole tecniche").

firma elettronica[3]. Le "firme elettroniche", non sono quindi rapportabili al concetto classico di sottoscrizione quanto piuttosto alla creazione di uno o più segni o marche identificative di un determinato soggetto.

2. *Tipologie di firme elettroniche e valore probatorio della sottoscrizione digitale*

Per comprendere al meglio le dinamiche normative e tecniche delle firme elettroniche risulta necessario analizzare i singoli modelli di firme.
La definizione di **firma elettronica**, contenuta nell'art. 1, comma 1, lett. *q*), del CAD, è "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*". Merita sottolineare come esistano numerosi molti tipi di firme elettroniche – e ciò spiega il genere plurale utilizzato nella direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche – descrivibili sulla base di una pluralità di criteri, fra i quali: il *metodo* utilizzato, la *finalità* e le *proprietà* della firma. Possono, infatti, essere utilizzati metodi fra loro diversi per apporre la firma elettronica, quali i codici di identificazione personale o le tecniche biometriche[4].

---

[3] La riferibilità, autenticità e sicurezza di riservatezza di un documento infatti sin dall'antichità era legata non tanto alla sottoscrizione quanto alla apposizione del sigillo, strumento conservato con particolare attenzione dal sovrano, dal vescovo o dal signore: il sigillo è quindi una marca che attesta l'immodificabilità del documento, la riferibilità ad un soggetto determinato e la difficile falsificabilità del sigillo con conseguente complessa disconoscibilità del documento così sigillato.
La firma o sottoscrizione costituisce da sempre, ed in particolare dalla diffusione della alfabetizzazione, lo strumento di individuazione della provenienza di un documento, la sua autenticità e la manifestazione di dichiarazione di volontà collegata alla scrittura, quale era precedentemente un segno "X" o altra marca identificativa.

[4] Con la locuzione **autenticazione biometrica** si fa riferimento all'identificazione o alla verifica automatica dell'identità attraverso strumenti di valutazione di caratteristiche fisiche o comportamentali (definizione risalente già alle "Linee Guida CNIPA 2004"). Con questa definizione l'ordinamento italiano ha preso in considerazione l'utilizzo di dati biometrici per la corretta identificazione personale. Tutti i sistemi biometrici sono caratterizzati da un processo che consiste nel confronto tra dati fisici o comportamentali propri di un determinato soggetto con un campione degli stessi dati precedentemente acquisiti: l'intero processo inizia con una fase di registrazione dei dati biometrici per mezzo di un dispositivo di acquisizione, i quali vengono elaborati per estrapolarne il c.d. *template*, ossia una rappresentazione matematica dei dati biometrici stessi. Questa sequenza di numeri che rappresenta i dati biometrici acquisiti viene poi registrata in un *database* o su una *smartcard*.

In particolare, secondo la classificazione ormai adottata, i metodi di autenticazione utilizzati per le firme elettroniche possono essere classificati in tre categorie a seconda che il meccanismo di autenticazione si basi ***sulle conoscenze dell'utente*** (ad es. la conoscenza di una parola chiave o di un numero di identificazione personale), ***sulle caratteristiche fisiche dell'utente*** (ad es. l'impronta digitale o della retina) o ***sul possesso di un oggetto da parte dell'utente*** (ad es. una tessera magnetica). Deve essere qui evidenziato che le caratteristiche tecniche della firma elettronica non sono predefinite così come il livello di sicurezza; infatti la firma elettronica può essere sia una semplice *password*, sia una firma autografa digitalizzata tramite *scanner*, sia una firma biometrica.

La firma elettronica avanzata[5] è una firma elettronica avente alcune peculiari caratteristiche di sicurezza. Più precisamente, il CAD, all'art. 1, comma 1, lett. *q bis*), la definisce come "*un insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*". Ad esempio un tipo di firma elettronica avanzata può ben essere quella apposta con tecniche biometriche (es. firma grafometrica) aventi garanzie di sicurezza maggiori rispetto alla semplice firma elettronica. La firma elettronica avanzata rappresenta un sistema neutro, sicuro e affidabile idoneo a garantire la riconducibilità di un documento informatico, reso immodificabile, al soggetto che l'ha sottoscritto[6].

---

[5] Le soluzioni tecnico-informatiche di firma elettronica avanzata (FEA), dopo le modifiche introdotte dal d.lgs. n. 235/2010 al CAD, sono state sviluppate e diffuse nel mercato.
Le Regole Tecniche hanno regolamentato le caratteristiche (art. 56), i limiti d'uso (art. 60) e gli obblighi dei soggetti che realizzano (art. 58) e erogano (art. 57) tali soluzioni affermando due principi fondamentali:
– l'assoluta libertà tecnologica (neutralità) lasciata agli sviluppatori di soluzioni di firma elettronica (art. 55, comma 1).
– l'assenza di qualsiasi controllo (art. 55, comma 1).
I soggetti che erogano sistemi di firma elettronica avanzata non sono quindi soggetti ad alcuna registrazione; il legislatore ha quindi voluto liberalizzare le tipologie di firma avanzata. L'art. 58 richiede alcune certificazioni obbligatorie per le soluzione di firma elettronica avanzata realizzate da privati in favore di amministrazioni pubbliche (ISO/IEC 27001 e ISO 9001).

[6] A tal fine, deve assicurare *ex* art. 56 delle Regole Tecniche:
a) l'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;

Le firme elettroniche avanzate hanno un valore limitato al solo contesto in cui vengono utilizzate, tra il sottoscrittore e il soggetto che offre il servizio di firma, rendendo quindi necessario che le loro condizioni di utilizzo siano preventivamente accettate per iscritto dagli utenti. Il soggetto che realizza la soluzione di firma elettronica avanzata dovrà informare gli utenti in merito agli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso[7].

Tra le varie firme che è possibile ottenere utilizzando dati biometrici rileva la cd. **firma grafometrica**. Tale firma, realizzata mediante la memorizzazione dei dati comportamentali dell'utente legati all'apposizione materiale della firma, ha il vantaggio di rendere possibile l'utilizzazione elettronica della sottoscrizione di un documento, permettendo allo stesso utente di firmare in modo abituale il documento, sia pure digitalmente. La firma grafometrica, in particolare, comprende diversi tipi di dati biometrico/comportamentali, che saranno poi legati al documento e al firmatario. I dati necessari per la firma grafometrica vengono acquisiti tramite apposito *hardware*: normalmente una tavoletta collegata ad un computer (tipicamente con USB) e pennina. Esistono però anche dispositivi *all-in-one*, capaci di acquisire il dato e anche di visualizzarlo ed elaborarlo. Questo *hardware* è in grado di rilevare il punto in cui la pennina tocca la superficie della tavoletta separata (o dello schermo, nel caso di un dispositivo *all-in-one*), la

c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
d) la possibilità di verificare che il documento informatico sottoscritto non abbia subìto modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto che eroga o realizza soluzioni di firma elettronica;
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
h) la connessione univoca della firma al documento sottoscritto

[7] Dalle Regole tecniche si evince che in capo ai soggetti che realizzano soluzioni di firma elettronica avanzata è posto l'obbligo di identificare in modo certo l'utente tramite un valido documento di riconoscimento, di informarlo circa gli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso, di subordinare l'attivazione del servizio stesso alla previa sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente, conservando copia dei documenti di riconoscimento e della dichiarazione di accettazione delle condizioni d'uso relativi a ogni utente per almeno venti anni.

pressione esercitata in quel punto, il momento temporale dell'evento, l'inclinazione della pennina[8].

Questi dati sono potenzialmente molto ricchi di informazioni, e riportano numerosi aspetti biometrici di tipo comportamentale del firmatario. Attraverso l'insieme di questi dati, un perito può determinare l'autenticità della firma con notevole precisione. Esistono anche metodi di riconoscimento automatico, che sono in grado di rilevare e misurare la somiglianza di una firma rispetto ad uno specimen registrato. Le applicazioni di firma grafometrica non sempre però richiedono la disponibilità di uno *specimen* o di un metodo di riconoscimento, e possono invece prevedere l'intervento di un perito solo in caso di contenzioso.

Occorre però distinguere le firme grafometriche dalle firme realizzate con prodotti *hardware* che si limitano ad acquisire l'immagine digitale della firma del sottoscrivente attraverso un *tablet*, poiché in tale procedimento non viene acquisito alcun dato biometrico. Questo tipo di firma può infatti essere facilmente disconosciuta, in quanto rimane priva degli ulteriori elementi grafometrici tipici della "sottoscrizione cartacea" e non possiede, quindi, elementi concretamente utilizzabili in un processo di verifica.

Nei sistemi in cui, invece, l'acquisizione di dati dal *tablet* non si limiti alla mera immagine della firma, ma riguardi anche i dati grafometrici che caratterizzano il comportamento del sottoscrivente (parametri quali la velocità di scrittura, la pressione esercitata, l'angolo d'inclinazione della penna, l'accelerazione del movimento, il numero di volte che la penna viene sollevata dalla carta), tale processo di firma grafometrica può essere utilizzato sia come modello di sottoscrizione digitale, assicurando in questo modo un accesso in remoto al proprio certificato di firma, sia come credenziale forte di autenticazione per garantire un accesso riservato.
L'utilizzo della firma grafometrica come modello di sottoscrizione digitale, che consente un accesso in remoto al relativo certificato, rende quindi

[8] È pertanto possibile ottenere, direttamente come dato campionato o mediante successivo calcolo, almeno i seguenti dati:
– coordinate e momento temporale di tutti i punti campionati; – pressione nei punti campionati;
– inclinazione della penna nei punti campionati; – velocità della penna in un dato intervallo;
– accelerazione in un dato intervallo; – numero di volte in cui la penna viene sollevata;
– coordinate dei punti in cui la penna viene sollevata; – forma della firma (tipo immagine scansionata).

indispensabile la creazione di una banca dati delle firme biometriche che ne permetta il relativo riscontro[9].

La firma elettronica qualificata è definita all'art. 1, comma 1, lett. *r*), del CAD, come "*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*". Da notare è che nella definizione di firma elettronica qualificata viene precisato come l'associazione al firmatario avvenga attraverso un certificato qualificato; il concetto di certificato non è invece menzionato nella definizione di firma elettronica avanzata.

La firma digitale, infine, è definita all'art. 1, comma 1, lett. *s*), del CAD, come "*un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici*". Nel presente caso viene scelta una peculiare tecnologia, quella della crittografia a chiavi asimmetriche; tale sistema garantisce un ulteriore livello di sicurezza rispetto a quello previsto per la firma elettronica qualificata[10].

Le **conseguenze dal punto di vista probatorio** meritano a questo punto una riflessione attraverso una analisi sintetica del valore giuridico delle firme elettroniche. Innanzitutto, come già prima citato, per documento informatico si deve intendere, ai sensi dell'art. 1, comma 1, lett. *p*), del CAD "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*". Il documento informatico cui è apposta una firma elettronica sotto il profilo probatorio è, secondo quanto dispone l'art. 21, comma 1, del CAD, liberamente valutabile dal giudice, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità[11].

---

[9] La firma biometrica grafometrica, pur in assenza di un certificato di firma digitale, può essere quindi ricompresa nel più ampio novero delle firme elettroniche avanzate (FEA) nelle ipotesi in cui sia caratterizzata da determinati requisiti, quali: l'identificazione certa del firmatario, il legame indissolubile tra firma e documento informatico sottoscritto, la garanzia dell'integrità del connubio composto dal documento e dal dato biometrico della firma.

[10] Come si può notare la principale differenza fra le varie firme è che le definizioni di firma elettronica e di firma elettronica avanzata non si riferiscono a un livello di sicurezza predeterminato o a una tecnologia precisa; invece, le definizioni di firma elettronica qualificata e digitale, sono collegate a livelli di sicurezza predeterminati e ad una tecnologia predefinita.

[11] Esistendo varie tipologie di firma elettronica ben si comprende come la valutazione dell'efficacia probatoria dei documenti cui la firma elettronica è apposta sia rimessa, caso per caso, al giudice che ne

Occorre, quindi, ribadire che le caratteristiche tecnologiche degli strumenti utilizzati e le caratteristiche organizzative del processo adottato determinano l'efficacia probatoria del documento informatico con firma elettronica così creato. Nel comma 2 dell'art. 21 del CAD si dispone, invece, sul valore giuridico dei documenti informatici con firma elettronica avanzata, qualificata e digitale: i documenti informatici con firma elettronica avanzata, firma elettronica qualificata, firma digitale, hanno la medesima efficacia probatoria di quella prevista dall'art. 2702 c.c. per la scrittura privata[12].

Ciò si afferma nell'art. 21, comma 2, del CAD ove si dispone che il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'art. 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'art. 2702 c.c.[13]

La scrittura privata sottoscritta con firma elettronica qualificata o con firma digitale, può essere disconosciuta dall'apparente sottoscrittore con la produzione da parte di questi della prova che egli non ha utilizzato il dispositivo di firma elettronica qualificata o digitale. A tal proposito risulta necessario chiarire quale sia concretamente il tipo di prova ammesso per il disconoscimento. Il CAD dispone che gli atti con firma elettronica qualificata e firma digitale possono integrare la forma scritta, anche nei casi previsti dall'art. 1350 c.c., comma 1, nn. 1-12. Così nell'art. 21, comma 2 *bis*, del CAD ove si afferma che "*salvo quanto previsto dall'art. 25, le scritture private di cui all'art. 1350, comma 1, nn. 1-12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale*".

---

valuterà le caratteristiche oggettive in concreto. I requisiti di qualità e sicurezza vanno riferiti al processo di creazione del documento informatico e i requisiti di integrità ed immodificabilità al documento informatico.

[12] Art. 2702 c.c. – *Efficacia della scrittura privata*. La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.

[13] Secondo la modifica introdotta alla disposizione sopra citata dal d.l. 18 ottobre 2012, n. 179, recante "*Ulteriori misure urgenti per la crescita del Paese*", convertito in legge il 13 dicembre 2012, "*l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria*". Prima di tale variazione, la prova del mancato utilizzo del dispositivo di firma era richiesta non soltanto per la firma elettronica qualificata e per la firma digitale, ma anche per la firma elettronica avanzata.

La previsione normativa è stata integrata dal d.l. n. 179/2012, disponendosi ora che "*gli atti di cui all'articolo 1350, primo comma, numero 13, del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale*". Tale importante modifica si riverbera in maniera diretta sulla firma elettronica avanzata, così come sopra evidenziata; infatti l'unica eccezione è dunque quella concernente la sottoscrizione degli atti di cui all'art. 1350 c.c., comma 1, nn. 1-12, come quelli aventi ad oggetto beni immobili: per questi la firma elettronica avanzata non sarà da ritenersi sufficiente. Solo per questi atti sono richieste la firma elettronica qualificata o la firma digitale[14].

3. *Profili tecnico-informatici della firma elettronica e disconoscibilità della firma digitale*

La non disconoscibilità (*non repudiation*) di una firma digitale prevede che il firmatario non possa sostenere – a livello tecnico – di non aver firmato. Questo non avviene ad esempio con un PIN o una *password*: in tal caso chi verifica tale PIN o *password* dal lato del fornitore del servizio potrebbe aver creato un messaggio o un'operazione inesistente, e un terzo non avrebbe modo di sapere quale soggetto (utente o fornitore del servizio) stia dicendo la verità, in quanto entrambi conoscono questo valore segreto. Nel caso della firma digitale, descritta in precedenza, possiamo diversamente avere la non disconoscibilità, in quanto solo il firmatario risulta essere a conoscenza della propria chiave privata. La firma sarà verificata dal fornitore del servizio o da terzi usando esclusivamente la chiave pubblica.

Al fine di mantenere la garanzia della non disconoscibilità di tale tipologia di firma digitale, sono necessari ulteriori componenti e determinazioni. Per prima cosa le chiavi pubbliche utilizzate devono essere quelle corrette, in secondo luogo deve essere noto in modo certo il momento in cui è stata apposta una firma ed infine si deve assumere che i dispositivi usati dal firmatario siano sicuri. Nella tipologia di firma digitale sopra descritta realizzata quindi mediante crittografia asimmetrica, esiste una fondamentale criticità: se la chiave pubblica con cui verifichiamo la firma non è quella corretta, quella che effettivamente corrisponde alla chiave privata del

[14] Non sarà invece necessaria la firma digitale o la firma elettronica qualificata, ma potrà utilizzarsi la firma elettronica avanzata, per tutti gli atti e i contratti che richiedano la forma scritta *ad probationem* o *ad substantiam* non aventi ad oggetto beni immobili.

firmatario, esiste il rischio di considerare valida una firma falsa. Si tratta di un problema collegato alla più generale tipologia di attacchi informatici meglio nota come "*man in the middle*".

È pertanto necessario collegare in modo univoco l'utente alla sua chiave pubblica[15]. La pubblicazione e il controllo delle chiavi avvengono accedendo, per via telematica, ad appositi registri mantenuti ed aggiornati presso le *Certification Authority* o Ente Certificatore, che ha il compito di gestire il *database* delle chiavi pubbliche e dei relativi certificati delle chiavi, nonché la responsabilità di procedere alla previa identificazione del soggetto che richiede la certificazione.

L'insieme degli elementi che compongono tale processo si definisce infrastruttura di chiave pubblica (*Public Key Infrastructure*, PKI), che si articola nei soggetti che vi partecipano (utente, certificatore, destinatario), nelle modalità in cui ciascuno di essi assolve al proprio ruolo e nelle forme di utilizzazione delle tecnologie disponibili. Chiunque conosca in modo certo, e a priori, la chiave pubblica del certificatore, e ne riconosca il potere certificativo, potrà così verificare la corrispondenza del soggetto alla sua chiave pubblica, come indicata nel certificato stesso. Sarà così possibile verificare firme elettroniche di un certo soggetto evitando i problemi relativi al "*man in the middle*", evitando cioè di usare la chiave pubblica sbagliata durante la verifica delle firme[16].

È pertanto necessario che ogni certificato abbia un limite di durata. È però possibile che gli eventi sopra citati si possano verificare anche in un momento antecedente alla naturale scadenza del certificato. La *Certification Authority* prevede quindi la possibilità che un certificato venga revocato, attraverso l'attivazione di una specifica procedura. La C*ertification Authority*

---

[15] Questa connessione viene posta in essere attraverso un certificato di chiave pubblica, che comprende almeno le seguenti informazioni:
– Identificativo del soggetto firmatario. – Chiave pubblica del soggetto firmatario. – Periodo di validità della chiave (data di inizio e data di fine validità). – Identificativo del soggetto certificatore (autorità di certificazione che ha emesso il certificato di firma). – Sottoscrizione da parte dell'ente certificatore delle informazioni sopra riportate.

[16] Non deve essere in ogni caso dimenticato che i certificati hanno una scadenza e ciò per una serie di motivi, tra cui: – La possibile compromissione della chiave privata del soggetto (ad esempio il soggetto ha perso il dispositivo ove sono memorizzate le sue chiavi). – La possibile obsolescenza delle tecnologie utilizzate dal soggetto e nel certificato. – Il soggetto non è più abilitato ad utilizzare quelle chiavi per gli scopi fino ad ora in essere (ad esempio perché ha cambiato lavoro o perché ha perduto i poteri di firma).

dovrà pertanto rendere disponibile online una c.d. lista di revoca, ovvero un elenco di certificati revocati e pertanto non più validi[17].

4. *Dispositivi di firma e sicurezza: firme automatiche e firme da remoto*

Da quanto fin qui esposto pare chiaro come l'elemento centrale della sicurezza della firma risulti essere la chiave privata del firmatario. La perdita o il furto di tale chiave comporta il serio rischio di una falsificazione della sottoscrizione digitale. Risulta pertanto essenziale che la chiave privata del firmatario sia prodotta e custodita su un dispositivo sicuro, il cui uso esclusivo sia limitato al sottoscrittore stesso; è quindi necessario prevedere sistemi di generazione *on-board* sul dispositivo delle chiavi asimmetriche del firmatario e di controllo in merito all'impossibilità di circolazione della chiave privata su sistemi di soggetti terzi. Sarà inoltre consigliabile l'utilizzo di un dispositivo sicuro di firma, non vulnerabile rispetto ad intrusioni informatiche ed a *malware*. Meglio ancora se tale dispositivo ha caratteristiche di *tamper-resistance* (resistente a manomissioni), che rendono difficile se non impossibile l'apertura del dispositivo stesso e di conseguenza l'accesso alle chiavi private ivi memorizzate[18].

La firma automatica, disciplinata dall'art. 35 del CAD e dalle relative Regole Tecniche che prevedono alcuni requisiti minimi obbligatori e determinati livelli minimi di sicurezza garantiti, è definita, all'art. 1, lett. *r*), delle Regole Tecniche, come quella particolare procedura di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di quest'ultimo.

---

[17] A tal proposito merita rammentare che ai sensi dell'art. 21, comma 3, del CAD "l'apposizione ad 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 revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate".

[18] Le *best practices* in materia di sicurezza informatica prevedono che i dispositivi utilizzati per la creazione di firme, nei casi in cui sia richiesto il più elevato livello di sicurezza, siano ad esempio *smart card*, o *token* con proprietà *anti-tampering*. Il soggetto firmatario dovrà pertanto dotarsi di tali dispositivi, ed essere in grado di utilizzarli insieme al proprio abituale strumento di lavoro individuale (PC, *tablet*, etc.), cosa peraltro di non semplice realizzazione tenuto anche conto dell'arretratezza culturale che nel nostro paese vige in tema di tecnologia ed informatica.

Nel dettaglio l'art. 35, comma 3, CAD, stabilisce che la firma con procedura automatica è valida se apposta previo consenso del titolare, non applicandosi la disposizione di cui al secondo periodo del comma 2 del medesimo articolo, in base alla quale i documenti informatici devono essere presentati al titolare prima dell'apposizione della firma con l'obbligo di richiedere allo stesso la conferma della volontà di generare la firma; inoltre, ai sensi di quanto prescritto dall'art. 4, comma 2, d.p.c.m. 30 marzo 2009, qualora il titolare del certificato di firma si serva di una procedura automatica di firma dovrà necessariamente utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso. Le firme automatiche, al fine di garantire gli standard di sicurezza richiesti, non vengono realizzate mediante l'utilizzo dei comuni dispositivi forniti dai certificatori (*token usb* o *smart card*), bensì vengono utilizzati strumenti tecnologicamente più avanzati e in grado di gestire più velocemente una maggiore quantità di dati come ad esempio gli HSM[19].

La firma remota è disciplinata dal d.p.c.m. 19 luglio 2012 20 ed è definita all'art. 1, lett. *q*), delle Regole Tecniche, come quella particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse. Attraverso l'utilizzo del HSM si potrà pertanto sottoscrivere più documenti in un'unica sessione, da remoto o anche in modalità automatica, attraverso l'utilizzo di un qualsiasi computer con accesso alla rete e mediante l'inserimento del solo codice PIN; tale codice risulterà essere l'unico dato in possesso del soggetto firmatario e su cui lo stesso dovrà "*mantenere in modo esclusivo la conoscenza o la disponibilità*".

C. SACCHETTO, Documento informatico e firme elettroniche alla luce delle nuove regole tecniche nel diritto tributario telematico, 7 BusinessJus 67 (2015)

Unless otherwise noted, this article and its contents are licensed under a
Creative Commons Attribution 3.0 Generic License.
http://creativecommons.org/licenses/by-nc-nd/3.0/
Se non altrimenti indicato, il contenuto di questo articolo è rilasciato secondo i termini della licenza
Creative Commons Attribution 3.0 Generic License.

[19] Acronimo di "*Hardware Security Module*", è definito dall'art. 1, lett. *p*) delle Regole Tecniche come insieme di *hardware* e *software* che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.